



Carrier VoIP

# MG 9000 Configuration Management

Document status: Standard  
Document version: 09.02  
Document date: 20 October 2006

Copyright © 2006, Nortel Networks  
All Rights Reserved.

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

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

---

## New in this release

---

The following sections detail what's new in *MG 9000 Configuration Management* for release (I)SN09U:

- "Features" (page 3)
- "Other changes" (page 5)

### Features

See the following sections for information about feature changes:

- "MG 9000: downloadable version of the GLC 32" (page 3)
- "MG 9000 GLC 12 line card providing NA coin services" (page 3)
- "Global line card field programmable gate array download" (page 4)
- "Routine exercise (REX) of intelligent card pairs" (page 4)
- "MG 9000 manager capacity performance robustness (CPR) simplification" (page 4)
- "PKI authentication on the MG 9000 - phase 1" (page 4)

#### **MG 9000: downloadable version of the GLC 32**

This feature introduces the NTNY53BA 32-circuit global line card (GLC 32) which offers field-programable firmware. Users can upgrade the configuration load of the GLC's Field Programmable Gate Array (FPGA) from the MG 9000 Element Manager (EM).

The NTNY53BA GLC 32 card replaces the POTS 32 card (the traditional telephone service card with 32 ports) and the NTNY53AB GLC 32 card. References to the NTNY53AB GLC 32 card have been removed from the Basics Guide because this card is discontinued.

#### **MG 9000 GLC 12 line card providing NA coin services**

This feature introduces the NTNY53CA 12-circuit global line card (GLC 12). 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 software to support the card is patched back to SN08.

### **Global line card field programmable gate array download**

This feature provides the software interface for the downloadable GLC 12 and 32 cards. Changes appear in the GLC Card View and the GLC Diagnostic View. The MG 9000 Upgrade Wizard has also been modified to include the GLC cards.

### **Routine exercise (REX) of intelligent card pairs**

Routine exercise (REX) allows you to perform a diagnostic test on the inactive card of an intelligent pair of cards. REX is intended to diagnose latent faults in inactive (or standby) cards.

The REX GUI view on the MG 9000 Element Manager allows you to schedule and to monitor the progress of a REX test on a selected network element (NE). Using the GUI, you can also

- add an NE for REX
- remove an NE for REX
- suspend REX on an NE
- resume REX on an NE

### **MG 9000 manager capacity performance robustness (CPR) simplification**

This feature allows the user to initiate an inband or out of band LCI session directly from the MG 9000 Manager Subnet View screen for all nodes present in the subnet (both discovered and undiscovered).

Clear persist and discover operations can be initiated from the MG 9000 Manager through a button on the NE Discovery View window. For additional information refer to "Using the Clear persist and discover function" in *MG 9000 Fault Management*, NN10074-911.

### **PKI authentication on the MG 9000 - 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 signatures to authenticate nodes attempting to establish an IPSec session

## Other changes

See the following sections for information about changes that are not feature-related.

- ["Software upgrade tools" \(page 5\)](#)
- ["Precautionary message for IPSec digital signature authentication" \(page 5\)](#)
- ["Decommissioning an MG 9000 shelf" \(page 5\)](#)

### Software upgrade tools

*MG 9000 Configuration Management* now contains information on the software upgrade tools, formerly found in *Upgrading the MG 9000*, NN10048-461.

### Precautionary message for IPSec digital signature authentication

Addition of precautionary message for networks that employ IPSec using digital signature authentication. Any changes that you make to the time, date and time zone settings, or to the Network Time Protocol (NTP) server that fall outside of the validity period for certificates supporting IP Security on call processing (CallP) and OAM connections can cause a service disruption.

### Decommissioning an MG 9000 shelf

Addition of ["Decommissioning an MG 9000 shelf" \(page 72\)](#).



---

## Configuration management strategy

---

Configuration management activities control system topology and establish the parameters within which the system functions. These activities include adding, removing, or modifying cards and services or the parameters that define their function.

Nortel installation personnel complete the initial configuration of the MG 9000 as part of the installation process. The installation process establishes the baseline for MG 9000 operation.

Configuration management refers to specifying the relationship between MG 9000 hardware and software with the network elements and nodes (cards) that reside in the MG 9000 shelf. Configuration of the MG 9000 is controlled through the MG 9000 Manager, which allows for provisioning of switched lines services, private lines services, and circuit cards in support of the following solutions:

- Universal Access-AAL1 (UA-AAL1)
- Universal Access IP (UA-IP)

The MG 9000 Manager must be installed and configured before configuring the MG 9000. Installation and configuration of the MG 9000 Manager are provided in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450. Procedures for configuring components in support of the solutions listed previously are provided in this document.

### Tools and utilities

The MG 9000 uses the following tools for all configuration management, fault clearing, performance monitoring, security, and upgrade tasks.

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

### Local craft interface (LCI)

A local craft interface (LCI) port on the data control card (DCC) provides another method for configuring the MG 9000. The LCI is used primarily for installation and initial commissioning of the MG 9000. The LCI can be used

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 is described in "MG 9000 local craft interface" (page 313).

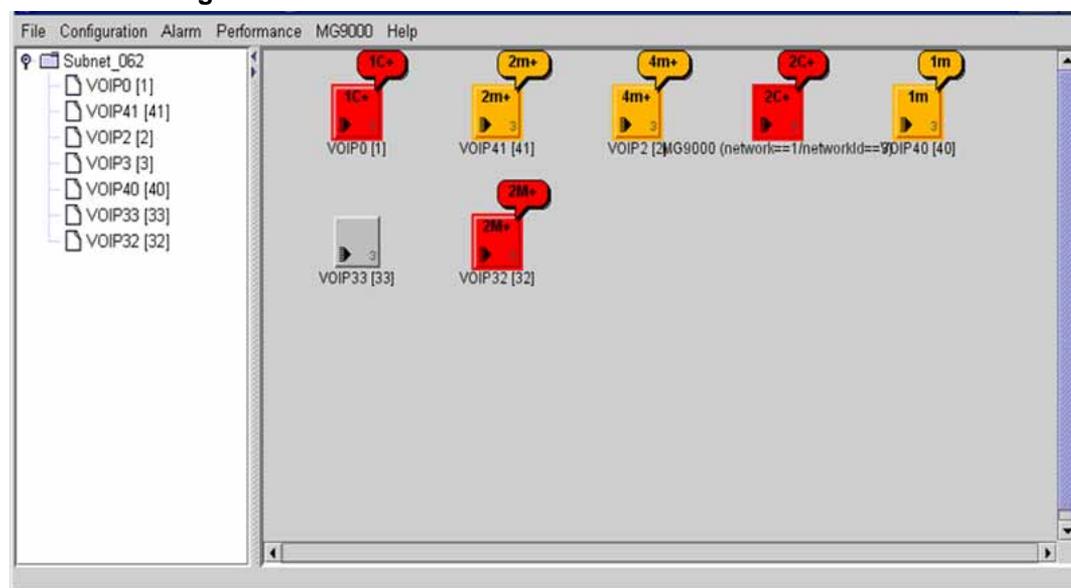
The LCI communicates to the DCC through an Ethernet port. The web browser must be Netscape 7.0 and above, or Microsoft Internet Explorer 5.5 and above on the Windows 2000 platform. Use the active DCC IP address (10.0.0.1) to locate the LCI through the browser. A security screen requests a user name and password.

### MG 9000 Manager graphical user interface

The MG 9000 Manager serves as the element management system for the MG 9000 and is responsible for the fault clearing, configuration, performance monitoring, and upgrade tasks for the MG 9000.

The following figure shows the MG 9000 Manager Subnet View.

MG 9000 Manager Subnet View



The MG 9000 Manager is used to manage the MG 9000 dealing with operations and issues that affect the network element. The following table lists the menus and sub-menus accessible from the Subnet View.

#### Subnet View menu options

Menu	Menu options	Explanation
File	Refresh Subnet View	Refreshes the Subnet View
	Exit	Closes the GUI View

Menu	Menu options	Explanation
Configuration	Add a new MG 9000 NE	Opens the MG 9000 Provisioning View. Refer to " <a href="#">Provisioning an MG 9000 network element</a> " (page 24).
	Audit NE	Opens the Audit GUI. Refer to " <a href="#">Auditing MG 9000 data</a> " (page 284).
	Delete NE	Opens the Network Element Deletion View. Refer to " <a href="#">Deleting an MG 9000 network element</a> " (page 50).
	Discover NE	<p>Opens the NE Discovery View which lists the properties of an MG 9000 network element (NE) that is discovered or is to be discovered. The Discover button is used to initiate the discovery of the MG 9000. The Discover button can be used in a troubleshooting scenario, such as when hardware mismatches occur between the MG 9000 Manager and the MG 9000.</p> <p><b>Note 1:</b> When using the Discover button, the NE must be in a discoverable state.</p> <p><b>Note 2:</b> Do not initiate the Discovery of an MG 9000 NE at the same time that</p> <ul style="list-style-type: none"> <li>• a line or trunk audit is running from the CS 2000 Manager</li> <li>• an autoapply is running on the NPM</li> <li>• any provisioning is running on the CS 2000 Manager</li> </ul> <p>After a Discover NE is complete - whether it is manual discovery or a result of a cold start or server restart an automatic NE Audit runs. For more information on the NE Audit, refer to "<a href="#">Performing an MG 9000 data audit</a>" (page 281).</p> <p>The Clear persist and discover button is used to clear the persistent data on an MG 9000 and reestablish (rediscover) communication between the MG 9000 and an NE that has failed discovery. Users must have emsadm privileges. For</p>

Menu	Menu options	Explanation
	View/Modify NE Properties	<p>more information, see the Using the Clear persist and discover function procedure in <i>MG 9000 Fault Management</i>, NN10074-911.</p> <p>Open the Properties View which contains three tabs labeled as NE Properties, NE Security, and IESA PVR Provisioning.</p> <ul style="list-style-type: none"> <li>• NE Properties - This tab lists the properties associated with an NE and allows for the NE Password and NE OM Collection status to be changed. The fields are describe in table "<a href="#">NE properties</a>" (page 14). The Apply and Refresh buttons apply any changes made to the NE Password field or the OM Collection checkbox.</li> <li>• NE Security - This tab reports the operational and administrative status of IP security for the network element and allows for the download of the security certificates that the gateway needs to secure the OAMP channel. The fields are described in "<a href="#">NE Security View</a>" (page 15)</li> <li>• IESA PVR Provisioning - This tab is used to configure Nortel Multiservice Switch Virtual Router (PVR) (MG 15000 or equivalent) settings for the network element to support Internodal ESA. Refer to "<a href="#">Configuring Nortel Multiservice Switch virtual router (PVR)</a>" (page 36)</li> </ul>

Menu	Menu options	Explanation
	REX NE	<p>Opens the Routine Exercise (REX) view for a network element. The REX GUI view allows you to schedule a test on the inactive card of a pair of cards. REX is intended to diagnose latent faults in inactive (or standby) cards.</p> <p>From the REX view you can schedule and monitor the progress of a REX performed on a selected NE. Using the GUI you can also</p> <ul style="list-style-type: none"> <li>- add an NE for REX</li> <li>- remove an NE for REX</li> <li>- suspend REX on an NE</li> <li>- resume REX on an NE</li> </ul> <p>For more information on REX, refer to <a href="#">"Performing a routine exercise (REX) on intelligent cards" (page 292)</a></p>
	Refresh Icon	Refreshes the MG 9000 icons.
	Launch LCI Session	<p>Opens the Launch LCI View window which allows you to connect to the LCI through</p> <ul style="list-style-type: none"> <li>- Inband - successful only if proper network routing is complete</li> <li>- Out of band - launching through slot 10 or 11</li> </ul> <p>Users must have emsadm privileges. For more information refer to <a href="#">"Launching the LCI from the MG 9000 Manager" (page 320)</a></p>
	ESA Download	<p>Users must have emsadm privileges.</p> <p>Opens the ESA Data Download GUI which is used to manually download ESA data from the Core to the MG 9000 Manager. Refer to <a href="#">"Changing MG 9000 Manager ESA data download properties" (page 305)</a> for information on setting up the MG 9000 Manager properties to support the ESA data download.</p>

Menu	Menu options	Explanation
	Internodal ESA	Opens the Internodal ESA View which is used to manage Internodal ESA communities of interest (COI). Refer to <a href="#">"Provisioning Internodal ESA and community of interest"</a> (page 31).
	Global Traffic Descriptors	Opens the TD Manager GUI. Refer to <a href="#">"Provisioning the Global Traffic Descriptors in the Traffic Descriptor Manager"</a> (page 126).
	Office-Wide Defaults	Opens the Office-Wide Defaults GUI. Refer to <a href="#">"Provisioning office-wide defaults"</a> (page 27).
	Central User Id and Password	Opens the User Id and Password GUI which is used to configure or change the user id and password to match that entered at the IEMS/Radius server. Refer to <a href="#">"IEMS/Radius authentication"</a> in <i>MG 9000 Security and Administration</i> , NN10162-611.
	PLoA Services Browser	Opens the PLoA Services Browser which lists all PLoA services on the network elements in the Subnet. Refer to <a href="#">"Viewing PLoA services from the PLOA Services Browser"</a> (page 172).
	VMG Browser	Opens the VMG Browser which lists all VMGs from across all network elements in the MG 9000 Manager. Refer to <a href="#">"Listing all VMGs using the VMG browser"</a> (page 199).
	VLAN Browser	Opens the VLAN Browser which lists all the virtual local area networks (VLAN) from across all network elements in the MG 9000 Manager that are configured with Gigabit Ethernet (GigE) DCC cards. Refer to <a href="#">"Listing all VLAN connections using the VLAN Browser"</a> (page 247).
	Tools	Opens the Connection Test Tool GUI for Ping and Traceroute tools. Refer to <a href="#">"Accessing the Connection test tool"</a> in <i>MG 9000 Fault Management</i> , NN10074-911.

Menu	Menu options	Explanation
	IPSec Tool	Launches a web browser on the client machine and loads the IPSec servlet used to configure IPSec and IKE entries. For more information on configuring IPSec entries, refer to <i>MG 9000 Security and Administration</i> , NN10162-611.
Alarm	Alarm Browser	Opens the Alarm Browser which is used to view and manage MG 9000 alarms. Refer to "Alarm Browser" in <i>MG 9000 Fault Management</i> , NN10074-911.
	Audit NE alarms	A command used to synchronize alarm data between the MG 9000 and the MG 9000 Manager. Refer to "Audit Alarm" in <i>MG 9000 Fault Management</i> , NN10074-911.
Performance	Performance Browser	Opens the Performance Statistics Browser used to monitor MG 9000 performance statistics. Refer to <i>MG 9000 Performance Management</i> , NN10140-711.
	Configure Collection Interval	Allows the user to configure sample and summary intervals uniformly for all SN08 MG 9000s in a Subnet. Refer to "Configuration of collection intervals" in <i>MG 9000 Performance Management</i> , NN10140-711.
MG9000	Persistence	Opens the Persist Date GUI and provides a command used to manually save provisioning data for an NE to the database. Refer to " <a href="#">Persisting MG 9000 provisioning data</a> " (page 47).
Help	About	Opens the About view and lists the software versions used at client, mid-tier, and server.

## NE Discovery and Deletion Views

The following table lists the NE property fields in the NE Discovery View. For a description of NE property fields in the NE Deletion View see table "[Network Element Deletion View fields](#)" (page 51). A more complete description of values that are common to the NE Provisioning View are provided in table "[Provisioning View properties](#)" (page 25).

### NE properties

Field	Explanation
NE Number	The selected element number
NE Name	The selected network element name
NE IP Address/Hostname	The IP address to the DCC card
NE Password	Enter the MG 9000 Manager SFTP password.
NE Encryption Key	Enter the 20-120 character alphanumeric Preshared Key. This key must match what is entered in the LCI Preshared Key field in the Connections->OAMP Connections screen. For more information, refer to <i>MG 9000 Security and Administration</i> , NN10162-611.
MG 9000 Manager IP Address	MG 9000 Manager IP address
SNMP Trap IP (from MG)	IP address to which the MG 9000 sends SNMP traps
NE Provisioning Mode	Auto-discover
Vendor	The name of the manufacturer of the physical component
MG 9000 Software Version	MG 9000 software version
SNMP Trap Port (expected)	SNMP Trap port number expected by the MG 9000 Manager.
SNMP Trap Port (from MG)	SNMP Trap port number set on the MG 9000.
NE Market	The market selected for the MG 9000
OM Collection	Not an active checkbox on this GUI (activated from the View/Modify NE Properties GUI). When checked the OM Collector will collect OM data starting from its next collection cycle. If unchecked, the OM Collector will stop collecting OM data starting from its next collection cycle.

## NE Security View

The following table lists the fields in the NE Security View. For more information, refer to *MG 9000 Security and Administration*, NN10162-611.

### NE Security View

Field	Explanation
IPSec Oper Status	IPSec operational status. Value: Enabled or Disabled.
IPSec Admin Status	IPSec administrative status. Value: Enabled or Disabled.
Gateway Authentication Method	The security authentication method currently used by the gateway: Value: Digital Certificate or Pre-shared Certificate PSK.
Managing Gateway Certificate	Indicates whether the MG 9000 EM is currently managing the certificates for the gateway. Value: Yes or No.
Last Pulled Certificate	The serial number of the last device certificate that was successfully downloaded to the MG 9000.
Last Pushed Certificate	The serial number of the last device certificate successfully received from the Certificate Manager.

## MG 9000 user inactivity time-outs

The MG 9000 Manager serves as the element management system for the MG 9000 and is responsible for the fault clearing, configuration, performance monitoring, and upgrade tasks for the MG 9000. The following user inactivity time-outs are configurable using the MG 9000 Manager:

- User Inactivity Time-out (Default: 10 minutes)
- User Termination Time-out (Default: 10 minutes)
- Re-Authentication Disable Time-out (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 Time-out), the client is iconized and a dialog appears prompting the user to log in to the client again. 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 Time-out), a warning dialog appears stating 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, time-out values are set independently for each side of the cluster. If time-out values have only been changed on the active side of a cluster and a SWACT occurs, the time-out values will take the inactive side settings. To ensure consistent interface performance following a SWACT, when a default time-out 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 time-outs on the CS 2000 Management Tools server, in *ATM/IP Security and Administration* (NN10402-600).

### OSS fault management system support

To support third-party operations support systems (OSS) fault management systems, the following information is needed to ensure correct registration and connection to the MG 9000 Manager to receive alarm information:

- MG 9000 Manager server IP address (specifically the CORBA Naming Service)
- CORBA Naming Service port - the default is 2001. To verify, check the T NAMES\_PORT in file  
`/opt/nortel/mg9ksrv_<release#>/bin/mg9kimpl`
- Fault Service Manager CORBA name - The entry in the CORBA Naming Service of the MG 9000 Manager fault system. For example,  
`Subnet_<release#>.Services.FaultServiceManager`
- CORBA entry for Fault Event Channel:  
`Subnet_<release#>.ec.Oss`  
where <release#> represents the release number.

### MG 9000 Manager server data backup and restore

To backup and restore data on the MG 9000 Manager server platform, go to the Solaris Platform Foundation Software (SPFS) for the Carrier VoIP Solaris platform backup and restore procedures. Refer to *ATM/IP Solution-Level Operational Configuration*, NN10409-500.

## Configuration management procedures

The procedures in this section address the following activities:

- ["Using the MG 9000 Manager to provision equipment and services" \(page 20\)](#)
- ["Provisioning an MG 9000 network element" \(page 24\)](#)
- ["Provisioning office-wide defaults" \(page 27\)](#)
- ["Provisioning Internodal ESA and community of interest" \(page 31\)](#)

- "Configuring Nortel Multiservice Switch virtual router (PVR)" (page 36)
- "Provisioning clock synchronization" (page 40)
- "Manually persisting MG 9000 provisioning data" (page 47)
- "Deleting an MG 9000 network element" (page 50)
- "Subtending shelves" (page 55)
- "Renumbering an MG 9000 frame" (page 60)
- "Provisioning a MG 9000 frame physical location" (page 66)
- "Decommissioning an MG 9000 frame" (page 69)
- "Decommissioning an MG 9000 shelf" (page 72)
- Provisioning MG 9000 cards
  - "Provisioning a World line card" (page 77)
  - "Provisioning a Global line card" (page 102)
  - "Provisioning an ADSL card" (page 122)
  - "Provisioning an SAA line card" (page 137)
  - "Provisioning a DS1 card" (page 142)
  - "Provisioning an ITX card" (page 158)
- "De-provisioning a line card" (page 160)
- "Provisioning private lines services" (page 162)
- "Provisioning switched lines services" (page 178)
- "Viewing and modifying DS1 IMA group and links" (page 224)
- "Provisioning and maintenance of OC3 APS" (page 230)
- "Viewing Gigabit Ethernet ports and links provisioning information" (page 238)
- "Provisioning SIC inputs and outputs" (page 252)
- "Provisioning IBIP inputs and outputs" (page 257)
- "Using the Bandwidth Manager" (page 263)
- "Using the Bandwidth Management Planning Tool" (page 273)
- "Performing an MG 9000 data audit" (page 281)
- "Performing a routine exercise (REX) on intelligent cards" (page 292)
- "Managing performance thresholds" (page 299)
- "Managing overload thresholds" (page 302)

- "Changing MG 9000 Manager ESA data download properties" (page 305)
- "MG 9000 local craft interface" (page 313)
- "LCI access" (page 315)
- "Launching the LCI from the MG 9000 Manager" (page 320)
- "LCI network element screen" (page 325)
- "LCI Connections view" (page 329)
- "LCI Maintenance view" (page 347)
- Software upgrades
  - "Upgrading software in MG 9000 cards" (page 420)
  - "Software Upgrade View" (page 422)
  - "Upgrade Wizard overview" (page 429)
  - "Software upgrade errors and problem resolution" (page 439)
  - "Card upgrade with user intervention" (page 444)
  - "Card upgrade without user intervention" (page 448)
  - "MG prep download" (page 452)
  - "MG upgrades" (page 454)
  - "Downloading software into the MTA card" (page 456)
  - "Downloading software into the xDSL card" (page 458)
  - "Downloading software into the GLC cards" (page 460)
  - DCC far-end port identification
  - "Upgrade history" (page 462)

**Note:** To promote recovery from the unlikely event of a simultaneous data loss and an MG 9000 Manager initialization, be sure to record all provisioning and configuration information.

After provisioning cards and services on the MG 9000, it is recommended that all the following configuration information be recorded or captured using screen captures:

- bandwidth manager
- automatic protection switching (APS)
- digital test access (DTA) setup
- metallic test access (MTA) setup

- floating IP address manager (refer to Nortel *Carrier Voice over IP Network Upgrades and Patches*, (NN10440-450))
- software download manager
- line card circuit type

In addition, use the Save PLoA services and Save SLoA services procedures to save provisioning information into a file that provides a list of all services on that network element. It is recommended that these files are printed and retained with office configuration information.

## Using the MG 9000 Manager to provision equipment and services

### When to use this procedure

Use this procedure when it is necessary to use the MG 9000 Manager to provision MG 9000 equipment and services.

After the MG 9000 is discovered by the MG 9000 Manager, several graphical user interface (GUI) windows that represent different levels of the MG 9000 hardware components can be accessed from the MG 9000 Manager. Each GUI window contains:

- icons which are graphic images used to represent particular objects of the MG 9000 hardware components
- menus at the top of each window which provide a means of performing various functions. The following table defines the "menus" that appear at the top of each window and the menu options.

**Note:** All menu options may not apply for each window or for the solution in which the MG 9000 is deployed.

### Menu options for GUI views

Menu	Menu options	Explanation
MG9000	Close	Close the window.
Actions	Save SLOA services	Refer to "Saving SLoA services" (page 223) in "Provisioning switched lines services" (page 178).
	Save PLOA services	Refer to "Saving PLoA Services" (page 175) in "Provisioning private lines services" (page 162). Not applicable to the UA-IP solution.
	Software Download Manager	Valid for XDSL Card and MTA Card view.
	Line Template Table	Refer to the "Provisioning a line template table" (page 89) procedure in "Provisioning a World line card" (page 77).

Menu	Menu options	Explanation
	Maintenance	<p>Indicates the type of maintenance to perform:</p> <ul style="list-style-type: none"> <li>• APS Provisioning - Refer to "Provisioning OC3 automatic protection switching" (page 231).</li> </ul> <p><b>Note:</b> APS Provisioning are valid at the Shelf View only.</p> <ul style="list-style-type: none"> <li>• Diagnostic - Refer to "Common equipment card diagnostics" for cards, and the "Line circuit diagnostics" for circuits in <i>MG 9000 Fault Management</i>, NN10074-911.</li> <li>• Swact - Refer to "Switching activity of a card" in <i>MG 9000 Fault Management</i>, NN10074-911.</li> </ul> <p><b>Note:</b> Diagnostic and Swact are valid for DCC, ITP, and ITX views only.</p>
	Software Upgrade	<p>Refer to "Upgrading software in the MG 9000" in <i>Nortel Carrier Voice over IP Network Upgrades and Patches</i>, NN10440-450</p> <p>Refer to "Software Upgrade View" (page 422).</p> <p><b>Note:</b> Valid for DCC, DS1, ABI (DS-512), ITP, and ITX card views only.</p>
	Software Image	<p>Software imaging is performed through the NPM using the SmartImage Task command. For more information on the SmartImage Task command, refer to <i>UA-AAL1 Solutions-level Basics</i>, NN10443-100, <i>PT-AAL2 Solution-level Basics</i>, NN10441-100, or <i>PT-IP Solution-level Basics</i>, NN10442-100.</p> <p><b>Note:</b> Valid for DCC, DS1, ABI (DS-512), ITP, and ITX card views only.</p>
Services	Bandwidth Manager	Refer to "Using the Bandwidth Manager" (page 263).

Menu	Menu options	Explanation
	Private Line Services Manager	Refer to "Provisioning private lines services" (page 162). Not applicable to the UA-IP solution.
	Switched Lines Services Manager	Refer to "Provisioning switched lines services" (page 178).
	DTA Test Manager	Refer to "DTA Test Manager" in <i>MG 9000 Fault Management</i> , NN10074-911.
	MTAP Test Manager	Refer to "MTAP Test Manager" in <i>MG 9000 Fault Management</i> , NN10074-911.
	Floating IP Address Manager	Refer to "Provisioning a floating IP address" in <i>Nortel Carrier Voice over IP Network Upgrades and Patches</i> , NN10440-450
Alarms	Alarm Browser	Refer to <i>MG 9000 Fault Management</i> , NN10074-911 for a discussion of alarms and accessing the Alarm Browser.

- The bottom of each window has "panels" which provide additional information for each hardware level. The following table describes the panels and their purpose.

#### GUI window panels

Panel	Explanation
Alarms	Indicates for the specific GUI view the number of active alarms for each severity.
Details	Indicates the specific frame and shelf for the component. <b>Note:</b> Valid for frame and shelf views only.
NE Info	Indicates information associated with the MG 9000. <ul style="list-style-type: none"> <li>• Name - Refer to "Provisioning an MG 9000 network element" (page 24)</li> <li>• Number - Refer to "Provisioning an MG 9000 network element" (page 24).</li> <li>• Version - Indicates the software version of the MG 9000 Manager software.</li> <li>• Vendor - Indicates the name of the manufacturer for the physical component.</li> <li>• IP Address - Refer to "Provisioning an MG 9000 network element" (page 24)</li> </ul>

The different levels of the MG 9000 hardware components can be accessed by double clicking an icon in a window.

## Prerequisites

There are no prerequisites.

## Action

### Accessing the MG 9000 Frame View

---

Step	Action
------	--------

---

#### *At the MG 9000 Manager*

- 1 Double click on the MG 9000 icon to access the MG 9000 element window, which represents a specific MG 9000 frame.
- 2 This procedure is complete.

---

—End—

---

### Accessing MG 9000 Shelf View

---

Step	Action
------	--------

---

#### *At the MG 9000 Manager*

- 1 Double click on an **MG 9000 shelf icon** to access the **MG 9000 Shelf** window, which represents a specific MG 9000 shelf.  
  
Each shelf displays icons for 21 slots. Slots 1, 10 and 11, 12 and 13, 14 and 15 are reserved for specific cards which are the SIC, DCC, ITP, and ITX respectively. The other slots are available for line cards.  
  
The slot number and name for each card is indicated below each slot.  
  
Above each slot are a triangle and a rectangle which represent the card's condition. Refer to "View current shelf-level alarms" in *MG 9000 Fault Management*, NN10074-911 or "Circuit card indicators" in *MG 9000 Basics*, NN10011-111 for details on LEDs.
- 2 This procedure is complete.

---

—End—

---

## Provisioning an MG 9000 network element

### When to use this procedure

The following procedure provides the steps to provision an MG 9000 from the MG 9000 Manager.

### Prerequisites

There are no prerequisites.

### Action

#### Provisioning an MG 9000 network element

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 From the **Subnet View**, select the **Configuration menu** option.
- 2 Select the **option** to "Add New MG 9000 NE..."
- 3 The **MG 9000 Provisioning View** appears.

#### MG 9000 Provisioning View

- 4 From the provisioning window, provide the following information:

#### Provisioning View properties

Field	Explanation
NE Number	A number (1-999) used for MG 9000 identification purposes.
NE Name	A descriptive name for the MG 9000. The name can contain any alphanumeric characters and underscore characters.
NE IP Address/ hostname	The IP address assigned to the DCC card. IP addresses must be in the form 0.0.0.0 through 255.255.255.255. Hostnames are allowed but must begin with a character (a-z, A-Z). Hostnames are translated immediately to IP addresses when a node is provisioned.
NE Manager IP Address/ Hostname	The IP address assigned to the MG 9000 Manager that manages the new NE. IP addresses must be in the form 0.0.0.0 through 255.255.255.255. Hostnames are allowed but must begin with a character (a-z, A-Z). Hostnames are translated immediately to IP addresses when a node is provisioned.
NE MG Password	Enter the password for secure FTP communication between the MG 9000 Manager and the MG 9000. The password entered in this field is provided for the MG 9000 Manager. The same password must be entered for the MG 9000 at the LCI. To change the password, the same value must be entered in this field (for the MG 9000 Manager) and in the Password Change screen at the LCI for the MG 9000.
NE Encryption Key	Enter the 20-120 character alphanumeric Preshared Key. This key must match what is entered in the LCI Preshared Key field in the <b>Connections-&gt;OAMP Connections</b> screen. For more information, refer to <i>MG 9000 Security and Administration</i> , NN10162-611.
NE provisioning mode	Auto Discover - The MG 9000 sends a cold start trap which allows the MG 9000 Manager to read the MG 9000 hardware information during the discovery process. This process is indicated by an up arrow symbol. Once auto discovery is complete, all the MG 9000 information may be queried and configurable fields may be changed as needed.
NE Market	Use this menu to select the appropriate market for the NE. The default setting is that which is selected in the Office-Wide Defaults view.
Download Digital Certificates	Activate this checkbox if you wish to use digital signature authentication for securing the OAMP channel for the NE. Before doing so, you must consult <i>MG 9000 Security and Administration</i> , NN10162-611

**Note 1:** If an invalid NE name is entered, an error message appears informing the user that the NE name must contain letters, numbers, and underscore characters only.

**Note 2:** If an invalid IP address or unknown host name for the MG 9000 is entered, an error message appears.

- 5 Select the **Apply** button to finish the process.

6 This procedure is complete.

---

—End—

---

## Provisioning office-wide defaults

### When to use this procedure

The following procedure provides the steps to provision office-wide Defaults for the MG 9000 Manager.

Values input in this view can be changed at any time. Changes will affect the values which are defaulted the next time VMGs are created. Changes have no affect on VMGs which have already been created.

MarketFit is an association of several pieces of data common to a country and operator. MarketFit is comprised of Custom Local Area Signaling Services (CLASS), tone, ringing, and coefficient data. When a Market-Fit is assigned to a VMG, the coefficient associated to the selected market is also assigned to that VMG. Coefficients are provisioned for the GLC card circuits and are described in "[Provisioning a Global line card](#)" (page 102).

The "[MarketFit comparisons](#)" (page 30) section lists the characteristics of the current North American Market Fit templates.

From within the Office-Wide Defaults GUI, the customer can configure one set of IP security (IPSec) parameters and have them applied to all, or a subset of, the provisioned MG 9000s.

**Note:** To ensure communications between the MG 9000 and the MG 9000 Manager, IPSec parameters on both ends must match. A mismatch in one parameter will prevent any communications from occurring.

### Prerequisites

There are no prerequisites.

### Action

#### Provisioning office-wide defaults

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 From the **Subnet View**, select the **Configuration menu** option.
- 2 Select the **Office-Wide** Defaults option.
- 3 The **MG 9000 Office-Wide Defaults view** appears.

## MG 9000 Office-Wide Defaults View

- 4 From the **Office-Wide Defaults View**, provide the following information:

Field	Explanation	Default
MarketFit Id	Select the appropriate Country/Operator combination from the menu.	NorthAmerica
<b>Silence Suppression (VoIP only):</b>		

Field	Explanation	Default
Voice Activity Detection	The menu has the following values: Off, Transparent, Conservative, Aggressive	Off
Comfort Noise Generation	The menu has the following values: Off, White, Pink, Spectral	Off
<b>QoS Thresholds (VoIP only):</b>		
Packet Loss%	Value float between 0.0 and 100.01	0.01
Latency (mSec)	An integer value representing the latency in milliseconds.	150
Jitter (mSec)	An integer value representing the jitter in milliseconds.	100
Bad Calls%	Value float between 0.0 and 100.00	0.00
<b>Security:</b>		
IKE Key	Internet Key Exchange (IKE) Key, a 20-120 alphanumeric character string to establish a secure call control link.	N/A
IKE Key (Verify)	IKE Key, same as above to confirm the value entered.	N/A
IKE Lifetime	Specifies the lifetime of the IKE phase 1 security association. Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours, or 28 days.	N/A
IKE Lifetime Unit	Units of life with the previous entry. In Seconds, Minutes, Hours, Days.	N/A
IPSec Lifetime	Specifies the lifetime of the IPSec security association. Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours, or 28 days.	N/A
IPSec Lifetime Unit	Units of life with the previous entry. In Seconds, Minutes, Hours, Days.	N/A

- 5 Select the **Apply** button to finish the process.

**Note:** The Market-Fit, Silence Suppression, and QoS parameters are saved to the Oracle database so the same data is presented in the VMG panels when a VMG is added. Clicking **Apply** here does not send data down to the network elements. Only when the **Apply** button on the VMGs are pressed will data be sent to the network elements.

- 6 This procedure is complete.

---

—End—

---

### MarketFit comparisons

The following table provides a listing of the characteristics of the North American MarketFits.

#### North American MarketFit comparisons

Characteristic	Template	
	NorthAmerica	NorthAmerica_v1
Ring voltage	85 V	100 V
<b>Note:</b> Only applies to Global line card. World line cards are not affected by this value since they are hard wired to 100 V.		
Payphone recognition tone	Matches the behavior of SN06/SN06.2 CS 2000	Matches behavior of SN07 CS 2000
Intrusion tone	1200 Hz/-5 dB, 100 ms, 150 ms off 1200 Hz/-5 dB, 100 ms, 75 ms off 2100 Hz/-5 dB, 200 ms on, 150 ms off 1700 Hz/-5 dB, 400 ms on, 2900 ms off, repeated	440 Hz/-13 dB, cadence: 100 on, 100 off, 100 on, 100 off, 100 on
Conference unlock tone	1200 Hz/-5 dB 100 ms, 150 ms off 1200 Hz/-5 dB 100 ms, 75 ms off 2100 Hz/-5 dB 200 ms on, 150 ms off 1700 Hz/-5 dB 400 ms on, 2900 ms off, repeated	480 Hz/-17 dB, 100 on, 100 off, 100 on, 100 off, 100 on, 100 off, 400 on
Warning tone	1400 Hz/ -7 dB, 500 ms	1400 Hz/-7 dB, 500 ms on, 15 s off repeated

# Provisioning Internodal ESA and community of interest

## When to use this procedure

Use the procedures in this section to

- provision Internodal ESA on an MG 9000
- provision a community of interest and to assign an MG 9000 network elements to a community of interest
- delete an MG 9000 network element from a community of interest

The Communities of Interest list contains a list of all currently defined communities. The maximum number of communities is limited to 32.

## Prerequisites

Ensure the MG 9000 network element (nodes) and VMGs are configured to support ESA. For information on configuring VMGs for ESA, refer to procedure "[Provisioning ESA](#)" (page 201).

## Action

### Provisioning Internodal ESA

Step	Action
<i>At the MG 9000 Manager</i>	
1	Identify the MG 9000 network element to be added to a community of interest.
2	Perform procedure " <a href="#">Configuring PVR</a> " (page 36).
3	Perform procedure " <a href="#">Provisioning an Internodal ESA community of interest</a> " (page 32).
4	Repeat <a href="#">step 1</a> through <a href="#">step 3</a> until all desired network elements are added to the community of interest and configured to support Internodal ESA.
5	This procedure is complete.
—End—	

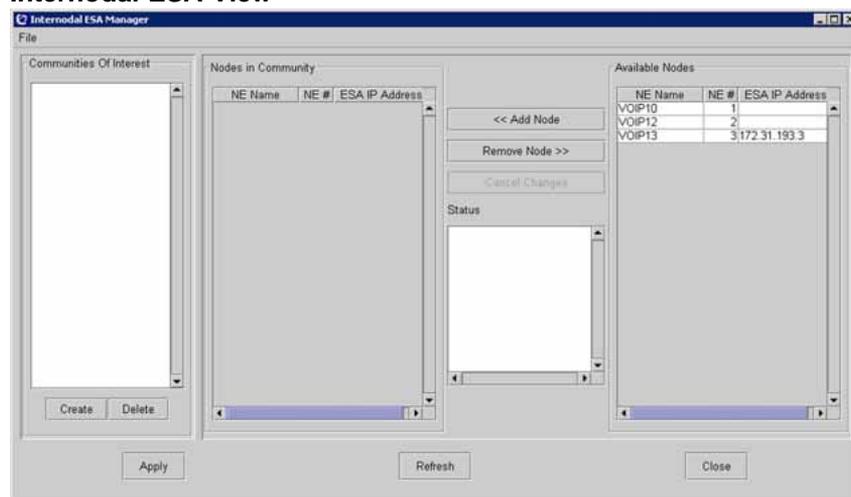
## Provisioning an Internodal ESA community of interest

Step	Action
------	--------

### At the MG 9000 Manager

- 1 From the **Subnet View**, select the **Configuration menu** option.
- 2 Select the option "**Internodal ESA...**"
- 3 The **Internodal ESA View** opens. The following figure shows the **Internodal ESA View**.

### Internodal ESA View



- 4 Use the information in the following table to assign an MG 9000 network element to a community of interest.

Field or function	Explanation
Communities of Interest	Contains a list of all currently defined communities. When clicking on an item in the list, the Nodes in Community list changes. The number of communities is limited to 32.
Nodes in Community	Lists all the nodes (MG 9000 network elements) currently in the selected community of interest. The number of nodes in a community is limited to 15.
Available Nodes	Displays all nodes (network elements) available to be added to a community, meaning they do not currently belong to a community. Only nodes at SN08 and up and currently in a community will be displayed.

Field or function	Explanation
Create button	<p>Allows the user to create community of interest names. Names are limited to 20 characters and can only contain characters a - z, A - Z, and underscore (_).</p> <p><b>Note:</b> Community of interest names are not case sensitive.</p>
Delete button	Allows the user to delete community of interest names.
Add Node button	Allows the user to add nodes (network elements) from the available list to the of community of interest node list. Before a node is added to a community, the ESA IP address must be set.
Remove Node button	Allows the user to remove nodes from the selected community. The community selected node in the Nodes in Community list will be removed from the list and it will appear in the Available Nodes list.
Cancel Changes button	Cancels the changes made to COI before clicking the Apply button.
ESA IP Address	<p>The ESA IP Address field in the Nodes in Community list and Available Nodes list is editable. The other fields in the lists are not editable.</p> <p>The IP Address field must be configured before a node is added to the community. When the user presses Enter or clicks in another window or button, the IP address will be validated and saved in the database. The IP address must be "well-formed" and unique in the system.</p>

Field or function	Explanation
Apply button	<p>Allows the user to apply changes to the Community. The button is disabled until there are changes to commit. When the user makes changes to a community, the button is disabled. If the user tries to leave the GUI or click on another community name, the user will be prompted to save or discard changes.</p> <p>When the user presses Apply a status window displays the status of NEs that are being updated. The status window scrolls as NEs are successfully updated or if there are any failures. A configuration alarm is generated if there are any configuration failures. However, if the user exits the GUI and returns to the GUI, there is no way to determine if there were any previous failures, but the alarm will continue to be displayed in the Alarm Browser until the configuration is successful. If there is a failure, the user can start an audit to re-configure the COI or the user can press the Apply button on the GUI. The Apply button causes the currently selected COI data to be sent to all affected nodes.</p>
Refresh button	Allows the user to completely refresh the GUI with data from the database.

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

If	Do
creating a new community of interest	<a href="#">step 6</a>
adding a network element to a community of interest	<a href="#">step 8</a>

- 6 Click on the **Create** button to create a new community of interest name. The New Community of Interest Name GUI appears.
- 7 Enter the New Community of Interest Name and click **OK**. The new name appears in the Communities of Interest field.

- 8 Click on the appropriate Community of Interest name to which a network element is to be added.
- 9 In the Available Nodes list, select a network element to be added to the community.
- 10 Set the ESA IP address of the network element by typing the ESA IP address in the ESA IP address field and press **Enter** on the keyboard.
- 11 Click on the **Add Node** button to add the network element to the community.
- 12 Click on the **Apply** button to apply the changes.
- 13 This procedure is complete.

---

—End—

---

### Deleting a network element from a community of interest

---

Step	Action
------	--------

---

*At the MG 9000 Manager*

- 1 From the **Subnet View**, select the **Configuration** menu option.
- 2 Select the option "**Internodal ESA...**" The Internodal ESA View opens.
- 3 Select the network element from the Nodes in Community and click on the **Remove Node** button.
- 4 Click on the **Apply** button to apply the changes.
- 5 This procedure is complete.

---

—End—

---

## Configuring Nortel Multiservice Switch virtual router (PVR)

### When to use this procedure

Use this procedure to configure a Multiservice Switch 15000 (or equivalent) to support Internodal ESA for an MG 9000 in a community of interest.

### Prerequisites

Ensure the MG 9000 network element (nodes) are configured to support ESA.

Ensure it has been determined how the network elements will be grouped into communities. Each MG 9000 must be configured with a new ESA IP address. This IP address should be chosen from an available IP address from the call control subnet (which is the same subnet used for VMG configuration). No default communities are provided so each community must be manually configured by the customer for internodal ESA to function.

### Action

#### Configuring PVR

Step	Action
<i>At the MG 9000 Manager</i>	
1	From the <b>Subnet View</b> , click on the MG 9000 network element to be added to the community.
2	From the <b>Subnet View</b> , select the <b>Configuration-&gt;View/Modify NE Properties</b> menu option.
3	The <b>Properties View</b> opens. Click on the <b>IESA PVR Provisioning</b> tab. The following figure shows the <b>Properties View</b> with the <b>IESA PVR Provisioning</b> tab.

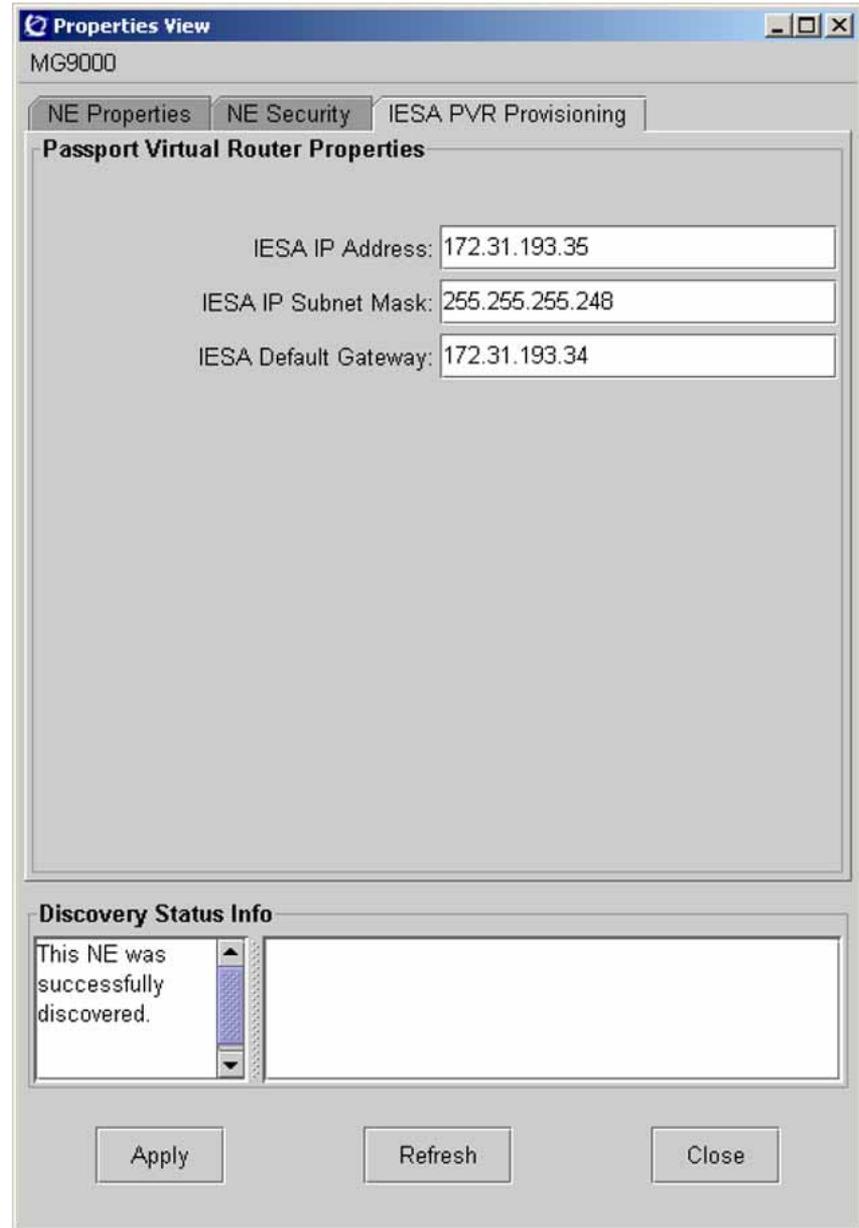
**Properties View with IESA PVR Provisioning tab for MG 9000 with OC3 or DS1-IMA**

The screenshot shows a 'Properties View' window for an MG9000 device. The 'IESA PVR Provisioning' tab is selected. The 'Passport Virtual Router Properties' section includes the following fields:

- ATM Service Category: Real-time Variable Bit Rate (dropdown menu)
- IESA IP Address: [Empty text box]
- IESA IP Subnet Mask: [Empty text box]
- IESA Default Gateway: [Empty text box]
- Virtual Channel Connection: 16
- Virtual Channel VPI: 16
- Virtual Channel VCI: 32
- Virtual Channel PCR: 4000
- Virtual Channel SCR: 2000
- Virtual Channel Burst Size: 32
- Virtual Channel Cell Delay: 3

The 'Discovery Status Info' section at the bottom contains a scrollable text area with the message: 'This NE was successfully discovered.' Below this section are three buttons: 'Apply', 'Refresh', and 'Close'.

Properties View with IESA PVR Provisioning tab for MG 9000 with GigE



- 4 Use the information in the following table to configure the PVR for the selected MG 9000 network element.

Field or function	Explanation
IESA IP Address	An address chosen from an available IP address from the call control subnet (which is the same subnet used for VMG configuration). These values apply to the Internodal ESA interface.
IESA IP Subnet Mask	
IESA Default Gateway	
<b>The following apply to MG 9000 with OC3 or DS1-IMA DCC card</b>	
ATM Service Category	Default value is Real-time Variable Bit Rate
Virtual Channel Connection	
Virtual Channel VPI	Virtual Path Identifier. A value from 1-254.
Virtual Channel VCI	Virtual Channel Identifier. A value from 33-2047.
Virtual Channel PCR	Peak cell rate. The value entered must be greater than or equal the value entered for the SCR.
Virtual Channel SCR	Sustainable cell rate. The value entered must be less than or equal to the value entered for the PCR.
Virtual Channel Burst Size	Virtual channel maximum burst size.
Virtual Channel Cell Delay	Virtual channel cell delay variation timing.

- 5 Click on **Apply** to accept provisioning changes.
- 6 This procedure is complete. If this activity is part of provisioning Internodal ESA, return to procedure "[Provisioning Internodal ESA](#)" (page 31).

---

—End—

---

## Provisioning clock synchronization

### When to use this procedure

Use this procedure when it is necessary to provision clock synchronization. All provisioning of clock synchronization is performed on the active ITP card in the master shelf through the Clock Sync tool. The Clock Sync tool initiated on ITP cards in subtending shelves will only monitor the status and sync reference. No provisioning is permitted on subtending shelves.

The Clock Synchronization view is divided into four sections:

- Provisioning - allows manual provisioning of clock sync
- Control - provides the ability to force a switch between valid reference sources
- Status - displays clock sync status and health
- Reference/Signal - shows the selected timing reference and status of the timing signal

The following procedures are provided in this section:

- ["Provisioning clock synchronization"](#) (page 40)
- ["Forcing a switch between valid reference sources"](#) (page 45)

### Prerequisites

There are no prerequisites.

### Action

#### Provisioning clock synchronization

Step	Action
<i>At the MG 9000 Manager</i>	
1	At the <b>Subnet View</b> , double click on the <b>MG 9000</b> that contains the ITP card which is to have the clock sync provisioned. The <b>NE Desktop View</b> appears.
2	From the <b>Frame View</b> in the <b>NE Desktop View</b> , double click on the master shelf containing the ITP card to be modified. The <b>Shelf View</b> appears.
3	From the <b>Shelf View</b> , double click on the active ITP card. The <b>ITP Card View</b> appears.

- From the menu bar, select **Actions->Clock Synchronization**. The **Clock Synchronization view** appears.

Depending on whether the active or inactive ITP card is selected depends on the information presented in the **Clock Synchronization view**.

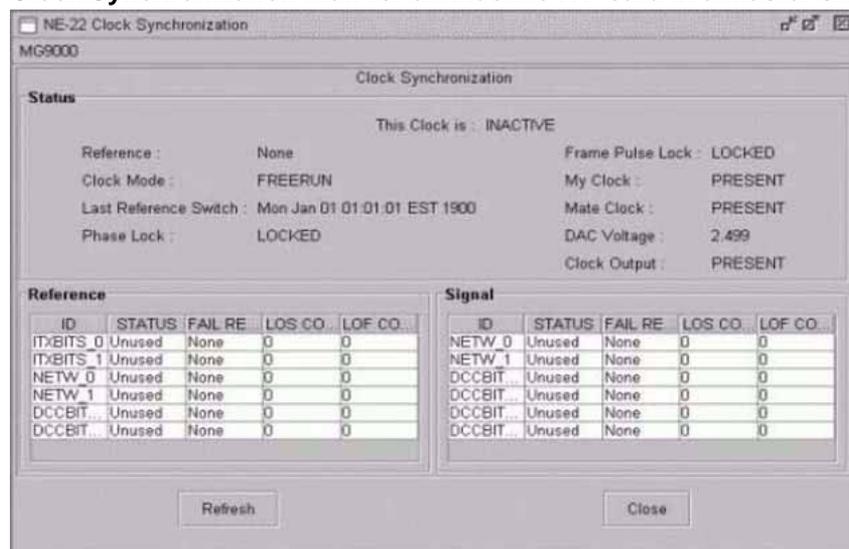
The following figure shows the **Clock Synchronization view** for an active ITP card in a master shelf.

**Clock Synchronization view for an active ITP card in a master shelf**



The following figure shows the Clock Synchronization view for an inactive ITP card in a master shelf.

### Clock Synchronization view for an inactive ITP card in a master shelf



- 5 Use the information in the following table to provision clock synchronization for the selected active ITP card. Use the fields in the Provisioning section of the Clock Synchronization view to make clock sync changes.

#### Clock synchronization

Field	Entry	Explanation and action
<b>Provisioning</b>		
Primary Reference	None, NETW, ITX BITS, DCC BITS, DCC SSU	<p>None - no timing reference is available and clocking will not be synchronized but will instead be in "Free Run" mode. None is only valid as a choice if both Primary and Alternate are selected to be None.</p> <p>NETW - this choice allows the clock sync to be extracted from the upstream network. Not supported for an MG 9000 configured with GigE DCC cards.</p> <p>ITX BITS - this choice stipulates that timing will be obtained from a Building Integrated Timing Supply (BITS). Selection of BITS requires the user to input the ITX pair that will be providing the BITS signal.</p> <p>DCC BITS - this choice indicates that timing will be obtained from a Building Integrated Timing Supply (BITS) connected.</p>

Field	Entry	Explanation and action
Alternate Reference <b>Note:</b> The default value for the Alternate Reference should be "None". In most cases, this parameter should NOT be changed. Changing to a value other than "None" requires knowledge of network timing topology. This parameter should only be changed if the user knows that by doing so the network elements subtending from the MG 9000 will not create a timing loop. If the user is unsure, "None" should be selected.	None, NETW, ITX BITS, DCC BITS, DCC SSU	<p>DCC SSU - this choice indicates that timing will be obtained from a Synchronization Supply Unit (SSU) when GigE DCC cards are provisioned. Only applies to International applications.</p> <p>None - no timing reference is available and clocking will not be synchronized but will instead be in "Free Run" mode. None is only valid as a choice if both Primary and Alternate are selected to be None.</p> <p>NETW - this choice allows the clock sync to be extracted from the upstream network. Not supported for an MG 9000 configured with GigE DCC cards.</p> <p>ITX BITS - this choice stipulates that timing will be obtained from a Building Integrated Timing Supply (BITS). Selection of BITS requires the user to input the ITX pair that will be providing the BITS signal.</p> <p>DCC BITS this choice indicates that timing will be obtained from a Building Integrated Timing Supply (BITS) connected to the DCC cards.</p> <p>DCC SSU - this choice indicates that timing will be obtained from a Synchronization Supply Unit (SSU) when GigE DCC cards are provisioned. Only applies to International applications.</p>
Framing	SF, ESF	<p>For OC3/DS1-IMA DCC cards, the Encoding types supported for DCC BITS/ITX BITS timing sources are:</p> <ul style="list-style-type: none"> <li>• Super Frames (SF)</li> <li>• Extended Super Frames (ESF)</li> </ul> <p>The default is SF.</p>
Revertive Switch	Enabled, Disabled	<p>This will enable or disable the revertive switching between provisioned clock sources.</p> <p>The default mode for revertive switching will be Disabled.</p>
Clock Sync Alarm	Enabled, Disabled	<p>This will enable/disable Clock Sync alarms to be sent up from the MG 9000. Disabling alarm reporting will prevent will prevent clock sync alarms from being reported to the Alarm Browser.</p> <p>The default value is that alarms are Enabled.</p>

Field	Entry	Explanation and action
ITX Slot# 0/1	Integer Number Range 2-21	<p>If ITX BITS is chosen as either Primary (recommended) or Alternate, then the ITX slot numbers must pass the following to be valid:</p> <p>The value must be an integer number.</p> <p>The value must be in the range of 2-21.</p> <p>The card in the slot entered must be an ITX.</p> <p>The slot numbers must be sequential.</p> <p>The Right Slot number cannot be less than the Left Slot number.</p>
<b>Control</b>		
Switch Type	Manual Switch Force Switch	<p>Manual Switch will perform a switch between the Primary and Alternate Reference Sources</p> <p>Force Switch will force a switch between Primary and Alternate References</p>
<b>Status</b>		
Clock Status	None	The clock status window indicates Status of the clock whether it is active or inactive and the health of the clock with below mentioned parameters.
Timing Reference	None	None, Bits, Network, Host
Clock Mode	None	Indicated the mode of synchronization unit. Acquired, Acquiring (a transient condition), HoldOver, or freeRun.
Last Reference Switch	None	Indicates the date and the time of Last Reference Switch or system requested (auto) switch.
Phase Lock	None	Indicates whether the phase is locked or not locked.
Frame Pulse Lock	None	Indicates whether pulse of the frame is locked or not locked.
My Clock	None	Indicates whether the status of my clock is present or missing/failed.
Mate Clock	None	Indicates whether the mate clock is present or missing/failed.
DAC Voltage	None	Indicates the DAC Voltage up to 3 decimal places.
Clock Output	None	Indicates whether the output of the clock is present or missing/failed.
<b>Reference/Signal</b>		

Field	Entry	Explanation and action
Sync Reference Status	None	Provides the current status of the sync reference such as, Used, Active, Inactive, Failed.
Sync Reference Fail Reason	None	Provides the reason for the failure of this sync reference.
Sync Reference Loss of Signal Count	None	Indicates loss of signal count for this sync reference.
Sync Reference Loss of Frame Count	None	Indicates the loss of frame count for this sync reference.
Timing Signal Status	None	Indicates whether the timing status is Unused, Active, or Inactive.
Timing Signal Fail Reason	None	Provides the reason for the failure of the timing signal.
Timing Signal Loss of Signal Count	None	Indicates timing signal loss of signal count.
Timing Signal Loss of Frame Count	None	Indicates the timing signal loss of the frame count

6 Click on **Apply** to submit changes.

7 This procedure is complete.

---

—End—

---

### Forcing a switch between valid reference sources

This procedure should be performed only if the Alternate Reference field is set to a value other than None. No action is required if the Alternate Reference is set to None.

### Forcing a switch between valid reference sources

---

#### Step Action

---

#### *At the MG 9000 Manager*

- 1 At the **Subnet View**, double click on the **MG 9000** that contains the ITP card which is to have the clock sync provisioned. The **NE Desktop View** appears.
  - 2 From the **NE Desktop View**, double click on the ITP card in the shelf to be modified. The **ITP Card View** appears.
  - 3 From the menu bar, select **Actions->Clock Synchronization**. The **Clock Synchronization view** appears.
-

- 4 In the Control section, click on **Force Switch**.
- 5 Click on Switch to submit the force switch action.
- 6 This procedure is complete.

---

—End—

---

## Manually persisting MG 9000 provisioning data

### When to use this procedure

MG 9000 Manager data is automatically persisted hourly. Use this procedure when it is necessary to manually persist data to the database. The following are the circumstances when this manual process would be used:

- after a significant amount of services data have been provisioned. This action would ensure a backup of the data will be available on the database.
- before shutting down the MG 9000 Manager

All the network elements (nodes) may be selected to persist or individual network elements can be manually selected to persist.

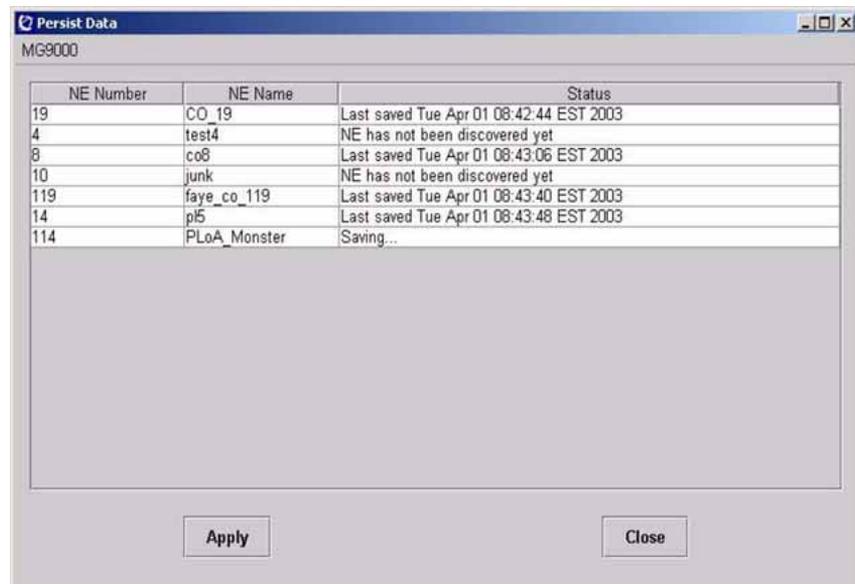
### Prerequisites

There are no prerequisites.

### Action

#### Persisting MG 9000 provisioning data

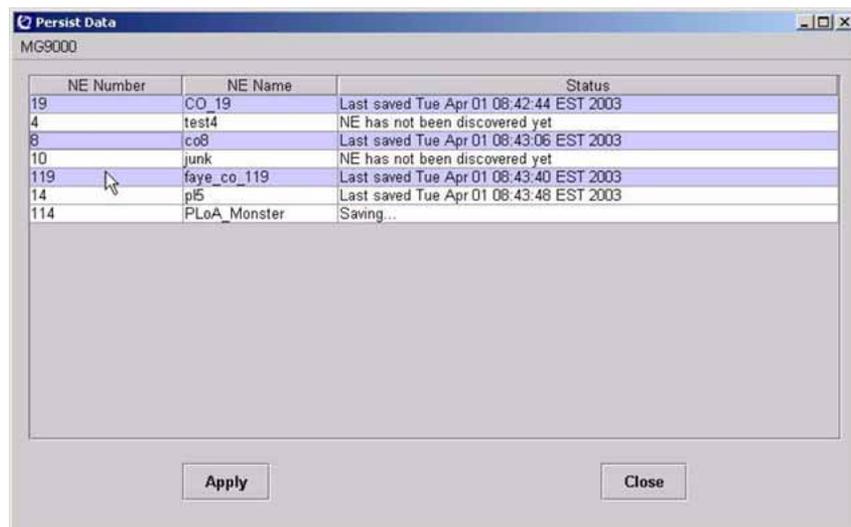
Step	Action
<i>At the MG 9000 Manager</i>	
1	At the <b>Subnet View</b> , from the menu select <b>MG9000-&gt;Persistence</b> . The <b>Persistence</b> window appears.



- 2 The next step is based on information in the following table.

If persisting	Do
all the nodes	<a href="#">step 3</a>
only selected nodes	<a href="#">step 4</a>

- 3 To persist all the nodes, select **Apply**. Go to [step 5](#).
- 4 To persist only selected nodes, highlight the rows that correspond to the desired nodes by holding down the CONTROL key while clicking. Then select **Apply**.



The following table lists the NE conditions, if persistence is allowed in that condition, and the system response.

#### Network element persistence conditions

NE condition	Persistence allowed?	System response
Undiscovered NE	No	This message is displayed under the status column: "NE has not been discovered yet."
Discovering	No	This message is displayed under the status column: "NE is still discovering."
Auditing	No	The node cannot be persisted at this time as a Data Audit is in progress. This message is displayed under the status column: "NE is still discovering."

NE condition	Persistence allowed?	System response
Database Recovery	No	The node is currently recovering data from database. This message is displayed under the status column: "NE is recovering from DB".
Discovered	Yes	The node can now be persisted to Database. The status column will display "Saving..." and when finished will display a time of completion.

5 This procedure is complete.

---

—End—

---

## Deleting an MG 9000 network element

---

### When to use this procedure

Use this procedure when it is necessary to delete an MG 9000 network element (node).

### Prerequisites

Ensure that any SLoA data on the NE is removed before deleting the NE. Deleting the NE without removing the SLoA data may result in the Core data being out of sync with the MG 9000 and the NE. For information on deleting the SLoA data, refer to "Deleting a termination" (page 195) and "Deleting a VMG" (page 196).

Ensure the MG 9000 has been removed from a community of interest. The NE cannot be deleted if it is in a community of interest. An error message will appear if the user attempts to delete an NE that is configured in a community.

### Action

#### Deleting an MG 9000 network element

---

Step	Action
------	--------

---

*At the MG 9000 Manager*

- 1 At the **Subnet View**, select the **MG 9000** icon to be deleted.
- 2 From the menu, select **Configuration->Delete Node**. The system responds with the **Network Element Deletion View**. A description of the fields follows the figure.

**Network Element Deletion View**

The following table lists the fields in the **Network Element Deletion View**.

**Network Element Deletion View fields**

Field	Explanation
NE Number	The selected element number
NE Name	The selected network element name
NE IP Address/Hostname	The IP address to the DCC card
NE Password	Enter the MG 9000 Manager SFTP password

Field	Explanation
NE Encryption Key	Enter the 20-120 character alphanumeric Preshared Key. This key must match what is entered in the LCI Preshared Key field in the Connections->OAMP Connections screen as described in "OAMP Connection screen fields for AAL1 and VoIP solutions" (page 339). For more information, refer to <i>MG 9000 Security and Administration</i> , NN10162-611.
MG 9000 Manager IP Address	IP address of MG 9000 Manager
SNMP Trap IP (from MG)	IP address to which the MG 9000 sends SNMP traps
NE Provisioning Mode	Auto-discover
Vendor	The name of the manufacturer for the physical component
MG 9000 Software Version	MG 9000 software version
SNMP Trap Port (expected)	SNMP Trap port number expected by the MG 9000 Manager.
SNMP Trap Port (from MG)	SNMP Trap port number set on the MG 9000
NE OM Collection	Not an active checkbox on this GUI. When checked the OM Collector will collect OM data starting from its next collection cycle. If unchecked, the OM Collector will stop collecting OM data starting from its next collection cycle.

- 3 Select the **Apply** button to begin the deletion process. The system will determine if the deletion is allowed. The following table identifies the conditions for which deletion will or will not be allowed and the system response.

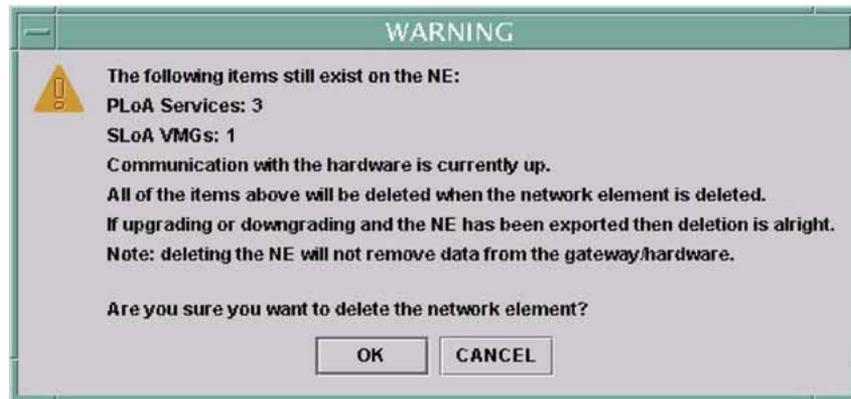
#### Network element deletion conditions

NE condition	Deletion allowed?	System response
Discovering	No	Node is discovering, deletion not allowed
Terminating	No	Node is already being deleted. No additional delete request allowed.

NE condition	Deletion allowed?	System response
Discovered - with PLoA/SLoA/xDSL services but has lost communications with the gateway	Yes	A warning message will be displayed listing the services on the NE. This warning message will give the user the option to proceed or cancel the deletion request. If the user chooses to proceed with the deletion request, the deletion process will remove all the equipment information associated with the NE.
Discovered - without any PLoA/SLoA/xDSL services	Yes	A confirmation warning message will be displayed. This warning message will give the user the option to proceed or cancel the deletion request. If the user chooses to proceed with the deletion request, the deletion process will remove all the equipment information associated with the NE.
Undiscovered NEs	Yes	A confirmation warning message will be displayed. This warning message will give the user the option to proceed or cancel the deletion request. If the user chooses to proceed with the deletion request, the deletion process will remove all the equipment information associated with the NE.
Discovered - with PLoA/SLoA/xDSL services	Yes	A warning message is displayed and is shown in the figure that follows this table.

**Note:** If an audit is in progress when deleting an NE, the audit will be safely abandoned. Any scheduled audits on the NE will be deleted. The Network element deletion warning will also contain a message if audit operations are to be abandoned.

**Network element deletion warning**



4 This procedure is complete.

—End—



---

## Subtending shelves

---

### What is a subtended shelf?

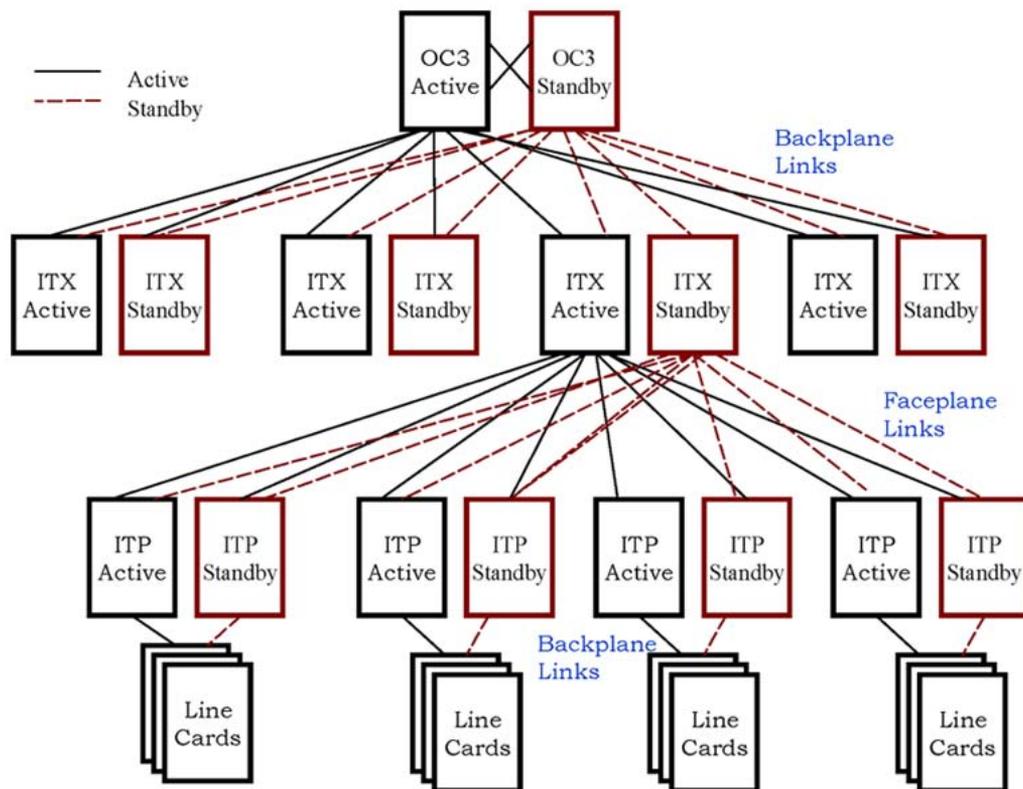
The concept of a subtending shelf applies to an MG 9000 Network Element (NE) that contains more than one shelf. Provisioning a subtended shelf is nearly identical to the provisioning of any other. For auto-discovered configurations both subtended and master shelves will be discovered with no additional configuration required.

The MG 9000 shelves are defined as follows:

- master shelf - any shelf which contains an active OC3/STM-1, DS1-IMA, or GigE DCC card
- subtending shelf - also known as a slave shelf, is any shelf which does not contain an active OC3/STM-1, DS1-IMA, GigE DCC card

There is no physical restriction on the location of a subtended shelf, nor is it necessary that it be adjacent to its associated master shelf. Subtended shelves allow multiple cards and shelves to utilize a single OC3/STM-1 (ATM) (OC3c or OC3 channelized), DS1-IMA, or GigE connection. In addition, DS1-IMA cards support a maximum of three subtended shelves.

The following figure shows the connections associated with a sample subtended shelf.

**MG 9000 subtended shelf card hierarchy****Shelf provisioning rules**

The MG 9000 Manager enforces the following rules associated with master and subtending shelf configuration:

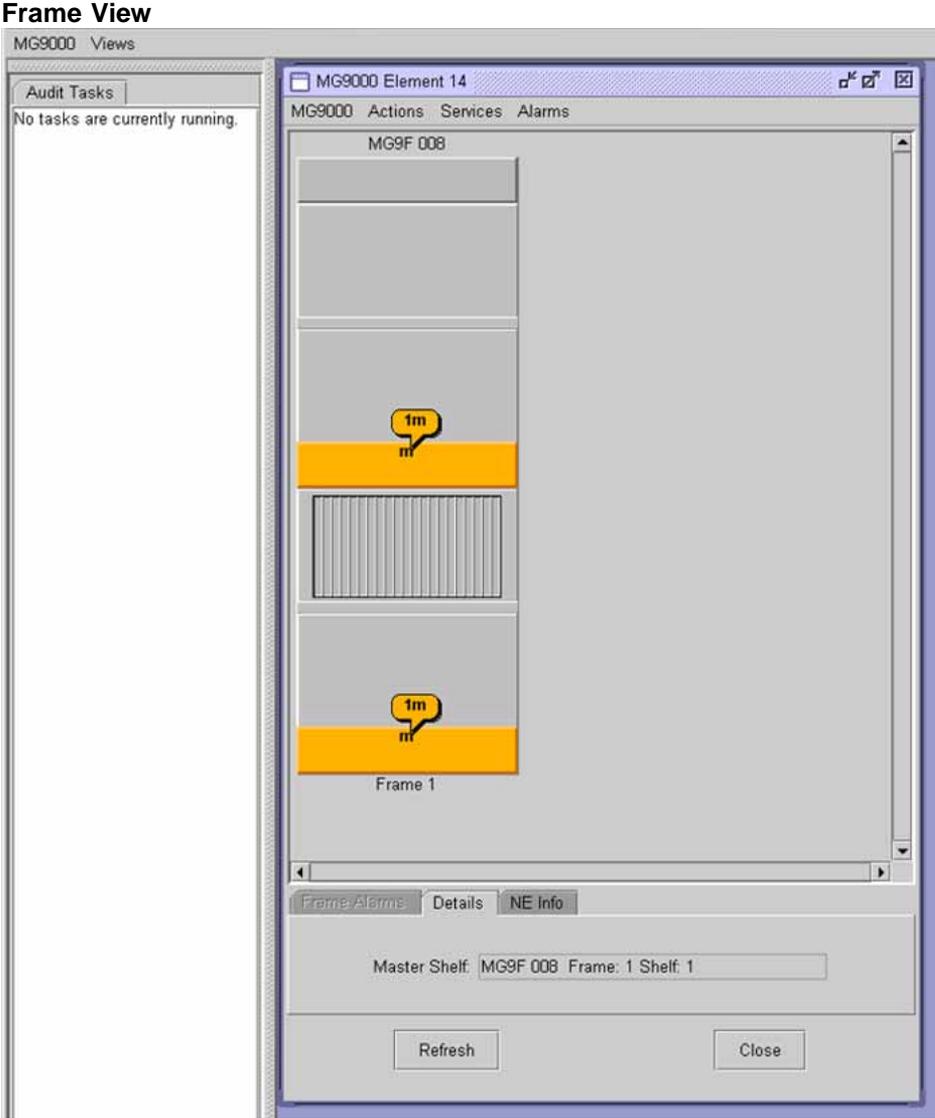
- There can only be one master shelf.
- A maximum of 15 subtended shelves per master shelf are supported in the UA-AAL1 solution.
- A maximum of 11 subtended shelves are supported in the UA-IP solution.
- A maximum of three subtended shelves are supported off of DS1-IMA cards.
- A master shelf is determined by the presence of an active OC3/STM-1, DS1-IMA, or GigE card.

**Differentiating a shelf type**

The following information identifies how to differentiate between master and subtending shelves using the Frame View and Shelf View in the MG 9000 Manager.

**Frame View**

In the Frame View, the master frame is always seen at the far left side of the Frame View, and subtending frames to the right of the master frame. The details tab pane at the bottom portion of the screen identifies the master shelf in the master frame. All other shelves are considered subtended or slave shelves. The following figure shows the Frame View within the NE desktop view with the Details tab selected at the bottom of the window.



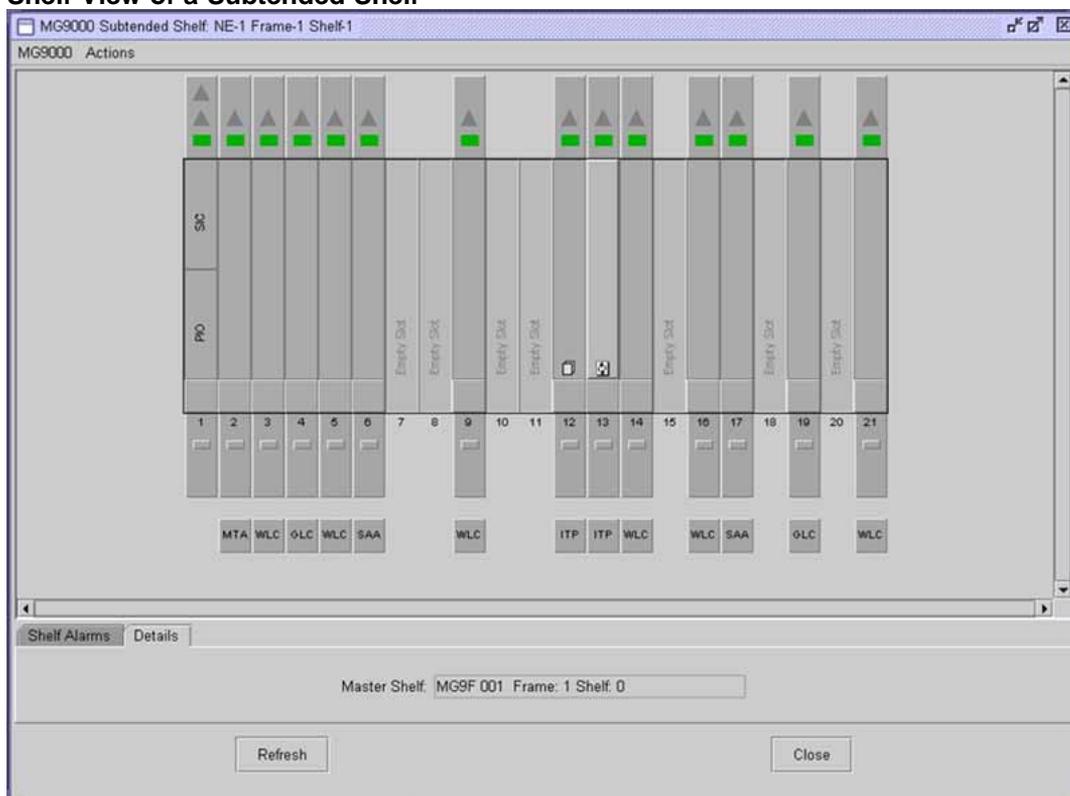
## Shelf View

In a Shelf View, there are two ways to determine if a shelf is a master or slave shelf.

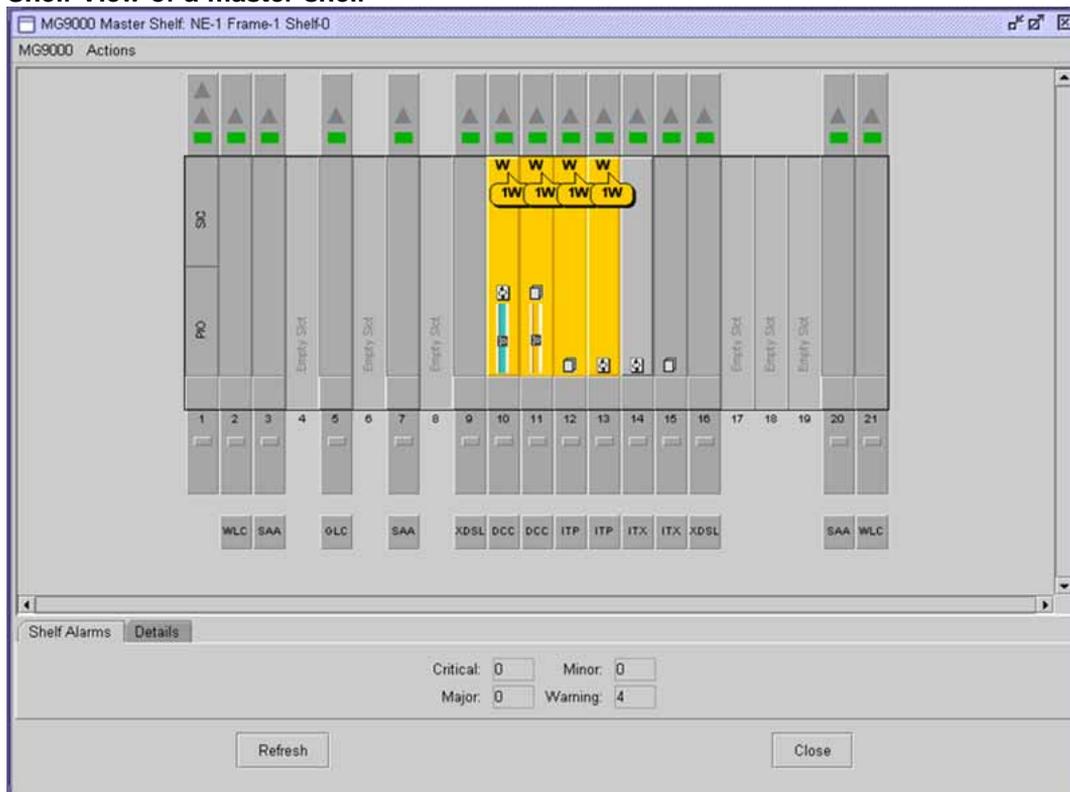
- First, the details tab pane at the bottom portion of the screen has the location of the master shelf, this can be compared to the shelf location displayed in the title bar.
- Second, look for the presence of a provisioned DCC (OC3/STM-1, DS1-IMA, or GigE card). The DCC card indicates a master shelf.

The following figures show the Shelf View with the Details tab selected at the bottom of the window for a subtended shelf and a master shelf.

### Shelf View of a Subtended Shelf



### Shelf View of a master shelf



### Provisioning subtended shelves

Autodiscovery detects additional shelves and updates the node/shelf view. Provisioning the virtual media gateway (VMG) on the subtended shelf is the same as for a master shelf, except that the shelf must be identified on which the VMG is to be provisioned.

## Renumbering an MG 9000 frame

### When to use this procedure

Use this procedure when it is necessary to change a frame number as part of an office reconfiguration of MG 9000 frames and shelves.

### Prerequisites

Perform this activity during periods of low traffic.

### Action

#### Renumbering an MG 9000 frame

Step	Action
------	--------

##### *At the CS2000 Management Tools*

- |   |   |
|---|---|
| 1 | Using OSSGate, deprovision all lines configured off the frame to be renumbered. |
|---|---|

##### *At the MG 9000 Manager*

- |   |  |
|---|--|
| 2 | Perform "De-provisioning a line card" (page 160) for all line cards in the frame.  |
| 3 | Remove all line cards from the frame.  |
| 4 | Deprovision all SIC cards in the frame by performing the following steps: <ol style="list-style-type: none"> <li>At the <b>Shelf View</b>, double-click on the SIC card in slot 1. The <b>SIC Card View</b> appears.</li> <li>Set the Administrative State of the card to Locked . The Operational State changes to Disabled.</li> <li>Repeat steps 4a and 4b for each SIC in the frame.</li> </ol>  |
| 5 | Deprovision the inactive ITP cards in the frame by performing the following steps: <ol style="list-style-type: none"> <li>At the Shelf View, double-click on the inactive (Hot_Standby) ITP card. The <b>ITP Card View</b> appears.</li> <li>Set the Administrative State of the card to Locked. Set the Configuration State to Offline. The Operational State changes to Disabled.</li> <li>Repeat steps 5a and 5b for each ITP card in the frame.</li> </ol> |

##### *At the MG 9000 frame*

**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.

- 6 Remove the inactive ITP cards from each shelf in the frame.

**At the MG 9000 Manager**

- 7 Deprovision the active ITP cards in the frame by performing the following steps:
- a. At the **Shelf View**, double-click on the active (Providing\_Service) ITP card. The **ITP Card View** appears.
  - b. Set the Administrative State of the card to Locked. Set the Configuration State to Offline. The Operational State changes to Disabled.
  - c. Repeat steps 7a and 7b for each ITP card in the frame.

**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.

Remove the active ITP cards from each shelf in the frame.

**At the MG 9000 Manager**

- 9 At the **Subnet View**, double click the **MG 9000** icon. The **Frame View** appears.
- 10 Double click on the **IBIP shelf** to access the IBIP Shelf View for the MG 9000 IBIP shelf with the alarm processor card in alarm.
- 11 Identify the alarm processor card with the alarm by observing the alarm balloon.
- 12 To lock the card, change the Administrative state by selecting Lock from the **administrative state** pull-down menu in the state section.

- 13 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**

- 14 Remove the IBIP front cover.

15



**WARNING**

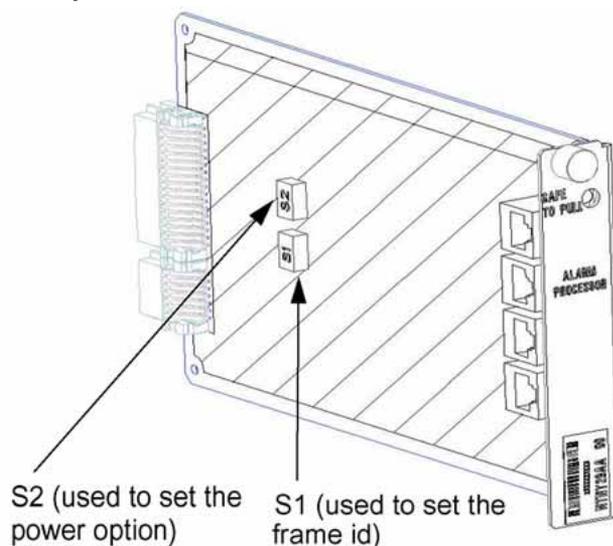
**Static electricity damage**

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.

Loosen the hold-down screw on the faceplate of the alarm processor card

- 16 Identify 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**



- 17 Set switch bank SW-1 to the frame id settings desired. Use the following note and table when setting the frame id.

**Note:** Ensure the frame id setting used for the renumbered frame is the logical frame number, not the physical frame number.

#### Switch 1 Frame ID switch settings

SW-2 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
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

**18** Insert the alarm processor card into the IBIP and secure the card into place with the hold-down screw.

**19** Replace the IBIP front cover.

#### **At the MG 9000 Manager**

**20** 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.

**21** Provision all SIC cards in the frame by performing the following steps:

- At the **Shelf View**, double-click on the SIC card in slot 1. The **SIC Card View** appears.
- Set the Administrative State of the card to Unlocked. The Operational State changes to Disabled.

- c. Repeat steps 21a and 21b for each SIC in the frame.

**At the MG 9000 frame**

22

	<p><b>WARNING</b> <b>Static electricity damage</b></p> <p>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.</p>
---	---

Install one ITP card into each shelf in the frame.

**At the MG 9000 Manager**

- 23 Provision the ITP cards that were just installed in the previous step by performing the following steps:
  - a. At the **Shelf View**, double-click on the discovered ITP card. The **ITP Card View** appears.
  - b. Set the Administrative State of the card to Unlocked. Set the Configuration State to Online. The Operational State changes to Enabled.
  - c. Repeat steps 23a and 23b for each ITP card in the frame.

**At the MG 9000 frame**

24

	<p><b>WARNING</b> <b>Static electricity damage</b></p> <p>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.</p>
---	---

Install the mate ITP card into each shelf in the frame.

**At the MG 9000 Manager**

- 25 Provision the mate ITP cards that were just installed in the previous step by performing the following steps:
  - a. At the **Shelf View**, double-click on the discovered mate ITP card. The **ITP Card View** appears.

- b. Set the Administrative State of the card to Unlocked. Set the Configuration State to Online. The Operational State changes to Enabled.
- c. Repeat steps 25a and 25b for each mate ITP card in the frame.

***At the MG 9000 frame***

26



**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.

Install all line cards that were removed from the frame in [step 3](#).

***At the MG 9000 Manager***

- 27 Provision all the line cards by line card type that were installed in the previous step. Use the line card provisioning procedures in this document for this activity.

***At the CS2000 Management Tools***

- 28 Using OSSGate, provision all lines configured off the frame that were deprovisioned in [step 1](#).
- 29 This procedure is complete.

---

—End—

---

## Provisioning a MG 9000 frame physical location

### When to use this procedure

Use this procedure when it is necessary to provision an MG 9000 frame's physical location in an office. The following information is displayed concerning a frame's physical location:

- Site identifier
- internal (logical) frame number
- floor position
- row position
- frame position within the row

After the frame is provisioned, the provisioned data is displayed in alarm logs, and the external office frame number will be displayed on the MG 9000 Frame View. The external office frame number will be displayed on the frame view and the details tab of the shelf views. For any non-ABI VMGs created after provisioning the frame, use the site and office frame number from the frame as part of the VMG name.

**Note 1:** This procedure must be completed before any new VMGs are created in a frame. If VMGs already exist, any attempt to provision or change a frame's site and office frame number will be blocked if the new site and office frame number conflict with existing VMG names. To continue with the provisioning activity, the VMGs that do not match the desired site and office frame number will have to be deleted and then recreated after the frame is provisioned.

**Note 2:** If Frame location is reprovisioned when an Alarm audit is in progress, the Frame location information for the MG 9000 alarm may not be updated immediately on Alarm browser.

### Prerequisites

Users must have emswr or emsadm permissions to update the frame location information.

### Action

#### Provisioning a MG 9000 frame physical location

Step	Action
------	--------

<i>At the MG 9000 Manager</i>	
-------------------------------	--

- 1 At the **Subnet View**, double click the **MG 9000** network element icon. The **NE desktop view** with **Frame View** appears.
- 2 From the **Frame View**, select **Actions->Provision Frame Location Information** from the menu bar.

The **Frame Provisioning Information View** displays all the frames in the NE in tabular form with the index being the internal frame number. For each frame, the following location information is displayed.

Field	Description
Frame #	Identifies the logical frame number of the frame in the MG 9000 network element.
Site	Specifies the MG 9000 frame site location. The value for this field is selected from the Site table at the CS 2000 XACore.
Office Frame #	Specifies the external office frame number that is physically labeled on the frame. Range is 0-511.
Floor	Specifies the floor number within the site where the MG 9000 frame is located. Range is 0-99.
Row	Specifies the row within the floor where the MG 9000 frame is located. The range is: A, B, ..., Z, AA, BB, ..., ZZ with the exclusion of I, O, II, and OO.
Frame Position	Specifies the frame position within the row where the MG 9000 frame is located. Range is 0-99.

The **Frame Provisioning Information View** appears as shown in the following figure.

#### Frame location information view

Frame #	Site	Office Frame #	Floor	Row	Frame Position
0	PERF	33	3	WW	3
1	PERF	1	3	J	3
2					
3	PERF	52	33	XX	34

Provision Frame Location for NE: 2

Frame #:

Site:

Office Frame #:

Floor:

Row:

Frame Position:

Apply Refresh Close

- 3 Select the frame from the table and modify the frame location fields on the right side of the view based on the information provided in the previous step.

**Note:** If non-ABI VMGs already exist, any attempt to provision or change a frame's site and office frame number will be blocked if the new site and office frame number conflict with existing VMG names. To continue with the provisioning activity, the VMGs that do not match the desired site and office frame number will have to be deleted and then recreated after the frame is provisioned.

Click **Apply** to submit the changes.

- 4 The procedure is complete.

---

—End—

---

## Decommissioning an MG 9000 frame

### When to use this procedure

Use this procedure when it is necessary to decommission an MG 9000 frame.

### Prerequisites

There are no prerequisites.

### Action

#### Decommissioning an MG 9000 frame

Step	Action
------	--------

##### *At the CS2000 Management Tools*

- |   |   |
|---|---|
| 1 | Using OSSGate, deprovision all lines configured off the frame to be decommissioned. |
|---|---|

##### *At the MG 9000 Manager*

- |   |  |
|---|--|
| 2 | Perform the "Deleting a VMG" (page 196) procedure in this document for all VMGs in the frame to be decommissioned.   |
| 3 | Perform the "De-provisioning a line card" (page 160) procedure in this document for all line cards in the frame.   |
| 4 | Remove all line cards from the frame.  |
| 5 | Deprovision all SIC cards in the frame by performing the following steps (each step may take up to 5 minutes to complete): <ol style="list-style-type: none"> <li>At the <b>Shelf View</b>, double-click on the SIC card in slot 1. The <b>SIC Card View</b> appears.</li> <li>Set the Administrative State of the card to Locked. The Operational State remains Enabled.</li> <li>Set the Configuration state of the card to Deprovision. Click <b>OK</b> in response to the confirmation message for deprovisioning to continue.</li> <li>Repeat steps 5a and 5b for each SIC in the frame.</li> </ol> |
| 6 | Deprovision the inactive ITP cards in the frame by performing the following steps: <ol style="list-style-type: none"> <li>At the <b>Shelf View</b>, double-click on the inactive (Hot_Standby) ITP card. The <b>ITP Card View</b> appears.</li> </ol>  |

- b. Set the Administrative State of the card to Locked. Set the Configuration State to Offline. The Operational State remains Enabled.
- c. Set the Configuration state of the card to Deprovision. Click **OK** in response to the confirmation message for deprovisioning to continue.
- d. Repeat steps 6a and 6b for each ITP card in the frame.

**At the MG 9000 frame**

- 7 Remove the inactive ITP cards from each shelf in the frame.

**At the MG 9000 Manager**

- 8 Deprovision the active ITP cards in the frame by performing the following steps:
  - a. At the **Shelf View**, double-click on the active (Providing\_Service) ITP card. The **ITP Card View** appears.
  - b. Set the Administrative State of the card to Locked. Set the Configuration State to Offline. The Operational State remains Enabled.
  - c. Set the Configuration state of the card to Deprovision. Click **OK** in response to the confirmation message for deprovisioning to continue.
  - d. Repeat steps 8a and 8b for each ITP card in the frame.

**At the MG 9000 frame**

- 9 Remove the active ITP cards from each shelf in the frame.

**At the MG 9000 Manager**

- 10 At the **Subnet View**, double click the **MG 9000** icon. The **Frame View** appears.
- 11 Double click on the IBIP shelf to access the **IBIP Shelf View** for the MG 9000 IBIP shelf with the faulty alarm processor card.
- 12 Identify the alarm processor card with the alarm condition by observing the alarm balloon.
- 13 To lock the card, change the Administrative state by selecting Lock from the administrative state pull-down menu in the state section.
- 14 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.

- 15 At the **Subnet View**, verify that the shelves and frame pertaining to the frame being decommissioned do not appear.

**At the MG 9000 frame**

- 16 Remove the IBIP front cover.

17



**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.

Remove power to the shelves by removing the fuse modules on the IBIP that provides power to the frame and shelves being decommissioned.

- 18 Replace the IBIP front cover.
- 19 The procedure is complete.

---

—End—

---

---

## Decommissioning an MG 9000 shelf

---

### When to use this procedure

Use this procedure when it is necessary to decommission an MG 9000 shelf.

### Prerequisites

There are no prerequisites.

### Action

#### Decommissioning an MG 9000 shelf

---

Step	Action
------	--------

---

*At the CS2000 management tools*

- 1 Using OSSGate, deprovision all lines configured on the shelf to be decommissioned.

*At the MG 9000 Manager*

- 2 Perform "Deleting a VMG" (page 196), beginning at step 2, for all VMGs in the shelf to be decommissioned.
- 3 Perform "De-provisioning a line card" (page 160) for all line cards in the shelf.
- 4 Remove all line cards from the shelf.
- 5 Deprovision the SIC card for the shelf by performing the following steps (each step may take up to five minutes to complete):
  - a. At the **Shelf View**, double-click on the SIC card in slot 1. The **SIC Card View** appears.
  - b. Set the Administrative State of the card to Locked and the Operational State to Offline.
  - c. Set the Configuration state of the card to Deprovision. Click **OK** in response to the confirmation message for deprovisioning to continue.
- 6 Deprovision the inactive ITP cards in the shelf by performing the following steps:
  - a. At the **Shelf View**, double-click on the inactive (Hot\_Standby) ITP card. The **ITP Card View** appears.

- b. Set the Administrative State of the card to Locked. Set the Configuration State to Offline. The Operational State remains Enabled.
- c. Set the Configuration state of the card to Deprovision. Click **OK** in response to the confirmation message for deprovisioning to continue.
- d. Repeat steps 6a and 6b for each ITP card in the shelf.

**At the MG 9000 frame**

- 7** Unseat and remove the inactive ITP card.

Ensure you physically unseat the cards in the shelf when directed or the proceeding steps will fail.

**At the MG 9000 Manager**

- 8** Deprovision the active ITP card in the shelf by performing the following steps:
- a. At the **Shelf View**, double-click on the active (Providing\_Service) ITP card. The **ITP Card View** appears.
  - b. Set the Administrative State of the card to Locked. Set the Configuration State to Offline. The Operational State remains Enabled.
  - c. Set the Configuration state of the card to Deprovision. Click **OK** in response to the confirmation message for deprovisioning to continue.

**At the MG 9000 shelf**

- 9** Unseat and remove the active ITP card.
- 10** Remove the IBIP front cover.
- 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.

Remove power by removing the fuse modules on the IBIP that provides power to the shelf being decommissioned. Ensure the shelf does not appear in the GUI.

## 74 Configuration management strategy

---

- 12 Replace the IBIP front cover.
- 13 The procedure is complete.

---

**—End—**

---

---

## Provisioning cards and services

---

Line/service cards in an MG 9000 shelf can be provisioned to support SLoA and PLoA services. The following tasks describe how to configure specific cards for service.

- "Provisioning a World line card" (page 77)
- "Provisioning a Global line card" (page 102)
- "Provisioning an ADSL card" (page 122)
- "Provisioning an SAA line circuit" (page 137)
- "Provisioning a DS1 card" (page 142)
- "Provisioning an ITX card" (page 159)
- "De-provisioning a line card" (page 160)

The following services and functions can be provisioned after the required hardware is installed and configured.

- "Provisioning private lines services" (page 162)
- "Provisioning switched lines services" (page 178)
- "Viewing and modifying DS1 IMA group and links" (page 224)
- "Provisioning and maintenance of OC3 APS" (page 230)
- "Viewing Gigabit Ethernet ports and links provisioning information" (page 238)
- "Provisioning SIC inputs and outputs" (page 252)
- "Provisioning IBIP inputs and outputs" (page 257)
- "Using the Bandwidth Manager" (page 263)
- "Using the Bandwidth Management Planning Tool" (page 273)

The following activity can be performed to audit provisioning data on the MG 9000:

- "Performing an MG 9000 data audit" (page 281)

The following activities can be performed when it becomes necessary to address performance issues or change the ESA data download properties:

- "Managing performance thresholds" (page 299)
- "Managing overload thresholds" (page 302)
- "Changing MG 9000 Manager ESA data download properties" (page 305)

## Provisioning a World line card

### When to use this procedure

Use this procedure to provision a POTS 32 World line card and its corresponding line circuits. The POTS 32-line card uses the single in-line package version of the World Line Card (WLC) and serves 32 subscriber loops. Provision a POTS line card using the following procedure.

**Note:** The WLC line card only supports potsLoopStart line service type, therefore when replacing a Global line card (GLC) with a WLC, any EBS/P-phone or postGroundStart lines on the GLC must be decommissioned prior attempting the card replacement. A failure to do so will result in a loss of service on these lines. Once the GLC card is replaced with a WLC, all line circuits on the card will assume the line service type of potsLoopStart.

Included are the following procedures:

- Provisioning a WLC
- Provisioning a line circuit on a WLC
- Viewing all WLC circuits
- Provisioning a line template table

### Prerequisites

A WLC card must have been installed in the slot to be provisioned using correct ESD precautions.

### Action

#### Provisioning a World line card

Step	Action
------	--------

##### *At the MG 9000 Manager*

- |   |   |
|---|---|
| 1 | At the <b>Subnet View</b> , double click on the <b>MG 9000</b> that is to have the WLC provisioned. The <b>Frame View</b> appears.  |
| 2 | At the <b>Frame View</b> , double click on the shelf in which the WLC resides. The <b>Shelf View</b> appears.   |
| 3 | At the <b>Shelf View</b> , double click on the slot in which the WLC resides. The <b>WLC Card screen</b> appears. Since the WLC card is already installed, autodiscovery datafills the data about the card. Any specific parameter that must be modified, can be performed as outlined in the next step, using the information in the WLC Card View data table. |

**Note:** When provisioning a World line card, click **Refresh** at the bottom of the **WLC Card View** to synchronize the data between the MG 9000 and the MG 9000 Manager.

4



**CAUTION**

**Affects subscriber service**

When commands are entered at the GUI that may affect service on the card, an "Are you sure" dialog box is displayed to allow the user to cancel or approve of the command.

Enter data in the fields that appear in the Line Circuit Management screen from the **WLC Card View**.

## WLC Card View

Refer to the following table for a list of the data fields and the possible values. Only the Administrative State and Configuration State may be changed. The following figure shows the **WLC Card View**.

## WLC Card View data fields

Box	Field	Explanation
Card Attributes	CLEI Code	Common Language Equipment Identifier (CLEI) indicates an inventory number assigned to each physical component.

Box	Field	Explanation
	Card Description	Indicates the manufacturer's name for the physical component.
	Hardware Version	Indicates the vendor-specific hardware revision for the physical component.
	Firmware Version	Indicates the vendor-specific firmware revision for the physical component.
	Software Version	Indicates the vendor-specific software revision for the physical component.
	Serial Number	Indicates the serial number for the physical component.
	Manufacturer	Indicates the name of the manufacturer for the physical component.
	PEC Code	Indicates the model name associated with the physical component.
Status	Availability Status	<p>Provides a more refined/detailed status of the card:</p> <ul style="list-style-type: none"> <li>• in test - The card is undergoing a test procedure which could cause maintenance requests to be rejected.</li> <li>• failed - The card has a fault that prevents it from providing service. The operational state is disabled.</li> <li>• off line - The card requires a routing operation to be performed to place it online and make it available for use.</li> <li>• dependency - The card cannot operate because some other resource on which it depends is unavailable.</li> <li>• degraded - The service available from the card is degraded in some respect, such as speed or operating capacity.</li> <li>• not installed - The card is not present or is only partially installed.</li> </ul>
	Usage Status	<p>Indicates whether or not the card is actively in use at a specific instance.</p> <ul style="list-style-type: none"> <li>• active - If the card is Unlocked/Enabled.</li> <li>• idle - If the card is Unlocked/Disabled or in the Locked state.</li> </ul>

Box	Field	Explanation
	Standby Status	Indicates whether the card is active or standby. <ul style="list-style-type: none"> <li>hot standby - The card is not providing service.</li> <li>providing service - The card is providing service.</li> </ul>
	Alarm Status	Indicates the severity of an alarm on the card. <ul style="list-style-type: none"> <li>none - No alarms have been detected on the card.</li> <li>critical - A critical alarm indicating a fault has been detected on the card.</li> <li>major - A major alarm indicating a fault has been detected on the card.</li> <li>minor - A minor alarm indicating a fault has been detected on the card.</li> <li>alarm outstanding - One or more alarms have been detected on the card.</li> </ul>
	Procedural Status	Indicates a card which is initializing after a restart and terminating before a restart. <ul style="list-style-type: none"> <li>initialization Required - The resource requires initialization to be invoked by the manager before it can perform its normal functions, and this procedure has not been initiated.</li> <li>not Initialized - The resource requires initialization before it can perform its normal functions, and this procedure has not been initiated.</li> <li>initializing - The resource requires initialization before it can perform its normal functions, and this procedure has been initiated but is not yet complete</li> <li>reporting - The resource has completed some processing operation and is notifying the results of the operation.</li> <li>terminating - The resource is in a termination phase.</li> </ul>
	Control Status	Not supported.

Box	Field	Explanation
State	Administrative State	<p>Indicates whether the card can be used or is prohibited from use.</p> <ul style="list-style-type: none"> <li>locked - The card is administratively prohibited from performing service for its users.</li> <li>force locked - The card is administratively prohibited from performing service for its users. The lock will be applied even if there are active calls on the card. Those calls will be stopped when the card is locked.</li> <li>unlocked - The card is administratively permitted to perform service for its users.</li> <li>force unlocked - The card is administratively permitted to perform service for its users. The unlock will be applied no matter what state the card is in.</li> </ul> <p><b>Note:</b> 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?"</p> <p>Select "OK" to submit the unlock request to the gateway or "Cancel".</p> <p><b>Note:</b> Changing the Administration State does not require selection of the Apply button.</p>
	Configuration State	<p>Indicates whether or not the card is actively in use at a specific instance.</p> <ul style="list-style-type: none"> <li>online - The card is administratively allowed to send messages, such as alarm messages, to the MG 9000 Manager.</li> <li>offline - The card is administratively prevented from sending messages, such as alarm messages, to the MG 9000 Manager.</li> <li>deprovisioned - The card is administratively removed and must be physically removed from the shelf to remove all associated data.</li> </ul> <p><b>Note 1:</b> When an WLC card goes from the Deprovisioned state to the Offline state, the associated terminations are configured in the MG 9000 Manager, the MG 9000, and the SESM.</p>

Box	Field	Explanation
	Operational State	<p><b>Note 2:</b> The Administrative State must be Locked prior to changing the Configuration State.</p> <p><b>Note 3:</b> Changing the Configuration State does not require selection of the Apply button.</p> <p>Indicates the operability of a card.</p> <ul style="list-style-type: none"> <li>disabled - The card is inoperable and unable to provide service.</li> <li>enabled - The card is partially or fully operable and available for use</li> </ul>

5 This procedure is complete.

---

—End—

---

### Provisioning a line circuit on a WLC

Step	Action
------	--------

*At the MG 9000 Manager*

- At the **Subnet View**, double click on the **MG 9000** that is to have the WLC line circuits provisioned. The **Frame View** appears.
- At the **Frame View**, double click on the shelf in which the WLC resides. The **Shelf View** appears.
- At the **Shelf View**, double click on the slot in which the WLC resides. The **WLC Card screen** appears.
- 



**CAUTION**

**Affects subscriber service**

When commands are entered at the GUI that may affect service on the card, an "Are you sure" dialog box is displayed to allow the user to cancel or approve of the command.

At the **WLC Card screen**, double click on an **individual circuit**. The window for **Line Circuit** appears.

- At the **Line Circuit screen**, select the **Locked** option for the Administrative Status in the **Circuit Status** box to change data.

When the circuit is Locked, the fields in the **Circuit Provisioning** box become available for modification.

- 6 Enter data in the fields that appear in the **Circuit Provisioning** box from the **Line Circuit** window. Refer to the following table for a list of the data fields and the possible values.

**Note:** When the MG 9000 Manager is having trouble retrieving circuit data from the MG 9000, the following conditions may exist when attempting to provision circuits. Each of these panels work independently of each other and any data that is available will be displayed.

- **Circuit Provisioning panel**, the fields in this panel will be greyed out and the **Apply** button is disabled. When this condition exists, move the cursor over the **Apply** button and a message appears informing the user that circuit provisioning is disabled because of the communication failure.
- **State Provisioning panel**, the fields indicate that states are unavailable.
- **Circuit Status panel**, though the Administrative Status can be modified, it will most likely fail. In addition, the Operational Status indicates the value is unavailable.
- **Software Load Status panel**, indicates the load state and name are unavailable.

#### WLC Circuit View data box fields

Box	Field	Explanation
Circuit Provisioning	Service Type	The line service type for WLC = POTS loop start.
	Min Flash Duration	The minimum flash time in milliseconds. Default value is 31 (31 x 8ms = 248ms)
	Min Inter Digit Time	The minimum time allowed between digits in milliseconds. Default value is 63 (63 x 2ms = 126ms)
	Template	The B11 template to use for the line circuit.  <b>Note:</b> The template is defined at the card level and configured at the circuit level.
	Min Disc Time	The minimum time, in milliseconds, to be considered on hook with flash enabled. Default value is 150 (150 x 8ms = 1200ms)
	Termination DN	The Termination Directory Number (DN) is a numeric string associated with the line circuit. If no DN is associated with the circuit, "None" appears in the Termination DN field.

Box	Field	Explanation
State Provisioning	Fault State	Indicates if the line is in a fault condition. <ul style="list-style-type: none"> <li>notInFault - No faults exist on the circuit.</li> <li>inFault - A fault has been detected on the circuit and a line fault notification is sent to the MG 9000 Manager.</li> <li>unknown - have not communicated with the card yet.</li> </ul>
	Protection State	Indicates if the line circuit is currently in over-voltage condition. <ul style="list-style-type: none"> <li>notInProtection - no foreign voltage has been detected.</li> <li>inProtection - foreign voltage has been detected and the cut-off relay operated.</li> <li>unknown - have not communicated with the card yet.</li> </ul>
	Babble State	Indicates if the line circuit is in a babbling state. <ul style="list-style-type: none"> <li>notInBabble - a babbling condition has not been detected on the circuit.</li> <li>inBabble - a babbling condition has been detected and the circuit is disabled from call processing.</li> <li>unknown - have not communicated with the card yet.</li> </ul>
	Cut Off Relay	Indicates if Cut Off Relay is operated. <ul style="list-style-type: none"> <li>on - the relay is on</li> <li>off - the relay is off</li> </ul>
Circuit Status	Administrative Status	Indicates whether the circuit can be used or is prohibited from use. <ul style="list-style-type: none"> <li>locked - The circuit is administratively prohibited from performing service for its users. The lock will be applied even if there is an active call on the circuit. The call will be stopped when the circuit is locked.</li> <li>unlocked - The circuit is administratively permitted to perform service for its users.</li> </ul> <p><b>Note:</b> Changing the Administrative State does not require selection of the Apply button.</p>

Box	Field	Explanation
	Operational Status	Indicates the operability of a circuit. <ul style="list-style-type: none"> <li>disabled - The circuit is inoperable and unable to provide service.</li> <li>enabled - The circuit is partially or fully operable and available for use</li> </ul>
	Faulty	Indicates whether or not a circuit is faulty <ul style="list-style-type: none"> <li>"Yes" indicates that the circuit is faulty</li> <li>"No" indicates that the circuit is not faulty</li> </ul> <p><b>Note:</b> Changing the Faulty status does not require selection of the Apply button.</p>

The following figure shows the WLC Line Circuit View.

#### WLC Line Circuit View

- 7 Select the **Apply** button at the bottom of the **Line Circuit** window to update the circuit with the data entered.
- 8 This procedure is complete.

—End—

### Viewing all WLC line circuits

**Step Action**

**At the MG 9000 Manager**

- 1 At the **WLC Card screen**, from the menu bar select **Services->Circuits Listing**.
- 2 The window for **Circuits Listing** appears. The **Circuits Listing View** is a table that shows a complete list of all ports contained within the card. Double clicking on any port row in the table opens up the corresponding **Port View** for that circuit.

**Note 1:** The values presented in the table cannot be edited. However, from the **Circuit Listing View** the technician can operate on multiple ports at the same time or apply certain commands like setting the Admin state.

**Note 2:** The alarm, configuration, and Admin state of the ports in the table get updated dynamically to reflect the state of the circuits on the MG 9000. The line service type and operational state do not get updated dynamically. Click on the **Refresh** button to see the current values.

### WLC Circuits Listing View

Num	Port State	Admin State	Op State	Type	Template
Voice-0	Voice-0	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-1	Voice-1	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-2	Voice-2	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-3	Voice-3	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-4	Voice-4	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-5	Voice-5	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-6	Voice-6	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-7	Voice-7	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-8	Voice-8	Unlocked	Enabled	potsLoopStart	(1) DEFAULT

Set Values

Admin State  As Is  Lock  Unlock

Apply Refresh Close

The following table lists the fields in the **Circuits Listing View**.

#### Circuits Listing View fields

Field	Entry	Explanation
Num	0-31	Port number.
Port State	None	Graphical representation of the port along with its state.
Admin State	Locked, Unlocked, Testing, ERROR	Administrative state of the port. This is updated dynamically.
Op State	Enabled, Disabled, Testing, Dormant, Not Present, Lower Layer Down, ERROR	Operational state of the port. Does not get updated dynamically.
Type	potsLoopStart, coin, pPhone, potsGroundStart, No Service	Specifies the line service type for the port. Does not get updated dynamically.
Template	N/A	Identifies the template selected for the circuit.
SetValues	None	This is a logical grouping of all the values that can be set for multiple selections of the ports in the table.  The technician must select a value in any of these subfields and after selecting the ports for which the operation is to be performed, click on Apply.
Admin State	As Is, Locked, Unlocked	Select any of the values to perform the respective operation on the selected port(s). The action is only performed after clicking on Apply.
Apply	None	Performs the specified action on the selected port(s).
Refresh	None	Causes the view to refresh itself.
Close or from the Menu->Close	None	Closes the view.

**3** This procedure is complete.

—End—

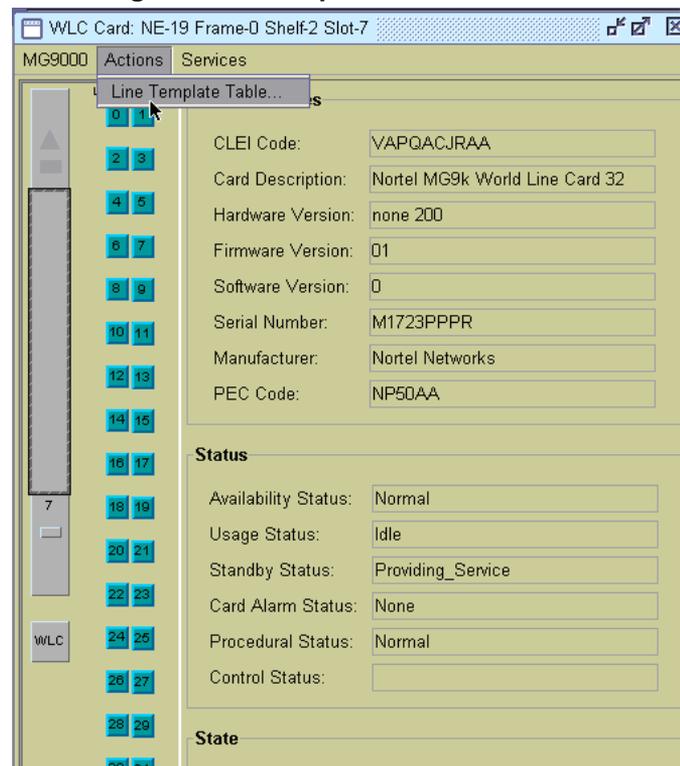
## Provisioning a line template table

### Step Action

#### At the MG 9000 Manager

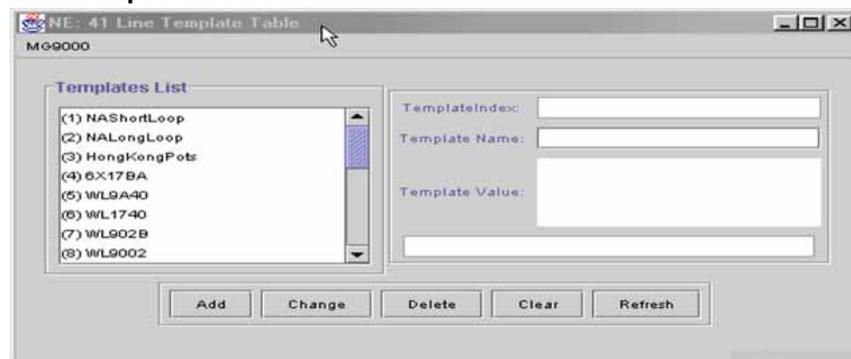
- 1 At the **Subnet View**, double click on the **MG 9000** that is to have the WLC line circuits provisioned. The **Frame View** appears.
- 2 At the **Frame View**, double click on the shelf in which the WLC resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the slot in which the WLC resides. The **WLC Card screen** appears.
- 4 From the **WLC Card View**, access the **Actions->Line Template Table....** menu item as shown in the following figure.

#### Accessing the Line Template Table



A **Line Template Table** window appears that contains a listing of default templates available for the circuits on the card. The **Line Template** is shown in the following figure.

#### Line Template Table View



Refer to the following table for a list of the data fields and the possible values. The supported templates and their characteristics are provided at the end of this procedure.

**Note:** The default template for North America is the NAShortLoop50ma for loop lengths under 30,000 feet, or NALongLoop50ma for loop lengths over 30,000 feet.

#### Line Template Table data fields

Fields	Explanation
Templates List	The name and numerical index associated with a Line Template.
Template Index	A numerical value from 1 to 256 indicating the index of the template in the Templates List. This value is autonomously generated when adding a template.
Template Name	The name associated with the template. Maximum number of characters specified is 20.
Te00mplate Value	A maximum of 37 bytes indicating the actual contents of the template.

#### *At the Line Template Table screen*

- 5 Determine the next action from the following Management options in the Line Template Table screen.

If the next step is to	Do
add a line template	step 6
change a line template	step 7
delete a line template	step 8
clear information for a line template	step 9
refresh a line template	step 10

- 6 To add a line template, perform the following steps:
- Enter a Template Name.
  - Enter the Template Value.
  - Select the **Add** option at the bottom of **Line Template Table** screen.
  - This procedure is complete.
- 7 To change a line template, perform the following steps:
- Highlight the template requiring change in the Templates List by clicking on the **template**.
  - Change the Template Name and/or the Template Value.
  - Select the **Change** option at the bottom of Line Template Table screen.
 

**Note:** Default templates that are provided during auto discovery may not be changed.
  - This procedure is complete.
- 8 To delete a line template, perform the following steps:
- Highlight the template requiring change in the Templates List by clicking on the template.
  - Select the **Delete** option at the bottom of **Line Template Table** screen.
 

**Note:** Default templates that are provided during auto discovery may not be deleted.
  - This procedure is complete.
- 9 To clear the line template being entered, perform the following steps:

- a. Select the **Clear** option at the bottom of **Line Template Table** screen.
  - b. This procedure is complete.
- 10** To refresh a line template, click on the **Refresh** button.

---

—End—

---

### Line template tables and characteristics

The following tables list the characteristics for each of the supported B11 POTS templates used in the World line card circuits and ADSL card voice circuits.

#### NAShortLoop50ma template characteristics (for loops less than 30 kft)

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	50 mA
Equalization loss	no

#### NAShortLoop40ma template characteristics (for loops less than 30 kft)

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law

Characteristic	Value
Current limit	40 mA
Equalization loss	no

**NAShortLoop30ma template characteristics (for loops less than 30 kft)**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	30 mA
Equalization loss	no

**NAShortLoop23ma template characteristics (for loops less than 30 kft)**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	23 mA
Equalization loss	no

**NALongLoop50ma template characteristics (for loops greater than 30 kft)**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	18 mA
PCM encoding	u-law

Characteristic	Value
Current limit	50 mA
Equalization loss	no

**NALongLoop40ma template characteristics (for loops greater than 30 kft)**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	18 mA
PCM encoding	u-law
Current limit	40 mA
Equalization loss	no

**NALongLoop30ma template characteristics (for loops greater than 30 kft)**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	18 mA
PCM encoding	u-law
Current limit	30 mA
Equalization loss	no

**NALongLoop23ma template characteristics (for loops greater than 30 kft)**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	18 mA
PCM encoding	u-law

Characteristic	Value
Current limit	23 mA
Equalization loss	no

**NP40AA template characteristics**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	50 mA
Equalization loss	yes

**6X17BA template characteristics**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
Balance impedance	NL: 88.9 ohms    (711.1 ohms + 63.3 nF) LD: 94.3 ohms    (1555.7 ohms + 5.6 nF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	50 mA
Equalization loss	no

**WLUKPSTN (short-line) template characteristics**

Characteristic	Value
Input impedance	298 ohms    (1055 ohms + 2.16 uF)
Balance impedance	259 ohms    (676.8 ohms + 400 nF) (194.3 ohms + 246 nF)
A-D gain at 1004Hz	-1 dB
D-A gain at 1004Hz	-6 dB
Off-hook supervision threshold	12 mA

Characteristic	Value
PCM encoding	A-law
Current limit	40 mA
Equalization loss	yes

**WLUKPTN1 (long-line heavy gauge) template characteristics**

Characteristic	Value
Input impedance	298 ohms    (1055 ohms + 2.16 uF)
Balance impedance	164 ohms    (1227 ohms + 350 nF) (162 ohms + 363 nF)
A-D gain at 1004Hz	-1 dB
D-A gain at 1004Hz	-6 dB
Off-hook supervision threshold	12 mA
PCM encoding	A-law
Current limit	40 mA
Equalization loss	yes

**WLUKPTN2 (long-line small gauge) template characteristics**

Characteristic	Value
Input impedance	298 ohms    (1055 ohms + 2.16 uF)
Balance impedance	270 ohms    (1434 ohms + 265 nF)(263 ohms + 358 nF)
A-D gain at 1004Hz	-1 dB
D-A gain at 1004Hz	-6 dB
Off-hook supervision threshold	12 mA
PCM encoding	A-law
Current limit	40 mA
Equalization loss	yes

**WL902B (9 and 2 balanced) template characteristics**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
Balance impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB

Characteristic	Value
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	50 mA
Equalization loss	no

**WL902B (9 and 2 ground) template characteristics**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
Balance impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	40 mA
Equalization loss	no

**WL93AA template characteristics**

Characteristic	Value
Input impedance	600 ohms    (0 ohms + 2.16 uF)
Balance impedance	85.7 ohms    (514.3 ohms + 68.1nF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	A-law
Current limit	50 mA
Equalization loss	no

**WL93CA template characteristics**

Characteristic	Value
Input impedance	200 ohms    (680 ohms + 100 nF)
Balance impedance	160 ohms    (780 ohms + 115 nF)
A-D gain at 1004Hz	0 dB

Characteristic	Value
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	A-law
Current limit	50 mA
Equalization loss	no

**WLAUBX template characteristics**

Characteristic	Value
Input impedance	220 ohms    (820 ohms + 120 nF)
Balance impedance	220 ohms    (820 ohms + 120 nF)
A-D gain at 1004 Hz	0 dB
D-A gain at 1004 Hz	-7 dB
On/Off hook threshold	12 mA
PCM encoding	A-Law
Current limiting	50 mA
Equalization loss	no
Loop resistance	2 k ohms
Battery voltage	44.5 - 53 V

**WLCHAX template characteristics**

Characteristic	Value
Input impedance	220 ohms    (820 ohms + 115 nF)
Balance impedance	220 ohms    (820 ohms + 115 nF)
A-D gain at 1004 Hz	0 dB
D-A gain at 1004 Hz	-6.5 dB
On/Off hook threshold	12 mA
PCM encoding	A-Law
Current limiting	55 mA
Equalization loss	no

Characteristic	Value
Loop resistance	600 - 2200 ohms
Battery voltage	43 - 57 V

**WLNAL (long-line) template characteristics**

Characteristic	Value
Input impedance	150 ohms    (830 ohms + 72 nF)
Balance impedance	150 ohms    (830 ohms + 72 nF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	-7 dB
On/Off hook threshold	12 mA
PCM encoding	A-Law
Current limiting	55 mA
Equalization loss	no
Loop resistance	2 k ohms
Battery voltage	44.5 - 53 V

**WLNALAS (short-line) template characteristics**

Characteristic	Value
Input impedance	150 ohms    (830 ohms + 72 nF)
Balance impedance	0 ohms    (600 ohms + 0 F)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	-7 dB
On/Off hook threshold	12 mA
PCM encoding	A-Law
Current limiting	55 mA
Equalization loss	no
Loop resistance	2 k ohms
Battery voltage	44.5 - 53 V

**WLNLBL (long-line) template characteristics**

Characteristic	Value
Input impedance	150 ohms    (830 ohms + 72 nF)
Balance impedance	150 ohms    (830 ohms + 72 nF)
A-D gain at 1004Hz	0 dB

Characteristic	Value
D-A gain at 1004Hz	-7 dB
On/Off hook threshold	12 mA
PCM encoding	A-Law
Current limiting	55 mA
Equalization loss	no

**WLNLBS (short-line) template characteristics**

Characteristic	Value
Input impedance	150 ohms    (830 ohms + 72 nF)
Balance impedance	0 ohms    (600 ohms + 0 F)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	-7 dB
On/Off hook threshold	12 mA
PCM encoding	A-Law
Current limiting	55 mA
Equalization loss	no

**WL9A40 (9 and 2) template characteristics**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
Balance impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	40 mA
Equalization loss	no

**WL1740 template characteristics**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
Balance impedance	88.9 ohms    (711.1 ohms + 63.3 nF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB

Characteristic	Value
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	40 mA
Equalization loss	no

**WL9002 (9 and 2 balanced) template characteristics**

Characteristic	Value
Input impedance	900 ohms    (0 ohms + 2.16 uF)
Balance impedance	900 ohms    (0 ohms + 2.16 uF)
A-D gain at 1004Hz	0 dB
D-A gain at 1004Hz	0 dB
Off-hook supervision threshold	12 mA
PCM encoding	u-law
Current limit	50 mA
Equalization loss	no

## Provisioning a Global line card

---

### When to use this procedure

Use this procedure to provision a Global line card (GLC) and its corresponding line circuits. This procedure applies to GLC 32 and GLC 12 cards. The GLC 32-line card serves 32 subscriber loops. The GLC 12-line card serves 12 subscriber loops and supports coin services. Coefficients are used to control circuit characteristics and may be assigned on an individual circuit basis similar to how templates are used for World Line Card (WLC) circuits. The circuit must be locked to change the coefficient.

**Note 1:** If you replace an SAA 12 card with a GLC 12 card, the SAA card does not need to be deprovisioned before installing the new GLC card. When a card is replaced, the Card View will be updated automatically with the GLC label; the card description and PEC will change to that of the GLC card. If either the Card or Circuit View is open, the view closes. The information for the updated card appears the next time you open the view.

**Note 2:** The WLC line card only supports potsLoopStart line service type, therefore when replacing a GLC with a WLC, any EBS/P-phone or postGroundStart lines on the GLC must be decommissioned prior attempting the card replacement. A failure to do so will result in a loss of service on these lines. Once the GLC card is replaced with a WLC, all line circuits on the card will assume the line service type of potsLoopStart.

Included are the following procedures:

- Provisioning a GLC
- Provisioning a line circuit on a GLC
- Viewing all GLC circuits
- Provisioning coefficients
- Checking the FPGA configuration load on NTNY53BA and NTNY53CA cards
- Bulk provisioning line services

### Prerequisites

A GLC card must be installed in the slot to be provisioned. Use electrostatic discharge (ESD) precautions when installing the card.

## Action

### Provisioning a Global line card

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 At the **Subnet View**, double click on the **MG 9000** that is to have the GLC provisioned. The **Frame View** appears.
- 2 At the **Frame View**, double click on the shelf in which the GLC resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the slot in which the GLC resides. The **GLC Card View** appears. Since the GLC card is already installed, autodiscovery datafills the data about the card. Any specific parameter that must be modified can be performed as outlined in the next step, using the information in the **GLC Card View** data table.

**Note:** When provisioning a Global line card, click **Refresh** at the bottom of the **GLC Card View** to synchronize the data between the MG 9000 and the MG 9000 Manager.

4



#### CAUTION

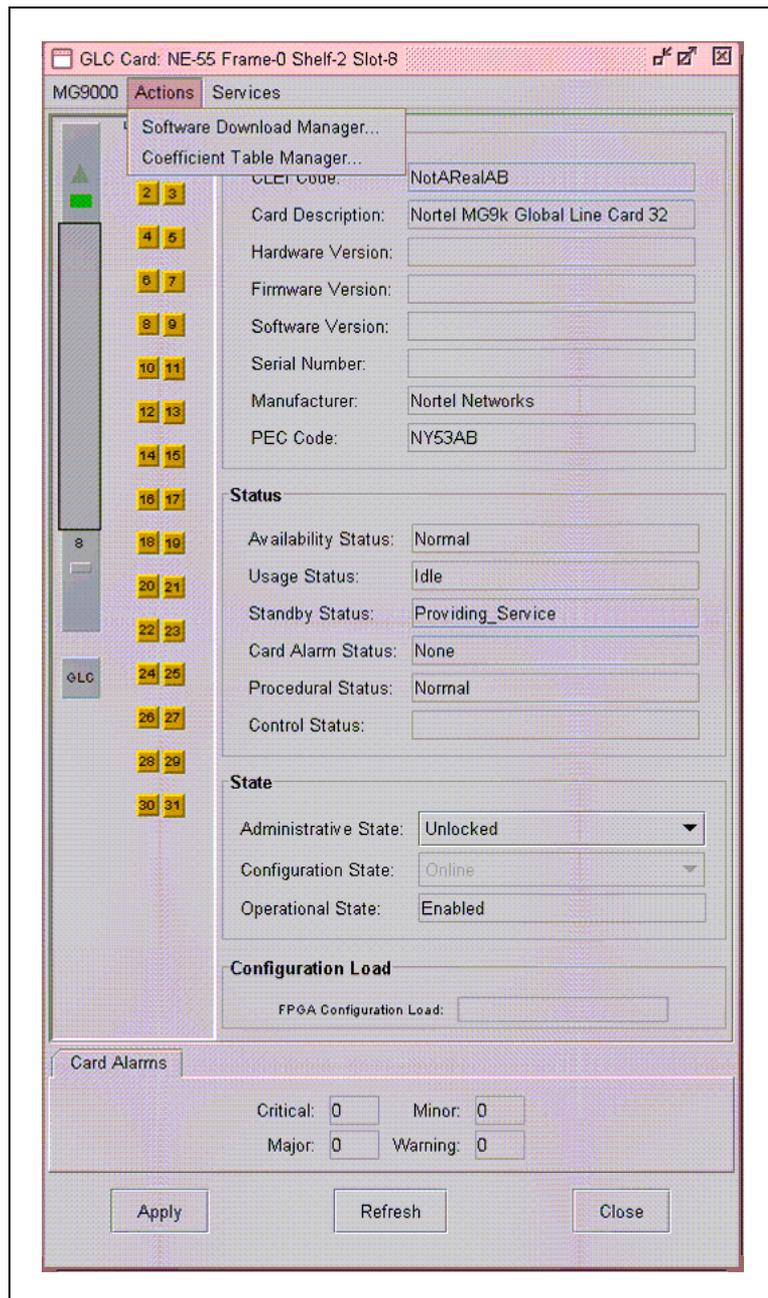
##### Affects subscriber service

When commands are entered at the GUI that may affect service on the card, an "Are you sure" dialog box is displayed to allow the user to cancel or approve of the command.

Enter data in the fields that appear in the Line Circuit Management screen from the GLC Card View. The following figures shows the GLC 32 and GLC 12 Card Views.

**Note:** If it is necessary to bulk provision all circuits on the new GLC card, perform procedure ["Bulk provisioning line services" \(page 119\)](#) while the GLC is offline and deprovisioned.

**GLC 32 Card View**



The following figure shows the GLC12 Card View:

**GLC 12 Card View**

GLC Card: NE-9 Frame-0 Shelf-2 Slot-8

MG9000 Actions Services

Line Circuits

1 2 3 4 5 6 7 8 9 10 11 12

13

GLC

**Card Attributes**

CLEI Code: NotARealAB

Card Description: Nortel MG9k Global Li

Hardware Version: none 200

Firmware Version: 01 F

Software Version: 0

Serial Number: MG4428V10

Manufacturer: Nortel Networks

PEC Code: NY53CA

**Status**

Availability Status: Normal

Usage Status: Idle

Standby Status: Providing\_Service

Card Alarm Status: None

Procedural Status: Normal

Control Status:

Refer to the following table for a list of the data fields and the possible values. Only the Administrative State and Configuration State may be changed.

**GLC Card View data fields**

Box	Field	Explanation
Card Attributes	CLEI Code	Common Language Equipment Identifier (CLEI) indicates an inventory number assigned to each physical component.
	Card Description	Indicates the manufacturer's name for the physical component.
	Hardware Version	Indicates the vendor-specific hardware revision for the physical component.
	Firmware Version	Indicates the vendor-specific firmware revision for the physical component.
	Software Version	Indicates the vendor-specific software revision for the physical component.
	Serial Number	Indicates the serial number for the physical component.
	Manufacturer	Indicates the name of the manufacturer for the physical component.

Box	Field	Explanation
	PEC Code	Indicates the model name associated with the physical component.
Status	Availability Status	Provides a more refined/detailed status of the card: <ul style="list-style-type: none"> <li>• in test - The card is undergoing a test procedure which could cause maintenance requests to be rejected.</li> <li>• failed - The card has a fault that prevents it from providing service. The operational state is disabled.</li> <li>• off line - The card requires a routing operation to be performed to place it online and make it available for use.</li> <li>• dependency - The card cannot operate because some other resource on which it depends is unavailable.</li> <li>• degraded - The service available from the card is degraded in some respect, such as speed or operating capacity.</li> <li>• not installed - The card is not present or is only partially installed.</li> </ul>
	Usage Status	Indicates whether or not the card is actively in use at a specific instance. <ul style="list-style-type: none"> <li>• active - If the card is Unlocked/Enabled</li> <li>• idle - If the card is Unlocked/Disabled or in the Locked state.</li> </ul>
	Standby Status	Indicates whether the card is active or standby. <ul style="list-style-type: none"> <li>• hot standby - The card is not providing service, but is in synchronism operation with another resource that is to be backed-up.</li> <li>• providing service - The card is providing service and is backing up another card</li> </ul>
	Alarm Status	Indicates the severity of an alarm on the card. <ul style="list-style-type: none"> <li>• none - No alarms have been detected on the card.</li> <li>• critical - A critical alarm indicating a fault has been detected on the card and has not been corrected.</li> <li>• major - A major alarm indicating a fault has been detected on the card and has not been corrected.</li> <li>• minor - A minor alarm indicating a fault has been detected on the card and has not been corrected.</li> <li>• alarm outstanding - One or more alarms have been detected on the card.</li> </ul>

Box	Field	Explanation
	Procedural Status	<p>Indicates a card which is initializing after a restart and terminating before a restart.</p> <ul style="list-style-type: none"> <li>initialization Required - The resource requires initialization to be invoked by the manager before it can perform its normal functions, and this procedure has not been initiated.</li> <li>not Initialized - The resource requires initialization before it can perform its normal functions, and this procedure has not been initiated.</li> <li>initializing - The resource requires initialization before it can perform its normal functions, and this procedure has been initiated but is not yet complete.</li> <li>reporting - The resource has completed some processing operation and is notifying the results of the operation.</li> <li>terminating - The resource is in a termination phase.</li> </ul>
	Control Status	Not supported
State	Administrative State	<p>Indicates whether the card can be used or is prohibited from use.</p> <ul style="list-style-type: none"> <li>locked - The card is administratively prohibited from performing service for its users.</li> <li>force locked - The card is administratively prohibited from performing service for its users. The lock will be applied even if there are active calls on the card. Those calls will be stopped when the card is locked.</li> <li>unlocked - The card is administratively permitted to perform service for its users.</li> <li>force unlocked - The card is administratively permitted to perform service for its users. The unlock will be applied no matter what state the card is in.</li> </ul> <p><b>Note:</b> 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?"</p> <p>Select "<b>OK</b>" to submit the unlock request to the gateway or "<b>Cancel</b>".</p> <p><b>Note:</b> Changing the Administration State does not require selection of the <b>Apply</b> button.</p>

Box	Field	Explanation
	Configuration State	<p>Indicates whether or not the card is actively in use at a specific instance.</p> <ul style="list-style-type: none"> <li>• online - The card is administratively allowed to send messages, such as alarm messages, to the MG 9000 Manager.</li> <li>• offline - The card is administratively prevented from sending messages, such as alarm messages, to the MG 9000 Manager</li> <li>• deprovisioned - The card is administratively removed and must be physically removed from the shelf to remove all associated data.</li> </ul> <p><b>Note 1:</b> When a GLC card goes from the Deprovisioned state to the Offline state, the associated terminations are configured in the MG 9000 Manager, the MG 9000, and the SESM.</p> <p><b>Note 2:</b> The Administrative State must be Locked prior to changing the Configuration State.</p> <p><b>Note 3:</b> Changing the Configuration State does not require selection of the <b>Apply</b> button.</p>
	Operational State	<p>Indicates the operability of a card.</p> <ul style="list-style-type: none"> <li>• disabled - The card is inoperable and unable to provide service.</li> <li>• enabled - The card is partially or fully operable and available for use.</li> </ul>
Configurati on load	FPGA Configuration Load	Indicates the FPGA load currently running on this card. Applicable only to NTNY53BA and NTNY53CA cards.

5 This procedure is complete.

---

—End—

---

## Provisioning a line circuit on a GLC

Step	Action
------	--------

*At the MG 9000 Manager*

- |   |  |
|---|--|
| 1 | At the <b>Subnet View</b> , double click on the <b>MG 9000</b> that is to have the GLC line circuits provisioned. The <b>Frame View</b> appears. |
| 2 | At the <b>Frame View</b> , double click on the shelf in which the GLC resides. The <b>Shelf View</b> appears.                                    |

3 At the **Shelf View**, double click on the slot in which the GLC resides. The **GLC Card View** appears.

4 At the **GLC Card View**, double click on an individual circuit. The window for Line Circuit appears.

**Note:** When commands are entered at the GUI that may affect service on the circuit, an "Are you sure" dialog box is displayed to allow the user to cancel or approve of the command.

5 At the **Line Circuit** screen, select the Locked option for the Administrative Status in the Circuit Status box to change data.

When the circuit is Locked, the fields in the Circuit Provisioning box become available for modification.

6 Enter data in the fields that appear in the Circuit Provisioning box from the **Line Circuit** window. Refer to the following table for a list of the data fields and the possible values.

**Note:** When the MG 9000 Manager is having trouble retrieving circuit data from the MG 9000, the following conditions may exist when attempting to provision circuits. Each of these panels work independently of each other and any data that is available will be displayed.

- Circuit Provisioning panel, the fields in this panel will be greyed out and the **Apply** button is disabled. When this condition exists, move the cursor over the **Apply** button until a message appears informing the user that circuit provisioning is disabled because of the communication failure.
- State Provisioning panel, the fields indicate that states are unavailable.
- Circuit Status panel, though the Administrative Status can be modified, it will most likely fail. In addition, the Operational Status indicates the value is unavailable.
- Software Load Status panel, indicates the load state and name are unavailable.

#### Circuit View data box fields

Box	Field	Explanation
Circuit Provisioning	Service Type	The line service type for NTNY53AA GLC 32 = potsLoopStart or potsGndStart. The line service type for NTNY53BA GLC 32 = potsLoopStart, potsGndStart, or pPhone. The line service type for GLC 12 = potsLoopStart, pPhone, postGndStart and coin.

Box	Field	Explanation
	Min Flash Duration	The minimum flash time in milliseconds. Default value is 31 (31 x 8ms = 248ms)
	Min Inter Digit Time	The minimum time allowed between digits in milliseconds. Default value is 63 (63 x 2ms = 126ms)
	Coefficient	Contains a pull down list of defined coefficients.
	Min Disc Time	The minimum time, in milliseconds, to be considered on hook with flash enabled. Default value is 150 (150 x 8ms = 1200ms)
	Termination DN	The Termination Directory Number (DN) is a numeric string associated with the line circuit. If no DN is associated with the circuit, "None" appears in the Termination DN field.
State Provisioning	Fault State	Indicates if the line is in a fault condition. <ul style="list-style-type: none"> <li>notInFault - No faults exist on the circuit.</li> <li>inFault - A fault has been detected on the circuit and a line fault notification is sent to the MG 9000 Manager.</li> <li>unknown - have not communicated with the card yet.</li> </ul>
	Protection State	Indicates if the line circuit is currently in over-voltage condition. <ul style="list-style-type: none"> <li>notInProtection - no foreign voltage has been detected.</li> <li>inProtection - foreign voltage has been detected and the cut-off relay operated.</li> <li>unknown - have not communicated with the card yet.</li> </ul>
	Babble State	Indicates if the line circuit is in a babbling state. <ul style="list-style-type: none"> <li>notInBabble - a babbling condition has not been detected on the circuit.</li> <li>inBabble - a babbling condition has been detected and the circuit is disabled from call processing.</li> <li>unknown - have not communicated with the card yet.</li> </ul>
	Cut Off Relay	Indicates if Cut Off Relay is operated. <ul style="list-style-type: none"> <li>on - the relay is on</li> <li>off - the relay is off</li> </ul>

Box	Field	Explanation
Circuit Status	Administrative Status	<p>Indicates whether the circuit can be used or is prohibited from use.</p> <ul style="list-style-type: none"> <li>locked - The circuit is administratively prohibited from performing service for its users. The lock will be applied even if there is an active call on the circuit. The call will be stopped when the circuit is locked.</li> <li>unlocked - The circuit is administratively permitted to perform service for its users.</li> </ul> <p><b>Note:</b> Changing the Administrative State does not require selection of the <b>Apply</b> button.</p>
	Operational Status	<p>Indicates the operability of a circuit.</p> <ul style="list-style-type: none"> <li>disabled - The circuit is inoperable and unable to provide service.</li> <li>enabled - The circuit is partially or fully operable and available for use.</li> </ul>
	Faulty	<p>Indicates whether or not a circuit is faulty</p> <ul style="list-style-type: none"> <li>"Yes" indicates that the circuit is faulty</li> <li>"No" indicates that the circuit is not faulty</li> </ul> <p><b>Note:</b> Changing the Faulty status does not require selection of the <b>Apply</b> button.</p>

The following figure shows the **GLC Line Circuit** View.

### Line Circuit View for GLC line circuits

- 7 Select the **Apply** button at the bottom of the **Line Circuit** window to update the circuit with the data entered.
- 8 This procedure is complete.

—End—

### Viewing all GLC line circuits

Step	Action
------	--------

#### *At the MG 9000 Manager*

- 1 At the **GLC Card View**, from the menu bar select **Services->Circuits Listing**.
- 2 The window for **Circuits Listing** appears. The **Circuits Listing View** is a table that shows a complete list of all ports contained within the card. Double clicking on any port row in the table opens up the corresponding Port View for that circuit.

**Note 1:** The values presented in the table cannot be edited. However, from the **Circuit List** View the technician can operate on multiple ports at the same time or apply certain commands like setting the Admin state.

**Note 2:** The alarm, configuration, and Admin state of the ports in the table get updated dynamically to reflect the state of the circuits on the MG 9000. The line service type and operational state do not get updated dynamically. Click on the **Refresh** button to see the current values.

### GLC Circuits List View

Num	Port State	Admin State	Op State	Type	Coefficient
Voice-0	Voice-0	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL
Voice-1	Voice-1	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL
Voice-2	Voice-2	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL
Voice-3	Voice-3	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL
Voice-4	Voice-4	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL
Voice-5	Voice-5	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL
Voice-6	Voice-6	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL
Voice-7	Voice-7	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL
Voice-8	Voice-8	Unlocked	Enabled	potsLoopStart	(1) NAmerica_SL

Set Values

Admin State  As Is  Lock  Unlock

Apply Refresh Close

The following table lists the fields in the **Circuits Listing** View.

#### Circuits Listing View fields

Field	Entry	Explanation
Num	0-31	Port number.
Port State	None	Graphical representation of the port along with its state.
Admin State	Locked, Unlocked, Testing, ERROR	Administrative state of the port. This is updated dynamically.
Op State	Enabled, Disabled, Testing, Dormant, Not Present, Lower Layer Down, ERROR	Operational state of the port. Does not get updated dynamically.
Type	potsLoopStart, coin, pPhone, potsGroundStart, No Service	Specifies the line service type for the port. Does not get updated dynamically.

Field	Entry	Explanation
Coefficient	N/A	Identifies the coefficient selected for the circuit.
SetValues	None	This is a logical grouping of all the values that can be set for multiple selections of the ports in the table.  The technician must select a value in any of these subfields and after selecting the ports for which the operation is to be performed, click on <b>Apply</b> .
Admin State	As Is, Locked, Unlocked	Select any of the values to perform the respective operation on the selected port(s). The action is only performed after clicking on <b>Apply</b> .
Apply	None	Performs the specified action on the selected port(s).
Refresh	None	Causes the view to refresh itself.
Close or from the Menu->Close	None	Closes the view.

3 This procedure is complete.

---

—End—

---

## Provisioning a coefficient table

**Provisioning a coefficient table** Coefficients are used to control circuit characteristics. Coefficients can be assigned on an individual circuit basis or on the GLC as a whole, in a manner similar to the way templates are used for WLC circuits. Several coefficients are available and can be assigned to a circuit or as part of a VMG Market Fit. The Coefficient Table Manager allows you to add new coefficients. Once added, the coefficients are available for assignment on an individual circuit basis.

**Note:** Values for coefficients are not editable, and must be provided by Nortel.

The market selected during the provisioning of the MG 9000 will determine what coefficients are available. For further details, see "[Provisioning an MG 9000 network element](#)" (page 24) and "[Provisioning switched lines services](#)" (page 178).

**Note 1:** A circuit will be configured with the coefficient selected for the VMG unless the selection is overridden in the GLC Line Circuit View.

**Note 2:** A circuit must be locked to change the coefficient.

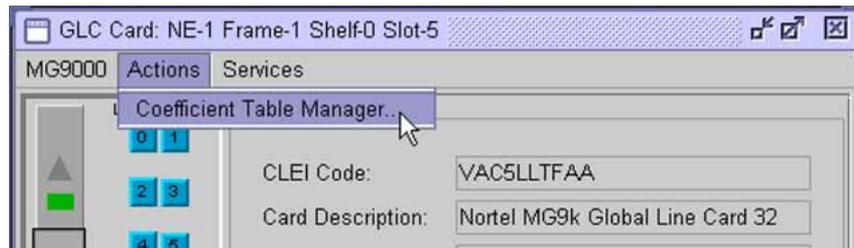
## Provisioning a coefficient table

Step	Action
------	--------

**At the MG 9000 Manager**

- 1 At the **Subnet View**, double click on the **MG 9000** that is to have the GLC line circuits provisioned. The **Frame View** appears.
- 2 At the **Frame View**, double click on the shelf in which the GLC resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the slot in which the GLC resides. The **GLC Card View** appears.
- 4 From the **GLC Card View**, access the **Actions->Coefficient Table Manager....** menu item as shown in the following figure.

### Accessing the Coefficient Table Manager



A Line Coefficient Table window appears that contains a listing of default coefficients available for the circuits on the card. The Line Coefficient Table window is shown in the following figure.

**Line Coefficient Table window**

NE: 18 Line Coefficient Table  
MG9000

Name	Index	PEC	Country Info	CRAM	Vinetic Ver.	Loop Info	Metering	Svc Type	Default
PPHONE_LL	90	NY53AA	Global	0	0x2484	LongLoop	false	pPhone	true
PPHONE_LL_LV	91	NY53AA	Global	0	0x2484	LongLoopLowVoltage	false	pPhone	false
POTS_SL	1	NY53AA	NorthAmerica	0	0x2484	ShortLoop	false	pots	true
POTS_LL_LV	13	NY53AA	NorthAmerica	0	0x2484	LongLoopLowVoltage	false	pots	false
POTS_LL	2	NY53AA	NorthAmerica	0	0x2484	LongLoop	false	pots	false
POTS_SL	10	NY53AA	Russia	0	0x2484	ShortLoop	false	pots	true
POTS_LL	11	NY53AA	Russia	0	0x2484	LongLoop	false	pots	false
POTS_LL_LV	12	NY53AA	Russia	0	0x2484	LongLoopLowVoltage	false	pots	false
POTS_SL	3	NY53AA	Spain	0	0x2484	ShortLoop	false	pots	true
POTS_LL	5	NY53AA	Spain	0	0x2484	LongLoop	false	pots	false
POTS_LL_WM_LV	14	NY53AA	Spain	0	0x2484	LongLoopLowVoltage	true	pots	false
POTS_LL_WM	6	NY53AA	Spain	0	0x2484	LongLoop	true	pots	false
POTS_SL_WM	4	NY53AA	Spain	0	0x2484	ShortLoop	true	pots	false
POTS_SL	7	NY53AA	Mexico	0	0x2484	ShortLoop	false	pots	true
POTS_LL	8	NY53AA	Mexico	0	0x2484	LongLoop	false	pots	false
POTS_LL_LV	9	NY53AA	Mexico	0	0x2484	LongLoopLowVoltage	false	pots	false
PPHONE_LL	95	NY53AB	Global	0	0x1490	LongLoop	false	pPhone	true
PPHONE_LL_LV	96	NY53AB	Global	0	0x1490	LongLoopLowVoltage	false	pPhone	false
POTS_SL	31	NY53AB	NorthAmerica	0	0x1490	ShortLoop	false	pots	true
POTS_LL	32	NY53AB	NorthAmerica	0	0x1490	LongLoop	false	pots	false
POTS_LL_LV	33	NY53AB	NorthAmerica	0	0x1490	LongLoopLowVoltage	false	pots	false
POTS_SL	50	NY53AB	Russia	0	0x1490	ShortLoop	false	pots	true
POTS_LL	51	NY53AB	Russia	0	0x1490	LongLoop	false	pots	false
POTS_LL_LV	52	NY53AB	Russia	0	0x1490	LongLoopLowVoltage	false	pots	false

Add Delete Refresh

Refer to the following table for a list of the data fields and the possible values.

**Line Coefficient Table data fields**

Fields	Explanation
Name	Provides the name assigned to the coefficient.
Index	Provides a system assigned index number associated with the selected coefficient.
PEC	Provides the GLC card PEC, NTNY53AA, NTNY53BA or NTNY53CA.
Country	Provides the country for which the coefficient is intended.
CRAM	Provides the cRAM information from the card.
Vinetic Ver.	Provides the Vinetic version from the GLC card.
Loop Info	Provides the loop status.
Metering	Identifies whether the circuit uses metering.
Svc Type	Identifies the coefficient service type.
Default	Identifies whether the coefficient is the default for the country in which it is used.

**At the Line Coefficient Table window**

- 5 Determine the next action from the following options in the Line Coefficient Table window.

**Note:** Coefficients cannot be edited.

If the next step is to	Do
add a line coefficient	<a href="#">step 6</a>
delete a line coefficient	<a href="#">step 7</a>
refresh a line coefficient	<a href="#">step 8</a>

- 6 To add a line coefficient, perform the following steps:

**Note:** This step is intended for Nortel personnel only. If you need to change a coefficient, you must contact Nortel. You cannot create your own coefficients.

- Click **Add**. The Enter Coefficient Filename box appears requesting that the fully qualified coefficient filename be entered.
- Enter a Coefficient filename.
- Click **OK**.
- Go to [step 9](#).

- 7 To delete a line coefficient, perform the following steps:

- Highlight the coefficient to be deleted from the Coefficient List by clicking on the Coefficient name.
- Click on **Delete** option at the bottom of Line Coefficient Table window.

**Note:** Default coefficients that are provided during auto discovery may not be deleted.

- Go to [step 9](#).

- 8 To refresh a line coefficient, Click on the **Refresh** button.

- 9 This procedure is complete.

---

—End—

---

## Checking the FPGA configuration load on NTNY53BA (GLC 32) and NTNY53CA (GLC 12) cards

You can upgrade the configuration load of the Field Programmable Gate Array (FPGA) on the NTNY53BA GLC 32 and NTNY53CA GLC 12 cards from the MG 9000 Manager.

**Note:** Nortel will inform you if the configuration load on the GLC cards needs to be updated.

The GLC Card View shows the FPGA configuration load on the GLC card. Use this field to determine if a new load needs to be downloaded to the FPGA.

The Software Download Manager menu, accessible from the Actions tab of the GLC Card View, allows you to download the configuration software of the FPGA from the SDM/CBM.

The following limitations and restrictions apply to this procedure

- The Software Download Manager and configuration load are only visible for GLCs which have a PEC code of NTNY53BA or above. The software download manager and configuration load do not appear on NTNY53AA GLC cards.
- The NTNY53BA or NTNY53CA version of the GLC must already be installed.

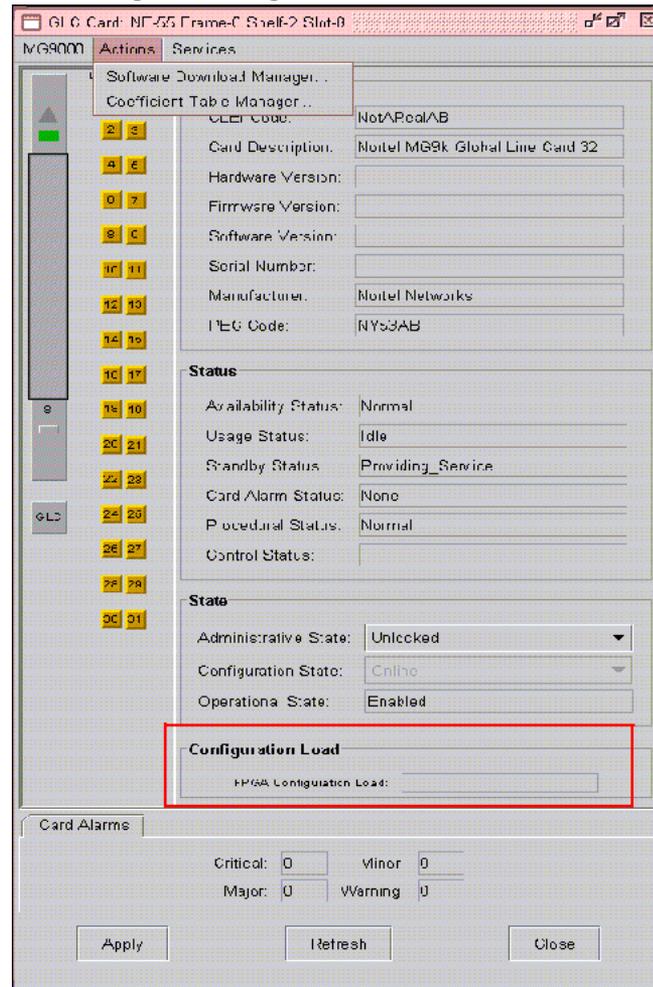
### Checking the FPGA configuration load on NTNY53BA (GLC 32) and NTNY53CA (GLC 12) cards

Step	Action
------	--------

*At the MG 9000 Element Manager*

- |   |   |
|---|---|
| 1 | At the Subnet View, double click on the MG 9000 that is to have the GLC configuration load. The Frame View appears.               |
| 2 | At the Frame View, double click on the shelf in which the GLC resides. The Shelf View appears.                                    |
| 3 | At the Shelf View, double click on the slot in which the GLC resides. The GLC Card View appears.                                  |
| 4 | In the Status area of the Card View, examine the Configuration Load field to determine if the FPGA has the correct software load. |

### Accessing the configuration load



- 5 If you need to upgrade the FPGA configuration load, see ["Downloading software into the GLC cards"](#) (page 460) for details about using the Software Download Manager.
- 6 This procedure is complete.

—End—

## Bulk provisioning line services

### Step Action

*At the MG 9000 Manager*

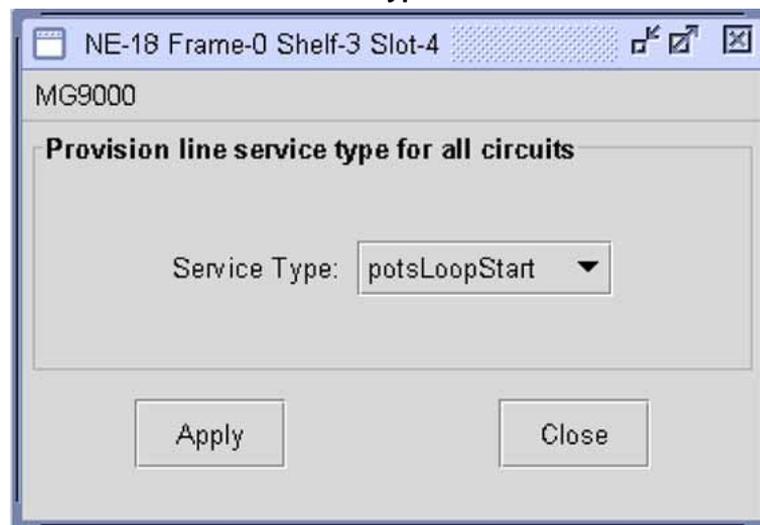
- 1 At the **Subnet View**, double click on the **MG 9000** that contains the GLC card on which line services are to be provisioned. The NE desktop view with **Frame View** appears.
- 2 At the **Frame View**, double click on the shelf in which the GLC resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the slot in which the GLC resides. The **GLC Card View** appears.

**Note:** The GLC card on which services are to be provisioned must be offline and deprovisioned. for the menu to appear and to proceed with this procedure.

- 4 From the **GLC Card View**, access the **Services->Provision Bulk Line Services** Types from the menu bar.

A Bulk Provision Line Services Types GUI appears that contains a pull-down selection list of service types available for the circuits on the card. The Provision Bulk Line Services Types GUI is shown in the following figure.

#### Bulk Provision Line Service Types GUI



Select the Services Type from the pull down. Options are

- potsLoopStart
- pPhone
- potsGroundStart

- 5 Press **Apply** to provision this service type for all the circuits on the card.

**6** This procedure is complete.

---

**—End—**

---

---

## Provisioning an ADSL card

---

### When to use this procedure

Use the procedures in this section when it is necessary to provision an asymmetrical digital subscriber loop (ADSL) card, and ADSL lines and data circuits. The ADSL combo 8+8 line card terminates eight fully compliant ADSL subscriber loops. Each loop interface has a splitter circuit to separate or join the lifeline voice service with the value-added ATM data cell traffic for the subscriber. The data traffic routes to the ATM common equipment MG shelf. In this section, the term ADSL signifies a specific type of DSL card, in this case, asymmetrical DSL. Throughout this section, XDSL is used to correspond with the screen title, where the "X" represents a variable to include multiple Digital Subscriber Loop versions.

Provisioning an XDSL card is the same as provisioning a World Line Card except that the XDSL card requires a software download. Refer to "[Provisioning a World line card](#)" (page 77) for more information. The XDSL card

- supports a software download menu. The software load used by the card is displayed under Software Load on the card view.
- supports Restart from the software load stored in RAM on the MG 9000. To restart the card, choose the Type to download (Restart Current Cold is the only type supported currently) and select the Restart button. The load used for the restart is displayed under Software Load, Restart Current on the card GUI.

**Note 1:** When an ADSL card goes from the Deprovisioned state to the Offline state, associated terminations are configured in the MG 9000 Manager, the MG 9000, and the SESM.

**Note 2:** XDSL voice circuits are only loop start.

**Note 3:** When commands are entered at the GUI that may affect service on the card, an "Are you sure" dialog box is displayed to allow the user to cancel or approve of the command.

**Note 4:** When provisioning an XDSL line card, click Refresh at the bottom of the XDLC Card View to synchronize the data between the MG 9000 and the MG 9000 Manager.

The following figure shows an XDSL Card View.

## XDSL Card View

**XDSL Card: NE-8 Frame-0 Shelf-2 Slot-8**

MG9000 Actions Services Alarms

	Data	Voice
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7
8		

**Card Attributes**

CLEI Code: VAAIL12HAA  
 Card Description: Nortel UEMG ADSL8x8 Line Card  
 Hardware Version: A  
 Firmware Version: 01  
 Software Version: notImplmented  
 Serial Number: M644280KG  
 Manufacturer: Nortel Networks  
 PEC Code: NY52AA

**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

**Card**

XDSL Card Alarms | NE Info

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

Apply Refresh Close

The following procedures are included

- Provisioning an xDSL voice circuit

- Provisioning the Global Traffic Descriptor
- Provisioning an xDSL data circuit
- Downloading software into the xDSL card
- Viewing all circuits on an xDSL card

**Note:** After provisioning an ADSL card and circuits on the MG 9000, it is recommended that all provisioning information be recorded. Use the Save SLoA services procedure to save provisioning information into a file that provides a list of all services on that network element.

Operations support systems (OSS) clients can perform provisioning operations such as add, delete, modify, and query ADSL circuit data using an XML-based machine interface using the OSSGate from the SESM server. The OSSGate forwards the ADSL provisioning requests from the SESM to the MG 9000 Manager.

To correctly identify the ADSL circuit on the MG 9000 from OSSGate, the following parameters must be entered in the following pattern:

```
<site><cf>-<rf>-<rs> tp/<ss>/<cc>
```

where

- site - a four character site name from the XACore table SITE
- cf - a contiguous office frame number, three digits, zero-padded if necessary (000-511)
- rf - a relative frame number (0-7)
- rs - a relative shelf number (0-3)
- ss - a slot which is the holder of one line card, padded with a zero if less than 10. For example, slot 9 appearing as 09.
- cc - a physical line circuit on a card, padded with a zero if less than 10. For example, 3 appearing as 03.

The following configuration parameters must be datafilled at the OSSGate for successful ADSL provisioning from the OSSGate:

#### ADSL configuration parameters

Attribute	Parameter	Meaning	Value
Circuit configuration	dnMaxSpeed	Max DownStream	32-13376 kbits, in multiples of 32
	upMaxSpeed	Max Upstream	32-1440 kbits, in multiples of 32
	dnMaxInterleaveDelay	Downstream delay	10-255 msec
	upMaxInterleaveDelay	Upstream delay	10-255 msec

Attribute	Parameter	Meaning	Value
Specific cross connection	dnSignalNoiseMargin	Downstream noise margin	6-31 db
	upSignalNoiseMargin	Upstream noise margin	6-31 db
	Transmission Mode		Auto Mode, ANSI, G.DMT
	VPI	Virtual Path Identifier	
	VCI	Virtual Circuit Identifier	
	upStream and dnStream Traffic Descriptors	ATM traffic characteristics	
	State of the cross connection		Inactive, Active, de-provision

Nortel recommends the following configuration for ADSL on the MG9K:

- Set the dnMaxSpeed to 12480 kbps.
- The VCC cross-connects for ADSL should use UBR. The MG9K does not apply the PCR value in a UBR service category traffic descriptor. Setting the PCR value will have no effect on the maximum download rate for the subscriber.

Use this configuration in association with traffic shaping on the edge of the ATM network (for example, PP7K/15K/20K) to provide a bandwidth-limited service to ADSL subscribers.

## Prerequisites

An ADSL line card must have been installed in the slot to be provisioned using correct ESD precautions.

## Action

The following procedures provide the steps for provisioning voice and data circuits on an XDSL card.

The basic steps for provisioning data circuits in a XDSL card include the following:

1. Provision the Global Traffic Descriptors in the Traffic Descriptor Manager. The Global Traffic Descriptor provides the rate of transmission rules and the service category used by the virtual path identifiers (VPI) and virtual channel identifiers (VCI) required for DSL traffic. The Global TD manager is launched from the Subnet View of the MG 9000 Manager.
2. The XDSL data circuit must be locked.

3. Provision the VCC fields at the X-Connects field in the XDSL data circuit view. There are 8 VCC allowed per data circuit.
4. Make required and recommended changes.
5. Click Apply.
6. Set the Administrative Status to Unlocked.
7. Click on Refresh (the operational status should become enabled).

**Note:** Before provisioning an XDSL data circuit, use the following procedure to access the Global Traffic Descriptor screen and provision the VPI and VCI values.

## Provisioning the Global Traffic Descriptors in the Traffic Descriptor Manager

Step	Action
------	--------

### At the MG 9000 Manager

- 1 At the **Subnet View**, from the menu bar, select **Configuration -> Global Traffic Descriptors...** The **TD Manager** screen appears. The following figure shows the **TD Manager** screen.

#### TD Manager screen

The screenshot shows the TD Manager window with the following table:

User Label	Service Category	Tagging	Frame Discard
Default TD	UBR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Below the table are buttons: New, Delete, Enter, Cancel.

Configuration fields:

- User Label:
- Uni Version:
- Service Category:
- No Clp:
- Transparent
- Tagging
- Frame Discard

Parameters section:

Peak Cell Rate (PCR) Clp:0: <input type="text"/>	Clp:0+1: <input type="text" value="0"/>
Sustained Cell Rate (SCR) Clp:0: <input type="text"/>	Clp:0+1: <input type="text"/>
Maximum Burst Size (MBS) Clp:0: <input type="text"/>	Clp:0+1: <input type="text"/>
CDVT: <input type="text" value="0"/>	MCR: <input type="text"/>

Close button at the bottom.

- 2 Click on **New** to add the upstream parameters.
- 3 Add the following traffic descriptor upstream information into the screen:

**ADSL upstream parameters**

Field	Datafill
User Label	UpTD (maximum 15 character limit)
Uni Version	UNI4.0
ServiceCategory	UBR
Tagging (box)	Check mark (click the box)
FrameDiscard (box)	Check mark (click the box)
CDVT	2500
Clp:0+1	2159

- 4 Select the **Enter** button.
- 5 Select the **New** button.
- 6 Add the following traffic descriptor downstream information into the screen:

**ADSL downstream parameters**

Field	Datafill
User Label	DownTD (maximum 15 character limit)
Uni Version	UNI4.0
ServiceCategory	UBR
Tagging (box)	Check mark (click the box)
FrameDiscard (box)	Check mark (click the box)
CDVT	2500
Clp:0+1	22978

- 7 Select the **Enter** button.
- 8 In the **XDSL Card View**, double-click one of the **data** icons. An **XDSL Circuit View** window appears.
- 9 Scroll down and select **Lock**.
- 10 Scroll up and provision the following fields, they will have a default value but they can be altered if required:
  - UpMaxSpeed=1440

- DnMaxSpeed=13376
  - UpSignalNoiseMargin=6
  - DnSignalNoiseMargin=6
  - UpMaxInterleaveDelay=10
  - DnMaxInterleaveDelay=10
- 11 Select the "**Transmission mode**" that the modem is capable of transmitting. The default value is 'Auto mode' and the other values are: ANSI or G.DMT.
  - 12 In VCC1:
    - VPI = (value between 16 - 31)
    - VCI = (value between 33 - 2047)
  - 13 Click on **SelectUpStreamTD**, highlight the UpTD and click **OK**.
  - 14 Click on Select **DownStreamTD**, highlight the DownTD and click **OK**.
 

**Note:** The UpTD and DownTD must be of the same service category.
  - 15 Set the Status to Active.
  - 16 Click **Apply**, then **OK**.
  - 17 After the VCCs are datafilled, unlock the circuit.
  - 18 This procedure is complete.

---

—End—

---

## Provisioning an XDSL voice circuit

---

### Step Action

---

#### *At the MG 9000 Manager*

- 1 Double click on an individual voice circuit to access the Voice Circuit View line circuit management screen.
 

The **XDSL Voice Circuit View** screen contains the same data fields described for the WLC as presented in the table "[WLC Circuit View data box fields](#)" (page 84). XDSL Voice circuit and WLC circuit provisioning are identical.
- 2 This procedure is complete.

---

—End—

---

## Provisioning an XDSL data circuit

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 At the **XDSL Card View**, double-click on an **individual data circuit** to access the **Data Circuit View** management screen. The following table lists the data fields that appear on this screen.

**Note:** Provision the upstream and downstream traffic descriptors through the Global Traffic Descriptor screen, described in Provisioning an XDSL data circuit procedure, before provisioning a data circuit.

### XDSL Data Circuit fields

Box	Field	Explanation
ADSL Data Provisioning	upMaxSpeed	The maximum upstream speed of the line toward the ATU-C.  The recommended value is 1440 kbit/s.
	upSignalNoiseMargin	Level of upstream line noise as seen by this ATU-C with respect to its received signal.  The recommended value is 6 dB.
	upMaxInterleaveDelay	Interleave delay defines the relative spacing between subsequent input bytes at the interleaver input and their placement in the bit stream at the interleaver output.  Larger numbers provide greater separation between consecutive input bytes in the output bit stream allowing for improved impulse noise immunity at the expense of payload latency.
	dnMaxSpeed	The recommended upstream setting is 10 ms. The maximum downstream speed of the line toward the ATU-R.  The recommended value is 13376 kbit/s.
	dnSignalNoiseMargin	Level of downstream line noise as seen by this ATU-R with respect to its received signal.  The recommended value is 6 dB.
	dnMaxInterLeaveDelay	The recommended downstream setting is 10 ms.

Box	Field	Explanation
	Transmission Mode	<p>Transmission Mode:</p> <p>The ADSL modems on the 8x8 line card are capable of supporting the following transmission modes:</p> <ul style="list-style-type: none"> <li>• ANSI (T1.413)</li> <li>• G.DMT (992.1)</li> <li>• AUTO (T1.413/992.1)</li> </ul> <p><b>Note:</b> The default provisioning for this field is, AUTO, thereby allowing the remote CPE to dictate the transmission mode during the training sequence. Some vendor CPE may require the mode to be set to either ANSI or G.DMT; therefore, this field would need to be changed, while the data circuit is locked. Upon unlocking the data circuit, the modems (ATUC/ATUR) will train utilizing the newly set transmission mode.</p>
	Modem Status	<p>This field is read only and displays the transitioning modem state from IDL to OPERATIONAL as reported by the MG 9000 during the training sequence. After the Modem is in OPERATIONAL state, the following two fields will be reported to indicate the current downstream transmit rate and current upstream transmit rate.</p>
	Sync upSpeed	<p>Current upstream transmit rate. These rates will be less than or equal to the maximum attainable rate of the loop. They are determined during the training sequence of the modems and are dependent on the quality of the loop, provisioned MaxTx speeds, error correction algorithms, etc.</p>
	Sync dnSpeed	<p>Current downstream transmit rate. These rates will be less than or equal to the maximum attainable rate of the loop. They are determined during the training sequence of the modems and are dependent on the quality of the loop, provisioned MaxTx speeds, error correction algorithms, etc.</p>
X-Connects for Each VCC	VPI	The range is 16 through 31.
	VCI	The range is 33 through 2047.

Box	Field	Explanation
Select UpStream TD	N/A	When clicked, the selected traffic descriptor GUI is displayed. After selecting the TD, the field next to it will display the name of the traffic descriptor selected for Up stream data.
Select DnStream TD	N/A	When clicked, the selected traffic descriptor GUI is displayed. After selecting the TD, the field next to it will display the name of the traffic descriptor selected for Down stream data.
	State	<p>The recommended value is Active.</p> <p><b>Note:</b> To change or select the state, the circuit must be locked. After provisioning is complete, the circuit must be returned to unlocked for the circuit to be able to transmit/receive data or be ready to be enabled when the state is changed from inactive to active.</p> <ul style="list-style-type: none"> <li>• Active - selected when provisioning the VCC and to indicate that data transmission is enabled. (Administrative Status of the cross-connect is Up.)</li> <li>• Inactive - selected when provisioning the VCC and to indicate that data transmission will not be enabled. (Administrative Status of the cross-connect is Down.)</li> <li>• De-provision - default state when VCC is not provisioned</li> </ul> <p><b>Note 1:</b> If the VCC is already provisioned, and if this state is selected, the VCC will be deprovisioned. The cross-connect is cleared and no more DSL service is provided to the customer.</p> <p><b>Note 2:</b> If selecting the de-provision state, it is recommended to leave the circuit in the locked Administrative Status.</p>
De-Provision	De-Provision	Clears the VCC fields.

Box	Field	Explanation
Status	Administrative Status	Place the circuit in one of two possible conditions: <ul style="list-style-type: none"> <li>locked</li> <li>unlocked</li> </ul>
	Operational Status	Read only box indicating the operational status of the circuit as: <ul style="list-style-type: none"> <li>enabled</li> <li>disabled</li> <li>unknown</li> </ul>

**XDSL Data Circuit view (top screen)**

The screenshot displays the 'Data Circuit: NE-8 Frame-0 Shelf-2 Slot-4 Ckt-0' configuration window. It is divided into several sections:

- Adsl Data Provisioning:** Contains input fields for upMaxSpeed (1440), dnMaxSpeed (13376), upSignalNoiseMargin (6), dnSignalNoiseMargin (6), upMaxInterleaveDelay (10), dnMaxInterLeaveDelay (10), Transmission Mode (Auto mode), Modem Status (IDL), Sync upSpeed (0), and Sync dnSpeed (0).
- X-Connects:** A list of five Virtual Channel Connections (VCC1-VCC5). Each VCC entry includes fields for VPI (0), VCI (0), and a State dropdown menu (set to De-Provision). There are also buttons for 'Select UpStream TD...' and 'Select DnStream TD...'.
- Data Circuit Alarms:** A section with 'NE Info' and counters for Critical (0), Minor (0), Major (0), and Warning (0).

At the bottom of the window are three buttons: 'Apply', 'Refresh', and 'Close'.

**XDSL Data Circuit view (bottom screen)**

The screenshot displays the 'Data Circuit: NE-8 Frame-0 Shelf-2 Slot-4 Ckt-0' configuration window. It features a menu bar with 'MG9000', 'Actions', 'Services', and 'Alarms'. The main area is divided into sections for VCC5, VCC6, VCC7, and VCC8. Each section contains a 'State' dropdown menu set to 'De-Provision', and input fields for 'VPI' and 'VCI', both set to '0'. To the right of each VPI/VCI field are buttons labeled 'Select UpStream TD...' and 'Select DnStream TD...'. Below the VCC sections is a 'De-Provision' button. The 'Status' section includes 'Administrative Status' set to 'Locked' and 'Operational Status' set to 'Disabled'. At the bottom, there is a 'Data Circuit Alarms' section with a 'NE Info' tab and four counters: 'Critical: 0', 'Minor: 0', 'Major: 0', and 'Warning: 0'. At the very bottom are 'Apply', 'Refresh', and 'Close' buttons.

- 2 To complete the circuit provisioning and set the circuit state, click on **Apply**.
- 3 This procedures is complete.

---

—End—

---

**Downloading software using the Software Download Manager**

The Software Download Manager menu option provides access to a Software Download Manager window. The following procedure provides the steps for downloading software into the ADSL card.

---

**Downloading software into the ADSL card**

---

**Step Action**

---

**At the MG 9000 Manager**

- 1 At the **Subnet View**, double click on the **MG 9000** that has the ADSL card to which software is to be downloaded. The **Frame View** appears.
- 2 At the **Frame View**, double click on the **shelf** in which the ADSL card resides. The **Shelf View** appears.
- 3 At the Shelf View, double click on the slot in which the ADSL card resides. The **ADSL Card** screen appears.
- 4 To request a download, select the **Locked** option for the Administrative Status in the Status box. The card must be Locked prior to requesting a download.
- 5 From the **ADSL Card View** menu level, select **Actions->Software Download Manager**
- 6 Enter data in the fields as follows:
  - File Path - the path and name of the file to be downloaded to the card (/mg9k/<loadname>)
  - IP address - the file location (IP address)
  - Server userName - the login name for the server where load resides
  - Server password - the password for the server where load resides
  - select **Force Download** if forced download is required. The force option is needed only when the card must be reloaded with the same load that already exists on the card.
- 7 Select the **Download** button at the bottom of the **Software Download Manager** window. When the download begins the **download** icon appears on the card.

Once the download is complete, the **download** icon disappears and the **initialization** icon appears. Once initialization is complete, the icon disappears and the software load used in the card is displayed in the Software Load section of the **Card View**.
- 8 This procedure is complete.

---

—End—

---

## Viewing all circuits on a xDSL card

### Step Action

#### At the MG 9000 Manager

- 1 At the **xDSL Card** screen, from the menu bar select **Services->Circuits Listing**.
- 2 The window for Circuits Listing appears. The **Circuits Listing View** is a table that shows a complete list of all ports contained within the card. Double clicking on any port row in the table opens up the corresponding **Port View** for that circuit.

**Note 1:** The values presented in the table cannot be edited. However, from the **Circuit Listing View** the technician can operate on multiple ports at the same time or apply certain commands like setting the Admin state.

**Note 2:** The alarm, configuration, and Admin state of the ports in the table get updated dynamically to reflect the state of the circuits on the MG 9000. The line service type and operational state do not get updated dynamically. Click on the **Refresh** button to see the current values.

### xDSL Circuits Listing View

Num	Port State	Admin State	Op State	Type	Template
Data-0	Data-0	Locked	Disabled	data circuit	data circuit
Data-1	Data-1	Locked	Disabled	data circuit	data circuit
Data-2	Data-2	Locked	Disabled	data circuit	data circuit
Data-3	Data-3	Locked	Disabled	data circuit	data circuit
Voice-0	Voice-0	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-1	Voice-1	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-2	Voice-2	Unlocked	Enabled	potsLoopStart	(1) DEFAULT
Voice-3	Voice-3	Unlocked	Enabled	potsLoopStart	(1) DEFAULT

Set Values

Admin State  As Is  Lock  Unlock

Apply Refresh Close

The following table lists the fields in the **Circuits Listing View**.

#### Circuits Listing View fields

Field	Entry	Explanation
Num	1-4	Port number.
Port State	N/A	Graphical representation of the port along with its state.
Admin State	Locked, Unlocked, Testing, ERROR	Administrative state of the port. This is updated dynamically.
Op State	Enabled, Disabled, Testing, Dormant, Not Present, Lower Layer Down, ERROR	Operational state of the port. Does not get updated dynamically.
Type	potsLoopStart, coin, pPhone, potsGroundStart, No Service	Specifies the line service type for the port. Does not get updated dynamically.
Template	N/A	Identifies the template selected for the circuit.
SetValues	N/A	This is a logical grouping of all the values that can be set for multiple selections of the ports in the table.  The technician must select a value in any of these subfields and after selecting the ports for which the operation is to be performed, click on <b>Apply</b> .
Admin State	As Is, Locked, Unlocked	Select any of the values to perform the respective operation on the selected port(s). The action is only performed after clicking on <b>Apply</b> .
Apply	N/A	Performs the specified action on the selected port(s).
Refresh	N/A	Causes the view to refresh itself.
Close or from the Menu->Close	N/A	Closes the view.

**3** This procedure is complete.

---

—End—

---

## Provisioning an SAA line card

### When to use this procedure

Use this information to provision an SAA line card and line circuits.

**Note:** The SAA card is not used in the UA-IP solution.

The Service Adapter Access (SAA) line card is a programmable line card that supports the following services:

- POTS (loop and ground start)
- Coin
- Meridian Business Set (P-phone)

Included are the following procedures:

- Provisioning an SAA line circuit
- Viewing all circuits on an SAA card

**Note 1:** When an SAA card goes from the Deprovisioned state to the Offline state, associated terminations are configured in the MG 9000 Manager, the MG 9000, and the SESM.

**Note 2:** After provisioning an SAA card and circuits on the MG 9000, it is recommended that all provisioning information be recorded. Use the Save SLoA services procedure to save provisioning information into a file that provides a list of all services on that network element.

### Prerequisites

An SAA line card must be installed in the slot to be provisioned.

### Action

SAA line card and World Line Card (WLC) provisioning are identical except that the SAA card does not use B11 templates. Refer to ["Provisioning a World line card" \(page 77\)](#) for information on SAA card provisioning.

### Provisioning an SAA line circuit

Step	Action
<i>At the MG 9000 Manager</i>	
1	At the <b>Subnet View</b> , double click on the <b>MG 9000</b> that is to have the SAA line circuits provisioned. The <b>Frame View</b> appears.

- 2 At the **Frame View**, double click on the shelf in which the SAA card resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the slot in which the SAA card resides. The **SAA Card** screen appears.
- 4 At the **SAA Card** screen double click on an individual circuit and the window for **SAA Circuit** screen appears.

**Note:** When commands are entered at the Nortel Carrier VoIP MG 9000 Manager that may affect service on the circuit, an "Are you sure" dialog box is displayed to allow the user to cancel or approve of the command.

- 5 At the **SAA Circuit** screen, select the **Locked** option for the Administrative Status in the Circuit Status box. The circuit must be Locked prior to modifying the circuit's data.

When the circuit is Locked, the fields in the Circuit Provisioning box become available for modification.

- 6 Enter data in the fields that appear in the Circuit Provisioning box from the **Line Circuit** window. The SAA Circuit screen contains the same data fields described for the WLC Line Circuit and presented in the Circuit View data box fields table. In addition to POTS ground start and POTS loop start, the Service Type for SAA may be Coin or P-phone. All SAA line circuits default to P-phone when provisioned. To change the service type option, use the Service Type pull-down combo box.

**Note 1:** When the MG 9000 Manager is having trouble retrieving circuit data from the MG 9000, conditions may exist when attempting to provision circuits affecting the ability to enter data into the fields. Each of these panels work independently of each other and any data that is available will be displayed. For more information refer to "[Provisioning a line circuit on a WLC](#)" (page 83).

**Note 2:** There are two approved ways to change the service type:

1. Using the XA-Core SERVORD command followed by a change using this GUI.
2. Using OSSGate/SERVORD+ command, which automatically sets the circuit Service Type in the MG 9000. If OSSGate commands are being used, changing the Service Type from this GUI may create a conflict between circuit data and line service data which could result in the LOSS OF SERVICE on this circuit. When OSSGate commands are being used the Service Type

should not be changed from this GUI unless it exactly matches the Service Type set in OSSGate.

The following figure shows the **SAA Circuit View**.

### SAA Circuit View

The screenshot shows the 'SAA Circuit View' window for 'SAA Circuit: NE-11 Frame-0 Shelf-2 Slot-2 Ckt-0'. The window is divided into several sections:

- Circuit Provisioning:** Service Type: pPhone; Min Flash Duration: 248 ms; Min Disc Time: 1200 ms; Min Inter Digit Time: 125 ms; Termination DN: 6193420200.
- 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.
- Software Load Status:** Load Status: success; Current LoadName: A34=1907AC20FB A37=1708AC01AN.
- SAA Circuit Alarms:** Critical: 0; Minor: 0; Major: 0; Warning: 0.

Buttons at the bottom include 'Apply', 'Refresh', and 'Close'.

- 7 Select the **Apply** button at the bottom of the **SAA Circuit** window to update the circuit with the data entered.

**Note:** When the line circuit is changed, no checks are made from the MG 9000 Manager for whether a DN exists on the termination associated with the circuit.

- 8 This procedure is complete.

—End—

## Viewing all circuits on a SAA card

### Step Action

#### At the MG 9000 Manager

- 1 At the **Subnet View**, double click on the **MG 9000** that is to have the SAA line circuits to be listed. The **Frame View** appears.

- 2 At the **Frame View**, double click on the shelf in which the SAA card resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the slot in which the SAA card resides. The **SAA Card** screen appears.
- 4 At the **SAA Card** screen, from the menu bar select **Services->Circuits** Listing.
- 5 The window for Circuits Listing appears. The Circuits Listing View is a table that shows a complete list of all ports contained within the card. Double clicking on any port row in the table opens up the corresponding **Port View** for that circuit.

**Note 1:** The values presented in the table cannot be edited. However, from the **Circuit Listing View** the technician can operate on multiple ports at the same time or apply certain commands like setting the Admin state.

**Note 2:** The alarm, configuration, and Admin state of the ports in the table get updated dynamically to reflect the state of the circuits on the MG 9000. The line service type and operational state do not get updated dynamically. Click on the **Refresh** button to see the current values.

### SAA Circuits Listing View

Num	Port State	Admin State	Op State	Type
Voice-0	Voice-0	Unlocked	Enabled	potsLoopStart
Voice-1	Voice-1	Unlocked	Enabled	potsLoopStart
Voice-2	Voice-2	Unlocked	Enabled	pPhone
Voice-3	Voice-3	Unlocked	Enabled	pPhone
Voice-4	Voice-4	Unlocked	Enabled	coin
Voice-5	Voice-5	Unlocked	Enabled	pPhone
Voice-6	Voice-6	Unlocked	Enabled	potsGroundStart
Voice-7	Voice-7	Unlocked	Enabled	coin
Voice-8	Voice-8	Unlocked	Enabled	pPhone

Set Values

Admin State  As Is  Lock  Unlock

Apply Refresh Close

The following table lists the fields in the **Circuits Listing View**.

#### Circuits Listing View fields

Field	Entry	Explanation
Num	1-12	Port number.
Port State	N/A	Graphical representation of the port along with its state.
Admin State	Locked, Unlocked, Testing, ERROR	Administrative state of the port. This is updated dynamically.
Op State	Enabled, Disabled, Testing, Dormant, Not Present, Lower Layer Down, ERROR	Operational state of the port. Does not get updated dynamically.
Type	potsLoopStart, coin, pPhone, potsGroundStart, No Service	Specifies the line service type for the port. Does not get updated dynamically.
SetValues	N/A	This is a logical grouping of all the values that can be set for multiple selections of the ports in the table.  The technician must select a value in any of these subfields and after selecting the ports for which the operation is to be performed, click on Apply.
Admin State	As Is, Locked, Unlocked	Select any of the values to perform the respective operation on the selected port(s). The action is only performed after clicking on Apply.
Apply	N/A	Performs the specified action on the selected port(s).
Refresh	N/A	Causes the view to refresh itself.
Close or from the Menu->Close	N/A	Closes the view.

**6** This procedure is complete.

—End—

## Provisioning a DS1 card

### When to use this procedure

Use this procedure when it is necessary to provision a DS1 card.

**Note:** The DS1 card is used only in the UA-AAL1 solution.

The DS1 AAL-1 line card supports private line services in the MG 9000 shelf. The initialization process creates 16 available 1.544 Mbps DS1 service facilities on the DS1 card. The channelization process divides a DS1 facility into 24 DS0 channels.

Included are the following procedures:

- Provisioning a DS1 card
- Provisioning DS1 ports
- Provisioning a DS0 bundle with contiguous channels
- Provisioning a DS0 bundle with non-contiguous channels
- Deleting DS0 bundles on DS1 ports
- Unchannelizing ports
- Viewing all DS1 circuits

**Note:** After provisioning a DS1 card and port data on the MG 9000, it is recommended that all provisioning information be recorded. Use the Save PLoA services procedure to save provisioning information into a file that provides a list of all services on that network element.

### Prerequisites

A DS1 card must have been installed in the slot to be provisioned using correct ESD precautions.

### Action

The following procedure provides steps for provisioning a DS1 card. After the card is provisioned, the DS1 ports must be provisioned to enable services through the DS1 card.

#### Provisioning a DS1 card

Step	Action
------	--------

*At the MG 9000 Manager*

- |   |   |
|---|---|
| 1 | At the <b>Subnet View</b> , double click on the <b>MG 9000</b> that is to have the DS1 card provisioned. The <b>Frame View</b> appears. |
|---|---|

- 2 At the **Frame View**, double click on the shelf in which the DS1 card resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the slot in which the DS1 card resides. The **DS1 Card View** appears. Since the DS1 card is already installed, autodiscovery datafills the data about the card.

**Note:** When provisioning a DS1 card, click **Refresh** at the bottom of the **DS1 Card View** to synchronize the data between the MG 9000 and the MG 9000 Manager.

The following figure shows a **DS1 Card View**.

### DS1 Card View

DS1 Card: NE-8 Frame-0 Shelf-2 Slot-20

MG9000 Actions Services Alarms

DS1 Port

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16

20

Relay

#### Card Attributes

CLEI Code: VAL1LM0EAA

Card Description: Nortel UEMG DS1 i/f Card

Hardware Version: 5

Firmware Version: 02

Software Version: 6

Serial Number: M1723PQSB

Manufacturer: Nortel Networks

PEC Code: NY40AA

#### 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: Offline

Operational State: Disabled

#### Card

Restart type Restart Current

#### Software Load

DS1 Card Alarms NE Info

Critical: 0 Minor: 30

Major: 0 Warning: 0

Apply Refresh Close

4 This procedure is complete.

—End—

The DS1 Ports box that appears to the right of the DS1 Card image provides access to a **Port View** window for each of the DS1 facilities. The following procedure provides steps for accessing and provisioning the DS1 ports.

---

## Provisioning DS1 ports

---

Step	Action
------	--------

---

### *At the MG 9000 Manager*

- 1 At the **Subnet View**, double click on the **MG 9000** that is to have the DS1 ports provisioned. The **Frame View** appears.
- 2 At the **Frame View**, double click on the shelf in which the DS1 card resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the DS1 card with DS1 ports to be provisioned. The **DS1 Card View** appears.
- 4 At the **DS1 Card View**, double click on the DS1 port to be provisioned. The **DS1 Port View** appears.
- 5 At the **DS1 Port View**, select Enabled if the DS1 facility channelization option is to be enabled. Choose Disabled if DS1 channelization is not to be enabled, the default is Disabled.

The **DS1 Port view** screen contains two management tabs:

- DS1 Attributes - manages the entire DS1 facility.
- DS0 Bundle - manages individual DS0 channels (disabled if channelization is set to Disabled).

The following figure shows a DS1 Attributes tab on the **DS1 Port Attributes** screen.

**DS1 Port View Attributes screen**

**Note 1:** Configuration data for a DS1, DS0, or a DS0 Bundle cannot be changed while in-service. Carrier maintenance (CARM) allows configuration changes only to locked DS carriers and interfaces. A locked DS facility is in an out-of-service condition that positions the carrier on-line with no subscriber traffic but still provides continuous defect monitoring.

**Note 2:** When attempting to lock a DS1 port with services provisioned, a pop-up message appears informing the user of this condition.

- 6 Enter the attributes for the DS1 port. The following table lists the fields that appear in the attributes screen of the **DS1 Port View**.

**DS1 Port View Attributes box fields**

Box	Field	Explanation
DS1 Provisioning	Circuit Identifier	A character string, created from the Private Line Creation screen, used for circuit identification.
	Facility Data Link	<ul style="list-style-type: none"> <li>ANSI T1403</li> <li></li> </ul>

Box	Field	Explanation
		AT&T 154016
	Line type	<ul style="list-style-type: none"> <li>None</li> </ul>
	Line Coding	ESF (Extended Super Frame) D4 [SF (Super Frame)] B8ZS coding
	Loopback configuration	AM1 coding Options are: <ul style="list-style-type: none"> <li>no loop</li> <li>pay load</li> <li>line</li> <li>inward</li> <li>dual (line and inward)</li> </ul>
	Line Length	655
	Send Code	<ul style="list-style-type: none"> <li>Send No Code</li> <li>Send Line Code</li> <li>Send Payload Code</li> <li>Send Reset Code</li> </ul>
Clock Source	Through Timing (required option)	
	Channelization	<p>Enabled - divides the 1.544 Mbps DS1 facility into 24 individual 64 kbps channels.</p> <p>Disabled - maintains the DS1 facility as a single 1.544 Mbps channel.</p> <p><b>Note:</b> Any DS0 Bundles must be removed from a port before unchannelizing a DS1 carrier.</p>

Box	Field	Explanation
Status	Administrative status	Places the port into one of the following conditions: <ul style="list-style-type: none"> <li>• unlocked</li> <li>• locked</li> </ul>
	Configuration status	Places the port into one of the following conditions: <ul style="list-style-type: none"> <li>• Online</li> <li>• Offline</li> </ul>
	Operational status	Indicates one of the following conditions: <ul style="list-style-type: none"> <li>• enabled</li> <li>• disabled</li> <li>• Lower Layer Down</li> </ul>
Bundle	Circuit Id	Customer assigned number based on the format used in each operating company.
	RBS Mode	Robbed bit signaling.

7 The next step is based on the information in the following table.

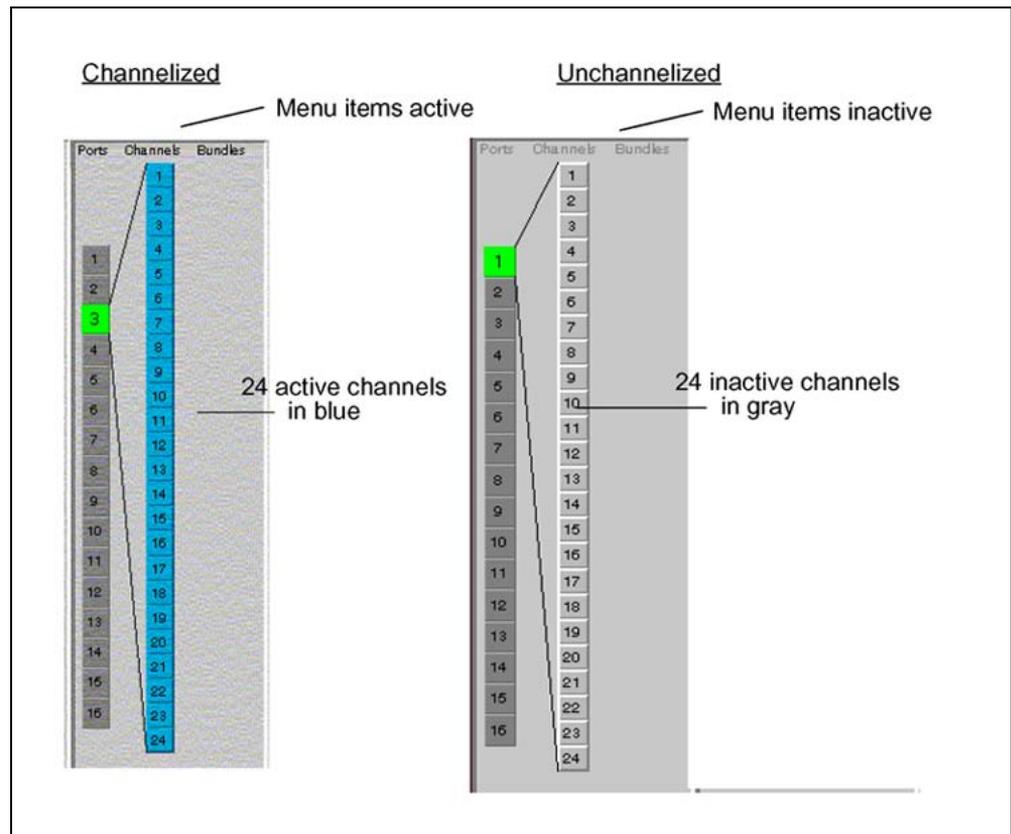
channelization was	Do
enabled	Proceed to the procedures for provisioning DS0 bundles
disabled	<a href="#">step 8</a>

8 This procedure is complete.

—End—

The following figure illustrates how the MG 9000 Manager presents a channelized versus an unchannelized DS1 port.

### Channelized versus unchannelized DS1 port



Bundled DS0 channels allow private line bandwidth variation by creating combinations of multiple 64 kbps DS0 channels. Structured (channelized) services can only be provided over bundled channels.

**Note:** DS0 channel bundles must be locked before making changes to a corresponding DS1 facility or DS0 channel.

DS0 bundles are provisioned from a channelized **DS1 Port View**. A bundle can consist of a minimum 1 channel or a maximum 24 channels. One DS1 port can support multiple DS0 bundles. Bundles can consist of contiguous channels or non-contiguous channels.

- contiguous channels (for example, channels 1, 2, 3, and 4)
- non-contiguous channels (for example, channels 2, 6, 9, and 12)

The following procedures provide two different methods for provisioning a bundle with contiguous channels.

---

### Provisioning a DS0 Bundle with contiguous channels, method 1

---

Step	Action
------	--------

---

*At the MG 9000 Manager*

- 1 From the channelized **DS1 Port View**, click the left mouse button on the first proposed channel in the bundle.
- 2 Continue to hold the button.
- 3 Drag the mouse to the last desired channel.
- 4 Click on **Create** to create the bundle.
- 5 This procedure is complete.

---

—End—

---



---

### Provisioning a DS0 Bundle with contiguous channels, method 2

---

Step	Action
------	--------

---

*At the MG 9000 Manager*

- 1 From the channelized **DS1 Port View**, click the mouse button on the first proposed channel in the bundle
- 2 Let go of the button.
- 3 Press the **Shift** button on the keyboard, and while holding it down, use the mouse to select the last proposed channel in the bundle.
- 4 Release the mouse button and click the **Create** button on the right panel under the Bundle title.
- 5 This procedure is complete.

---

—End—

---

The following procedure describes the process to create a bundle with noncontiguous channels.

### Provisioning a DS0 bundle with non-contiguous channels

---

Step	Action
------	--------

---

*At the MG 9000 Manager*

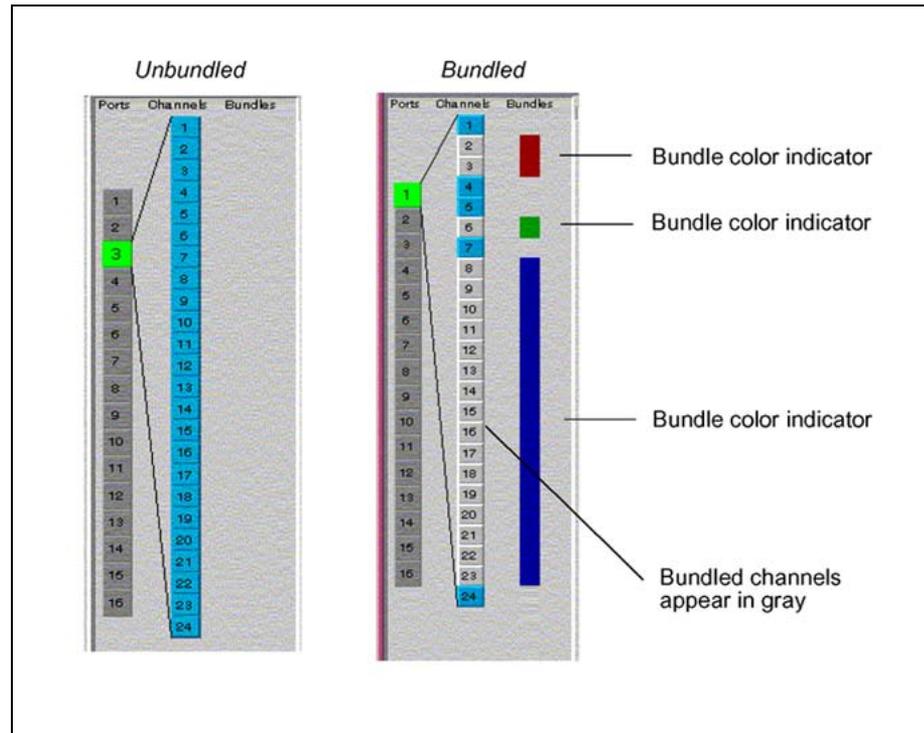
- 1 From a channelized **DS1 Port View**, click the mouse button on the first proposed channel in the bundle.
- 2 Hold down the Control key on the keyboard.
- 3 Click the next desired channel.
- 4 Still holding the control key, repeat step 3 until all the desired channels are selected.
- 5 Click the **Create** button on the right panel under the Bundle title.

Creating one or more bundles changes the GUI DS0 channel presentation. Non bundled channels continue to appear in blue. Bundled channels become gray and a color code to the right of bundle is used for identification when using the Bundle Tab. The following figure shows a channelized unbundled, DS1 port 3 and a channelized bundled, DS1 port 1.

Also, the color of the port representation on the **DS1 Card View** change as follows:

- Blue - if no bundles exist
- Light Blue - if bundles exist on the port but there are still channels available for creating the bundles
- Dark Blue - if bundles exist and no more can be created as all channels have been taken.

### Unbundled versus bundled DS0 channels



In the previous figure, the Bundled view on the right Port 1 contains three bundles:

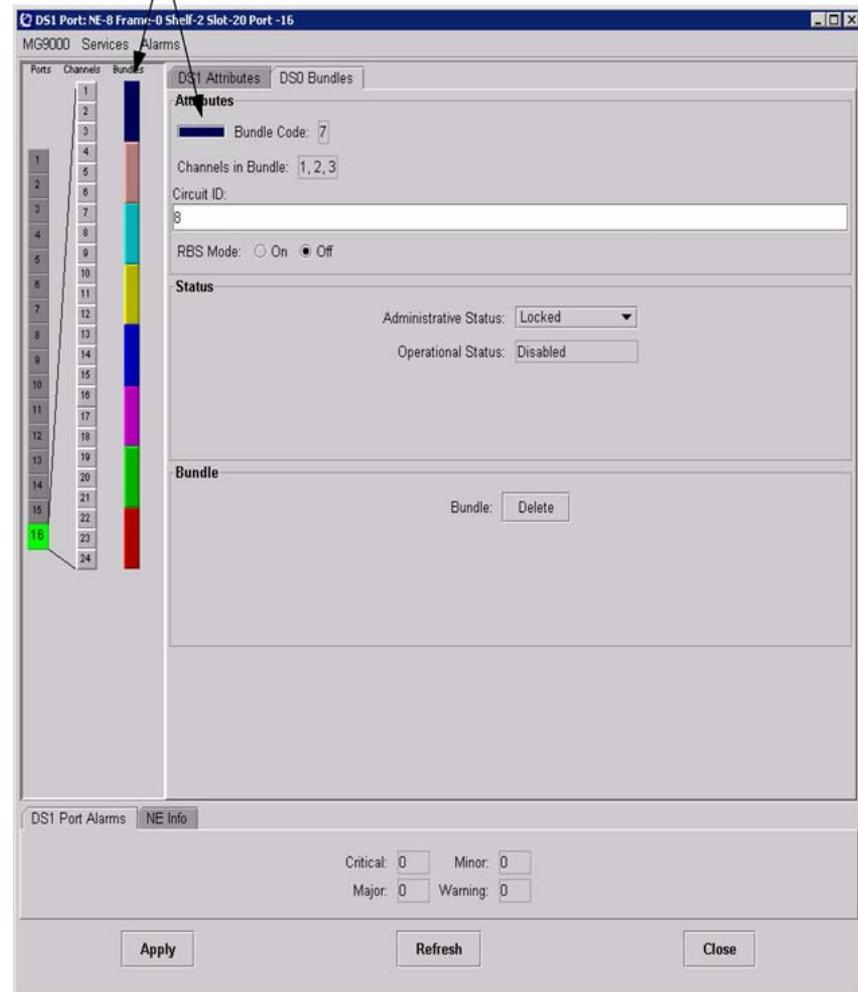
- channels 2 and 3
- channel 6
- channels 8 through 23

Each bundle has a color bar indicator to the right of the DS0 channel. In this example, the color bars are red, green, and blue.

The DS0 Bundles tab provides information detail regarding a selected bundle's attributes and also the ability to perform bundle administration. The following figure shows an example of a DS1 Port view with the Bundles Tab selected.

### DS1 Port View Bundles tab

Matching color codes



The following table lists the fields that appear in the DS0 Bundles screen from the **DS1 Port View**.

#### DS0 Bundles tab

Box	Field	Explanation
Attributes	<color_code>	The color indicator that appears next to the channel.
	Bundle code	Hexadecimal bundle identification.
	Channels in Bundle	The DS0 channel numbers that make up the bundle.
	Circuit ID	A character string used for the restart discovery process.

Box	Field	Explanation
Status	Administrative Status	Place the selected bundle in one of two possible conditions: <ul style="list-style-type: none"> <li>locked (when locking a bundle, the user will be warned with a message if a service exists on it)</li> <li>unlocked</li> </ul>
	Operational Status	Informational box indicating the operational status of the bundle as: <ul style="list-style-type: none"> <li>enabled</li> <li>disabled</li> <li>Testing</li> <li>Lower Layer Down</li> </ul> <p><b>Note:</b> This information is not automatically updated by the MG 9000. Use the Refresh button to obtain the latest status.</p>
	Delete this Bundle	Removes the bundle and returns the channels in the bundle to individual 64 kbps DS0 channels. If a service exists on the bundle, the user will not be able to delete the bundle and a pop-up message will appear informing him of that. <p><b>Note 1:</b> Delete all DS0 Bundles on a DS1 port before unchannelizing the port.</p> <p><b>Note 2:</b> The bundle must be locked before it is deleted.</p>

6 This procedure is complete.

—End—

### Deleting DS0 bundles on DS1 ports

Step	Action
------	--------

*At the MG 9000 Manager*

- |   |  |
|---|--|
| 1 | Access the <b>DS1 Port View</b> .  |
| 2 | Double click on the <b>DS0 bundle</b> to be deleted. The <b>DS0 Bundles</b> tab appears. |

- 3 Change the Administrative State of the bundle to Locked.
- 4 Click on the **Delete Bundle** button.
- 5 This procedure is complete.

---

—End—

---

### Unchannelizing ports

---

Step	Action
------	--------

---

*At the MG 9000 Manager*

- 1 Access the **DS1 Circuits List View** for the DS1 card which is to have ports unchannelized.
- 2 Select each channelized port using Shift + Click with left mouse button.
- 3 Select the Unchannelize selection button at the bottom of the **DS1 Circuits List View**.
- 4 Click on **Apply**.
- 5 This procedure is complete.

---

—End—

---

### Viewing all circuits on a DS1 card

---

Step	Action
------	--------

---

*At the MG 9000 Manager*

- 1 At the **DS1 Card screen**, from the menu bar select **Services->Circuits Listing**.
- 2 The window for Circuits Listing appears. The Circuits Listing View is a table that shows a complete list of all ports contained within the card. Double clicking on any port row in the table opens up the corresponding **Port View** for that circuit.

**Note 1:** The values presented in the table cannot be edited. However, from the Circuit Listing View the technician can operate on multiple ports at the same time or apply certain commands like setting the Admin state.

**Note 2:** The alarm, configuration, and Admin state of the ports in the table get updated dynamically to reflect the state of the

circuits on the MG 9000. The line service type and operational state do not get updated dynamically. Click on the **Refresh** button to see the current values.

**DS1 Circuits Listing View**



The following table lists the fields in the **Circuits Listing View**.

**Circuits Listing View fields**

Field	Entry	Explanation
Num	1-16	Port number.
Port State	N/A	Graphical representation of the port along with its state.
Admin State	Locked, Unlocked, Testing, ERROR	Administrative state of the port. This is updated dynamically.

Field	Entry	Explanation
Op State	Enabled, Disabled, Testing, Dormant, Not Present, Lower Layer Down, ERROR	Operational state of the port. Does not get updated dynamically.
Config	Online, Offline, ERROR	Configuration State of the port. This is only applicable to the DS1 ports. Gets dynamically updated.
Channel	Channelized, Unchannelized	Channelization information of the port. Indicates whether the port has been channelized. Gets dynamically updated.
Bundle	Unbundled, Free Channels, No Free Channels	Bundle information of the port. Indicates if the channel has bundles and if there are any free channels available for further bundles. Gets dynamically updated.
SetValues	N/A	This is a logical grouping of all the values that can be set for multiple selections of the ports in the table.  The technician must select a value in any of these subfields and after selecting the ports for which the operation is to be performed, click on <b>Apply</b> .
Admin State	As Is, Locked, Unlocked	Select any of the values to perform the respective operation on the selected port(s). The action is only performed after clicking on <b>Apply</b> .
ConfigSt	As Is, Online, Offline	The technician can set the configuration state of the selected port(s) by selecting the appropriate value and clicking on <b>Apply</b> .  <b>Note:</b> Selecting a value other than "As Is" will disable the user from selecting other input values.
ChannelSt	As Is, Channelized, Unchannelized	The technician can (un)channelize a port(s) by selecting the appropriate value and clicking on <b>Apply</b> .  <b>Note:</b> Selecting a value other than "As Is" will disable the user from selecting other input values.
Apply	N/A	Performs the specified action on the selected port(s).
Refresh	N/A	Causes the view to refresh itself.
Close or from the Menu->Close	N/A	Closes the view.

**3** This procedure is complete.

---

—End—

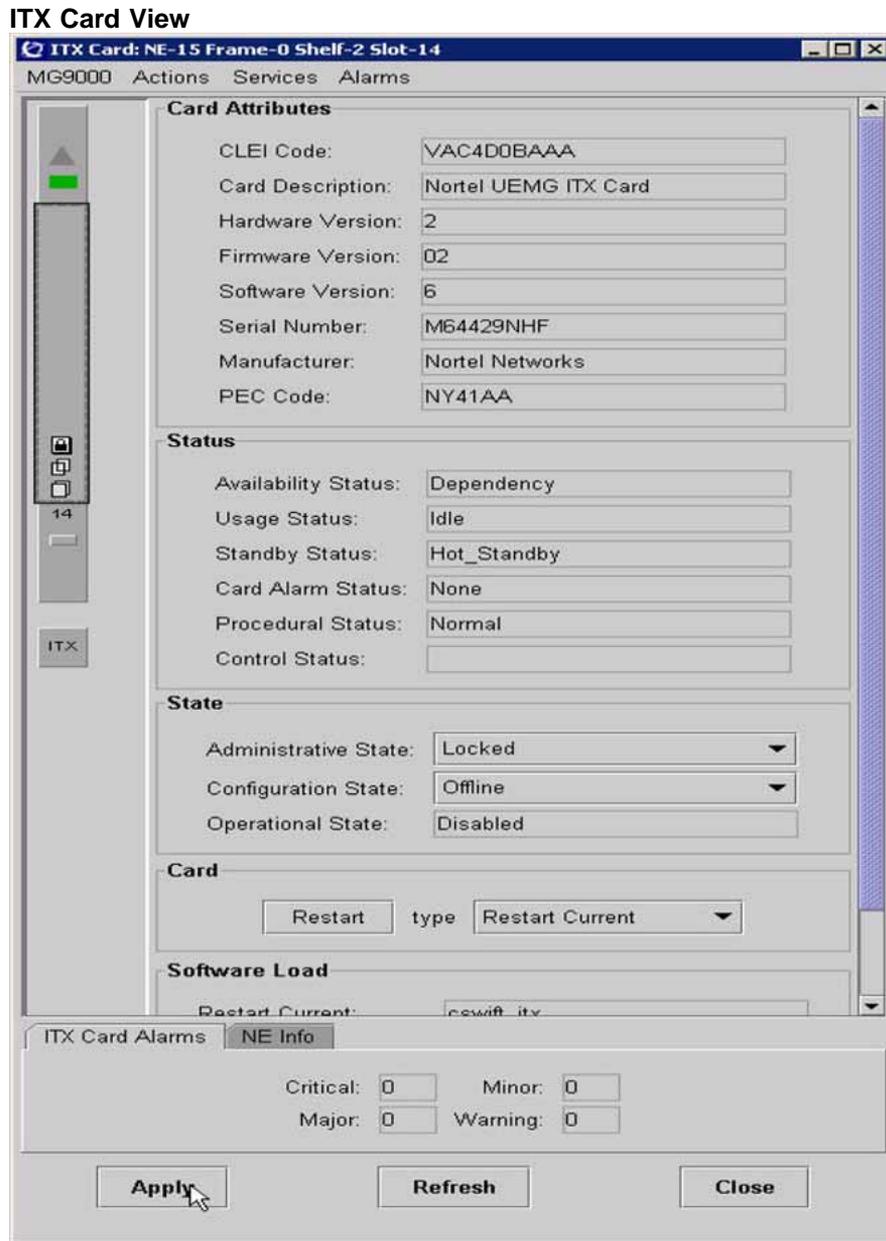
---

## Provisioning an ITX card

### When to use this procedure

Use the procedures in this section when it is necessary to provision additional ITX cards to support subtending shelves.

The following figure shows an ITX Card View.



## Prerequisites

The ITX cards must have been installed in pairs in the slots to be provisioned using correct ESD precautions. Appropriate cables have been connected to the faceplate of the ITX card according to the configurations requirements for the MG 9000.

**Note:** Ensure all provisioning requirements and considerations for growth are considered before provisioning additional ITX card.

## Action

The following procedure provides the steps for provisioning an ITX card.

### Provisioning an ITX card

Step	Action
<i>At the MG 9000 Manager</i>	
1	At the <b>Subnet View</b> , double click on the <b>MG 9000</b> that is to have the ITX card provisioned. The <b>Frame View</b> appears.
2	At the <b>Frame View</b> , double click on the shelf in which the ITX card resides. The <b>Shelf View</b> appears.
3	At the <b>Shelf View</b> , double click on the slot in which the ITX card resides. The <b>ITX Card View</b> appears. Since the ITX card is already installed, autodiscovery datafills the data about the card.  <b>Note:</b> When provisioning an ITX card, click <b>Refresh</b> at the bottom of the ITX Card View to synchronize the data between the MG 9000 and the MG 9000 Manager.
4	This procedure is complete.
—End—	

## De-provisioning a line card

### When to use this procedure

Use this procedure when it is necessary to de-provision one of the following line cards: ADSL, DS1, WLC, GLC, or SAA. This procedure may be used when it is necessary to move cards from one shelf or slot to another.

**Note:** After de-provisioning card and port data on the MG 9000, it is recommended that all provisioning information be recorded. Use the Save PLoA or Save SLoA services procedure to save provisioning information into a file that provides a list of all services on that network element.

### Prerequisites

A line card must be equipped in the slot to be de-provisioned.

### Action

The following procedure provides the steps for de-provisioning a line card in the MG 9000 shelf.

#### De-provisioning a line card

Step	Action
------	--------

##### *At the MG 9000 Manager*

- 1 At the **Subnet View**, double click on the **MG 9000** that is to have the line card de-provisioned. The **Frame View** appears.
- 2 At the **Frame View**, double click on the shelf in which the line card resides. The **Shelf View** appears.
- 3 At the **Shelf View**, double click on the slot in which the line card resides. The appropriate card view appears.
- 4 At the card view for the card to be de-provisioned, remove all DNs from the card to be de-provisioned. For example, remove all terminations from the WLC, GLC, SAA, or ADSL card or remove all private lines services (channelization, DS0 bundling) from a DS1 card.

**Note:** When a card is de-provisioned the associated terminations will be removed from the MG 9000 Manager, the MG 9000, and the SESM. To update the current list of configured terminations, use the Saving SLoA Services tool.

- 5 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 card with services, a warning message appears, informing the user that to proceed, Forced Lock must be used. Ensure all services and terminations have been removed before proceeding.
- 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. (If an Offline card is removed, a card of the same type may be inserted in the slot. The card and circuit data on the MG 9000 Manager are not affected.)
- 7 Set the Configuration State to Deprovision from the configuration state pull-down menu in the State pane. When a Deprovisioned card is pulled, the data for that card and associated circuits are removed from the MG 9000 Manager.

**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.

The card can be removed from the shelf.

- 9 This procedure is complete.

---

—End—

---

## Provisioning private lines services

---

### When to use this procedure

Use the following procedure to provision the private lines services.

**Note:** Provisioning private lines services is not supported on an MG 9000 in a UA-IP solution.

Included are the following procedures:

- "Provisioning private lines services" (page 163)
- "Accessing the PLoA Services Browser" (page 172)
- "Performing a bulk reconnect of PLoA services" (page 173)
- "Deleting private lines services" (page 174)
- "Saving PLoA Services" (page 175)
- "Diagnosing PLoA services" (page 176)

**Note 1:** After provisioning private lines services on the MG 9000, it is recommended that all provisioning information be recorded. Use the Save PLoA services procedure to save provisioning information into a file that provides a list of all services on that network element.

**Note 2:** When provisioning private lines data, or deleting a private lines data and an error occurs which precludes the process from completing, indicating corrupted data, perform "Auditing MG 9000 data" (page 284). If this does not clear the data corruption, refer to the "Reinitialize intelligent cards in the MG 9000" procedure in *MG 9000 Fault Management*, NN10074-911. This procedure is used to clear corrupted data out of the MG 9000. However, reinitializing the applicable cards is disruptive and is not for normal fault clearing activities.

### Prerequisites

Private lines services requires that:

- MG 9000 hardware has been discovered and communication established to the MG 9000 Manager
- ATM connectivity has been established and maintained
- DS1 card, port, or bundle has been unlocked
- channelization and bundles have been created for structured services

## Action

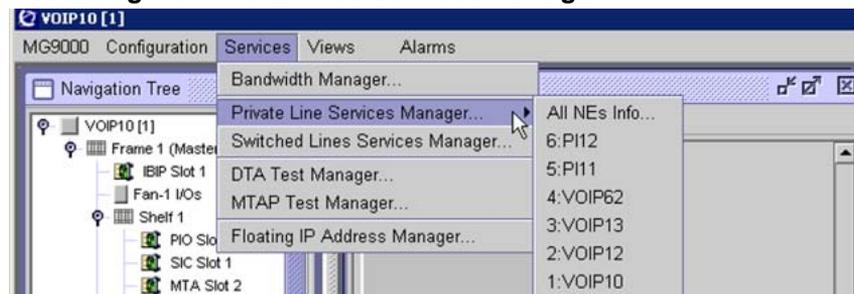
### Provisioning private lines services

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 At the **Subnet View**, double click on the **MG 9000** icon for which PLoA services are to be provisioned. The NE desktop view with Frame View appears.
- 2 From the **NE desktop view**, select **Private Lines Services Manager** from the **Services** menu and continue to the sub-menu which allows private lines services for all MG 9000s within the same subnet manager or private lines services for a specific MG 9000 to be displayed. To display services for all MG 9000s, select the sub-menu **All NEs info...** To display services for a specific MG 9000, select the specific NE from the sub-menu. When either sub-menu is selected a **Private Lines Services Manager** appears as shown in the following figure.

#### Accessing the Private Lines Services Manager



When either sub-menu is selected, a **Private Lines Services Manager** is opened that displays the appropriate services.

- 3 From the **Private Line Services Manager**, select the **Create** button.

**Note:** All private lines services which have been created on any MG 9000 within the same subnet manager are shown. This is because private line services are normally from one MG 9000 to another MG 9000 and require knowledge of the MG 9000s within the same subnet.

### Private Line Services Manager

CircuitId	LineType	AdminStatus	OperStatus	ProvType	PrimaryEM
10110173-10110174	Full	Unlocked	Enabled	Discov	Yes
10110171-10110172	Full	Unlocked	Disabled	Discov	Yes
10110177-10110178	Full	Unlocked	Enabled	Discov	Yes
10110175-10110176	Full	Unlocked	Enabled	Discov	Yes

Service sidebar buttons: Create, Delete, Lock, Unlock, Properties, Diagnose, Bulk Reconnect

Buttons: Refresh, Close

- 4 Provision the private line service from the **Private Line Service Creation** screen.

### Private Line Service Creation

Private Line Type: Full Private Line

Circuit Id: Full Private Line

CES Attributes:

- Clock Mode: Synchronous
- CAS: Basic
- Partial Fill: 0
- Maximum Buffer Size: 4775
- CdvRXT: 800
- Cell Loss Integration Period: 2500
- Recovery Priority: 127
- Red Line: Normal Line
- For Active Svc only:
  - First Retry Interval: 10
  - Retry Limit: 3

Active End Point:

- NE Number&Name: 8:co8
- Frame Number: Frame 0
- Shelf Number: Shelf 2
- Card Number: Slot 20 Card
- DS1 Port: Port 1 Unchannelized
- Carrier: Unchannelized DS1

Passive End Point:

- ATM Address: [Empty]
- NE Number&Name: 8:co8
- Frame Number: Frame 0
- Shelf Number: Shelf 2
- Card Number: Slot 20 Card
- DS1 Port: Port 1 Unchannelized
- Carrier: Unchannelized DS1

Buttons: Apply, Refresh, Close

The **Private Line Service Creation** screen is used to create services through MG 9000 end point definitions. An endpoint is one end of a private line service across an ATM network. End points represent the Interworking Function (IWF) used to provide interconnections of two Narrowband networks through an ATM

network using ATM Virtual Connections. The following table defines the four private line service type options available through the **Private Line Service Creation** screen.

#### Private line service types

Type	Explanation
Full Private Line	An ATM circuit emulation service that provides a permanent connection between two MG 9000s. A full private line contains a passive and an active end point. (This is used to cross MG 9000s within the network.)
Active End Point	One end of a half private line. The end point that initiates an ATM circuit emulation connection. (This is used when the passive endpoint is not in the network.)
Passive End Point	One end of a half private line. The end point where the ATM address is waiting for a connection or passively connected. (This is used when the active endpoint is not in the network.)
Hair Pin	A private line where both end points reside on the same MG 9000. With both connections on the local gateway, the hair pin connection does not connect to the ATM network.

**Note:** When an Active or Passive end point is recovered from the MG 9000 after restarting the MG 9000 Manager, the active and passive services are converted to Full Private Line service. This occurs when the active end point is created with a remote ATM address matching the ATM address of a passive endpoint on the same subnet.

The following table shows the data boxes and fields contained in the **Private Line Service Creation** screen. The GUI does not provide access to fields that do not apply to a selected **Private Line type**. The following table indicates when a default value exists for a field.

#### Private Line Service Creation data fields

Box	Field	Explanation
Private Line Type	Private Line Type	Select a Private Line Type. <ul style="list-style-type: none"> <li>• Full Private Line</li> <li>• Active End Point</li> <li>• Passive End Point</li> <li>• Hair Pin</li> </ul>

Box	Field	Explanation
CES Attributes	Circuit ID	Create a character string to provide a description for the circuit.  If one is not provided by the technician, then a default ID will be assigned based on the physical equipment over which the service being carried.
	Clock Mode	Define the DS1 service clocking mode. <ul style="list-style-type: none"> <li>• synchronous (default)</li> <li>• SRTS (not currently supported)</li> <li>• adaptive (not currently supported)</li> </ul> <p><b>Note:</b> Refer to the CES clocking options table for more information. The selection made here is based on the selection made at the DSI interface.</p>
	CAS	Select an AAL1 format. <ul style="list-style-type: none"> <li>• Basic (default)</li> <li>• DS1 SF</li> <li>• DS1 ESF</li> <li>• E1 (not currently supported)</li> <li>• J2 (not currently supported)</li> </ul> <p><b>Note:</b> The Basic (default) selection does not carry Channel Associated Signalling (CAS) bits.</p>
	Partial Fill	Enable partial cell fill and determine the number of user octets used in the ATM payload cell.  0 (zero) disables partial cell fill. (default)  A number from 1 to 47 defines the number of user octets and enables partial cell fill.
	Maximum Buffer Size	Define the maximum size, in 10 microsecond increments, of the reassembly buffer.  Values are 1 through 65536.
	CdvRxt	Define the maximum cell arrival jitter, in 10 ms increments, that the reassembly process can tolerate without producing errors on the CBR service interface.  Values are 1 through 65536.
	Cell Loss Integration Period	The cell loss integration time, in milliseconds.  Values are 1000 through 65536.

Box	Field	Explanation
	Recovery Priority	Define the recovery priority for an end point. Where 1 is the highest priority. 0 means no priority.  (not currently supported)  Values are 0 through 255. The default value is 127.
	Red Line	Determine if the endpoint is a special code of the CES IWF. Indicates if the circuit is a special line (such as 911). (not currently supported)
	First Retry Interval	The amount of time, in seconds, to wait before attempting to establish the SVC after the first failed call attempt. (Used only for the active side of a PLoA service.)  Values are 1 through 3600.  Valid for Full Private line and Active End Point only.
	Retry Limit	The maximum limit of consecutive unsuccessful call setup attempts allowed before ending the connection attempt. (Used only for the active side of a PLoA service.)  Values are 0 through 65535.  0 denotes infinite retry attempts.  Valid for Full Private Line and Active End Point only.
Active End Point	Node 9000 Number & Name	The defined name and number for the MG 9000 endpoint location.
	Frame Number	The sequential MG 9000 frame number endpoint location.
	Shelf Number	The shelf number endpoint location
	Card Number	The slot number endpoint location.
	DS1 Port	The port number endpoint location.
	Carrier	The private line carrier status. The status options appear in Table that immediately follows this table.
Passive End Point	ATM Address	The ATM net prefix address of the UNI. The ATM address is required for Active and Passive End Point lines. For Passive End Point lines, the GUI automatically fills in the ATM Address field after the Apply button has been selected. If the active end point is created with an address matching the address of a passive end point on the same subnet, then the active and passive services are converted to Full Private Line service.

An Active End Point service establishes a connection to a Passive End Point that has provided an ATM Address.

The allowed clocking options for CES is based on selections made at the DS1 port. SRTS can be used only when there is a common network card. When selecting the DS1 port from the DS1 port list in the Active End Point and Passive End Point panes of the **Private Line Service Creation window**, the word channelized or unchannelized follows the port number. This is used to determine the CES clock option that applies based on the port that was selected. The following table provides the CES clock options.

### CES clock options

DS1 clock option	CES clock option being configured	
	Unstructured (type of service created on an unchannelized DS1 port)	Structured (type of service created on a channelized DS1 port)
Looped	Synchronous, Adaptive, SRTS	Synchronous
Local	Synchronous, Adaptive, SRTS	Synchronous
Through	Adaptive, SRTS	Not an option

The following table shows the options that appear in the carrier field.

### Carrier Data field options

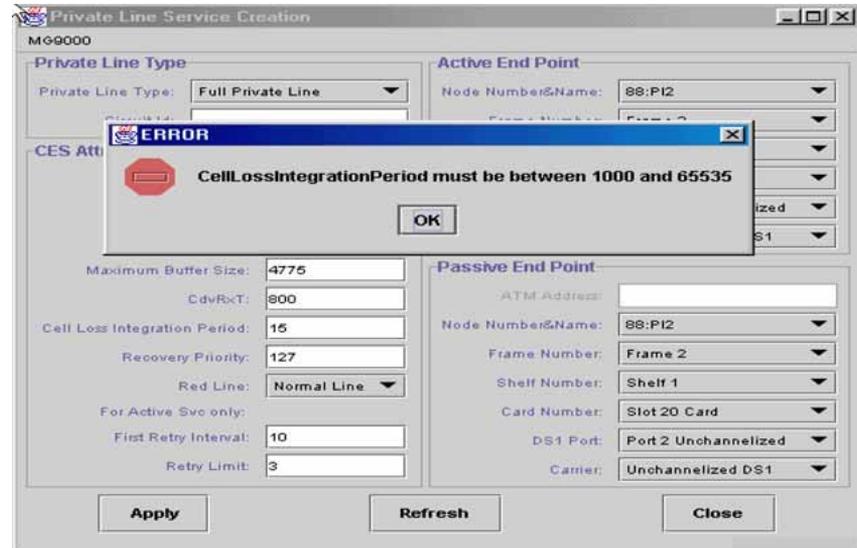
Option	Explanation
Unchannelized DS1	The selected DS1 port has not been channelized. The carrier provides full T1 service.
Channelized bundles	The selected DS1 port has been channelized and bundled. The "x" is a variable, used for identification, and shows the first channel in the bundle.
Channelized no bundles	The DS1 port has been channelized but no bundles have been created.

- 5 Select the **Apply** button to create the private line service. When the message in the status bar at the bottom goes away, indicating the service is successfully created, return to the **Private Line Services Manager** screen.

If any equipment is added or if DS0 bundles are created while the **creation** window is open, the Private Lines Service Creation view is updated automatically.

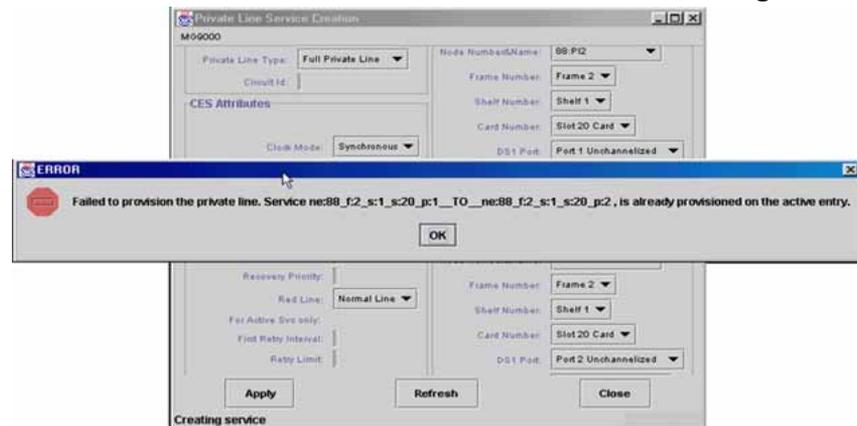
If the service creation data fields are invalid, a message indicating the first error encountered is displayed, as shown in the following figure.

#### Private Line Service Creation error message



If a service already exists on the endpoint being created, a message indicating which endpoint already has a service including the existing service name is shown.

#### Private Line Service Creation service creation error message



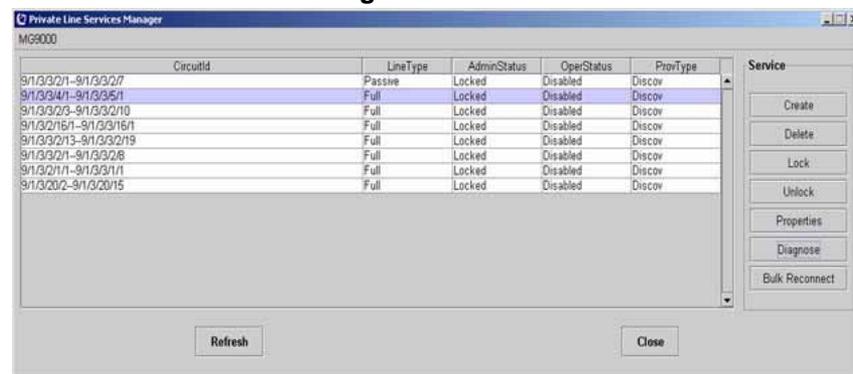
Management options from the **Private Line Services Manager** screen for a selected service include:

- delete the service or bulk delete all selected services
- lock the service or bulk lock all selected services
- unlock the service or bulk unlock all selected services

- show properties for the service
- perform ATM diagnostic tests on the service
- bulk reconnect all selected services

At the **Private Line Services Manager**, when the technician is ready for the private line service to go in service, select the **service**. Select the **Unlock** button to allow traffic flow.

#### Private Line Services Manager



Services whose OperStatus indicates disabled will not be able to carry traffic.

- 6 Select **Properties** to show the data properties of the created Private Line Service. The **Service Properties** screen appears as shown in the following figure. The properties of the service may be viewed any time after its creation.

## Service Properties screen

**Service Properties**  
MG9000 Actions

**Active End Point**

MG9000 Number:	9	ATM VPI:	0	Ctv RxT:	800
Frame Number:	1	ATM VCI:	417	Cell Loss Period:	2500
Shelf Number:	3	CBR Clock Mode:	Synchronous	Admin Status:	Locked
Card Number:	3	CAS:	Basic	Oper Status:	Disabled
DS1 Port:	4	Patial Fill:	0	Row Status:	Active
DS0 Bitmap:	000003	Buf Max Size:	4775		

**Passive End Point**

MG9000 Number:	9	ATM VPI:	0	Ctv RxT:	800
Frame Number:	1	ATM VCI:	418	Cell Loss Period:	2500
Shelf Number:	3	CBR Clock Mode:	Synchronous	Admin Status:	Locked
Card Number:	3	CAS:	Basic	Oper Status:	Disabled
DS1 Port:	5	Patial Fill:	0	Row Status:	Active
DS0 Bitmap:	000003	Buf Max Size:	4775		

**SVC Details**

Passive Endpoint Address:	39345678901234567890123a2a9999999900000c				
First Retry Interval:	10	Svc Oper Status:	Connected		
Retry Timer:	0	Last Release Cause:	8		
Retry Limit:	3	Release Diagnostics:			
Retry Failures:	0				

Refresh Close

**Note:** When existing bundles, that is, those bundles already persisted in the database either manually or automatically, are deleted and recreated for provisioning PLoA services, manually persist the data to the database. Refer to "[Persisting MG 9000 provisioning data](#)" (page 47). This action ensures proper recovery of PLoA services in the event of an MG 9000 Manager restart.

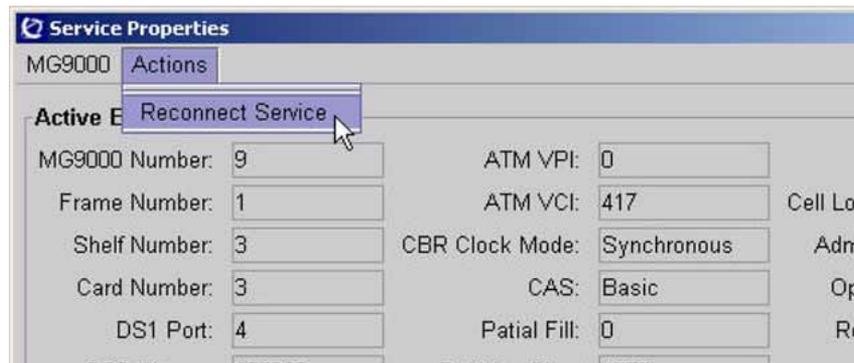
For active endpoints or full services, the SVC OperStatus indicates if the service is

- Connected
- In progress
- Failed
- Retries Exhausted
- NoAddress Supplied
- LowerLayerDown, meaning one of the lower layers, such as the ATM layer or the physical layer is down

The last release cause will indicate the cause for service connection failure.

One particular service can be reconnected by using the **Actions->Reconnect** command at the menu bar of the Service Properties view. The following figure shows the Reconnect command being accessed from the Service Properties view.

#### Accessing Reconnect Service from Service Properties



- 7 This procedure is complete.

---

—End—

---

#### Viewing PLoA services from the PLoA Services Browser

From the **Subnet View**, all PLoA services can be viewed and accessed by selecting **Configuration->PloA Services Browser** from the menu bar.

#### Accessing the PloA Services Browser

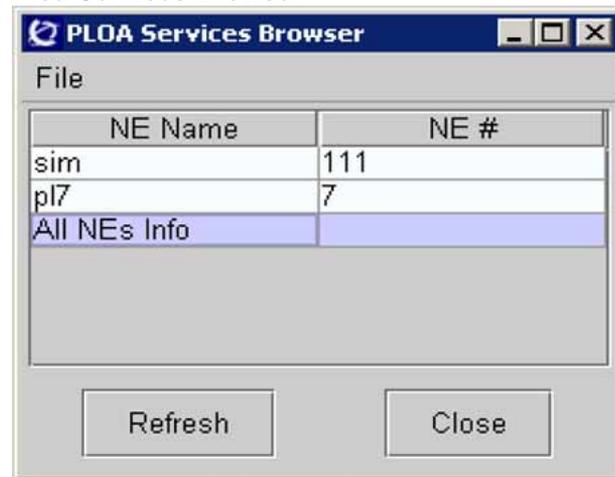
Step	Action
------	--------

##### *At the MG 9000 Manager*

- |   |   |
|---|---|
| 1 | At the <b>Subnet View</b> , select <b>Configuration-&gt;PloA Services Browser</b> . The <b>PloA Services Browser</b> appears. The following figure shows the PloA Services Browser. |
|---|---|

**Note:** When the MG 9000 Manager performs a restart or there is a failover condition (for offices with the N240 HA configuration), PLoA services are recovered from the database. The time it takes to recover depends on the number of PLoA services configured. During recovery, if the Private Lines Services Manager window is opened, no PLoA services will appear. Wait 15-20 minutes, if 300 or more PLoA services are provisioned, before opening the Private Lines Services Manager. No services are lost; this delay allows the MG 9000 Manager to finish updating following the restart or failover.

## Ploa Services Browser



- 2 To list all PLoA services on a network element, double click on that **NE name**. To view all PLoA services, double click on "**All NEs info**." The **Private Line Services Manager** appears.
- 3 This procedure is complete.

---

—End—

---

### Performing a bulk reconnect of PLoA services

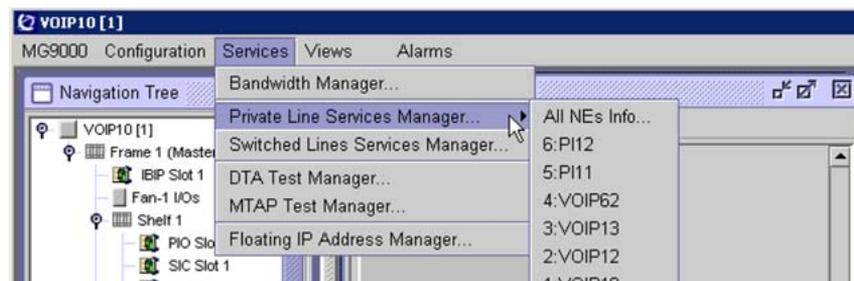
When it is necessary to perform a bulk reconnect of PLoA services in response to a network failure, use the following procedure.

### Performing a bulk reconnect of PLoA services

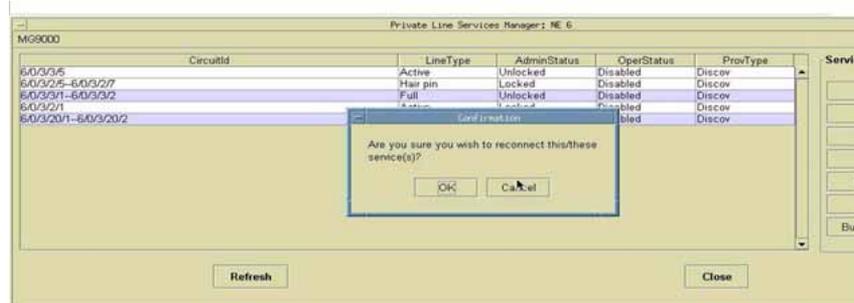
Step	Action
------	--------

#### *At the MG 9000 Manager*

- 1 At the **NE desktop view**, from the **Services** menu, select **Private Lines Services Manager**. The **Private Lines Services Manager** appears.



- 2 To select all the services to be connected, press and hold **Ctrl** and click to highlight the services.
- 3 Select **Bulk Reconnect** and respond to the confirmation message. The services will be reconnected.



- 4 This procedure is complete.

—End—

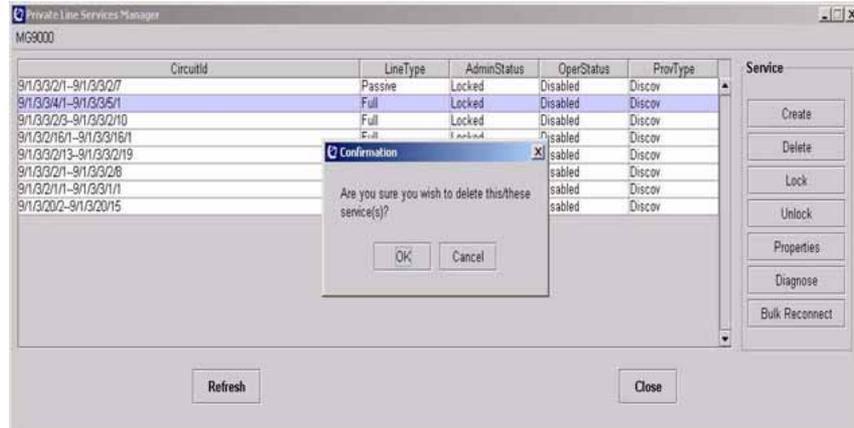
## Deleting private lines services

### Step Action

#### At the MG 9000 Manager

- 1 At the Frame View, from the **Services** menu, select **Private Lines Services Manager**.
- 2 Select the service which is to be deleted and select the **Lock** button if the service is unlocked. Click on **Ok** when prompted with the message Are you sure, the service(s) should be locked? The following figure shows the confirmation message.
 

**Note:** More than one service can be selected at a time.
- 3 Once the service is locked, select the **Delete** button.
- 4 Select **OK** when prompted with the message Are you sure you wish to delete this/these service(s)? The service will be deleted from the MG 9000 and removed from the **Private Line Services Manager** window. The following figure shows the confirmation message.

**Private Line Service Manager services deletion confirmation message**

5 This procedure is complete.

—End—

**Saving a list of PLoA services to a file**

When it is necessary to view all the services on the MG 9000, a listing of the private lines services can be obtained using the Save PLoA Services tool. This tool is also used to save a list the services to a flat file for inventory management or when manual re-provisioning is required, such as in the unlikely event that persistence is lost, and to preclude the need for writing the information manually. Files are written in both HTML and text format. The information is always output to the server. The directory in which the files are written to is the /tmp directory on the server and the file name is displayed in the information dialog message that is output. The user should FTP the file to any desired location to retain the information.

These files must be regularly moved to another directory since the /tmp directory is cleaned periodically.

The following procedure provides the steps for saving PLoA services information into a file.

**Saving PLoA Services****Step Action****At the MG 9000 Manager**

- 1 From the **Frame View**, access the Save PLoA Services tool from the **Actions** menu. The **Save PLoA services** dialog box appears as shown in the following figure.

**Save PLoA Services dialog**

- 2 The PLoA services have been saved into the file noted in the dialog box. Note the file name. Click **OK** to close the dialog box.
- 3 This procedure is complete.

---

—End—

---

**Diagnosing PLoA services**

On the **Private Line Services Manager**, there is a **Diagnose** button, which when clicked, displays the available private lines with corresponding virtual connections and associated endpoints available for testing.

When it is necessary to diagnose PLoA connections, perform the following procedure.

**Diagnosing PLoA services****Step Action*****At the MG 9000 Manager***

- 1 At the **Subnet View**, double click on the **MG 9000** icon on which PLoA services are to be diagnosed. The **Frame View** appears.
- 2 From the **Frame View** menu bar, select **Services->Private Line Services Manager** and choose whether to view all private line connections for all network elements in the subnet or choose one network element.
- 3 Select a private line to be tested then click on **Diagnose**. Depending on the line type selected, full or passive, a Passive Endpoint ATM Diagnostics view or Full Private Line Diagnostics view appears.

There are two kinds of maintenance actions, loopback test and continuity check, which appear as four tabbed panes corresponding to each test:

- loopback tests - provides the ability to send out a loopback OAM cell to verify the existence of connectivity for an entire connection (end-to-end) or a segment of a connection.
  - End to End Loopback Test
  - Segment Loopback Test
- continuity checks - provides the ability to perform a continuity check for an entire connection (end-to-end) or a segment of a connection.
  - Segment Continuity Check
  - End to End Continuity Check

- 4 Click on the appropriate tab based on the kind of test to be performed.
- 5 Click **Execute** to start the test. The Current Status field changes from Not Activated to Activation Requested to Activated. The system reports the test status in the Test Owner Details panel. Click **Query** to query the status of the test and the results are displayed in the Results field as Success or Failed. If the test failed, the reason is displayed.

If the test is complete, a message dialog box appears indicating the test is complete.

If the technician clicked **Abort** to stop the test and then clicked on **Query**, the message dialog will indicate the test is aborted.

**Note:** If the Diagnostics GUI is closed after starting a test, the test is aborted.

- 6 This procedure is complete.

---

—End—

---

---

## Provisioning switched lines services

---

### When to use this procedure

Use these procedures when provisioning switched lines services. The following procedures are included in this section.

- "Adding a VMG" (page 181)
- "Displaying a termination" (page 195)
- "Deleting a VMG" (page 196)
- "Changing VMG data" (page 197)
- "Changing VMG Market Country/Operator data" (page 197)
- "How to refresh data in Switched Lines Services GUI screens" (page 198)
- "Listing all VMGs using the VMG Browser" (page 199)
- "Provisioning ESA" (page 201)
- "Viewing termination ESA data" (page 215)
- "Provisioning an ESA Pretranslator" (page 216)
- "Deleting a service code translation" (page 219)
- "Downloading ESA data" (page 220)
- "Disabling ESA in a VMG" (page 221)
- "Saving SLoA services" (page 223)

**Note 1:** After provisioning switched lines services on the MG 9000, it is recommended that all provisioning information be recorded. Use the Save SLoA services procedure to save provisioning information into a file that provides a list of all services on that network element.

**Note 2:** When provisioning VMG data, changing VMG data, creating a termination, or deleting a termination and an error occurs which precludes the process from completing which indicates corrupted data, first perform the "Auditing MG 9000 data" (page 284) procedure in this document. If this does not clear the data corruption, refer to the "Reinitialize intelligent cards in the MG 9000" procedure in *MG 9000 Fault Management*, NN10074-911 and reinitialize the shelf's pair of ITP cards. This procedure is used to clear corrupted data out of the MG 9000. However, reinitializing the applicable cards is a last resort. It is disruptive and is not for normal fault clearing activities.

**Note 3:** After the site and office frame number are provisioned in the Frame Provisioning Information view (using "Provisioning a MG 9000

[frame physical location](#) (page 66)), the user need not input the site and frame location information when provisioning VMGs. When the location is selected during non-ABI VMG provisioning, the Site Name, Office Frame Number, and VMG name fields automatically reflect the site and office frame number for the selected frame.

### What is a Virtual Media Gateway?

Switched lines services use a VMG to divide the physical hardware into logical entities. A VMG can be thought of as a container for terminations. A termination is a logical representation of a circuit. There is a one-to-one mapping between terminations and circuits.

When examining a termination and VMG combination, the circuit can be revealed. For example; if the termination "tp/5/15" is contained in a VMG named "CO10007-0-1", it can be determined that the termination is on Frame 7, Shelf 1, Slot 5, and circuit 15. See the figure titled "[Provision a Virtual Media Gateway window](#)" (page 182) in the following procedure. The VMG name and termination points have the following formats:

SITExxx-y-z tp/aa/bb, where

- xxx is the office frame number (000 to 511)
- y is the internal frame number, which is set to 0

**Note:** VMGs provisioned in SN05/SN06+ with a non-zero Internal frame number, continue to exist as they are, that is, the VMGs continue to exist with a non-zero Internal frame number.

- z is the shelf number (0 to 9)
- aa is the card number (02 to 09 and 14 to 21)
- bb is the circuit number (00 to 47)

The line equipment numbers (LEN) associated with MG 9000 lines are determined based on the VMG and termination names. The following table shows the method used to calculate the LEN number.

Value	Format	Example
Physical MG 9000 name	<site><cf><any string>	HOST001-123-MAINST-LSVGNV
Virtual MG Name + TP	<site><cf>-<rf>-<rs> tp/<ss>/<cc>	HOST001-0-2 tp/03/04
LEN format	<site><cf><rs><ss><cc>	HOST 01 2 03 04

The abbreviations in the previous table are defined as follows:

- site - a site name from the XA-Core table SITE

- cf - a contiguous frame or office frame which is the frame number in the office. This field must be three characters where the maximum is 511. Office frame numbers less than 100 are padded with a zero (0), for example 99 appearing as 099. Office frames less than 10 are padded with two zeros (00), for example 9 appearing as 009 when the VMG names are generated. The ServOrd+ query commands will only pad one zero if the number is less than 10 but will still show the full number if the number is greater than 99.
- rf - a relative frame which is the offset of the VMG frame inside the physical MG 9000 (0-7).
- rs - a relative shelf which is offset of the VMG shelf inside the VMG frame (0-3).
- ss - a slot which is the holder of one line card on a frame. This field will be padded with a zero (0) if less than 10, for example 9 appearing as 09.
- cc - a physical line circuit on a card. This field will be padded with a zero (0) if less than 10, for example 9 appearing as 09.

### **Silence suppression in the UA-IP solution**

Silence suppression is a mechanism meant to reduce bandwidth of voice calls in the UA-IP solution. Silence suppression uses a voice activated detector (VAD) to detect periods of silence in a call and then send special silence insertion descriptor (SID) packets in place of silence encoded into voice packets. For silence suppression to be enabled on an MG 9000, the following must be provisioned:

- At the GWC, the comfort noise box available from the Network Configuration panel must be set to On. The comfort noise box is Off by default.
- In the Switched Lines Services Provisioning window, in the GW Config tab, the Voice activity detector must be enabled.

### **Prerequisites**

The appropriate POTS 32, GLC32, SAA, or ADSL line cards or DS-512 (ABI) cards are installed in the shelf.

When provisioning VMGs on a UA-IP MG 9000, and silence suppression is to be used, the comfort noise box at the SESM Network Configuration level must be checked.

The floating IP address must be provisioned for the MG 9000 before Enhanced ESA can be enabled for VMGs on the MG 9000. To provision a floating IP address, refer to "Provisioning a floating IP address" in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450.

Ensure the security values in the Office-Wide Defaults GUI in the Subnet View have been provisioned before provisioning VMGs. Refer to "[Provisioning office-wide defaults](#)" (page 27) for more information.

For information about downloading security certificates for the OAMP link for an NE or modifying Public Key Infrastructure (PKI) options (such as Call links), for the VMGs, you must refer to *Nortel CVoIP IPsec Security Service Implementation Guide*, NN10453-100.

## Action

### Adding a Virtual Media Gateway

When adding a VMG, use the following guidelines to avoid data corruption and a mismatch of configuration data between the MG 9000, MG 9000 Manager, SESM, GWC, and Core:

- Always provision a VMG from the MG 9000 Manager.
- After the VMG is created, set the ESA flag to ON. (This will allow recovery of the directory numbers from the MG 9000 when the network element is deleted from MG 9000 Manager using the Delete Node command.)
- Use the correct VMG format identified at the beginning of this section.
- Make sure no extra spaces are present in the VMG name or in IP addresses.

Use the following procedure to add a virtual media gateway.

### Adding a VMG

Step	Action
------	--------

#### *At the MG 9000 Manager*

- |   |  |
|---|--|
| 1 | From the <b>Subnet View</b> , double click on the <b>MG 9000</b> icon on which switched lines services are to be provisioned. The <b>NE desktop view</b> with <b>Frame View</b> appears. |
| 2 | At the <b>NE desktop view</b> , from the menu bar select <b>Services-&gt;Switched Lines Services Manager</b> . The <b>Switched Lines Services view</b> appears.                          |
| 3 | Select the <b>Create</b> button from the Switched Line Services view. The <b>Provision a Virtual Media Gateway view</b> appears.   |

The following figure shows the Provision a Virtual Media Gateway view.

**Provision a Virtual Media Gateway window**

- 4 Select the type of VMG from the top most combo box: (ABI-ATM, ITP-ATM, ITP-IP, or ABI-IP). The VMG types are related to the PEC code for the ABI or ITP cards installed in the MG 9000 and are listed next:

- ABI-ATM - NTNY43AA in UA-AAL1 solution
- ABI-IP - NTNY43BA in UA-IP solution
- ITP-ATM - NTNY30AB in UA-AAL1 solution
- ITP-IP - NTNY30CA or NTNY30BA in UA-IP solution

**Note:** If Frame location information for a VMG is only partially available, then Frame location information was not pushed to the SESM while provisioning ITP VMGs. When this occurs, the Frame location information must be provisioned completely and then reprovision the VMG.

Frame location information for a frame is considered only partially available when only Logical Frame number, Office Frame number, site name are available and the remaining parameters floor, row, and framePos are not available or set. Frame location information becomes partially available if the NE is deleted from the MG 9000 Manager and rediscovered from the MG 9000.

- 5 Select the physical location for the VMG's type from the second combo box. This combo box will have a list of all possible locations for the type of VMG that was selected in [step 4](#).
- 6 The next step depends on the information in the following table.

If	Do
ITP-ATM or ITP-IP was selected in <a href="#">step 4</a>	<a href="#">step 8</a>
ABI-ATM or ABI-IP was selected in <a href="#">step 4</a>	<a href="#">step 7</a>

- 7 For ABI VMGs, the Virtual Media Gateway Name field is editable. Append an LGC node number to the end of the provided external XPM (EXPM) string.
- 8 In the Provision a Virtual Media Gateway window the GUI automatically supplies the VMG name, simply click the **Apply** button. The GUI conforms to the following naming convention:  
`<site><cf>-<rf>-<rs> tp/<ss>/<cc>`  
 Provisioning of the VMG will not proceed until all the following requirements are met.
- The VMG name must begin with an alphabetical character.
  - The VMG name must contain only alphanumeric characters and the delimiter "-".
  - VMG names must be unique across the network.
  - The VMG name seen at the CS 2000 GWC Manager GUI matches the one created by the MG 9000 Manager GUI.
- 9 The Switched Line Services provisioning screen contains the following seven tabs. Each tab provides a different provisioning view.
- ESA Config (refer to "[Provisioning ESA](#)" (page 201) later in this section)
  - GW Config
  - GW Controller Config
  - GW Market Config
  - GW Status Config
  - GW Security Config (addressed in [step 20](#))
  - GW Termination Config (refer to "[Displaying a termination](#)" (page 195) later in this section)
- Note:** The status information in the GW Configuration and GW Controller Config tabs are not updated in real time. Use the **Refresh** button on the tab to update the values in the status fields.
- 10 Select the **GW Config** tab and enter the following information:
- Gateway Controller Name: GWC-<unit number>
  - Signaling Address: <ITP or ABI card CIPOA address>
  - Bearer Address (only applies to ABI-IP or any VMG on an MG 9000 with GigE)

**Note:** For all other VMG types, the Bearer Address is set to the Signaling Address value.

- Port: 2944
- Protocol: MEGACO/H248
- Administrative Status: Unlocked

When an ITP-IP or ABI-IP VMG is provisioned, the silence suppression and quality of service (QoS) threshold values must be entered.

Use the following table when provisioning these values.

**GWC Config tab - Silence Suppression and QoS Thresholds values**

Function	Field	Entry	Explanation
Silence Suppression	Voice Activity Detection Mode	Off, transparent, conservative, aggressive	Silence Suppression parameter controlling how voice activity should be detected.
	Comfort Noise Generation Mode	Off, white, pink, spectral	Silence Suppression parameter controlling comfort noise generation.
QoS Thresholds	Packet Loss (%)	Default is 0.01%	Maximum acceptable value of (QoS threshold) for the percentage of packets lost in a 15 minute interval. Also, if the value for a particular call is above this threshold, then the call is counted as a 'bad call'.

Function	Field	Entry	Explanation
	Latency (mSecs)	Default is 150 ms	Maximum acceptable value (QoS threshold) for the one-way delay in a 15 minute interval (averaged) for Latency. Also, if the value for a particular call is above this threshold, then the call is counted as a 'bad call'.
	Jitter (mSecs)	Default is 100 ms	Maximum acceptable value (QoS threshold) for jitter in a 15 minute interval (averaged). Also, if the value for a particular call is above this threshold, then the call is counted as a 'bad call'.
	Bad Calls (%)	Default is 0%	Maximum acceptable value (QoS threshold) for the percentage of bad calls over a 15 minute interval. Also, if the value for a particular call is above this threshold, then the call is counted as a 'bad call'.

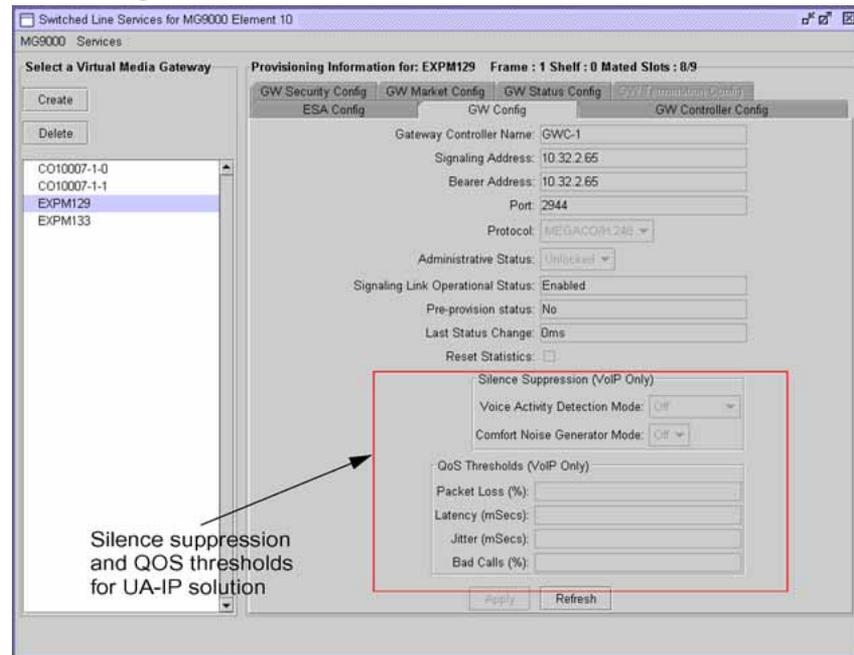
Select **Apply** when done.

**Note 1:** When **Apply** is selected for an ITP VMG (IP or ATM), the entered information is used to obtain the GWC IP from the Carrier VoIP Element Subnode Management (SESM). Once obtained, this IP is displayed on the GWC Configuration tab. Also, the VMG information is propagated to the SESM so that both the MG 9000 Manager and the SESM contain the same VMG information. All the terminations that may be associated with the VMG are provisioned in the MG 9000 Manager, the GWC, and the SESM when Apply is selected.

**Note 2:** For ABI VMGs (IP or ATM), frame location information (frame type [MG9F], floor position, row position, frame number, shelf number, and card slot) is sent to the SESM.

The following figure shows the GW Config tab window.

**GW Config tab**



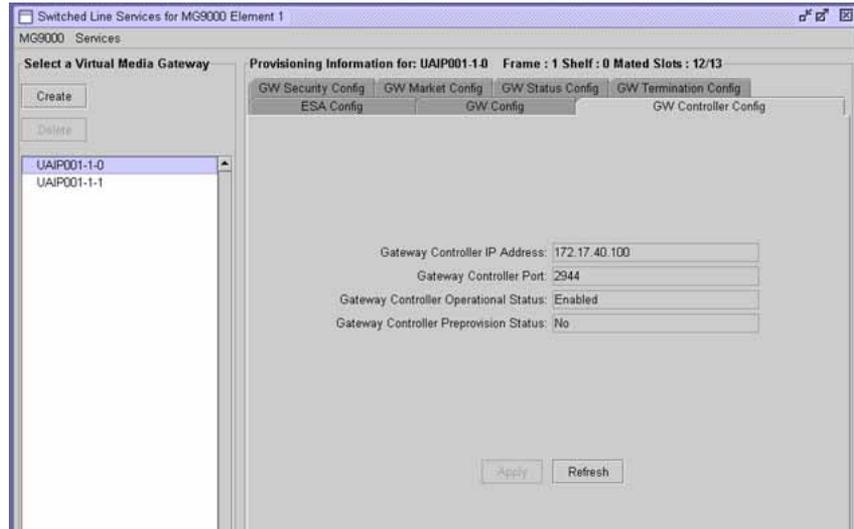
11 The next step depends on the information in the following table.

If	Do
this is an ITP VMG	<a href="#">step 13</a>
this is an ABI VMG	<a href="#">step 12</a>

12 Select the **GW Controller Config** tab and enter the following information:

- Gateway Controller IP Address
- Gateway Controller Port: enter 2944

The following figure shows the GW Controller Config tab.

**GW Controller Config tab**

Click **Apply**.

- 13** The next step depends on the information in the following table.

If	Do
Market Fit information was provisioned from the Subnet View using the Configuration->Office-Wide Defaults command. This default data is to be used for the VMG.	Click <b>Apply</b> . Go to <a href="#">step 15</a> .
Market Fit information needs to be changed for the MG 9000 Manager VMGs	<a href="#">step 14</a>

- 14** To provision the market data, select the **GW Market Config** tab and select the Market Fit based on the Country/Operator that applies from the pull down. If the Country/Operator does not appear, click on **Get Market** to retrieve a list.

**Note 1:** If the VMG is in-service and enabled, the market information can be changed if the market belongs to the same country code as that of the set market.

**Note 2:** For any VMG, the value that you select from the Country/Operator field must be the same as that which was chosen during the provisioning of the NE. After the VMGs are created, the market can be modified only if the new market selected belongs to the same country code as that of the set market. If the user tries to select a market which does not belong

to the same country code, an error message is displayed. If there are no VMGs, the market can be modified to any other market (different country code). When the line coefficient audit runs, those coefficients are sent to the GW.

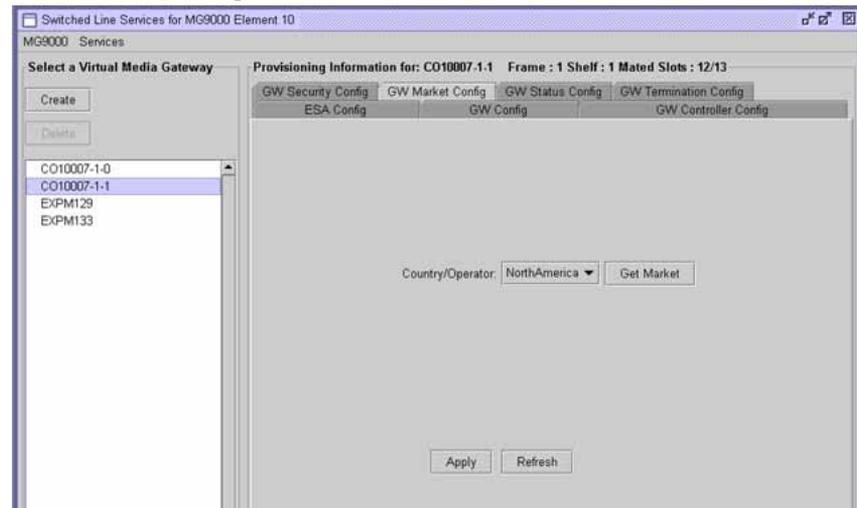
**Note 3:** To successfully provision a set of data pertaining to the selected country, the selected VMG must be out-of-service before clicking the **Apply** button. When the **Apply** button is clicked, a **warning message** appears with user confirmation required before the ITP card is restarted.

**Note 4:** After selecting the **Country/Operator** from the pull down and clicking on **Apply**, this triggers provisioning of the VMG and subsequently the MG 9000. While this operation is in progress, the buttons and pull down list will become disabled until the operation is complete. If an error occurs during provisioning, the user will be notified using a pop-up dialog box that contains details of the error.

Select **Apply** when done.

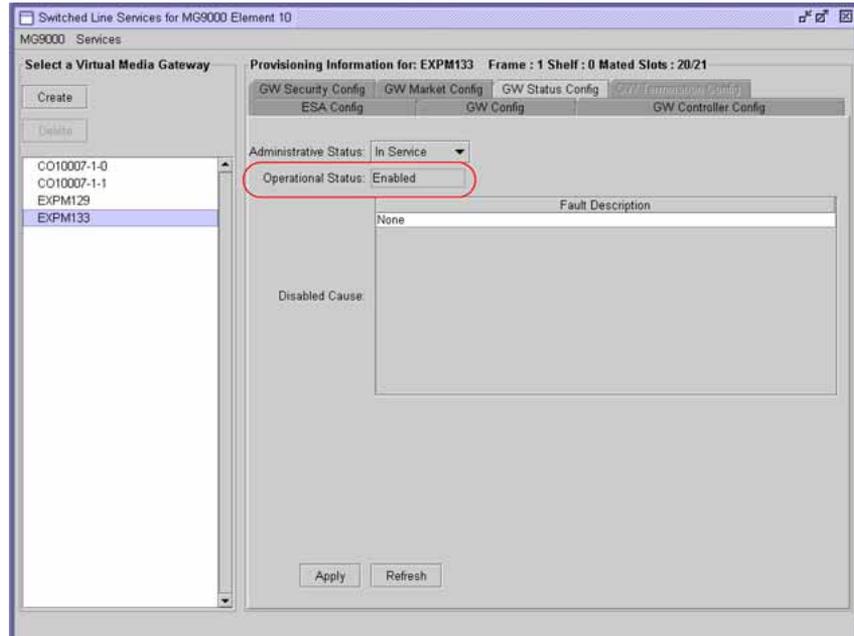
The following figure shows the GW Market Config tab window.

#### GW Market Config tab



- 15 The GW Status Config tab will be activated. If not already set change the Admin status to In Service. Select **Apply** when done.

The following figure shows the GW Status Config screen after successfully provisioning a VMG, with the Operational Status as Enabled.

**GW Status Config screen showing a successful VMG provisioned**

The following figure shows the GWC Status Config screen after a VMG provisioning failure, with the Operational Status as Disabled.

**GW Status Config screen showing a VMG provisioning failure**

The following table lists the VMG faults that appear in the Fault Description pane, the related VMG logs that are output at the alarm browser.

#### VMG faults seen in Fault Description pane

Fault type	VMG log report	Description
vmgAdminStatusOutOfService	VMG322	VMG is administratively set to out of service
vmgOOSCardLocked	VMG323	Card is locked
vmgOOSCardDisabled	VMG324	Card is disabled
vmgInitializing	VMG325	Card is initializing
vmgOOSLineMtcNotReady	VMG328	Line maintenance is not ready
vmgOOSMegacoMtcNotReady	VMG329	Card is locked or disabled
vmgOOSGWCUnreachable	VMG373	Pings to reach GWC failed
vmgOOSNoReplyFromGWC	VMG374	GWC unreachable, but no reply to service change. Check LGRP/GWC state, call processing is out of service.
vmgOOSAAL1BearerSubsystemOnPairNotReady	VMG376	AAL1 bearer not ready
vmgOOSIPBearerSubsystemOnPairNotReady	VMG377	IP bearer not ready

#### 16 The next step depends on the information in the following table.

If	Do
If VMG374 is seen in Fault description pane	<a href="#">step 17</a>
VMG faults were seen in Fault description pane	Clear the VMG faults as described in "Clearing MG 9000 ITP card and VMG alarms" in <i>MG 9000 Fault Management</i> , NN10074-911. When complete, return to <a href="#">step 15</a> .
the VMG did not come in service after clearing the fault and after the second Apply attempt	<a href="#">step 17</a>
no faults are seen	<a href="#">step 18</a>

**At the XA-Core MAP terminal**

- 17** Set the VMG in service by performing the following steps:
- At the XACore MAP terminal, type  

```
> MAPCI;MTC;PM;LGRP
```
  - Post the logical group (LGRP) representing the VMG by typing  

```
> Post lgrp <lgrpno>
```

 where  

```
lgrpno
```

 is the logical number of the VMG, such as lgrp 01 0
  - Busy the posted LGRP by typing  

```
> BSY
```
  - Return the LGRP to server by typing  

```
> RTS
```

For more information, refer to "Provisioning lines on the MG 9000 using the MAP interface" in *Communication Server 2000 Configuration Management*, NN10105-511.
  - Go to [step 15](#) to set the VMG in service.

**At the MG 9000 Manager**

- 18** The next step depends on the information in the following table.

If provisioning the VMG was	Do
successful	<a href="#">step 20</a>
not successful	<a href="#">step 19</a>

- 19** Determine the reason for the VMG provisioning failure by performing the following steps until the failure is cleared:
- Ensure the VMG was put in service from both the MAP terminal and the MG 9000 Manager as directed in [step 15](#) and [step 17](#).
  - At the **MG 9000 Alarm Browser**, check for alarms against the MG 9000 network element, especially an alarm for locked DCC cards. Clear the alarm. Refer to *MG 9000 Fault Management*, NN10074-911
  - Check the service state of the GWC. Refer to *GWC Fault Management*, NN10202-911.
  - In the Switched Lines Services screen, in the GW Controller Config tab, verify that the IP address for the VMG is correct, and for ABI VMGs, that the correct GWC was entered.

- e. If this is the first ITP VMG, or the first ABI VMG provisioned on this NE, access the LCI and verify that the Call Control subnet (for ITP VMGs) or ABI subnet (for ABI VMGs) has been provisioned.
  - f. If this is an ABI VMG, verify that the LGRP has been provisioned on the CS 2000, verify that the IP address for the VMG is provisioned on the correct GWC.
  - g. Ping the Multiservice Switch 15000 and SAM21 shelf controller IP addresses. A lack of response may reveal some place in the network that is not configured correctly or is having a problem. Refer to the "Connection test tool" procedure in *MG 9000 Fault Management*, NN10074-911.
  - h. If the problem cannot be cleared, contact Nortel Global Product Support for assistance.
- 20** You must define the security parameters to be used to secure the call control link between the VMG and the GWC. For details on how secure the Call Server 2000 office, see *Nortel ATM/IP Solution-level Security and Administration*, NN10402-600. For information on provisioning IPSec between the VMG and the GWC, see *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100.

**CAUTION****Risk of communication disruption, loss of service, or outage.**

To define security parameters, you must use the procedures documented in *Nortel ATM/IP Solution-level Security and Administration*, NN10402-600 and *Nortel CVoIP IPSec Security Service Implementation Guide* NN10453-100

- 21** This procedure is complete.

---

—End—

---

**How terminations are created and their format**

Terminations are created by the MG 9000 Manager when one of the following occur:

- a VMG is created
- a line card is set to the Offline state after having been Deprovisioned
- a new line card is inserted and is discovered by the MG 9000 Manager
- a new line has been provisioned from OSSGate, if the termination was not created by one of the three events listed above

## Configuring a termination

When configuring a termination use the following guidelines to avoid data corruption and a mismatch of configuration data between the MG 9000, MG 9000 Manager, SESM, GWC, and Core:

- All line/terminations may be configured by using OSSGate/SERVORD+ or from the Core using SERVORD. Since the ESA flag is turned On, the directory number will be sent to the MG 9000. When a termination is successfully configured, the next time this termination is selected from the GW Termination Config tab, the termination's updated status will be displayed. However, if this termination is already selected, click the Refresh button on the GUI to retrieve the updated status.
- For Basic ESA, the directory number for a termination must only be changed using OSSGate/SERVORD+ CDN or CTP command.
- For Enhanced ESA, line/terminations may be configured from the Core using SERVORD or by using OSSGate/SERVORD+.

**Note:** If you change the DN from the MG 9000 Manager, it will not change the data at the Core. Such a situation leads to data inconsistency. Therefore always use OSSGate/SERVORD+ or Enhanced ESA download to ensure data at the Core, SESM, and MG 9000 Manager are correctly changed / rolled back in the event of any operational failure.

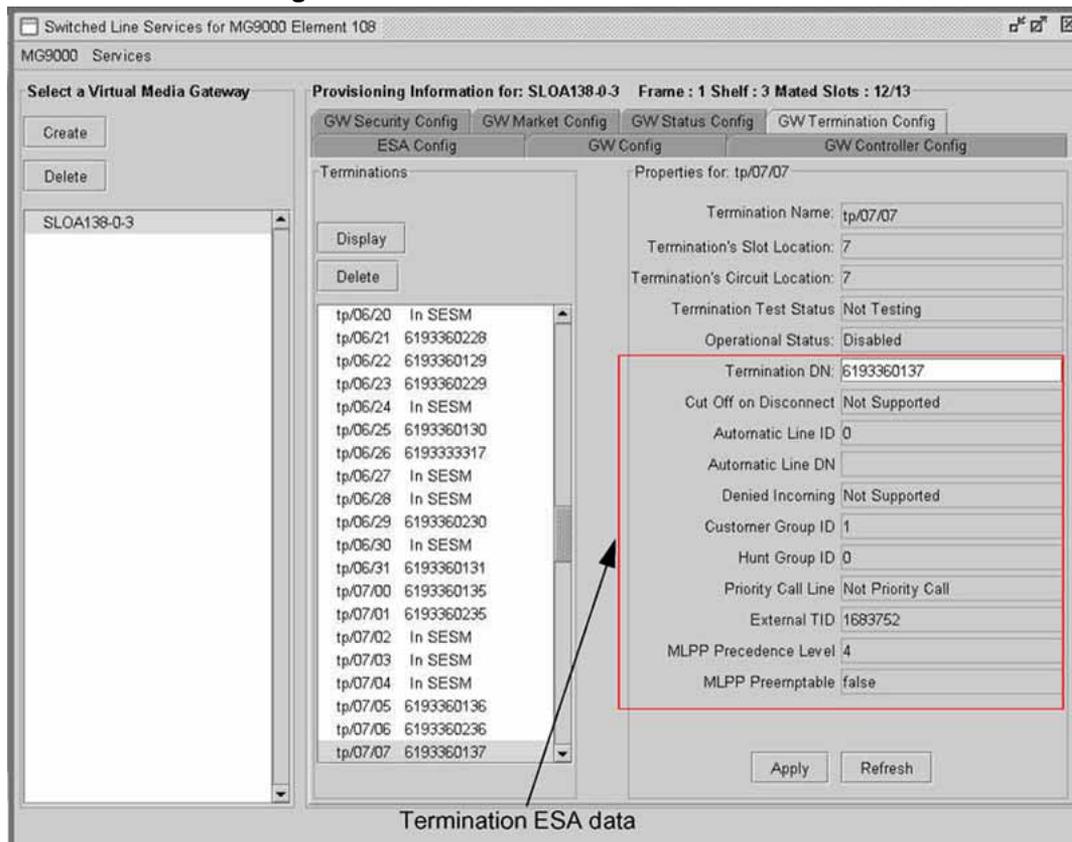
## Displaying a termination

There are two ways to view termination information. First is to view the termination information displayed in the GW Termination Config Tab. The second is to click on the **Display** button within the same window and any unprovisioned terminations will appear.

The following figure shows the GW Termination Config tab window.

**Note:** The fields outlined in red in the following figure are applicable to ESA data and are described later in "[Viewing termination ESA data](#)" (page 215).

## GW Termination Config tab



The GW Termination Config tab gives the associated card status for each termination whenever a DN does not exist. The following are the status indicators:

- In SESM - indicates the terminations on an associated card have been added to SESM. Terminations cannot be deleted for this case. This is the normal case.
- Not in SESM - indicates the terminations on an associated card have not been added to SESM. Terminations can be deleted for this case.
- DN - a DN appears in place of the status next to the termination name whenever a DN exists.
- Unknown - indicates the card associated with the termination is not available. When this occurs, deletion of the termination is allowed.

The termination naming convention is as follows:

tp/<ss>/<cc>

**Note:** Termination names begin with "tp/" followed by the slot number (ss), a "/", and finally the circuit number (cc).

Use the following procedure to display a termination.

### Displaying a termination

---

#### Step Action

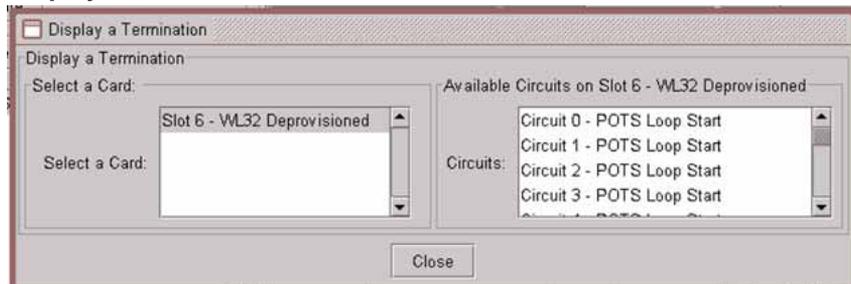
---

#### *At the MG 9000 Manager*

- 1 Click on the **GW Termination Config** tab and use this tab to display the circuits (lines) registered in the Gateway Controller.
- 2 To view specific information on an individual termination, click on that **termination** from the Terminations list. Properties for the termination are provided in the Properties pane on the right.
- 3 To view unprovisioned terminations, from the Terminations portion of the window, select **Display**.
- 4 The system locates all circuits that do not already have an associated termination. The **Display a Termination window** appears allowing the user to view unprovisioned termination(s) based on this information.

The following figure shows the Display a Termination window.

#### Display a Termination window



- 5 This procedure is complete.

---

—End—

---

### Deleting a termination

Terminations are deleted automatically when a line card is deprovisioned or when a VMG is deleted. When a termination is seen as "Unknown" at the GUI, meaning no line card is provisioned to connect to the termination, the termination can be deleted manually by selecting the "unknown" termination on the **GW Termination Config** tab, then clicking on **Delete**.

### Deleting a VMG

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

Step	Action
1	Deletion of the VMG must always be done from the MG 9000 Manager by a user with Admin privileges.
2	Before a VMG is deleted, all lines associated with the VMG must be removed from SESM, Core, GWC, and MG 9000 using the OSSGate. Use the following steps: <ol style="list-style-type: none"> <li>Launch the CS 2000 Management Tool Manager. Access table DNINV and list all DNs associated with the VMG or at the Switched Lines Services Manager, select the <b>VMG</b>, then select the <b>GW Termination Config</b> tab to list all the circuits associated with the VMG.</li> <li>Use the OSSGate to remove the lines.</li> <li>Repeat <a href="#">step 2a</a> and verify that the line data does not show up in the MG 9000 Manager.</li> </ol>
3	Deletion of the VMG will be blocked at the MG 9000 Manager if there are lines associated with that VMG in the SESM.

—End—

Use the following procedure to delete a VMG.

### Deleting a VMG

Step	Action
<i>At the CS 2000 GWC Manager</i>	
1	Set the associated VMG terminations to be deleted to out of service.
<i>At the MG 9000 Manager</i>	
2	From the <b>Services</b> menu, select the <b>Switched Lines Services Manager</b> .
3	Delete the VMG by selecting <b>Delete</b> .

The VMG will also be deleted from the CS 2000 Management Tools server. If the VMG fails to be deleted from SESM, unless the user attempting to delete the VMG has admin privileges, the deletion cannot continue.

The tuple for the VMG in table MTAVERT must be deleted before it can be deleted in the GUI.

- 4 This procedure is complete.

---

—End—

---

### Changing VMG data

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 From the **GW Status Config** tab, set the Administrative Status of the VMG to Out of Service.

**Note:** Setting the VMG to out of service is service affecting and a warning message is output.

- 2 From the **GW Config** tab, the Administrative Status may be changed.
- 3 From the **GW Status Config** tab, set the Administrative Status of the VMG to In Service if desired.
- 4 This procedure is complete.

---

—End—

---

### Changing VMG Market Country/Operator data

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 Use the following table to determine the steps to perform in this procedure.

If	Do
the VMGs Market Country/Operator data is to be set to the same value in an attempt to reset existing Market data	<a href="#">step 3</a> then proceed to <a href="#">step 5</a> .
the VMGs Market Country/Operator data is to be changed	<a href="#">step 2</a>

- 2 From the **GW Status Config** tab, set the Administrative Status of the VMG to Out of Service.

**Note:** Setting the VMG to out of service is service affecting and a warning message is output.

- 3 From the **GW Market Config** tab, the Country/Operator may be changed. Click **Apply**.
- 4 From the **GW Status Config** tab, set the Administrative Status of the VMG to In Service if desired.
- 5 This procedure is complete.

---

—End—

---

### Refreshing data in Switched Lines Services GUI screens

The status information in the following tabs are not updated in real time. Therefore, when entering or changing data in the following tabs, the **Refresh** button must be clicked to update status information in the fields:

- GW Configuration tab
- GW Controller Config tab

### How to refresh data in Switched Lines Services GUI screens

Step	Action
------	--------

#### *At the MG 9000 Manager*

- |   |  |
|---|--|
| 1 | From the <b>GW Configuration</b> tab or <b>GW Controller Config</b> tab, enter the prescribed changes. |
| 2 | To update status information in the tab changed in the previous step, click on <b>Refresh</b> .        |
| 3 | This procedure is complete.  |

---

—End—

---

### Listing all VMGs using the VMG browser

The VMG Browser, accessed from the Configuration menu at the Subnet View, allows the user to view all the VMGs in the Subnet. The following information is displayed in the VMG Browser:

- NE Name
- NE number
- VMG Name
- VMG Type
- GWC
- VMG Oper Status
- IP Address

The following limitations apply to the VMG Browser:

- The VMG Browser is not updated in real time. Click on Refresh to update the browser.
- Only one Switched Lines Services view can be opened at a time.
- Data cannot be edited.
- No termination information is provided in the VMG Browser. Fields with Unknown indicate that the VMG is partially provisioned.

### Listing all VMGs using the VMG Browser

---

Step	Action
------	--------

---

#### *At the MG 9000 Manager*

- |   |   |
|---|---|
| 1 | From the <b>Subnet View</b> , select <b>Configuration-&gt;VMG Browser</b> from the menu bar. The <b>VMG Browser</b> appears as shown in the following figure. |
|---|---|

**VMG Browser**

NE Name	NE #	VMG Name	VMG Type	GWC	VMG Oper Status
CO10	10	EXPM129	ABI ATM	GWC-1	Enabled
CO10	10	EXPM133	ABI ATM	GWC-1	Enabled
CO10	10	EXPM172	ABI ATM	GWC-1	Enabled
CO10	10	EXPM173	ABI ATM	GWC-1	Enabled
ud18	18	EXPM189	ABI ATM	GWC-19	Enabled
CO14	14	EXPM165	ABI IP	GWC-0	Enabled

- 2 To sort the list based on NE Name, NE#, VMG Name, GWC, or VMG Oper Status, click on the **column header**. To reverse the order to sort descending, use Shift-click on the header.
- 3 To view specific data on an individual VMG, double click on that line and the **Switched Lines Services view** opens.
- 4 This procedure is complete.

---

—End—

---

**Emergency stand alone**

Emergency stand alone (ESA) provides the ability to support basic calls within an MG 9000 while one or more of the VMGs in the MG 9000 are out of communication with its assigned Gateway Controller (GWC).

ESA is provisioned on an individual VMG basis. Each VMG can be provisioned to support ESA.

**Note 1:** For ABI VMGs, only Enhanced ESA is supported. Warm exit is not supported for ESA on ABI VMGs.

**Note 2:** If an ABI VMG does not have Enhanced ESA enabled, or if Enhanced ESA is enabled, but there are not any lines datafilled on the subtending XPM, the PM:QUERYPM status displays "ABI Enhanced ESA disabled - check Element Manager". After the first line has been datafilled off of the subtending XPM, the PM:QUERYPM status displays "ABI Enhanced ESA enabled - check Element Manager".

If Enhanced ESA is enabled and there are already lines datafilled on the subtending XPM, the PM:QUERYPM immediately displays "ABI Enhanced ESA enabled - check Element Manager".

The floating IP address must be provisioned for the MG 9000 before Enhanced ESA can be enabled for VMGs on the MG 9000. To provision a floating IP address, refer to "Provisioning a floating IP address" in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450.

The following procedure describes how to set up a VMG to support ESA.

## Provisioning ESA

### Step Action

#### At the MG 9000 Manager

- 1 From the **Subnet View**, double click on the **MG 9000** icon on which ESA is to be provisioned. The **Frame View** appears.
- 2 At the **Frame View**, select **Switched Lines Services Manager** from the **Services** menu.
- 3 Select the **VMG** from the list of VMGs at the left pane in the **Switched Line Services** screen.
- 4 In the Provisioning Information pane at the right, select the **ESA Config tab**

#### ESA Config tab

The screenshot shows the MG9000 Manager interface for provisioning a Virtual Media Gateway (VMG). The left pane, titled "Select a Virtual Media Gateway", lists several VMGs: CO10007-1-0, CO10007-1-1 (selected), EXPM129, and EXPM133. The main pane, titled "Provisioning Information for: CO10007-1-1 Frame : 1 Shelf : 1 Mated Slots : 12/13", displays the "ESA Config" tab. The configuration options include:

- ESA Mode:** Select an ESA Mode (radio buttons for Enhanced (North American) and Basic, with Basic selected).
- ESA Capability:** Yes (dropdown menu).
- ESA Dialing Plan:** 7 Digit Dialing (dropdown menu).
- ESA Notify Tone:** 7 Digit Dialing (dropdown menu).
- Default Pretranslator Name:** Prefix 1 (text field).
- ESA Operational Status:** Not in ESA (text field).
- ESA Duplicate NOC:** Not Supported (text field).
- ESA Last Pull Time:** Not Set (text field).
- ESA Last Push Time:** Not Set (text field).

Buttons at the bottom include Download, Customer Group, Hunt Group, Translations, Apply, and Refresh.



**CAUTION**

**Potential ESA data mismatch because of nightly ESA data file creation in Core**

If a VMG is deleted from the Switched Line Services GUI, data related to that VMG must be removed from the ESA data file in the Core and reloaded in the MG 9000 Manager. Otherwise, if the VMG is recreated before the next scheduled Core ESA data download, the previously saved data will be reloaded.



**CAUTION**

**Potential data mismatch between XA-Core, MG 9000, and MG 9000 Manager - Enhanced ESA download**

Changes propagated to the MG 9000 Manager through Enhanced ESA data downloads may take up to 24 hours to take effect. Data that has been deleted in the Core will still be visible in the MG 9000 Manager and data that has been added may not be visible, unless a new Core file is created and manually downloaded to the MG 9000 Manager.



**CAUTION**

**Potential data mismatch between XA-Core, MG 9000, and MG 9000 Manager - automated ESA downloads**

The automatic download time in the MG 9000 Manager must be configured promptly following the Core file generation time (office parameter ESA\_GWDATAUPD\_HOUR) in table OFCENG, but must be at least 30 minutes preceding. This minimizes the amount of time until the next download to the MG 9000 Manager, while allotting 30 minutes for the Core ESA download to complete.

**CAUTION****Potential data mismatch between XA-Core, MG 9000, and MG 9000 Manager due to VMG deletion and Core file not regenerated**

If a VMG and its corresponding lines are deleted and the Core ESA download data file is not regenerated, then re-creation of the VMG will result in the appearance of "ghost DNS" at the MG 9000 Manager. This situation will be corrected within 24 hours when the scheduled Core ESA download completes.

Enter the values in the ESA Config panel. The following table lists the fields that appear in the ESA Config panel.

**Note:** To provision this panel, a VMG must be provisioned and, for Basic ESA only, at least one ESA pretranslator name must be provisioned.

**ESA Config tab fields and buttons**

Field	Entry	Explanation
ESA Mode	Select an ESA Mode using the following radio buttons: <ul style="list-style-type: none"> <li>• Enhanced</li> <li>• Basic</li> </ul>	<p>The Enhanced mode uses ESA data from the Core. This mode is used by both ABI and ITP VMGs. When selected, the Download, Customer Group, Hunt Group, and Translations button are no longer greyed out and become functional. Their description is provided later in this table</p> <p>The Basic mode relies on ESA data configured within the MG 9000 Manager. The Basic mode is not supported for ABI VMGs.</p> <p><b>Note 1:</b> If Basic ESA is being provisioned (through OSSGate), a Pretranslator must also be provisioned. However, if Enhanced ESA is being provisioned, a Pretranslator cannot be selected.</p> <p><b>Note 2:</b> If Enhanced ESA is being provisioned, several interactions may be observed between Enhanced ESA and OSSGate for ITP VMGs that cause temporary data mismatches between the core, the MG 9000 Manager, and the MG 9000. The scenarios that follow describe those interactions and how they are cleared:</p> <ul style="list-style-type: none"> <li>• Scenario A               <ul style="list-style-type: none"> <li>— 1. An ESA data XML file is created at the Core.</li> </ul> </li> </ul>

Field	Entry	Explanation
		<ul style="list-style-type: none"> <li>— 2. The Batch command with changeDN is run, changing the data in the Core and the MG 9000 Manager, though it is not automatically reflected in the Core XML file,</li> <li>— 3. The Core XML file is downloaded to the MG 9000 Manager which then overwrites the changes made in step 2.</li> </ul> <p>This scenario is self-correcting since steps 1 and 2 automatically run once each day. However, there is the possibility that lines would have the wrong DN for 24 hours.</p> <ul style="list-style-type: none"> <li>• Scenario B <ul style="list-style-type: none"> <li>— 1. The Core file is downloaded to the MG 9000 Manager and processing begins.</li> <li>— 2. Before the XML file processing is complete, a CDN command is invoked from OSSGate.</li> <li>— 3. If the termination being changed by the CDN command has already been processed by the MG 9000 Manager, not problem arises. However, if the termination has not been processed, or is currently in process, inconsistent data results.</li> </ul> </li> </ul> <p>This scenario is corrected within 24 hours or when the next ESA download occurs.</p> <ul style="list-style-type: none"> <li>• Scenario C (this scenario is unlikely to occur) <ul style="list-style-type: none"> <li>— 1. The Core file is downloaded to the MG 9000 Manager and processing completes for a VMG.</li> <li>— 2. The technician attempts to download data to an MG 9000 for a specific VMG. The MG 9000 Manager creates XML information to send to the ITP card using data from step 1.</li> <li>— 3. Before the file FTP in step 2 completes, the OSSGate command comes in to change the DN and makes its way to the VMG.</li> <li>— 4. File FTP completes and the MG 9000 overwrites data in step 3 with data from step 2. The MG 9000 Manager has the latest data but the VMG does not.</li> </ul> </li> </ul> <p>This scenario is corrected within 24 hours.</p>

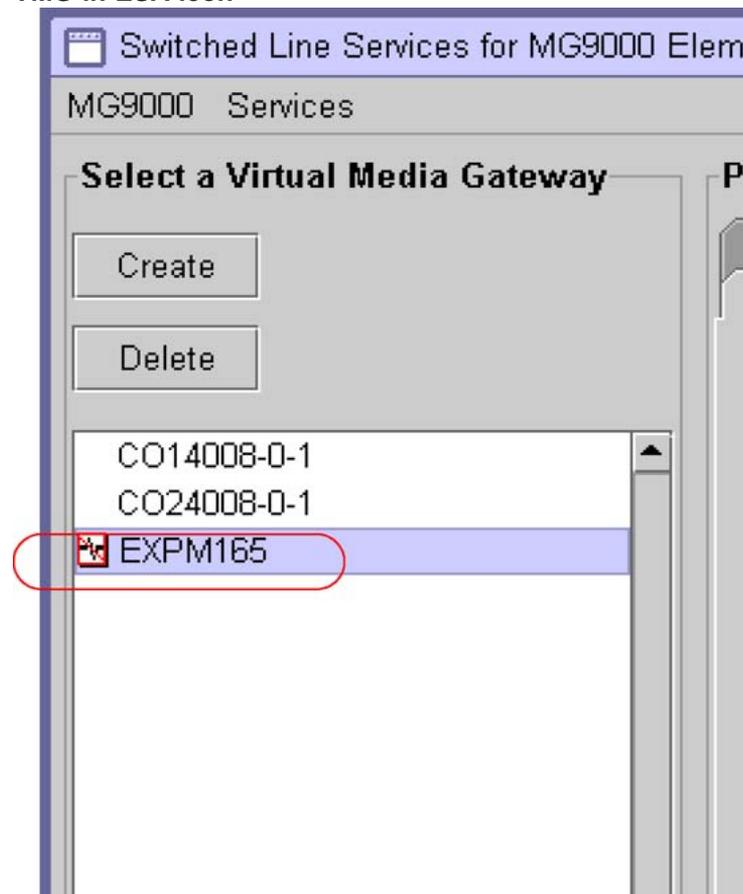
Field	Entry	Explanation
		<p>If the customer needs to synchronize the data without waiting for the automated nightly download, perform the following:</p> <ol style="list-style-type: none"> <li>1. Regenerate the ESA data XML file on the Core.</li> <li>2. Download the updated XML file to the MG 9000 Manager.</li> <li>3. For the relevant VMGs with enhanced ESA capability, download the ESA data to the MG 9000.</li> <li>4. This procedure is complete.</li> </ol>
ESA Capability	Yes	The selected VMG is capable of going into ESA. Selecting Yes causes all data associated with ESA provisioning for the selected VMG to be provisioned on the MG 9000.
	No	The selected VMG is not capable of going into ESA. All ESA data associated with the selected VMG is deleted from the MG 9000.
ESA Dialing Plan	7 digit dialing through 13 digit dialing	Select the dialing plan.
		<ul style="list-style-type: none"> <li>• For the UA-AAL1 and UA-IP solutions, 7 and 10 digit dialing plan lengths are supported in Enhanced ESA.</li> <li>• For the UA-IP solution, 6 through 13 digit dialing plan lengths are supported.</li> </ul>
ESA Notify Tone	Yes	A notify tone is given to alert that the VMG is in ESA mode.
	No	No indication is provided that the VMG is in ESA mode.
Default Pretranslator Name	The choices that appear are dependant on values from Service Code Translations	This field is the Default Pretranslator name that is associated with the selected VMG.
		<b>Note:</b> If no translations exist, go to Provisioning an ESA pretranslator
ESA Operational Status	Not in ESA	Means the VMG is not in ESA mode.

Field	Entry	Explanation
	In ESA	Means the VMG is in ESA mode. This gets updated when the Refresh button is selected or the MG 9000 Manager receives an ESA Alarm from the MG 9000. In ESA means communication with the Gateway Controller is down. An ESA icon appears next to the VMG in ESA.
ESA Duplicate NXX		A value received from the Core that is used to determine the dialing plan, 7, 10 or 7 and 10.  If NUMDIG_PER_DN = 7 then 7 digit dialing.  If NUMDIG_PER_DN = 10 and dupNXX = true then 7 and 10 digit dialing.  If NUMDIG_PER_DN = 10 and dupNXX = false then 10 digit dialing.
ESA Last Pull Time		The time stamp of the last XML file that was created on the Core. This is the last time the data was pulled from the Core tables into the file
ESA Last Push Time		The last time ESA data was sent to the MG 9000.
Download button		When selected, a manual download of the MG 9000 Manager ESA data to the MG 9000 to sync the MG 9000 with the latest ESA data from the Core in the MG 9000 Manager for the selected VMG. The Download button can be used when it is determined that the ESA data in the MG 9000 Manager is newer than the data in the MG 9000. This can be determined when the ESA Last Pull Time is more recent than the ESA Last Push Time.
<b>Note:</b> Enabled only if Enhanced ESA mode is selected.		<b>Note:</b> Do not use the Download button while the VMG is in ESA.
Customer Group button		When selected, the ESA Customer Group List view appears.
<b>Note:</b> Enabled only if Enhanced ESA mode is selected.		
Hunt Group button		When selected, the ESA Hunt Group List view appears.
<b>Note:</b> Enabled only if Enhanced ESA mode is selected.		

Field	Entry	Explanation
Translations button		When selected, the ESA Translations List view appears.
<b>Note:</b> Enabled only if Enhanced ESA mode is selected.		
ABI Node List button		When selected, the ABI Note Data view appears and lists the ABI node properties including the node number, name, and type.
<b>Note:</b> Enabled only if Enhanced ESA mode is selected and if an ABI VMG is selected.		

The following figure shows the VMG in ESA as noted by the ESA icon adjacent to the VMG

#### VMG in ESA icon



- 6 To determine the next step, use the information in the following table.

If ESA mode selected in step 5 is	Do
Enhanced	<a href="#">step 7</a>
Basic	<a href="#">step 13</a>

- 7 To provision Enhanced ESA, use the following checklist.

#### Enhanced ESA provisioning checklist

Step	Description	Documentation reference
1	Review the Enhanced ESA capabilities.	<i>MG 9000 Basics</i> , NN10011-111.
2	Generate a separate disk volume and change the value for the OFCENG parameter to the name of the volume that is to be built.	Refer to "Generating the ESA information file" in <i>CS2000 Configuration Management</i> , NN10105-511, NN10188-511, NN10201-511, or NN10193-511.
3	<p>Create the volume with a file name in compliance with operating company engineering guidelines. Use the following volume creation steps:</p> <ol style="list-style-type: none"> <li>1. From the MAP terminal, at the CI level, enter diskadm to enter the Disk Administration level and press enter.</li> <li>2. To create the new volume on the disks, enter the following command <pre>&gt; createvol esadata 500 ftfs</pre> <p>where</p> <ul style="list-style-type: none"> <li>• esadata is the volume name</li> <li>• 500 is the volume size in Mbytes</li> <li>• ftfs is the volume type keyword</li> </ul> </li> <li>3. To view the data on the new name and all others, type <pre>&gt; displayvols</pre> </li> </ol>	Refer to " <a href="#">Changing ESA download properties</a> " (page 309).

Step	Description	Documentation reference
	<p>4. To exit the DISKADM level, type</p> <p style="padding-left: 40px;"><code>&gt; quit</code></p> <p><b>Note:</b> The value of the volume size is administered by the operating company.</p>	
4	Change the "ESA_GWDATA_DEVICE" parameter in table OFCENG to reflect the new volume to which the file is to be generated (for example, esadata).	Refer to "Generating the ESA information file" in <i>CS2000 Configuration Management</i> , NN10105-511, NN10188-511, NN10201-511, or NN10193-511.
5	Populate the ESAPXLA table for each node that will utilize local lines to handle Emergency Service (911) calls while in ESA. An entry must be made for every VMG (MG 9000 shelf) to be served by a particular code/line. If no emergency service lines are available, MG 9000 treatment may also be applied. The documentation references provide guidance on for the selector to be used. The operating company's Network Control and Translations Engineering departments should evaluate and agree upon the entries in this table.	Refer to "Generating the ESA information file" in <i>CS2000 Configuration Management</i> , NN10105-511, NN10188-511, NN10201-511, or NN10193-511.
6	If data is to be manually collected at any time into the download file (ESA_SYSTEM_SD\$XML) enter the ESATOOLS level from the CI prompt in the MAP terminal and execute the ESACOLL command. If this command is successful in performing the data collection and writes the data to the file, an ESA120 log is output. If it fails, an ESA121 log is output. The XA-Core data collection is generated automatically on a daily basis on the time specified by	Refer to "Generating the ESA information file" in <i>CS2000 Configuration Management</i> , NN10105-511, NN10188-511, NN10201-511, or NN10193-511.

Step	Description	Documentation reference
7	<p>ESA_GWDATAUPD_HOUR parameter in table OFCENG. The default value of this parameter is 6:00 AM.</p> <p>This step is required to assure new ESA data added to the XA-Core is propagated immediately to the MG 9000 and is active if an ESA condition occurs before the next automated download</p> <p>Ensure the IPHOST table contains a tuple for the CM with the appropriate parameter values.</p>	Refer to "Core configuration" (page 305).
8	Configure the Base server to permit the download of the XA-Core data file (ESA_SYSTEM_SD\$XML) from the SDM.	Refer to "Changing ESA download properties" (page 309).
9	Perform the procedure "Changing ESA download properties" (page 309) to synchronize the MG 9000 Manager data collection times and device to the XA-Core. Ensure the notes and information about setting the ESA.DataDownloadTime in the MG 9000 Manager to a value at least 30 minutes greater than ESA_GWDATAUPD_HOUR in the XA-Core is followed. The ESA_GWDATAUPD_HOUR parameter is added to the OFCENG table and this time is configurable.	
10	Configure the VMGs that require Enhanced ESA at the Switched Line Services Manager.	Refer to "Provisioning ESA" (page 201).
11	If desired, manually pull the data from the XA-Core to the MG 9000 Manager by accessing the Configuration menu of the Subnet View and selecting the "ESA	Refer to the description of the Download button in the "ESA Config

Step	Description	Documentation reference
	<p>Download" option. When the Apply key is pressed, the manual download is initiated. Data is provided on the progress of the download in this view until it is complete.</p> <p>This step is required to assure that new ESA data added to the XA-Core is propagated immediately to the MG 9000 and is active if an ESA condition occurs before the next automated download.</p>	<p><a href="#">tab fields and buttons" (page 203).</a></p>
12	<p>Once the ESA_SYSTEM_SD\$XML is downloaded and parsed into the VMG files on the MG 9000 Manager, a manual download may be performed on the "ESA Config" tab of the "Switched Line Services Manager" to push the VMG file to the MG 9000 node.</p> <p>This step is required to assure that new ESA data added to the XA-Core is propagated immediately to the MG 9000 and is active if an ESA condition occurs before the next automated download</p>	<p>Refer to the description of the Download button in the <a href="#">"ESA Config tab fields and buttons" (page 203).</a></p>

- 8 To determine the next step, use the information in the following table.

If	Do
the Customer Group data for a selected VMG must be displayed	<a href="#">step 9</a>
the Hunt Group data for a selected VMG must be displayed	<a href="#">step 10</a>
the Translations List for a selected VMG must be displayed	<a href="#">step 11</a>
the ABI node properties for a selected ABI VMG node must be displayed	<a href="#">step 12</a>

- 9 To display the Customer Group data, click on the **Customer Group** button. The **ESA Customer Group List** appears as shown in the following figure.

### ESA Customer Group List View

Group Id	Translation Id	Extension Id	Group Number	Avt Id
0	1	0	4095	0
0	1	0	4095	0
1	0	0	256	0
1	0	0	256	0
2	2	32769	4	0
2	2	32769	4	49156

The following table lists the fields in the ESA Customer Group List View and their descriptions.

### ESA Customer Group List View field descriptions

Field	Descriptions
Group Id	The customer group index.
Translation Id	The Pre Translation index which indicates which Pre Translation table to use.
Extension Id	The Pre Translation index which indicates which Pre Translation table to use for extension dialing.  When the indexes are for DGCOD, the column name changes to DGCOD Id (only visible to MLPP offices).
Group Number	External customer group number.
AVT Id	The customer group's AVT index (only visible to MLPP offices).

- 10 To display the Hunt Group data, click on the **Hunt Group** button. The **ESA Hunt Group List** appears as shown in the following figure.

### ESA Hunt Group List View

Group Id	Member Id	Pilot DN	External TID
0	0	9095500061	553222

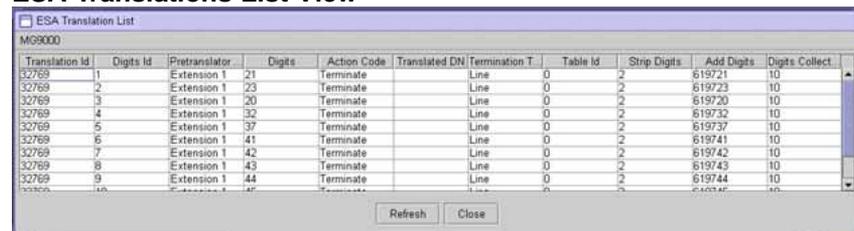
The following table lists the fields in the ESA Hunt Group List View and their descriptions.

#### ESA Hunt Group List View field descriptions

Field	Descriptions
Group Id	The index to the hunt group table.
Member Id	The HuntGroup member index.
Pilot DN	Pilot Directory Number for the Hunt Group.
External TID	The terminal number.

- 11 To display the Translations data, click on the **Translations** button. The **ESA Translations List** appears as shown in the following figure.

#### ESA Translations List View



The screenshot shows a window titled "ESA Translation List" with a table of data. The table has the following columns: Translation Id, Digits Id, Pretranslator, Digits, Action Code, Translated DN, Termination T, Table Id, Strip Digits, Add Digits, and Digits Collect. The data rows show translations for group 32769 with various digits and actions.

Translation Id	Digits Id	Pretranslator	Digits	Action Code	Translated DN	Termination T	Table Id	Strip Digits	Add Digits	Digits Collect
32769	1	Extension 1	21	Terminate	Line	0	2	619721	10	
32769	2	Extension 1	23	Terminate	Line	0	2	619723	10	
32769	3	Extension 1	20	Terminate	Line	0	2	619720	10	
32769	4	Extension 1	32	Terminate	Line	0	2	619732	10	
32769	5	Extension 1	37	Terminate	Line	0	2	619737	10	
32769	6	Extension 1	41	Terminate	Line	0	2	619741	10	
32769	7	Extension 1	42	Terminate	Line	0	2	619742	10	
32769	8	Extension 1	43	Terminate	Line	0	2	619743	10	
32769	9	Extension 1	44	Terminate	Line	0	2	619744	10	

The following table lists the fields in the ESA Translations List View and their descriptions.

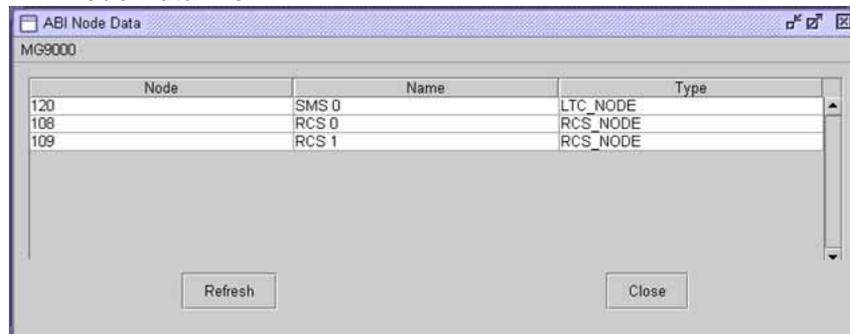
#### ESA Translations List View field descriptions

Field	Descriptions
Source (only visible to MLPP offices)	Indicates which Core translator the entry came from - ESAPLXA, IBNXLX, ESADGCOD and AVT.
Translation Id	An identification number assigned to the translation.
Digits Id	An identification number assigned to the prefix Digit.  <b>Note:</b> For MLPP offices, for ESADGCOD and AVT translations entries, this field will display the To and From digits in the 111...222 format.
Pretranslation Name	The name of this prefix translation.
Digits	Dialing digits.

Field	Descriptions
Action Code	This specifies which action to take: Terminate; Giveorder; Strip and pretranslate; Ambiguous termination; Second dial strip and pretranslate; Second dial and terminate; Spare.
Translated DN	Translated directory number for the service code.
Termination Type	Type of termination: Line; Trunk route; Hunt; Customer Group.
Table Id	An index to either HuntGroupTable, CustomerGroupTable, or RouteTable.
Strip Digits	This specifies how many digits to remove.
Add Digits	The digits to add before the directory number.
Digits Collected	The total number of digits to collect for this translation.

- 12 To display the ABI Node properties, click on the **ABI Node Data** button. The **ABI Node Data view** appears as shown in the following figure.

#### ABI Node Data View



The following table lists the fields in the ESA Translations List View and their descriptions.

#### ABI Node Data view field descriptions

Field	Descriptions
Node	The number of the ABI node.
Name	The name of the ABI node.
Type	The type of XPM ABI node.

13 This procedure is complete.

—End—

## Viewing termination ESA data

### Step Action

#### At the MG 9000 Manager

- 1 From the **Subnet View**, double click on the **MG 9000** icon on which ESA is provisioned. The **Frame View** appears.
- 2 At the **Frame View**, select **Switched Lines Services Manager** from the **Services** menu.
- 3 Select the **VMG** from the list of VMGs at the left pane in the **Switched Line Services** screen.
- 4 In the Provisioning Information pane at the right, select the **GW Termination Config** tab. The view changes as shown in the following figure.

#### GW Termination Config tab showing termination ESA information fields

Terminal ESA information  
Refer to the GW Termination Config tab - ESA termination information table.

Termination	Termination Name	Termination's Slot Location	Termination's Circuit Location	Termination Test Status	Operational Status	Termination DN	Cut Off on Disconnect	Automatic Line ID	Automatic Line DN	Denied Incoming	Customer Group ID	Hunt Group ID	Priority Call Line	External TID	MLPP Precedence Level	MLPP Preemptable
tp/05/20	In SESM															
tp/05/21	6193360228															
tp/05/22	6193360129															
tp/05/23	6193360229															
tp/05/24	In SESM															
tp/05/25	6193360130															
tp/05/26	6193333317															
tp/05/27	In SESM															
tp/05/28	In SESM															
tp/05/29	6193360230															
tp/05/30	In SESM															
tp/05/31	6193360131															
tp/07/00	6193360135															
tp/07/01	6193360235															
tp/07/02	In SESM															
tp/07/03	In SESM															
tp/07/04	In SESM															
tp/07/05	6193360136															
tp/07/06	6193360236															
tp/07/07	6193360137					6193360137								1683752	4	false

The following table lists the fields that provide information on ESA terminations.

#### GW Termination Config tab - ESA termination information

Field	Explanation
Termination DN	The directory number of this termination as provisioned by the Core.
Cut Off on Disconnect	Cut Off on Disconnect - Supported or Not Supported
Automatic Line ID	An index to the Automatic lines table.
Automatic Line DN	The directory number of the terminator for Automatic lines.
Denied Incoming	Denied incoming - Supported or Not Supported
Customer Group ID	Customer group number to which this line belongs.
Hunt Group ID	Index to the Hunt Group Table.
Priority Call Line	Indicates the line is for the priority call - Priority Call or Not Priority Call
External TID	External termination identifier.
MLPP Precedence Level (only visible to MLPP offices)	Shows the termination's Precedence Level. The Precedence levels are: <ul style="list-style-type: none"> <li>FlashOverride = 0</li> <li>Flash = 1</li> <li>Immediate = 2</li> <li>Priority = 3</li> <li>Routine = 4</li> </ul>
MLPP Preemptable (only visible to MLPP offices)	Indicates if the termination is preemptable.

5 This procedure is complete.

---

—End—

---

When it becomes necessary to provision a ESA pretranslator, use the following procedure.

**Note:** This procedure only applies to Basic ESA.

#### Provisioning an ESA Pretranslator

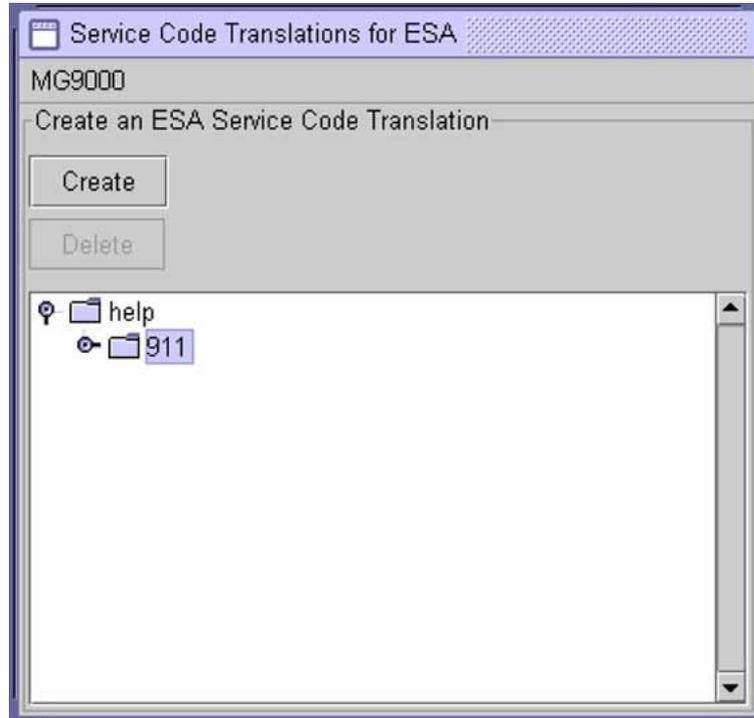
---

Step	Action
------	--------

---

*At the MG 9000 Manager*

- 1 From the **Subnet View**, double click on the **MG 9000** icon on which ESA is to be provisioned. The **Frame View** appears.
- 2 At the **Frame View**, select **Switched Lines Services Manager** from the **Services** menu.
- 3 From the **Switched Lines Services Manager** menu bar, select **Services->ESA Service Code Translations**. The **ESA Pretranslator screen** appears.

**ESA Pretranslator screen**

- 4 Select **Create** to create a new Service Code Translation. The **Create a Service Code Translation** window appears.

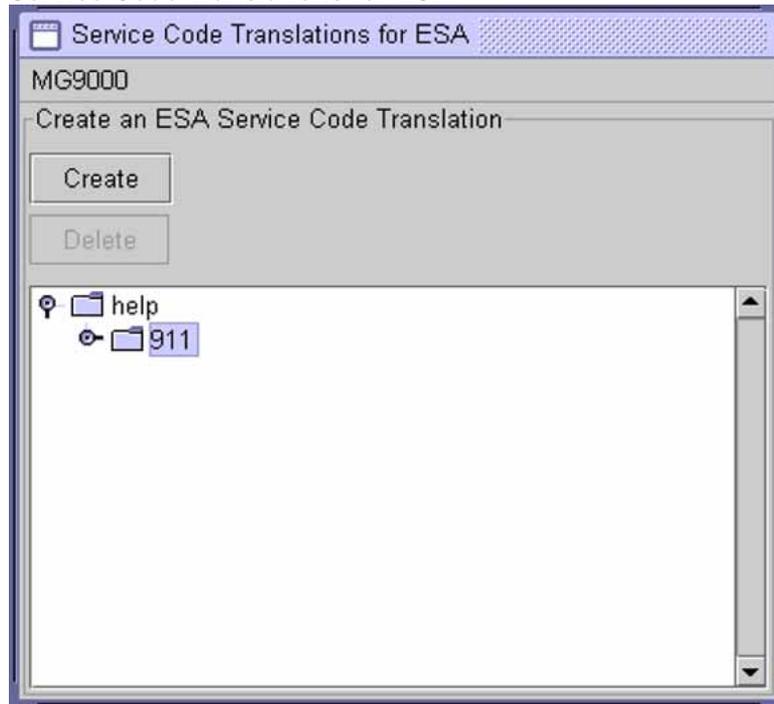
### Create a Service Code Translation for ESA

- 5 Provision the fields associated with the translator. The following table lists the fields associated with the translator:

#### ESA Service code translation fields and explanation

Field	Explanation
Pretranslator Name	This field can be an alphanumeric string representing the name of the translator. The field length allows for 1 to 8 characters.  <b>Note:</b> The Pretranslator Name and Dialed Service Code must be a unique combination. For example, a translator with the name "default" can have several translations provisioned but those translations cannot have the same dialed service code.
Dialed Service Code	This field is a numeric field representing the digits to be dialed by the customer. The field allows for 1 to 10 numbers.
Translated DN	This field is a numeric field containing the DN that the dialed digits will terminate/translate to when dialed by the customer. The Translated DN should contain the Full DN, including the NPA. If the Full DN is not used, whenever a change DN occurs for the Translated DN, the Service Code Translation will not be automatically updated. For the updates to occur, the Translated DN needs to contain the same number of digits that are received from OSSGate. The Translated DN may contain from 1 to 15 digits.

- 6 Click **Apply** when complete. The data is displayed in the Service Code Translations for ESA, as shown in the following figure.

**Service Code Translations for ESA**

The Pretranslator Name will now appear in the **ESA Config** tab in the **Switched Line Services** window.

- 7 This procedure is complete.

---

—End—

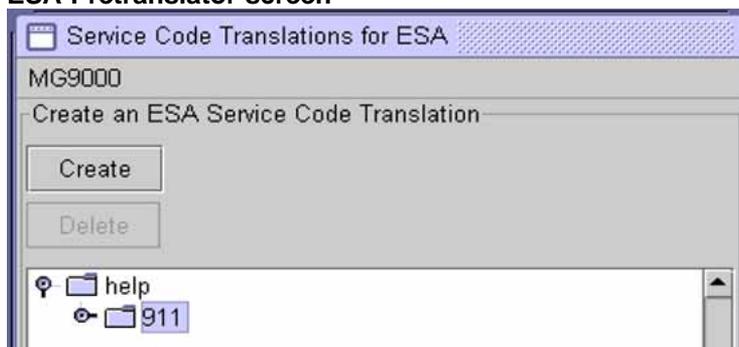
---

### Deleting a service code translation

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 From the **Subnet View**, double click on the **MG 9000** icon on which ESA is to be provisioned. The **Frame View** appears.
- 2 At the **Frame View**, select **Switched Lines Services Manager** from the **Services** menu.
- 3 From the Switched **Lines Services Manager** menu bar, select **Services->ESA Service Code Translations**. The **ESA Pretranslator** screen appears.

**ESA Pretranslator screen**

- 4 Expand the translator and select the **DN** to be deleted. The **Delete** button becomes visible after selecting the target **DN**.

**ESA Pretranslator screen with DN selected to be deleted**

- 5 Click on the **Delete** button.
- 6 This procedure is complete.

---

—End—

---

**Download ESA data from the Core**

ESA data is automatically downloaded from the Core to the MG 9000 Manager nightly. For more information on setting up ESA data download and changing the download properties, refer to ["Changing MG 9000 Manager ESA data download properties"](#) (page 305).

Use the following procedure when it is necessary to manually download ESA data from the Core to the MG 9000 Manager.

**Downloading ESA data**

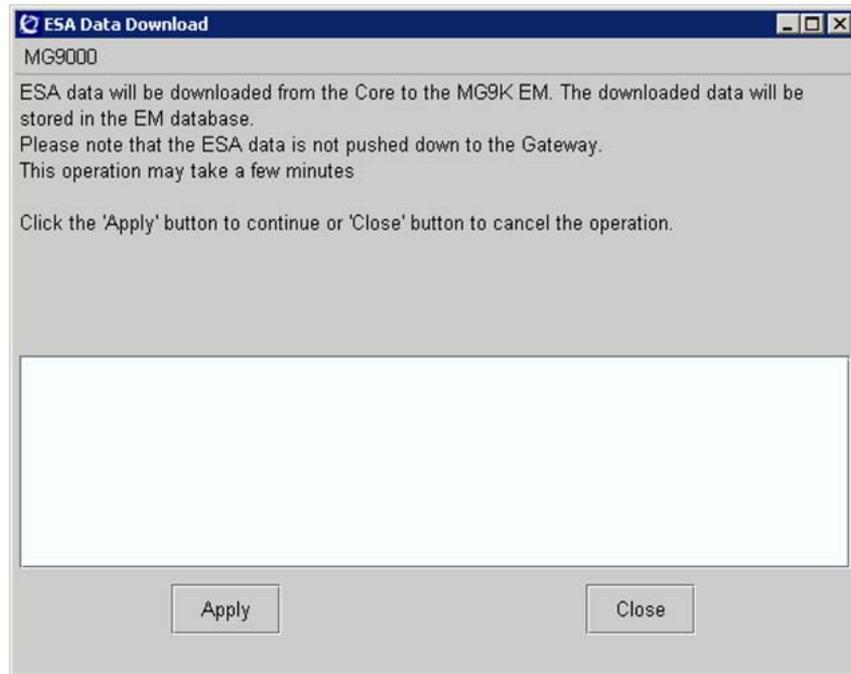
---

**Step Action**


---

**At the MG 9000 Manager**

- 1 From the **Subnet View** menu bar, select **Configuration->ESA Download**. The **ESA Data Download View** appears as shown in the following figure.

**ESA Data Download View**

- 2 Click **Apply** to continue with the download.
- 3 This procedure is complete.

---

—End—

---

**Disabling ESA in a VMG**


---

**Step Action**

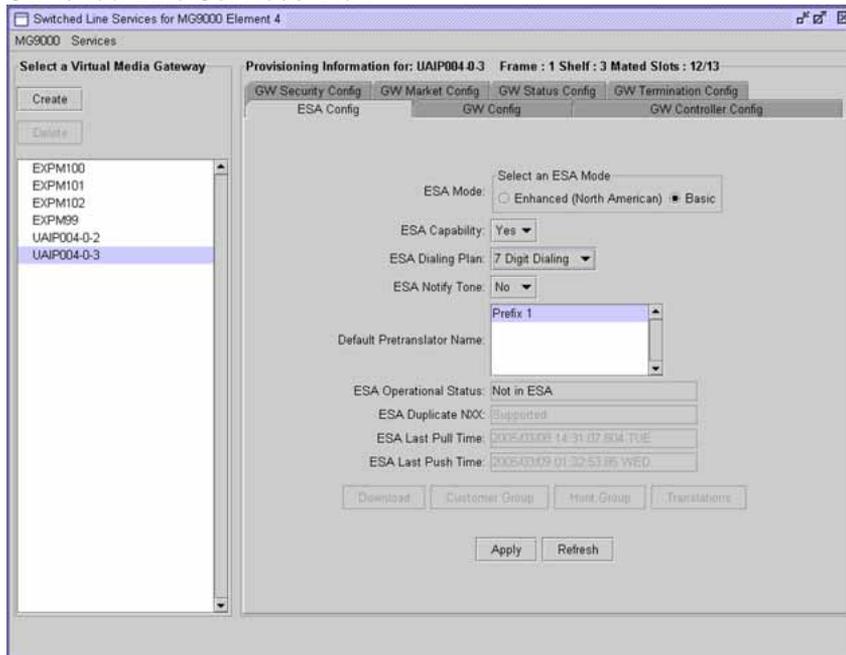

---

**At the MG 9000 Manager**

- 1 From the **Subnet View**, double click on the **MG 9000** icon on which ESA is to be provisioned. The **Frame View** appears.
- 2 At the **Frame View**, select **Switched Lines Services Manager** from the **Services** menu.

- 3 Select the **VMG** from the list of VMGs at the left pane in the **Switched Line Services** screen.
- 4 In the Provisioning Information pane at the right, select the **ESA Config** tab

### Switched Line Services View



- 5 In the ESA Capability field, select **No**. Click on **Apply**.
- 6 This procedure is complete.

—End—

### Saving a list of SLoA services to a file

When it is necessary to view all the services on the MG 9000, a listing of the VMG names can be obtained using the Saving SLoA Services tool. This tool is also used to save a list of the services to a flat file for inventory management or when manual re-provisioning is required, such as in the unlikely event that persistence is lost, and to preclude the need for writing the information manually. Files are written in both HTML and text format. The information is always output to the server. The directory in which the files are written is /tmp directory on the server and the file name is displayed in the information dialog message that is output. The user should FTP the file to any desired location to retain the information.

**Note:** These files must be regularly moved to another directory since the /tmp directory is cleaned periodically.

The filenames for SLoA services are the same as VMG names to make the names unique. If there are multiple VMGs, then the dialog will have multiple filenames that have been written

The following procedure provides the steps for saving SLoA services information into a file.

### Saving SLoA services

---

Step	Action
------	--------

---

#### *At the MG 9000 Manager*

- 1 From the **Frame View**, access the Save SLoA Services tool from the **Actions** menu. The **Save SLoA services dialog box** appears as shown in the following figure.

#### Save SLoA Services dialog



- 2 The VMG names have been exported into the file noted in the dialog box. Note the file name. Click **OK** to close the dialog box.
- 3 This procedure is complete.

---

—End—

---

## Viewing and modifying DS1 IMA group and links

### When to use this procedure

Use the procedures in this section to view and modify DS1 IMA links.

The following procedures are provided:

- viewing DS1 IMA group or link attributes
- modifying (adding or deleting) links in the DS1 IMA group
- locking DS1 IMA ports

**Note:** In the DS1 IMA Port View, the state of the links in the IMA group are viewed on the active card only. When viewing the DS1 IMA Port View for the inactive card, the Administrative State and Configuration State and not enabled (greyed out) and the state of the links is reported as "No Links on Inactive Card."

### Prerequisites

There are no prerequisites.

### Action

#### Viewing DS1 IMA group and link attributes

Step	Action
------	--------

##### *At the MG 9000 Manager*

- 1 At the **Subnet View**, double click the **MG 9000** network element 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**, select **Actions->View** IMA Group from the main menu bar.

The **IMA Group Attributes View** appears as shown in the following figure.

## IMA Group Attributes View

IMA Group Attributes	
MG9000	
DS1-IMA Group Status	
Operational Status	Up
Administrative State	Unlocked
Configuration State	Online
Near-end State	Operational
Far-end State	Operational
Failure Status	No Failure
Tx Timing Reference Link	274665604
Rx Timing Reference Link	274885604
Diff Delay Max	60
Number of Tx Config Links	0
Number of Rx Config Links	0
Number of Tx Active Links	0
Number of Rx Active Links	0
Tx QAM Label Value	1
Rx QAM Label Value	1
DS1-IMA Group Attributes	
Symmetry	Symmetric Operation
Minimum No. of Tx Links in Group	2
Minimum No. of Rx Links in Group	2
Near-end Tx Clock Mode	Common Transmit Clock (GTC)
Far-end Tx Clock Mode	Common Transmit Clock (GTC)
Tx Id	0
Rx Id	2
Tx Frame Length	m128
Rx Frame Length	m128
Alpha Value	2
Beta Value	2
Gamma Value	1
<input type="button" value="Refresh"/> <input type="button" value="Close"/>	

4 This procedure is complete.

—End—

## Modifying (adding or deleting) links in the DS1 IMA group

Step	Action
------	--------

### 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**, double click on the active DCC (DS1 IMA) card. The **IMA Card view** appears.
- 4 Use the information in the following table to determine the next step.

If	Do
adding links to an IMA group	<a href="#">step 5</a>
deleting links from an IMA group	<a href="#">step 11</a>

- 5 To add links to an IMA group, double click on the DS1-IMA Port corresponding to the link to be added to the group. The **DS1-IMA Port View** appears.
- 6 In the Port Status pane, set these Configuration status to Online. Then, set the Administrative status of the port to Unlocked. Observe that the Operational State is Up.

**Note:** If the link does not come up check the connections. Perform the procedure "Performing DS1 IMA diagnostics" in *MG 9000 Fault Management*, NN10074-911.

Repeat [step 5](#) and [step 6](#) for each link to be added to the IMA group. The following figure shows a Unlocked DS1 IMA port.

**DS-IMA Port View showing a Unlocked port**

MG9000 Services Alarms

DS1 Provisioning  
Circuit Identifier:

Facility Data Link  ANS1 T1403  AT&T 54016  None

Line Type: B5P Line Length: 655

Line Coding: B5ZS 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

DS1-IMA Port Alarms **NE Info**

Critical: 0 Minor: 0

Major: 0 Warning: 0

Apply Refresh Close

- 7 At the **Shelf View**, select **Actions->Edit IMA Group** from the main menu bar.

The Add/Remove Links to/from **IMA Group View** appears as shown in the following figure.

**Note:** DS1-IMA link attributes are not automatically updated by the MG 9000, when links are added from other applications such as the LCI. Use the **Refresh** button to obtain the latest status.

## Add/remove Links to/from IMA Group View

MG9000

DS1-IMA Group Status

Group Operational Status: Up      Group Administrative Status: Unlocked      Group Configuration Status: Online

Group Near End State: Operational      Group Far End State: Operational      Group Failure Status: No Failure

Link Selection

Link 1    Link 2    Link 3    Link 4    Link 5    Link 6    Link 7    Link 8

Links on Active IMA Card

	#1	#2	#3	#4	#5	#6	#7	#8
Link Operational Status	Up	Up	Down	Up	Up	Up	Up	Up
Link Administrative Status	Unlocked	Unlocked	Unlocked	Unlocked	Unlocked	Unlocked	Unlocked	Unlocked
Link Configuration Status	Online	Online	Online	Online	Online	Online	Online	Online
Link Near End Transmit State	Active	Active	Usable	Active	Active	Active	Active	Active
Link Near End Receive State	Active	Active	Usable	Active	Active	Active	Active	Active
Link Far End Transmit State	Active	Active	Unusable No Ove...	Active	Active	Active	Active	Active
Link Far End Receive State	Active	Active	Unusable No Ove...	Active	Active	Active	Active	Active
Link Near End Receive Failure Status	No Failure	No Failure	No Failure	No Failure	No Failure	No Failure	No Failure	No Failure
Link Far End Receive Failure Status	No Failure	No Failure	LF Failure	No Failure	No Failure	No Failure	No Failure	No Failure
Link Highest Severity Alarm	No alarms	No alarms	Minor	No alarms				

DS1 Carries on Active IMA Card

	#1	#2	#3	#4	#5	#6	#7	#8
Port Operational Status	Up							
Port Administrative Status	Unlocked							
Port Configuration Status	Online							
Port Highest Severity Alarm	No alarms							

DS1 Carries on Inactive IMA Card

	#1	#2	#3	#4	#5	#6	#7	#8
Port Operational Status	Down							
Port Administrative Status	Locked							
Port Configuration Status	Offline							
Port Highest Severity Alarm	No alarms							

Apply      Refresh      Close

- 8 Select the links to be added to the IMA group by clicking in the box next to each link number, making the check mark appear in the box.
- 9 At the **IMA Group View**, click on **Apply** to initiate the changes.
- 10 In the Link status pane, online the link by setting the Configuration status to Online. Then, set the Administrative status of the link to Unlocked. The Operational State of the link should show Up. If the IMA link does not come up, perform the "Performing DS1 IMA diagnostics" procedure in *MG 9000 Fault Management*, NN10074-911.  
Repeat this step for each link that was added to the group.  
This procedure is complete.
- 11 To remove links from an IMA group, double click on the DS1-IMA Port representing the link to be removed from the group. The **DS1-IMA Port View** appears.
- 12 In the Link status pane, set the Administrative status of the link to Locked. Then, set the Configuration Status to Offline.

- Repeat [step 11](#) and [step 12](#) for each link to be removed from the IMA group.
- 13 At the Shelf View, select **Actions->Edit IMA Group** from the main menu bar.  
The Add/Remove Links to/from **IMA Group View** appears.
  - 14 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.
  - 15 At the **IMA Group View**, click on **Apply** to initiate the changes.
  - 16 For each link that was removed from the group, the corresponding DS1 IMA port can be locked, depending on local policy. If it is determined that the DS1 IMA port should be locked, go the "[Locking DS1 IMA ports](#)" (page 229) procedure.  
Repeat this step for each link that was locked in this procedure.

---

—End—

---

## Locking DS1 IMA ports

---

Step	Action
------	--------

---

*At the MG 9000 Manager*

- |   |  |
|---|--|
| 1 | At the <b>Subnet View</b> , double click the <b>MG 9000</b> node icon. The <b>Frame View</b> appears.                              |
| 2 | At the <b>Frame View</b> , double click on the master shelf. The <b>Shelf View</b> appears.  |
| 3 | At the <b>Shelf View</b> , double click on the active DCC (DS1 IMA) card. The <b>IMA Card view</b> appears.                        |
| 4 | To access the port to be locked, double click on the DS1-IMA Port. The <b>DS1-IMA Port View</b> appears.                           |
| 5 | At the <b>DS1 IMA Port View</b> , set the Administrative Status of the port to Locked and set the Configuration Status to Offline. |
| 6 | This procedure is complete.  |

---

—End—

---

## Provisioning and maintenance of OC3 APS

---

### When to use this procedure

Use the procedures in this section to provision and maintain OC3/STM-1 automatic protection switching (APS). The procedures included are

- provisioning OC3 automatic protection switching
- maintaining OC3 automatic protection switching

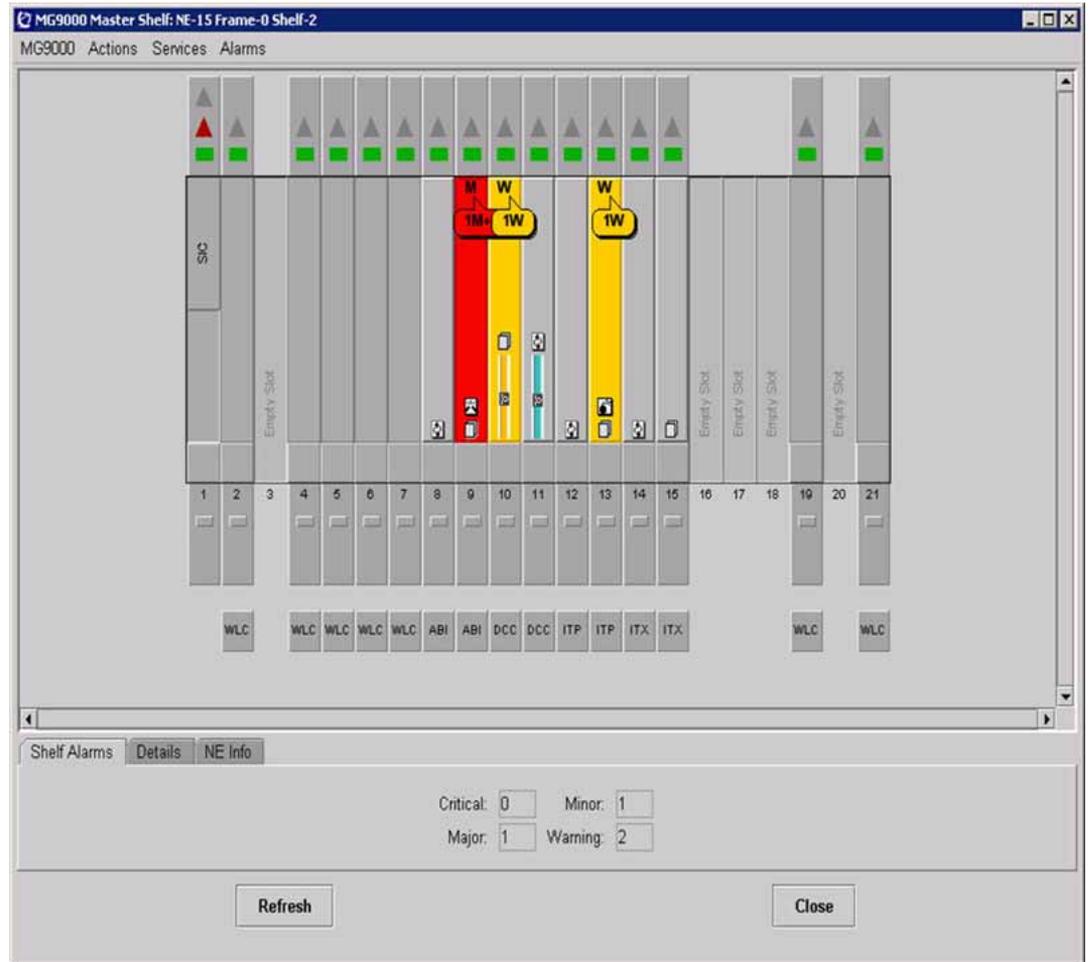
In 1+1 configuration, the MG 9000 is required to spare the OC3 line carrier and guarantee all stable calls survive over the spare. The term 1+1 comes from the fact that there is one working carrier and one protection carrier at both the head-end and tail-end of the transmission path. Both head-end units transmit identical data/payload to the tail-end equipment. The receiving equipment at each end chooses the signal (working or protection) to which it will listen.

**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 indicating an APS failure. When the mismatch is corrected, the X icon on the Shelf View and Card View will clear. The following figure shows the X icon.



The following figure shows the Shelf View with icons displayed on the DCC-OC3 cards.

**Shelf View showing the APS icons on the DCC-OC3 cards**



The unit from which the data/payload is sourced and transmitted and also the unit which selects, receives, and processes the incoming line signal is referred to as the Active Unit. The Inactive Unit is considered standby equipment to spare the active line carrier.

**Prerequisites**

There are no prerequisites.

**Action**

**Provisioning OC3 automatic protection switching**

**Step Action**

*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**, select **APS Provisioning** from the **Actions->Maintenance** menu on the main menu bar.

**Note:** The APS Provisioning GUI is not available if only one OC3 Card is installed or if the system has a DS1-IMA network interface. An information message will appear in this case.

The **APS Provisioning View** appears as shown in the following figure. Steps described in this section are optional.

#### APS Provisioning View



- 4 To disable the APS group, use the "**Set Disable**" button.
- 5 To Enable APS, use the "**Set Enable**" button.
- 6 To Rename the APS Group, disable the APS group using the "**Set Disable**" button. The **Rename** button will become enabled. Change the APS group name by typing in the new name. Press the **Rename** button for the change to take effect. Set the APS Group Status to **Enable**.
- 7 The **Refresh** button may be clicked at any time to update the GUI with fresh information from the MG 9000.
- 8 This procedure is complete.

---

—End—

---

## Maintaining OC3 automatic protection switching

---

Step	Action
------	--------

---

*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 DCC (OC3) cards in the master shelf, double click on the **Active DCC (OC3) card**. The **OC3 Card View** appears.
- 4 At the **OC3 Card View**, double click on the **OC3 port**. The **OC3 Port View** appears.
- 5 At the **OC3 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 OC3 port on the active OC3 card. The APS Maintenance View is shown next.

**APS Maintenance View with protection switch commands shown**

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 OC3 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.

#### Applicable Protection switch commands

Command	Effect
LockOut Protection Switching	<p>Disables or blocks manual/Force Protection Switching features by locking out the protected (spare) carrier.</p> <p><b>Note:</b> Even though lockout of protection switching normally applies to both Automatic (APS) as well as Manual Protection Switching, an APS triggered by a fiber fail connection will NOT be blocked by the LockOut setting since call processing redundancy would be at risk.</p>
ForcedSwitch Working to Protected Carrier	<p>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.</p>
ManualSwitch Working to Protected Carrier	<p>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.</p>
ForcedSwitch Protected to Working Carrier	<p>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.</p> <p><b>Note:</b> 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.</p>
ManualSwitch Protected to Working Carrier	<p>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.</p>

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 OC3 carrier.
	The OC3 Carrier is untroubled and ready to handle the protection switch (APS).  This is the normal configuration for the Standby OC3 carrier.
	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.

Icon	Meaning
	The carrier is switched and protected. The mate carrier is ready to switch back.
	The carrier is manually switched
	The carrier is forced switched.

7 This procedure is complete.

---

—End—

---

## Viewing Gigabit Ethernet ports and links provisioning information

---

### When to use this procedure

Use section when it is necessary to view or change the NTNY45FA GigE DCC card port and link attributes. Changes are made through the GigE Port View which is accessed by double-clicking on a GigE Port icon in the GigE Card view.

The following procedures are included in this section:

- "Viewing GigE port and link provisioning information" (page 240)
- "Provisioning GigE link protection" (page 244)
- "Provisioning GigE link integrity" (page 245)
- "Viewing VLAN provisioning data" (page 246)
- "Listing all VLAN connections using the VLAN Browser" (page 247)
- "Adding links to and deleting links from a protection group" (page 248)
- "Viewing GigE link protection group" (page 250)
- "Setting OM thresholds for GigE link" (page 250)

The GigE Card views for the NTNY45FA appears as followings:

**GigE Card view showing 4-port NTNY45FA**

GigE Card: NE-4 Frame-1 Shelf-2 Slot-10

MG9000 Actions

GigE Port

3  
2  
1  
0

10

DCC

**Card Attributes**

CLEI Code: -

Card Description: Nortel MG9k SC GigE Card

Hardware Version:

Firmware Version:

Software Version: 08\_0

Serial Number:

Manufacturer: Nortel Networks

PEC Code: NY45FA

**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**

GigE Card Alarms

Critical: 0 Minor: 0

Major: 0 Warning: 0

Apply Refresh Close

**Prerequisites**

There are no prerequisites.

## Action

### Viewing GigE port and link provisioning information

#### Step Action

#### At the MG 9000 Manager

- 1 From the **Shelf View**, double click on the GigE DCC card in the master shelf. The **GigE Card view** appears.
- 2 From the **GigE Card view**, double click on the port icon for which information is to be viewed. The **GigE Port view** appears.
- 3 The View opens. The following figure shows the View.

#### GigE Port View showing the Link Details tab

The following figure shows the GigE Port view showing the Link Controls tab.

**GigE Port View showing the Link Controls tab**

- 4 Use the information in the following table to provision link information.

Tab	Pane	Field or Function	Explanation
Link Details	Port Attributes	Description	Displays the port description
		MAC Address	Physical address of the port
		Port Type	Port type
		OpticsType	Optics type
	Link Attributes	Link Type	Specifies whether the link is network or subtending
		Auto-negotiation Mode	auto negotiation variable

Tab	Pane	Field or Function	Explanation
Link Controls	Local Advertised Values	Auto-negotiation Status	
		Duplex	
		Speed in bps	
		Pause Admin Mode	Link attribute's pause Tx
		MTU Size	Mtu Size
	Partner Advertised Values	Duplex	Local advertised duplex
		Speed	Local advertised speed values
		Pause Admin Mode	Local advertised Pause Admin Mode
	State	Duplex	Partner advertised duplex
		Speed	Partner advertised speed
		Pause Admin Mode	Partner advertised Pause Admin Mode
	Status	Administrative Status	Administrative status of the link as Unlocked, Locked, Forced Lock, or Forced Unlock
		Configuration Status	Configuration status of the link as Online or Offline
Operational Status		Operational status of the link as enabled or disabled	
	Loopback	Identifies if loopback is enabled as No Loop or Facility Loop. Not supported in SN08.	

Tab	Pane	Field or Function	Explanation
		Tx RFI	Link State as Enable or Disable. Set to Enable by default. When enabled, RFI alarms will be raised and when RFI alarms are received, results in a sparing activity. When set to disabled, RFI alarms will not be sent the MG 9000 Manager.
		Rx RFI	Link State as Enable or Disable. Set to Enable by default. When set to enabled, RFI alarms will be raised and when RFI alarms are received, results in a sparing activity. When set to disabled, RFI alarms will not be sent the MG 9000 Manager.
	Soak Values	Bw/Link in bps	
		UAS Count	Count of UnAvailable Seconds, represents 10 SES.
		SES Percent	Number of Severely Errored Seconds (10 SES for 1 UAS)
	Threshold Crossings	Rx EER in percent	
		Rx SD in percent	

5 This procedure is complete.

---

—End—

---

### Creating and deleting protection groups or modifying provisioning details

To create and delete protection groups or modify the provisioning details use the following procedure.

## Provisioning GigE link protection

### Step Action

#### At the MG 9000 Manager

- 1 From the **Shelf View**, select **Actions->Maintenance->Link Protection Provisioning** from the menu bar. The **GigE Protection Provisioning View** appears.

#### GigE Protection Provisioning View

- 2 Use the information in the following table to create or delete protection groups or to modify the provisioning details.

Field	Explanation and action
Protection Group Number	Protection Group Number
Select Group Number	Selecting the protection group number from the pull-down menu will display the provisioning details for the group number
Protection Group Type	Protection group type, 1:1
Protection Mode	Protection mode, select Revertive or Non-revertive
Wait to Revert	Number of seconds to revert, which by default is 600.
Create Group button	Create protection group.

Field	Explanation and action
Delete Group button	Delete protection group.
Modify Group button	Modify the provisioning details (group mode and wait to revert) for the group number.

- 3 This procedure is complete.

—End—

### Provisioning GigE link integrity

#### Step Action

#### *At the MG 9000 Manager*

- 1 From the **Shelf View**, select **Actions->Maintenance->Link Integrity Provisioning**. The **Link Integrity GUI** appears.

#### Link Integrity GUI

NE-4 Link Integrity

MG9000

Link Integrity Data

PROTECTION GROUP 1 ▼

LOSS RATE 2

FREQUENCY in mSec 10

LINK\_MONITORING ENABLE ▼

Refresh Apply Close

- 2 Use the information in the following table to provisioning link integrity. The Link\_Threshold and Link\_Interval values are for the link integrity test which sends a packet between links on the active and inactive GigE DCC cards.

Field	Explanation and action
Protection Group	Select the protection group number
Link_Threshold (Integrity threshold)	Identifies how many packets in a row that must be lost before a error is detected. Default is 2.
Link_Interval (Integrity interval)	Identifies the time for which a packet is expected. Default is 10 ms.
	Using the defaults in Link_Threshold and Link_Interval, 2 packets in a row must be lost, with each packet loss being looked for over a period of 10 ms. This means a problem will detected in 20 ms. After the problem is detected the system will attempt to Address Resolution Protocol (ARP) out on each link to determine if that link has a problem and attempt this twice. If the ARPs fail, than the link is declared bad. If the failed link is the active link, a SWACT will occur.
Link_Monitoring (Integrity monitoring)	Select Enabled or Disabled

- 3 This procedure is complete.

---

—End—

---

### Viewing VLAN provisioning data

---

#### Step Action

---

#### *At the MG 9000 Manager*

- 1 From the **Shelf View**, select **Actions->Maintenance->VLAN Provisioning**. The **VLAN Manager GUI** appears. The following figure shows the VLAN Manager.

**VLAN Manager GUI**

VLAN ID	161	162	163	160
VLAN_NAME	oamp62	ccc62	bc62	dcc62
VLAN_TYPE	OAMP	CALL_CONTROL	BEARER	UNIT
PRIORITY	2	3	3	1
PEAK_RATE	56500	588000	5500000	12500
PRIM_SUBNET_ADDR	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
PRIM_SUBNET_MASK	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
SEC_SUBNET_ADD	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
SEC_SUBNET_MASK	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Buttons: Refresh, Apply, Close

- 2 The information in the following table describes the fields in the VLAN Manager GUI.

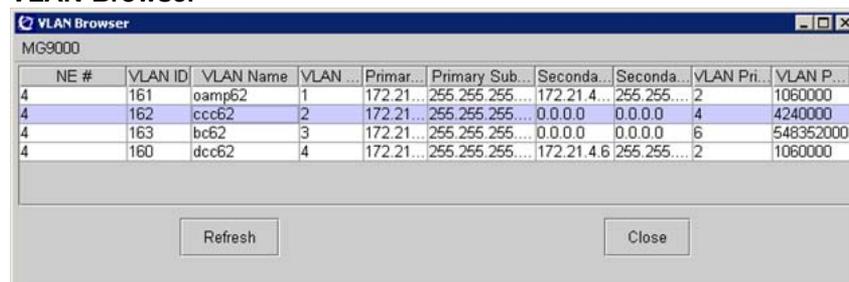
Field	Explanation
VLAN ID	Identifier for each port in the VLAN
VLAN Name	VLAN name
VLAN Type	Purpose for the VLAN
Priority	Priority of the VLAN
Peak Rate	Peak rate for the VLAN
Primary and Secondary Subnet Address and mask	Primary and Secondary address and subnet mask of the VLAN.

- 3 This procedure is complete.

—End—

**Listing all VLAN connections using the VLAN Browser****Step Action****At the MG 9000 Manager**

- 1 From the **Subnet View**, select **Configuration->VLAN Browser** from the menu bar. The **VLAN Browser** appears. The VLAN Browser is shown in the following figure.

**VLAN Browser**


NE #	VLAN ID	VLAN Name	VLAN ...	Primar...	Primary Sub...	Seconda...	Seconda...	VLAN Pri...	VLAN P...
4	161	oamp62	1	172.21...	255.255.255...	172.21.4...	255.255...	2	1060000
4	162	ccc62	2	172.21...	255.255.255...	0.0.0.0	0.0.0.0	4	4240000
4	163	bc62	3	172.21...	255.255.255...	0.0.0.0	0.0.0.0	6	548352000
4	160	dcc62	4	172.21...	255.255.255...	172.21.4.6	255.255...	2	1060000

- 2 Use the information in the following table to identify the information presented in the VLAN Browser.

Field	Description
NE number	MG 9000 network element number
VLAN ID	Port VLAN id. Each port belongs to a VLAN.
VLAN name	VLAN name
VLAN type	
Primary Subnet Address	Primary subnet address of the VLAN.
Primary Subnet Mask	Primary subnet mask address of the VLAN.
Secondary Subnet Address	Secondary subnet address of the VLAN.
Secondary Subnet Mask	Secondary subnet mask address of the VLAN.
VLAN Priority	Priority of the VLAN
VLAN Peak	Peak rate for the VLAN id.

- 3 This procedure is complete.

---

—End—

---

**Adding links to and deleting links from a protection group**

Use the following procedure when it becomes necessary to add links to or delete links from a protection group.

**Adding links to and deleting links from a protection group**


---

**Step Action**

---

*At the MG 9000 Manager*

- 1 From the **Shelf View**, double click on the active GigE DCC card in the master shelf. The **GigE Card view** appears.
- 2 Double click on the active port. The **GigE Port view** appears. From the **GigE Port view**, select **Actions->Maintenance->Link Protection Maintenance** from the menu bar. The **Link Protection Maintenance View** appears.

#### Link Protection Maintenance View

- 3 Use the information in the following table to add a link or delete a link from a protection group.

Field	Explanation and action
Protection Group Number	Protection Group Number
Working or Protection	Protection group type, Working, Protected, or Not Used.
Protection Status	Identifies the current status of the selected link.
Add Link To Group button	Used to add a link to a protection group.
Pull down	Used to select the protection group the link is to be added to or deleted from.
Delete Link From Group button	Used to delete a link from a protection group.

- 4 This procedure is complete.

—End—

### Viewing GigE link protection group

Use the LCI to view the GigE link protection group and status. Select the Maintenance button in the LCI banner. Click on the master shelf and click on the Active GigE DCC card. Click on Link->Protection->Status. The GigE Link Protection Status screen appears. Refer to "[GigE link protection status](#)" ([page 387](#)) for information on viewing the GigE link protection group status.

It is recommended that customers set up Remote LCI to support any node recovery or troubleshooting from a central location. 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.

### Setting OM thresholds

Use the following procedure to set the OM threshold values for

- ES - errored seconds
- SES - severely errored seconds
- UAS - unavailable seconds

When the threshold values are exceeded, a notification will be generated by the MG 9000.

### Setting OM thresholds for GigE link

Step	Action
------	--------

*At the MG 9000 Manager*

- |   |  |
|---|--|
| 1 | From the <b>Shelf View</b> , double click on the active GigE DCC card in the master shelf. The <b>GigE Card view</b> appears.  |
| 2 | Double click on the active port. The <b>GigE Port view</b> appears. From the <b>GigE Port view</b> , select <b>Actions-&gt;Maintenance-&gt;Set Thresholds</b> from the menu bar. The <b>OM Thresholds GUI</b> appears. |

**OM Thresholds View**

Type	Short Period	Short Ratio	Long Period	Long Ratio	Notify
ES	15	5	15	5	Enable ▼
SES	15	5	15	5	Enable ▼
UAS	15	1	15	1	Enable ▼

Buttons: Apply, Refresh, Close

- 3 Use the information in the following table to set the link OM Thresholds.

Field	Explanation and action
Type	The OM parameters (ES, SES, and UAS) whose thresholds can be changed.
Short Period	Short period for each of the parameters.
Short Ratio	The threshold value for the short period of each parameter.
Long Period	Long period for each of the parameters.
Long Ratio	The threshold value for the long period of each parameter.
Notify	Used to select if a notification will be generated by the MG 9000.
Apply button	Set the new values.

- 4 This procedure is complete.

---

—End—

---

## Provisioning SIC inputs and outputs

---

### When to use this procedure

Use this to provision shelf interface card (SIC) inputs and outputs.

The SIC Input/Output Provisioning screen displays the following characteristics of the SIC inputs and outputs:

- Input/Output name
- Input/Output description
- Administration state (outputs only)
- Operational state
- Alarm severity

### Prerequisites

There are no prerequisites.

### Action

The SIC Card View is accessed by double clicking on the SIC card in the Shelf View. The SIC Card View displays characteristics and states for the SIC card. To access the SIC Input/Output View use the INPUTS/OUTPUTS button on the SIC Card View.

The following figure shows the SIC Card View.

## SIC Card View

The screenshot shows the 'SIC Card View' window with the following details:

- Card Attributes:**
  - CLEI Code: SAPQAEGAAA
  - Card Description: Nortel UEM Shelf Card
  - Hardware Version: (empty)
  - Firmware Version: 02 M171
  - Software Version: (empty)
  - Serial Number: M171ZWWG9
  - Manufacturer: Nortel Networks
  - PEC Code: NY23AA
- Status:**
  - Availability Status: NORMAL
  - Usage Status: IDLE
  - Standby Status: PROVIDING\_SERVICE
  - Card Alarm Status: NONE
  - Procedural Status: Normal
  - Control Status: (empty)
- State:**
  - Administrative State: UNLOCKED
  - Configuration State: ONLINE
  - Operational State: ENABLED
- Inputs/Outputs:**
  - INPUTS / OUTPUTS
- SIC Card Alarms:**
  - Critical: 0
  - Minor: 0
  - Major: 0
  - Warning: 0

Buttons at the bottom: Apply, Refresh, Close.

## Viewing a SIC input

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 At the **Subnet View**, double click on the **MG 9000** to be modified. The **Frame View** appears.

- 2 From the **Frame View**, double click on the shelf. The **Shelf View** appears.
- 3 From the **Shelf View**, double click on the SIC card. The **SIC card View** appears.
- 4 Click the **Inputs/Outputs** button to view the SIC card inputs.
- 5 Select the **Inputs radio** button in the top left hand corner of the **SIC Input/Output View**.
- 6 Select the **SIC input** to view in the **Inputs scroll pane window** on the left hand side of the view.
- 7 This procedure is complete.

---

—End—

---

### Modifying the Input Name or the In Alarm Severity

---

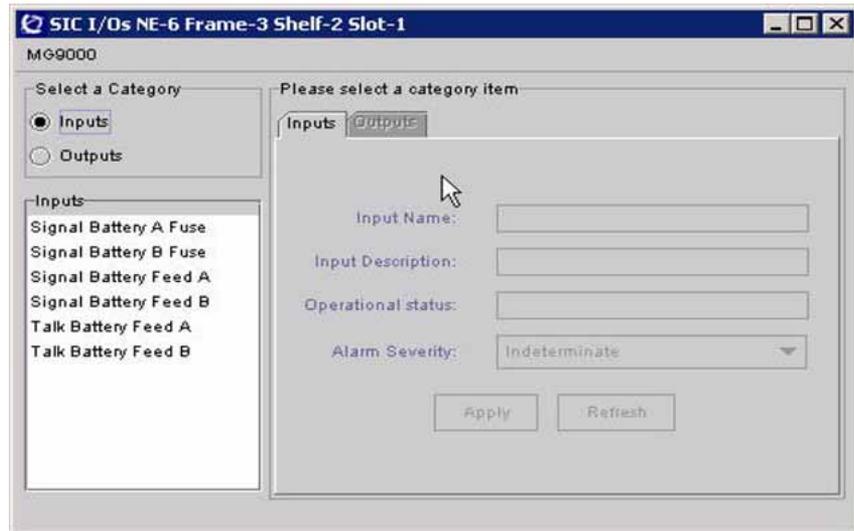
Step	Action
------	--------

---

*At the MG 9000 Manager*

- 1 At the **SIC Input/Output View**, change the value(s)
- 2 Press the **Apply** button.  
**Note:** The Refresh button can be used to resync the **Input/Output view** with the data that is currently applicable to the selected input.

The following figure shows the **SIC Input/Output** window with the inputs listed.

**SIC Input/Output View (inputs)**

- 3 This procedure is complete.

---

—End—

---

**Viewing a SIC output**

Step	Action
------	--------

**At the MG 9000 Manager**

- 1 At the **SIC Input/Output View**, select the **Outputs** radio button in the top left hand corner of the **SIC Input/Output View**.
- 2 Select the **SIC output** to view in the **Outputs scroll pane** window on the left hand side of the view.
- 3 This procedure is complete.

---

—End—

---

**Changing the Output Name and/or Output Alarm Severity**

Step	Action
------	--------

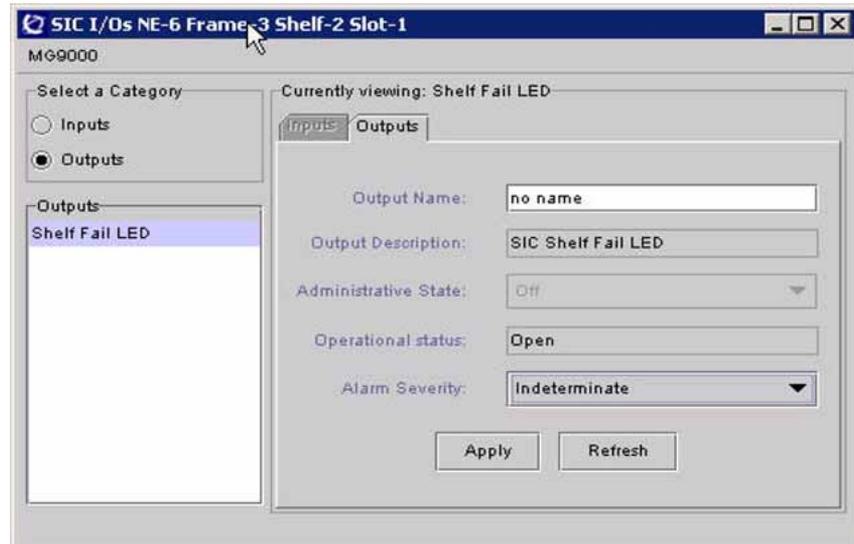
**At the MG 9000 Manager**

- 1 At the **SIC Input/Output View**, change the value(s).
- 2 Press the **Apply** button.

**Note:** The **Refresh** button can be used to resync the **Input/Output view** with the data that is currently applicable to the selected output.

The following figure shows the **SIC Input/Output** window with outputs listed.

### SIC Input/Output (outputs)



3 This procedure is complete.

---

—End—

---

---

## Provisioning IBIP inputs and outputs

---

### When to use this procedure

Use this information to provision intelligent bay interface panel (IBIP) alarm inputs and outputs (I/O).

The IBIP I/Os screen displays the following characteristics of the IBIP inputs and outputs:

- Input/Output name
- Input/Output description
- Administration state (outputs only)
- Operational state
- Alarm severity

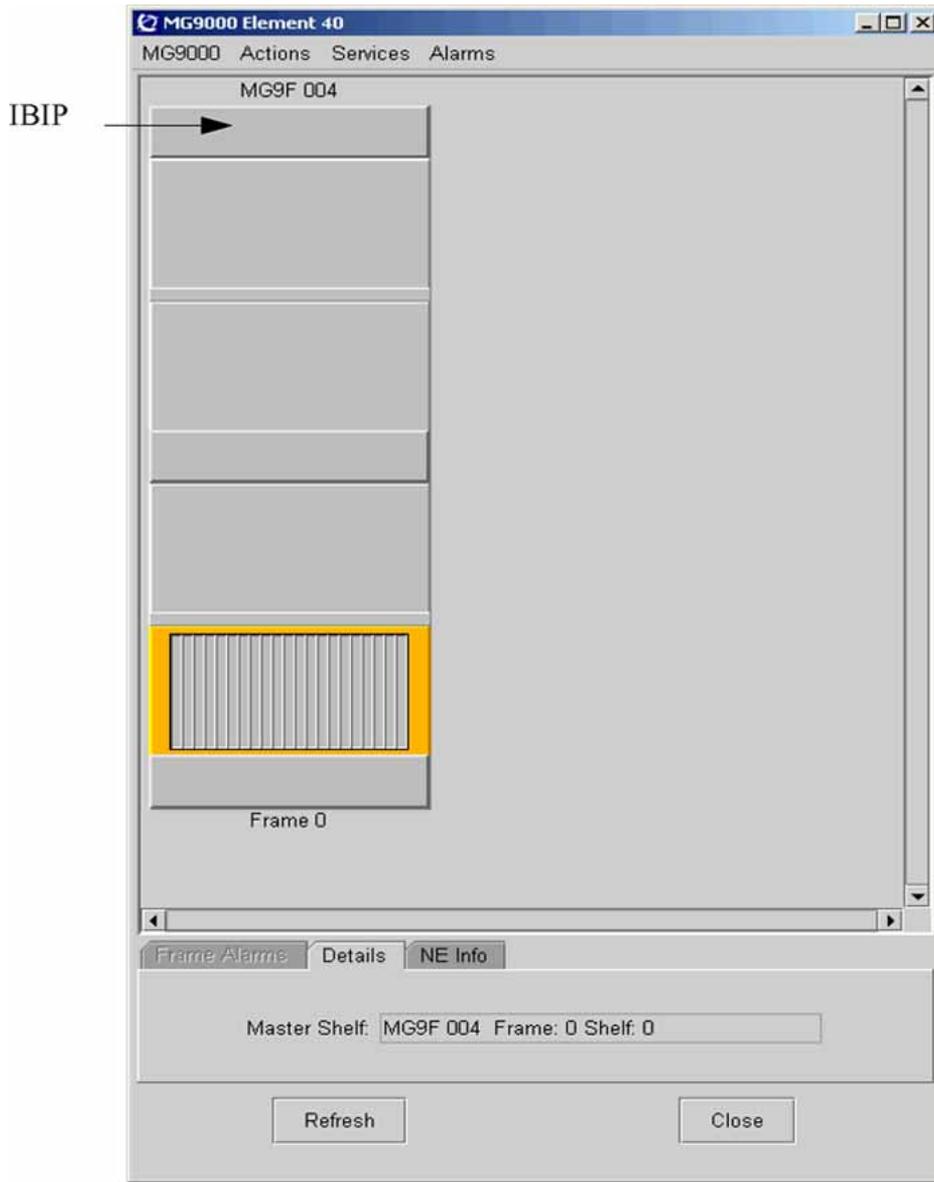
### Prerequisites

There are no prerequisites.

### Action

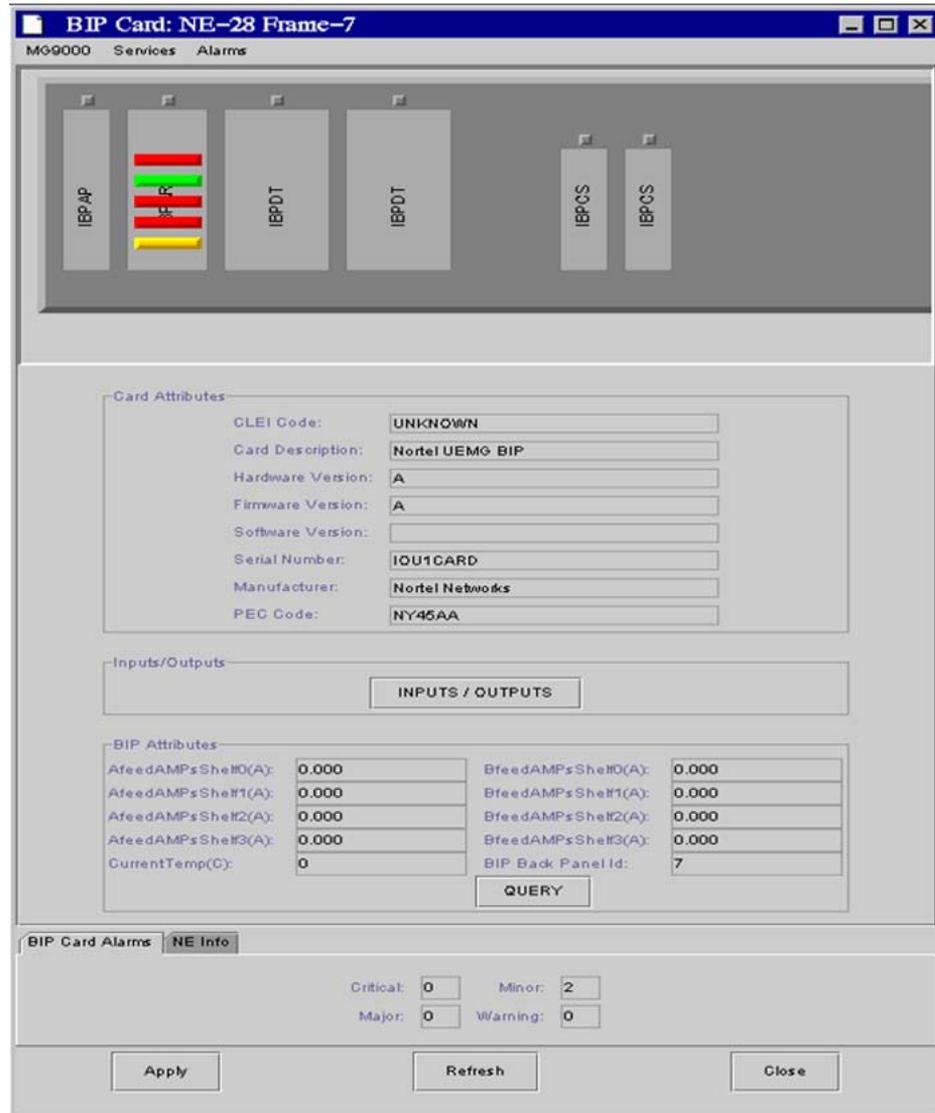
The BIP Card View, accessed by double clicking on the IBIP in the Frame View, can be used to access the BIP I/Os View. The following figure shows the IBIP's location in the MG 9000 frame.

Frame View showing the IBIP



The BIP Card view also displays characteristics and LED states for the IBIP.

**BIP Card View showing the LEDs**



To access the IBIP I/Os View use the INPUTS/OUTPUTS button on the BIP Card View. To access the BIP I/O View for a specific set of ECU (Environmental Control Unit) Inputs/Outputs double click on either fan unit in the Frame view.

To view a IBIP input perform the following procedure.

**Viewing IBIP inputs**

**Step Action**

***At the MG 9000 Manager***

- 1 From the **IBIP I/O View**, select the **Inputs radio** button in the top left hand corner of the IBIP Input/Output View
- 2 Select the IBIP input to view in the Inputs scroll pane window on the left hand side of the view.
- 3 This procedure is complete.

---

—End—

---

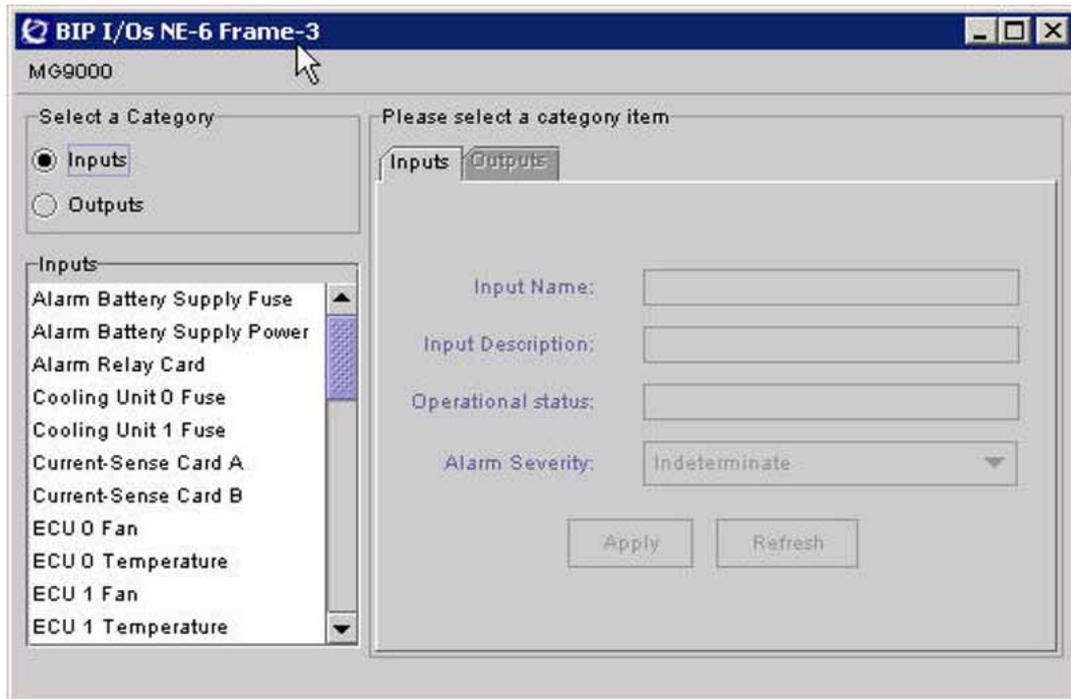
For the IBIP inputs the Input Name and Input Alarm Severity are configurable. To modify either the Input Name and/or Input Alarm Severity perform the following steps:

1. Change the Input Name and Input Alarm Severity value(s).
2. Press the Apply button.
3. This procedure is complete.

**Note 1:** The MG 9000 Manager will not permit any Indeterminate Input scan point alarms to appear at the Subnet View or the IBIP icon in the Frame View. If any of the scan point alarms inputs must appear, the alarm severity must be changed to some value other than Indeterminate.

**Note 2:** The Refresh button can be used to resync the Input/Output view with the data that is currently applicable to the selected input.

**Note 3:** The Query button is used to refresh the threshold attributes on the IBIP reported to the BIP Card View from the MG 9000.

**BIP I/Os View (Inputs)**

To view a IBIP output perform the following procedure.

**Viewing IBIP Outputs****Step Action****At the MG 9000 Manager**

- 1 At the **IBIP I/O View**, select the **Outputs radio** button in the top left hand corner of the IBIP Input/Output View.
- 2 Select the IBIP output to view in the Outputs scroll pane window on the left hand side of the view.
- 3 This procedure is complete.

—End—

For the IBIP outputs the following fields are configurable:

- Output Name
- Output Administrative State (Signal Distribution Points only)
- Output Alarm Severity

**Note:** The MG 9000 Manager will not add any Indeterminate Output alarms to the alarm browser. This prevents the LED events from showing up as alarms. If any of the outputs must appear in the alarm browser, the alarm severity must be changed to some value other than Indeterminate.

To modify either of the fields perform the following steps:

1. Change the value(s)
2. Press the Apply button.
3. This procedure is complete.

**Note:** The **Refresh** button can be used to resync the Input/Output view with the data that is currently applicable to the selected output.

### BIPI/Os View (Outputs)

The screenshot shows a web-based configuration window titled "BIP I/Os NE-6 Frame-3" for an "MG9000" device. On the left, there is a "Select a Category" section with radio buttons for "Inputs" and "Outputs", where "Outputs" is selected. Below this is a list of output categories: "Aisle Alarm status", "Alarm Cut-off LED", "Alarm Fail LED", "Alarm Relay Card LED", "Audible Critical Alarm", "Audible Major Alarm", "Audible Minor Alarm", "Critical LED Bank", "Current-Sense Card A LED", "Current-Sense Card B LED", and "ECU 0 LED". The main area is titled "Please select a category item" and has two tabs: "Inputs" and "Outputs". The "Outputs" tab is active, showing a form with the following fields: "Output Name:" (text input), "Output Description:" (text input), "Administrative State:" (dropdown menu set to "On"), "Operational status:" (text input), and "Alarm Severity:" (dropdown menu set to "Indeterminate"). At the bottom of the form are "Apply" and "Refresh" buttons.

## Using the Bandwidth Manager

### When to use this procedure

The MG 9000 Manager's Bandwidth Management application provides

- the capability to enforce maximum bandwidth values for each of the main service types (SLoA, PLoA, ABI, and xDSL) for VCs (virtual channels) through the network interface for AAL1 systems. In the case of VoIP, only the SLoA and DSL service type partitions can be used. ABI bearer and ITP bearer traffic falls under the umbrella of the SLoA partition on a VoIP system.
- the capability to monitor the currently allocated reserved bandwidth on the Network interface and the SLoA reserved bandwidth to monitor per shelf capacity
- a way to manage configurable thresholds

The MG 9000 Manager also receives corresponding state change notifications. These are useful for scenarios where the reserved bandwidth is nearing capacity.

There are no thresholds for PLoA or xDSL since these connections are provisioned by the MG 9000 Manager, which can check the currently reserved capacity before provisioning.

**Note:** After provisioning bandwidth management data on the MG 9000, it is recommended that a record be maintained of all provisioning information.

### Bandwidth allocation overview

The following describes the way bandwidth is available for various main services on either an AAL1 or a VoIP system.

- Voice over AAL1 - SLoA, PLoA, DSL and ABI all share the same bandwidth. The total of all of these items together must be less than or equal to 100% of the Maximum Partitionable Bandwidth. The Total Partitionable Bandwidth displayed on the MG 9000 Manager is

where

Total partitionable = Total - OAM - ITP CallIP messaging - ABI CallIP messaging

- Voice over IP - The total bandwidth for VoIP is divided into three PVCs plus any DSL PVCs

The three PVCs are described as follows:

— PVC A (CCB) - Carries ITP H.248 and all ITP and ABI bearer traffic.

- PVC B (OAM) - Carries MG 9000 Manager traffic such as, data collection and sftp.
- PVC C (ABI) - Carries ABI H.248 and XPM messaging

The Bandwidth Manager ensures that bandwidth only from the appropriate PVC is used.

PVC A is normally much bigger than PVC B or C.

The Total Partitionable Bandwidth shown on the MG 9000 Manager = Total Partitionable Bandwidth - PVC B - PVC C

SLoA partition uses bandwidth from PVC A only.

- Gigabit Ethernet - When the MG 9000 is equipped with NTNY45FA GigE DCC cards, private lines and DSL services are not supported. The Bandwidth Manager will monitor the following network interface bandwidth data for an MG 9000 with GigE DCC cards:
  - current ITP voice usage
  - current ABI voice usage
  - overall network interface utilization

The data is displayed in bits/sec on GigE systems. Bandwidth partitioning is supported on GigE systems.

There is no significance of putting any partition values for PLoA or ABI for an IP system. ABI voice uses the CCB PVC. ABI messaging uses a PVC not partitionable using the Bandwidth Manager.

Each DSL data service has a PVC. This is created through the MG 9000 Manager. The remainder of (Total Partitionable Bandwidth - PVC A) can be used for partitioning guaranteed DSL on the Bandwidth Manager GUI.

## Prerequisites

There are no prerequisites

## Action

### Starting the Bandwidth Manager

Step	Action
------	--------

*At the MG 9000 Manager*

- |   |  |
|---|--|
| 1 | From the <b>NE desktop view</b> menu bar, select <b>Services-&gt;Bandwidth Manager</b> . The <b>Bandwidth Manager view</b> appears showing the current values for the MG 9000. |
|---|--|

2 This procedure is complete.

---

—End—

---

The following table lists the commands, controls and tabs available from the Bandwidth Manager view.

#### Bandwidth Manager GUI commands, controls and GUI tabs

Command / control	Tab	Description and purpose
<b>Managing section</b>		
	Partition tab	<p>For UA-IP switched lines, the Maximum Partitionable Bandwidth on the Partition tab allows the technician to view the maximum bandwidth in cells/sec. While the PVC traffic parameters are fixed, this field serves to further limit that bandwidth if the available bandwidth is needed for other services. Attempts to set values greater than the available CallP VCC bandwidth will result in the new value being rejected.</p> <p>Setting the value to 0 indicates that the traffic descriptor associated with the CallP VCC will be used to provide bandwidth management. That is, all available bandwidth on that VCC will be used for switched lines traffic.</p>
Partition Enabled option	Partition tab	<p>The Partition Enabled option can be changed to Yes/No. This option enables or disables connections admission control (CAC) for all services except switched lines in a UA-IP solution.</p> <p>When the "No" radio button is selected, CAC is disabled and the UA-IP switched lines connection admission control remains active because quality of service would be severely degraded once the combined bandwidth for all UA-IP switched line calls exceed the available call processing (CallP) virtual channel connection (VCC) bandwidth. To disable partitioning, select the "No" radio button and click on the Apply button.</p> <p>When the "Yes" radio button is selected, all the percentage fields (PLoA, SLoA, and Guaranteed DSL) except the "Total Partitionable" become editable. The values can be entered in the corresponding text fields.</p> <p><b>Note:</b> When the "Yes" radio button is selected for an MG 9000 with GigE DCC cards, the only editable field available is Bearer. Values are presented in bits/sec.</p>

Command / control	Tab	Description and purpose
		<p>For UA-IP, the SLoA partition is bandwidth limited by the CallP PVC provisioned at the LCI. The SLoA partition cannot be equal to the Total Partitionable bandwidth, it must be less than or equal to the bandwidth reserved for the CallP PVC. The SLoA partition is calculated against the CallP PVC instead of Total Partitionable bandwidth. The DSL partition can use the remainder of the Total Partitionable bandwidth displayed on the MG 9000 Manager; the bandwidth not consumed by the CallP PVC. This means the DSL partition is also bandwidth limited by the CallP PVC, not the SLoA partition configured. As mentioned earlier, partition values for PLoA and ABI do not apply to a UA-IP solution. The sum of the three partitions (DSL, ABI and PLoA) cannot be configured to be greater than (Total Partitionable Bandwidth on MG 9000 Manager - CallP PVC Bandwidth).</p> <p>Refer to the following example:</p> <ul style="list-style-type: none"> <li>• Call PVC = 342,600 cells/sec</li> <li>• OAM PVC = 5000 cells/sec</li> <li>• SLoA Partition: 80%</li> </ul> <p><b>Note:</b> This allows switched lines to use 80% of the bandwidth reserved for the CallP PVC which is less than 80% of the Total Partitionable bandwidth because the bandwidth reserved for SLoA is calculated against the CallP PVC instead of the Total Partitionable bandwidth.</p> <ul style="list-style-type: none"> <li>• Guaranteed DSL: 2%</li> </ul> <p><b>Note:</b> This is the remaining bandwidth (Total Partitionable bandwidth - CallP PVC - OAM PVC - ABI PVC.)</p> <p>There can be cases where the percentage values displayed on the Bandwidth Manager GUI might be misleading for a UA-IP solution.</p> <p>For example,</p> <ul style="list-style-type: none"> <li>• CallP PVC = 94500</li> <li>• Total Partitionable Bandwidth = 103268</li> </ul> <p>This leaves only 8768 cell/seconds for the other three services.</p> <p>Consider the following valid partition values entered by the user and their corresponding cell/seconds:</p> <ul style="list-style-type: none"> <li>• PLoA Partition: 0% 0 cells/sec</li> <li>• SLoA Partition: 100% 94500 cells/sec</li> <li>• DSL Partition: 6% 6196 cells/sec</li> <li>• ABI Partition 0% 0 cells/sec</li> </ul>

Command / control	Tab	Description and purpose
Apply	Partition tab	<p>The SLoA bandwidth is calculated against the CallP PVC instead of Total Partitionable Bandwidth. Whereas, bandwidth for DSL service is calculated with respect to the Total Partitionable Bandwidth.</p> <p>Since this is an IP system, there is no point in allocating partition for ABI or PLoA though they are enabled. The total partitioned bandwidth for all the four services will not be allowed to exceed the Total Partitionable Bandwidth. However the total percentage may appear to have crossed 100%.</p> <p>Click on the Apply button at any point and the values shown in the fields are validated and sent to the MG 9000.</p>
	Threshold tab	<p>The new Bandwidth Congestion Threshold, DSL utilized bandwidth congestion threshold, and queue congestion threshold value can be set according to the following rules:</p> <ul style="list-style-type: none"> <li>• The acceptable range is from 50 to 100</li> <li>• If the user does not enter the valid value, an error message is displayed when the "Apply" button is clicked.</li> </ul> <p><b>Note:</b> Bandwidth Congestion Threshold is the only value that appears when the MG 9000 is provisioned with GigE DCC cards.</p>
	Priority tab	<p>The Priority tab allows the technician to make changes to the hold (release) priority related attributes for DS1 IMA links.</p> <p><b>Note:</b> The Priority tab does not appear when the MG 9000 is provisioned with GigE DCC cards.</p>
<b>Monitoring section</b>		
	Network Interface tab	<p>None of the fields shown are editable. They display the current values in the MG 9000.</p> <p><b>Note:</b> When the MG 9000 is provisioned with GigE DCC cards, values are provided in bits/sec. The only fields that appear are the ITP Bearer, ABI Bearer, and Total.</p>
	Per Shelf tab	<p>None of the fields shown are editable. They display the current values in the MG 9000.</p> <p><b>Note:</b> When the MG 9000 is provisioned with GigE DCC cards, the Bandwidth values are provided in bits/sec.</p>
	Switch Fabric Congestion tab	<p>None of the fields shown are editable. They display the current values in the MG 9000.</p> <p><b>Note:</b> The Switch Fabric Congestion tab does not appear when the MG 9000 is provisioned with GigE DCC cards.</p>

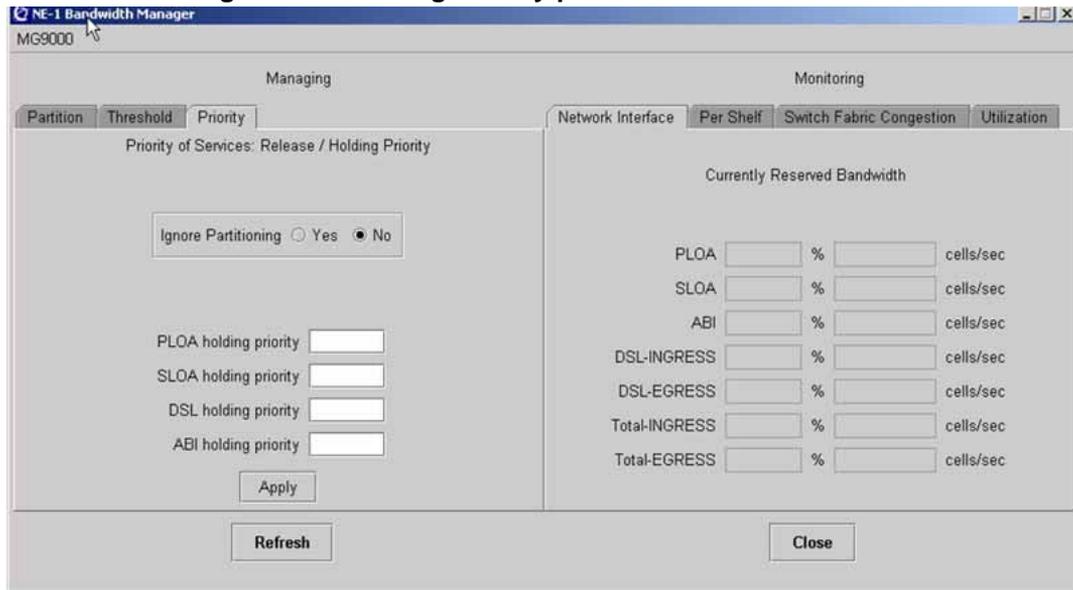
Command / control	Tab	Description and purpose
	Utilization tab	None of the fields shown are editable. They display the current values in the MG 9000.  <b>Note:</b> When the MG 9000 is provisioned with GigE DCC cards, values are provided in bits/sec. In addition, the only fields that appear are Mean Ingress Rate and Mean Egress Rate.
Close		Closes the Bandwidth Manager screen
Refresh		Retrieves all the field values and displays them on the screen.

The Partition tab is shown in the following figure.

Bandwidth Manager View showing Partition panel

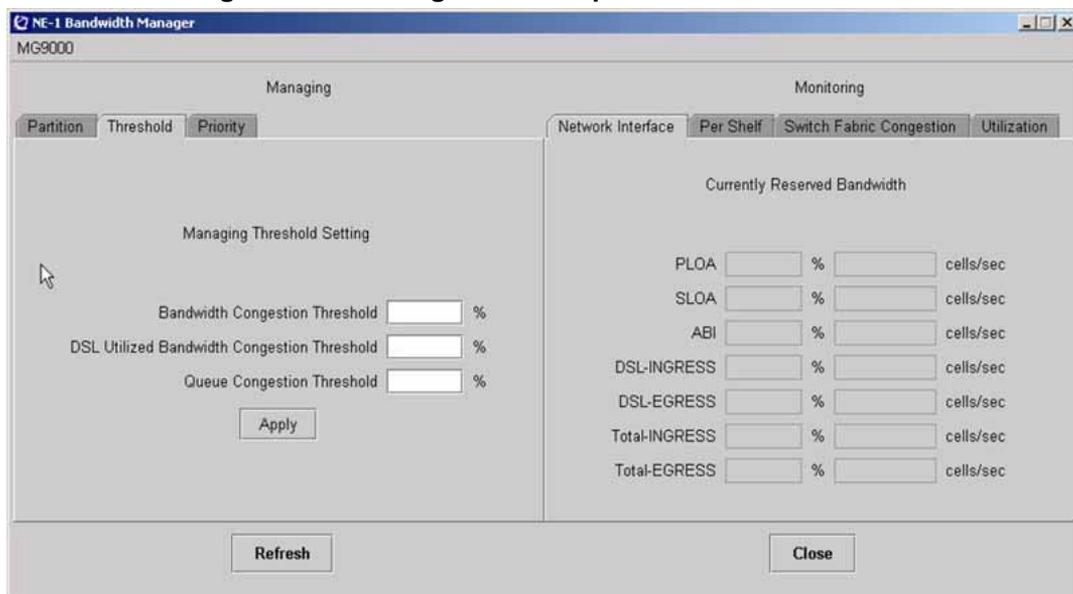
The Priority tab is shown in the following figure.

### Bandwidth Manager View showing Priority panel



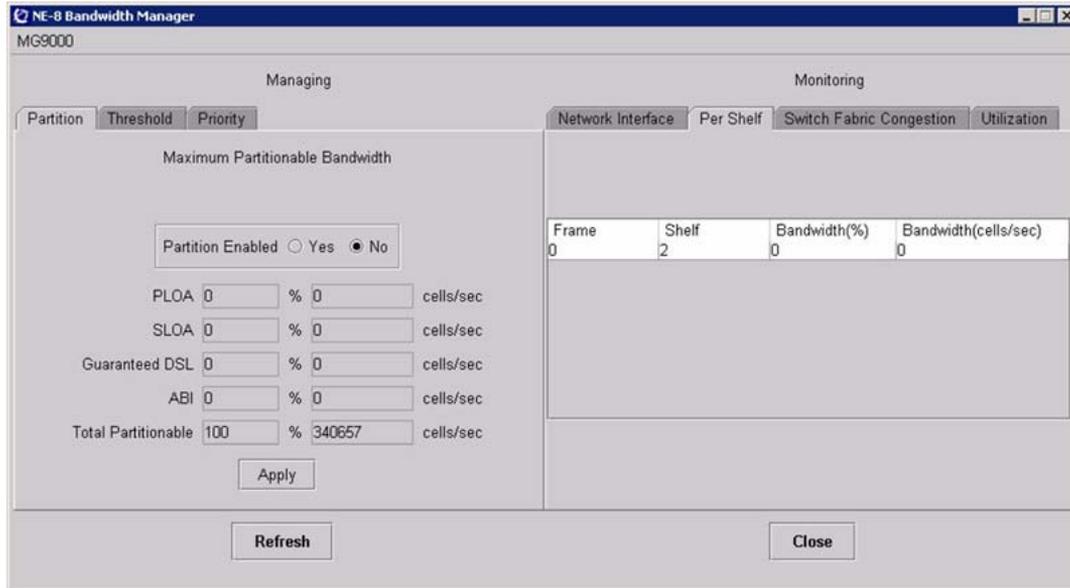
The Threshold Panel selected is shown in the following figure. The Network Interface tab on the right side of the GUI is also shown.

### Bandwidth Manager View showing Threshold panel



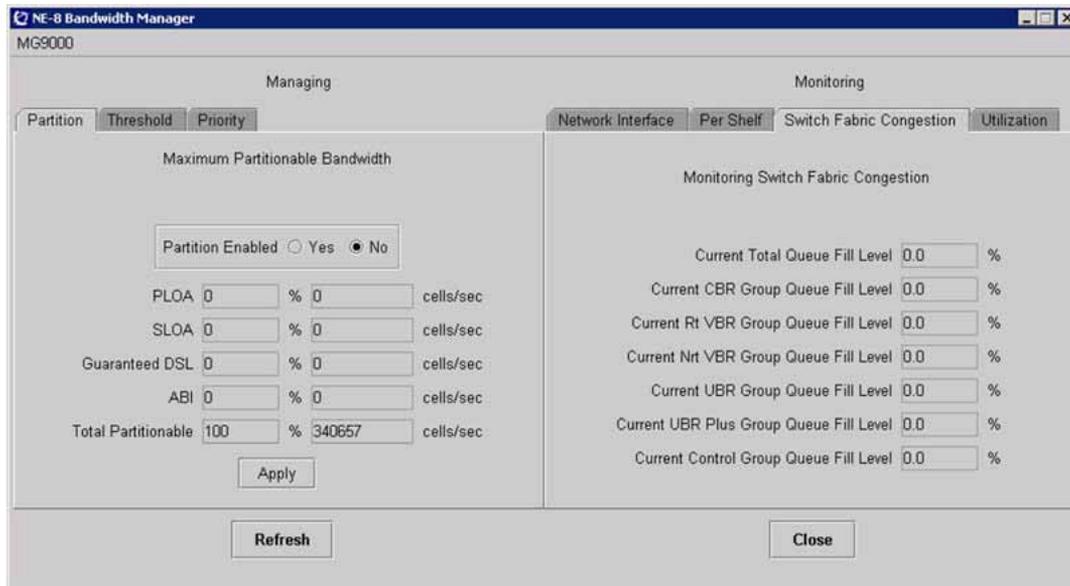
The Per Shelf Panel is shown in the following figure.

**Bandwidth Manager View showing Per Shelf panel**



The Switch Fabric Congestion Panel is shown next.

**Bandwidth Manager View showing Switch Fabric Congestion panel**



The Utilization Panel is shown in the following figure.

### Bandwidth Manager View showing Utilization panel

The screenshot shows the 'NE-8 Bandwidth Manager' window for MG9000. It is divided into two main sections: 'Managing' and 'Monitoring'. The 'Managing' section has tabs for 'Partition', 'Threshold', and 'Priority'. The 'Monitoring' section has tabs for 'Network Interface', 'Per Shelf', 'Switch Fabric Congestion', and 'Utilization'. The 'Utilization' tab is active, showing 'Network Interface Bandwidth Utilization' with fields for Mean Ingress Cell Rate, Mean Egress Cell Rate, Mean Ingress DSL Cell Rate, and Mean Egress DSL Cell Rate, each with a percentage and cells/sec value. The 'Managing' section shows 'Maximum Partitionable Bandwidth' with a 'Partition Enabled' radio button set to 'No', and fields for PLOA, SLOA, Guaranteed DSL, ABI, and Total Partitionable bandwidth, each with a percentage and cells/sec value. 'Apply', 'Refresh', and 'Close' buttons are visible at the bottom.

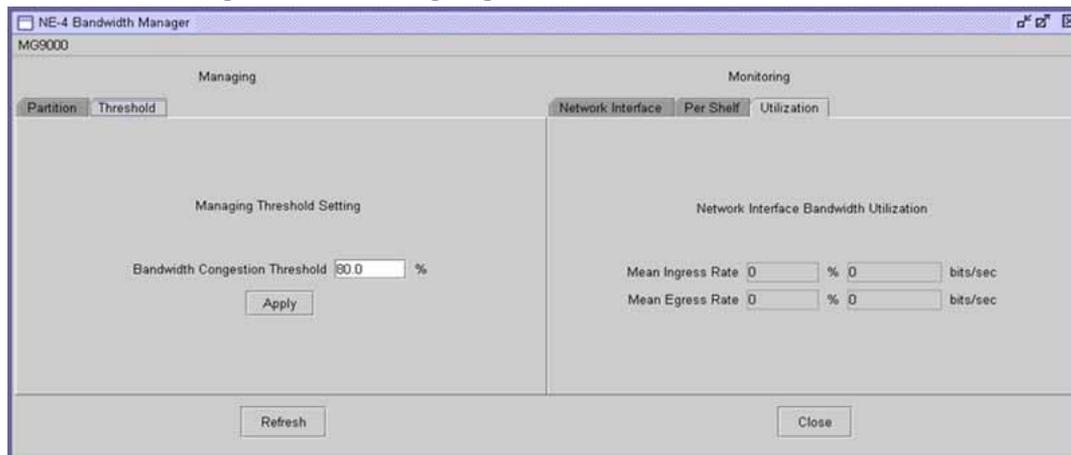
The following figure shows the Partition tab when GigE DCC cards are provisioned.

### Bandwidth Manager view showing GigE Partition and Network Interface tabs

The screenshot shows the 'NE-4 Bandwidth Manager' window for MG9000. It is divided into two main sections: 'Managing' and 'Monitoring'. The 'Managing' section has tabs for 'Partition' and 'Threshold'. The 'Monitoring' section has tabs for 'Network Interface', 'Per Shelf', and 'Utilization'. The 'Partition' tab is active, showing 'Maximum Partitionable Bandwidth' with a 'Partition Enabled' radio button set to 'Yes', and fields for Bearer, Upper Bound, and Network Interface bandwidth, each with a percentage and bits/sec value. The 'Network Interface' tab is also active, showing 'Currently Reserved Bandwidth' with fields for ITP Bearer, ABI Bearer, and Total bandwidth, each with a percentage and bits/sec value. 'Apply', 'Refresh', and 'Close' buttons are visible at the bottom.

The following figure shows the Managing Threshold and Monitoring Utilization tabs.

### Bandwidth Manager view showing GigE Threshold and Utilization tabs



---

## Using the Bandwidth Management Planning Tool

---

### When to use this procedure

This procedure is used to assist in planning an MG 9000 deployment by estimating various combinations of lines (SLoA, SLoIP, PLoA, DS-512 [ABI] and DSL) given the target service levels. The Bandwidth Management Planning Tool is a stand alone JAVA application that runs on Windows or Solaris operating systems. The Solaris version is packaged with the MG 9000 Manager.

**Note:** More information on the Bandwidth Management Planning tool is available in the help document that accompanies the tool. Also available with the tool is an explanation of the mathematics used in the tool.

The following are the high level steps followed to obtain bandwidth calculations from the Bandwidth Management Planning Tool:

1. Site information
2. Network interface
3. Solution type
4. Operational mode
5. Switched lines
6. Private lines
7. DSL lines
8. DS-512 (ABI) channels
9. Obtain results

### VCC parameters

On the Results panel, the user may generate the VCC parameters that will be used by the MG 9000 for

- Call Control Signalling - this VCC is used for Megaco ITP CallP messaging
- OAM - this VCC is used to communicate with the MG 9000 Manager and any other OAMP device
- ABI - this VCC is used to support ABI CallP

For the UA-IP solution, this information may be used as a guide to configure the MG 9000's Call Control PVC and OAM PVC.

For the UA-AAL1 solution, these VCCs are not configurable.

## Toolbar and menu commands

The following commands are available from the toolbar and menu:

- New - creates a new empty MG 9000 site configuration data set
- Open - opens an MG 9000 site data file with a file type extension of .mg9k)
- Save/Save As - saves MG 9000 site data to a file with a file type extension of .mg9k
- Generate Report - generates a report reflecting all of the site data entered in the various steps and outputs the results from the Results panel. The report is a plain text temporary file that is displayed using NotePad on Windows and using VI on Solaris. The report can be printed or saved as a permanent file. To change the editor used to display the report to any plain text editor available on the system use the Options dialog box.
- Options - displays the Options dialog box. See Options for more details.
- Erlang Calculator - displays a general purpose Erlang calculator
- Help - displays the Help document. The document is normally presented in the user's default web browser on Windows. The tool attempts to present the Help document using the Netscape Navigator web browser on Solaris machines. If the Netscape web browser is not installed on a Solaris machine the user may need to bring up the Help document manually using any available html browser.
- Exit - exits the program

## Options

The Options dialog box provides the following options:

- Intraswitching Percentage - specifies the default intraswitching percentage value used for new switched lines table entries
- CCS - specifies the default CCS value used for new switched lines table entries.
- Grade of Service - specifies the default grade of service (blocking probability) value used for switched lines
- Mean Rate - specifies the default mean rate value used for new DSL table entries
- Guaranteed Bandwidth - specifies whether the Guaranteed field of new DSL table entries defaults to being checked or unchecked (that is, true or false)
- Utilization Percentage - specifies the default utilization percentage value used for new DSL table entries

- Operational Mode - specifies whether the default operational mode for new sites is bandwidth mode or lines mode
- Network Interface - specifies whether the default network interface for new sites is OC3 or DS1-IMA. If the choice is DS1-IMA, the default number of DS1s in the IMA group may be specified also.
- Report Editor - specifies the text editor used to display site reports via the Generate Report action. An example for switching to the Windows WordPad editor might be the following:  
C:\Program Files\Windows NT\Accessories\WORDPAD.EXE
- Show Button Hints - specifies whether the small popup button help windows are displayed when the cursor is paused over a toolbar button
- Include Site Notes in Site Report - specifies whether the site notes from the Site Information step are included in the site report

## Prerequisites

There are no prerequisites

## Action

### Using the Bandwidth Management Planning tool

Step	Action
<i>At the MG 9000 Manager workstation or Windows-based PC</i>	
1	Enter information describing the MG 9000 site being configured <ul style="list-style-type: none"> <li>• site name - user defined name for the MG 9000</li> <li>• site notes - user defined notes associated with the MG 9000 site</li> </ul>
2	Select the network interface type (OC3 or DS1-IMA). If DS1-IMA is chosen, select the number of DS1s that constitute the DS1-IMA group.
3	Enter the solution type, UA-AAL1 or UA-IP. If UA-IP is entered, select the desired voice codec and packetization rates.  Include the desired number of shelves for the MG 9000. This entry aids in the calculation of bandwidth requirements for signaling and OAMP.
4	Select the mode of operation from the following: <ul style="list-style-type: none"> <li>• Bandwidth - determine the amount of network interface bandwidth used for a given number of lines. Specify the number of lines for each line type in the switched lines, private lines,</li> </ul>

and DSL lines steps. The Results step calculates the amount of bandwidth required for each defined line type as both a percentage and as units of Mbps.

- Lines - determine the number of lines that can be supported if the percent of each service type is known. Specify the percentage of available network interface bandwidth to be allocated to each defined line type in the switched lines, private lines, and DSL lines steps. The Results step calculates the number of lines that can be supported for each defined line type.

**Note:** While in Bandwidth mode, the column labeled "# of lines" appears in switched lines, private lines, and DSL lines tables in the corresponding steps. The column is replaced by the "Bandwidth %" column when the operational mode is changed to Lines mode.

**5** Define the switched lines types to be included in the tool's calculations. The following fields appear in the switched lines table:

- included - determines whether the line type is included in the tool's calculations. A checked box indicates the line type is included in the tool's calculations. An unchecked box indicates the line type is ignored during calculations. Uncloaking a line type is easier than removing and then readding a line type when experimenting with different line configurations.
- line type - an identifying name for the line type. Choose a name such as POTS, Coin, or ISDN.
- # of lines/Bandwidth % - The definition of this field varies according to the selected operational mode as follows:
  - # of lines - specify the number of lines to be provisioned for the line type when the operation mode is set to bandwidth
  - Bandwidth % - specify the percentage of total available network interface bandwidth to be allocated to traffic from lines of the defined line type when the operational mode is set to lines mode
- intrasw % - specify the percentage of call traffic which is intraswitched for the defined line type
- CCS - specify the per line CCS traffic level expected for the defined line type
- Grade of service - specify the tolerable percentage of switched lines traffic that is blocked because of unavailable network interface bandwidth. The specified value applies to all line types.

The switched lines panel includes buttons for adding new line types to the table and deleting existing line types from the table. It also includes buttons for reordering the line type entries within the table.

**6** Specify the number of lines, or bandwidth percentage, for DS0 and DS1 private lines. The following fields appear in the private lines table:

- **Included** - determines whether the line type is included in the tool's calculations. A checked box indicates the line type is included in the tool's calculations. An unchecked box indicates the line type is ignored during calculations.
- **Line Type** - distinguishes the DS0 and DS1 line types. The names cannot be modified.
- **# of Lines/Bandwidth %** - the definition of this field varies according to the selected operational mode as follows:
  - **# of Lines** - specify the number of lines to be provisioned for the line type when the operational mode is set to bandwidth mode
  - **Bandwidth %** - specify the percentage of total available network interface bandwidth to be allocated to traffic from lines of the defined line type when the selected operational mode is set to lines mode

**Note 1:** Narrow band specials should be included as DS0s for calculation purposes.

**Note 2:** The calculations performed for private lines do not take into account Partial Cell Fill or Robbed Bit Signaling.

**7** Define the DSL line categories to be included in the tool's calculations. The defined DSL line categories appear in a table with the following fields:

- **Included** - determines whether the DSL category is included in the tool's calculations. A checked box indicates the DSL category is included in the tool's calculations. An unchecked box indicates the DSL category is ignored during calculations. Unchecking a DSL category is easier than removing and then re-adding a DSL category when experimenting with different line configurations.
- **Category** - an identifying name for the DSL category such as, Gold, Silver, and Bronze referring to differing levels of DSL service
- **# of Lines/Bandwidth %** - the definition of this field varies according to the selected operational mode as follows:

- # of Lines: Specify the number of lines to be provisioned for the DSL category when the operational mode is set to bandwidth mode
  - Bandwidth %: Specify the percentage of total available network interface bandwidth to be allocated to bearer traffic from lines of the defined DSL category when the selected operational mode is set to lines
- Mean Rate - the mean data rate in Mbps for lines in the DSL category
  - Guaranteed - indicates whether the mean rate value is considered to be guaranteed. If the mean rate is not guaranteed subscribers may experience periods of lower data throughput when the MG 9000 is under heavy load. Such lines are referred to as best effort lines.
  - Utilization % - indicates the percentage of lines that are "in use." "In use" refers to a DSL line which is actively transmitting or receiving data at a given point in time. Utilization % is always 100% for guaranteed bandwidth DSL lines. The utilization percentage can also be thought of as the reverse of the oversubscription percentage (that is, oversubscription % = 100% minus utilization %).

The DSL Lines panel includes buttons for adding new DSL categories to the table, and deleting existing DSL categories from the table. It also includes buttons for reordering the DSL type entries within the table.

- 8** Specify whether the MG 9000 being configured includes any subtended XPMs connected through DS-512 (ABI) links. The presence of DS-512 links affects the amount of network interface bandwidth available for bearer traffic. This is because a portion of the network interface bandwidth is reserved for XPM maintenance messaging when subtended XPMs are present. This step also allows the user to specify the number of channels that will be used for bearer traffic for the subtended XPMs. The DS-512 channels table has the following fields:
- Included - determines whether the line type is included in the tool's calculations. A checked box indicates the line type is included in the tool's calculations. An unchecked box indicates the line type is ignored during calculations. For DS-512, if this is checked the bandwidth required for XPM maintenance messaging will be subtracted from the available network interface bandwidth.
  - Line Type - an identifying name for the line type such as, ESMA

- # of Channels/Bandwidth % - the definition of this field varies according to the selected operational mode as follows:
  - # of Channels: Specify the number of channels needed for subtended XPM bearer traffic when the operational mode is set to bandwidth mode
  - Bandwidth %: Specify the percentage of total available network interface bandwidth to be allocated to traffic from lines of the defined line type when the selected operational mode is set to lines mode

The DS-512 Channels panel includes buttons for adding new line types to the table, and deleting existing line types from the table. It also includes buttons for reordering the line type entries within the table. This should be used to separate each subtended XPM into its own type.

- 9 Display the results of the tool's calculations as a set of bar graphs as follows:
  - The first bar graph indicates the total amount of available network interface bandwidth used by the line types defined in the previous steps which are marked to be "included" in the calculations. This bar graph also includes the bandwidth required for CallP signalling and OAM. If there are no line types included, this bar graph will only include the required bandwidth for CallP signalling and OAM. The color of this bar graph is
    - green if the amount of bandwidth used by the lines does not exceed the bandwidth available on the network interface
    - red if the network interface available bandwidth is exceeded and indicates by how much the available bandwidth was exceeded
  - A bar graph is displayed for each line type marked as "included" in the previous steps. Each bar graph shows the percentage of available network interface bandwidth required by that line type, the amount of bandwidth in Mbps, and the number of lines that can be provisioned against that bandwidth.

**Note:** The tool always recalculates the results whenever the user transitions to the Results panel from any other step. This means the user can go back and change one or more steps and immediately go back to the Results panel to see the affect without going back through each step.

- 10 This procedure is complete.

---

—End—

---

---

## Performing an MG 9000 data audit

---

### When to use this procedure

Use this procedure to schedule an NE audit or to run a manual NE audit of the data in the MG 9000 Manager and MG 9000.

All service provisioning is performed through the MG 9000 Manager. The MG 9000 Manager displays hardware and service states and receives and displays alarms. Performance data is also displayed using the MG 9000 Manager. The service provisioning, alarm, and performance data are saved and stored in both the MG 9000 and the MG 9000 Manager and the data must be kept up to date and accurate.

The NE audit compares the information in the MG 9000 Manager with the data in the MG 9000, identifies mismatches, and displays the results of the audit. There are two types of audits, automatic and manual.

An automatic NE audit occurs in the following scenarios:

- post delivery after discovery is complete - whether it is manual discovery or a result of a cold start or server restart
- ITP card fault - the MG 9000 can request the MG 9000 Manager to run an audit by generating a fault, if for example after a restart the ITP card finds that it has lost its persistent data. This will cause the MG 9000 Manager to audit VMG data and reprovision the data on the card.

A manual NE audit can be performed for the following reasons:

- when the services in the MG 9000 database do not match what is in the MG 9000 Manager database or the CS 2000.
- when audit logs (described below) determine a manual audit is needed because a mismatch was discovered that could not be fixed, requiring manual action
- when an audit was not able to complete because, for instance, the MG 9000 Manager lost communication temporarily with the MG 9000
- when a card was replaced without deprovisioning services, such as a DS1 card
- when VMG errors are seen, such as
  - audit logs reporting data mismatch errors
  - data mismatches in general, such as Market Fit data
  - errors encountered during OSSGate provisioning

The NE audit checks the following:

- alarms - synchronizes the alarms between the MG 9000 Manager and the MG 9000
- DS1 audit - synchronizes DS1 provisioning data, including channelization
- PLoA audit - synchronizes private lines data and attempts to recreate missing lines
- Card audit - retrieves cards states from the MG 9000
- Line circuit audit -
- SLoA audit - synchronizes VMG data between the MG 9000 Manager, MG 9000, and CS 2000
- DS1-IMA link audits
- DS1-IMA port audits
- DS1-IMA group
- Bandwidth management
- ADSL
- DTA
- MTA
- APS
- Floating IP audits
- Line coefficients
- Line templates
- Clock Sync data
- OM Collection interval
- Encryption Key

For each NE audit, an MGAU600 log is generated which indicates why the audit was run. There are three types of MGAU600 logs that are output

- status logs - indicate the progress (start and stop) of the audit
- mismatch logs - report data mismatches discovered during the audit and also identify the resource having the data mismatch, the reason for the mismatch, and possible instructions for correcting the mismatch
- summary logs - summarize the status of an operation typically when specific details were unavailable

For a description of Log MGUA600, see *CVoIP Fault Management Logs Reference*, NN10275-909.

The following restrictions apply when performing a scheduled audit:

- There may only be one audit per NE.
- The maximum period of an audit is 1 week. For example, a user may create an audit to run on Mondays and Wednesdays. Monthly, bi-monthly, multi-monthly, and yearly audits are not allowed.
- For an MG 9000 with a large line capacity, the audit may not complete in the allowed time. The audit will start where it left off during the next window.
- Only one audit may be scheduled per day on an NE, that is, an audit cannot be scheduled to run at 6 A.M. and 6 P.M. on the same NE on the same day.
- The audit duration cannot be less than 30 minutes.

The Immediate Task Audit function allows users to audit individual subsystems on an MG 9000 network element. Such selective audits allow users to fix data mismatches on specified systems without the need to run an audit on the entire NE.

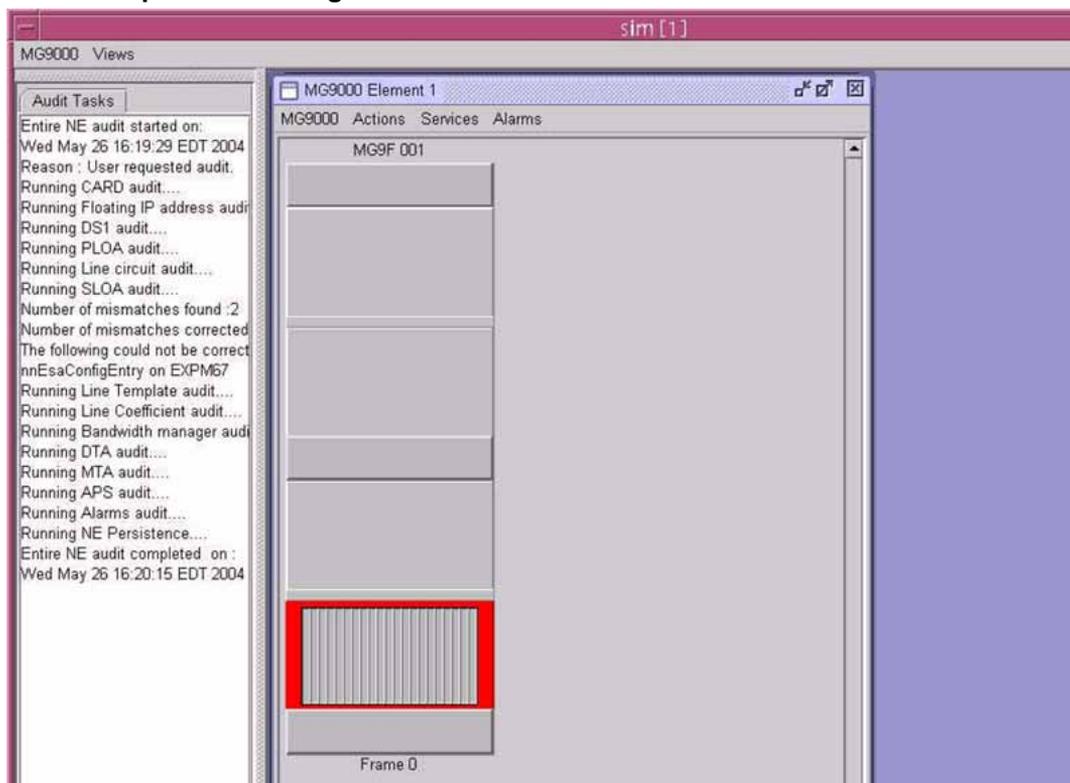
The following restrictions apply when performing an immediate audit:

- An audit that has been created as a result of the "Run Immediately" option, will run once only. The user must modify its properties after it is created to make it a recurring audit.
- Subsystem audits are available only for non-scheduled audits.
- Subsystem audits of individual Virtual Media Gateways (VMG) are restricted to SLOA.

Audit progress details are visible in the Progress details window of the Audit window. In addition, progress details are also visible in the NE Discovery View, Properties View, and the NE desktop view.

The audit progress shown in the NE desktop view is meant as an audit indicator for those tasks that run in the background so the user is aware that an audit is currently in progress for the NE. The text in the audit area is only persistent during the lifetime of the audit, meaning if the client is closed and re-opened after the audit is complete, nothing will appear in the Audit task tab of the NE desktop view. The following figure shows the NE desktop view with the Audit task tab.

## NE Desktop View showing Audit Tasks tab



## Prerequisites

There are no prerequisites.

## Action

## Auditing MG 9000 data

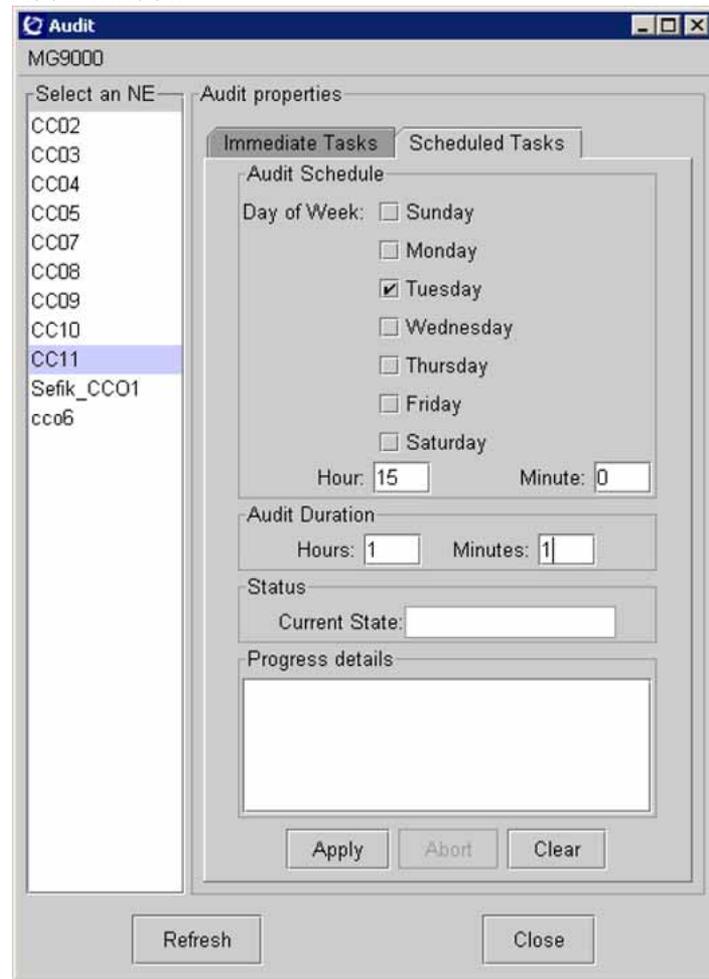
Step	Action
------	--------

*At the MG 9000 Manager*

- 1 At the **Subnet View** or the **NE desktop view**, from the **Configuration** menu, select **Audit NE**.

*The Audit window appears.*

**Audit window**



The following table lists and describes the fields contained in the **Audit** window.

**Audit window fields**

Field	Description
Select an NE	This field lists the network elements available for audit.
	<b>Note:</b> Only fully discovered network elements appear in the Select an NE list.

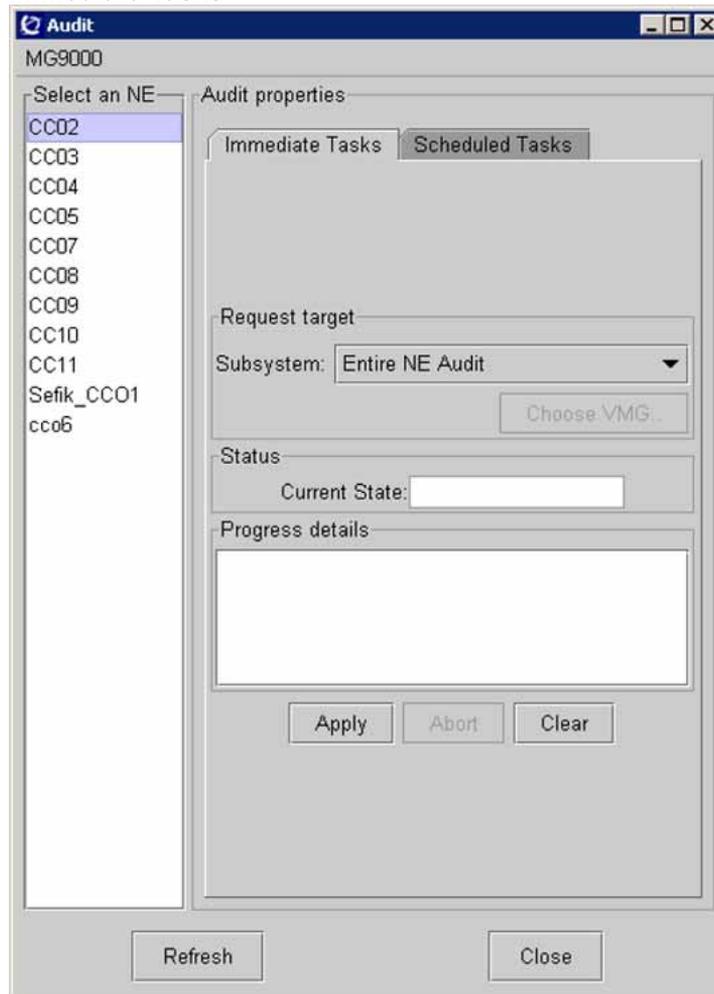
Field	Description
Audit properties	<p>This field has two tabs:</p> <ul style="list-style-type: none"> <li>• Immediate Tasks</li> <li>• Scheduled Tasks</li> </ul>

- 2 Select a network element from the **Select an NE** list.  
*There are two types of audits that you can perform.*

If you wish to perform	Go to
immediate audit	<a href="#">step 3</a>
scheduled audit	<a href="#">step 4</a>

- 3 Click on the **Immediate Tasks** tab.  
*The Immediate Task tab opens.*

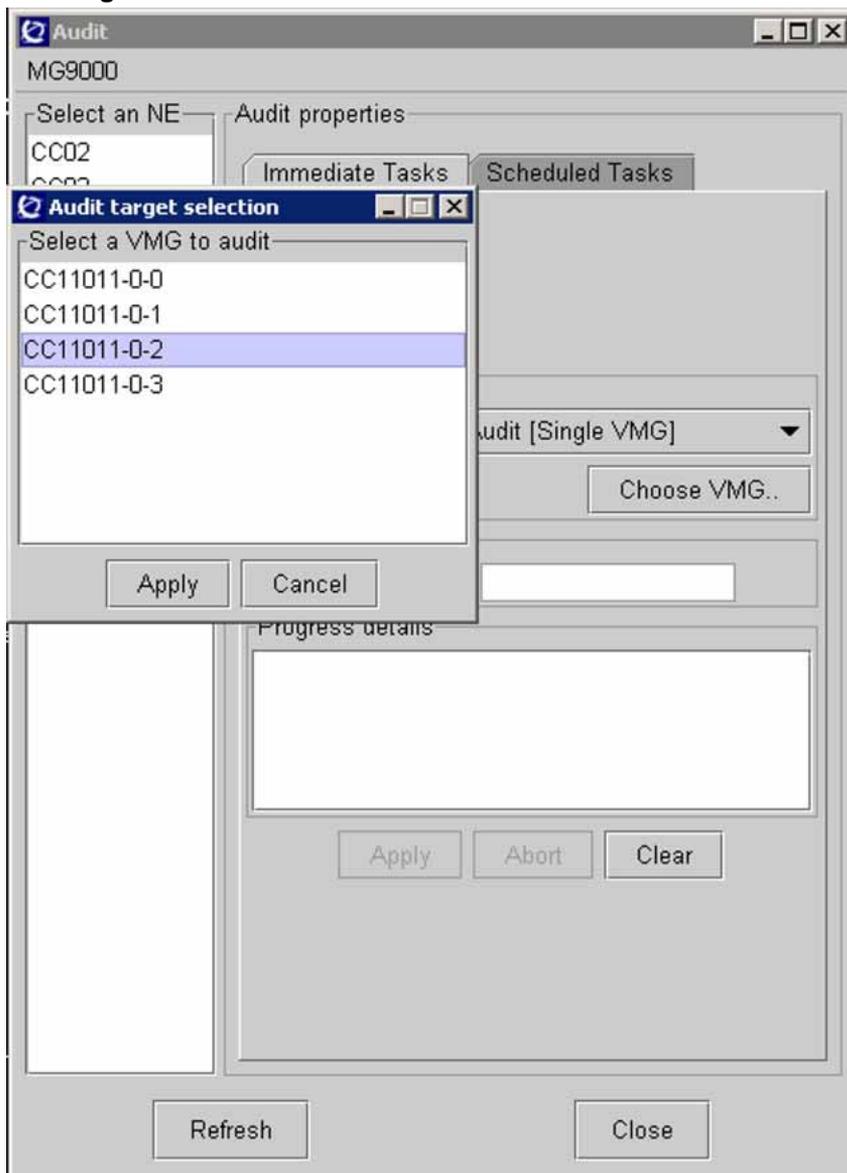
### Immediate Tasks



- a. If you wish to audit
- a subsystem of the NE, select one from the **Subsystems** drop down menu
  - a Virtual Media Gateway (VMG), choose Select **VMG Audit** from the **Subsystems** drop down menu, then click the **Choose VMG** button.

*An Audit target selection view appears from which you can select a VMG, as shown in the following figure:*

## Running a VMG audit



- b. Click the **Apply** button.

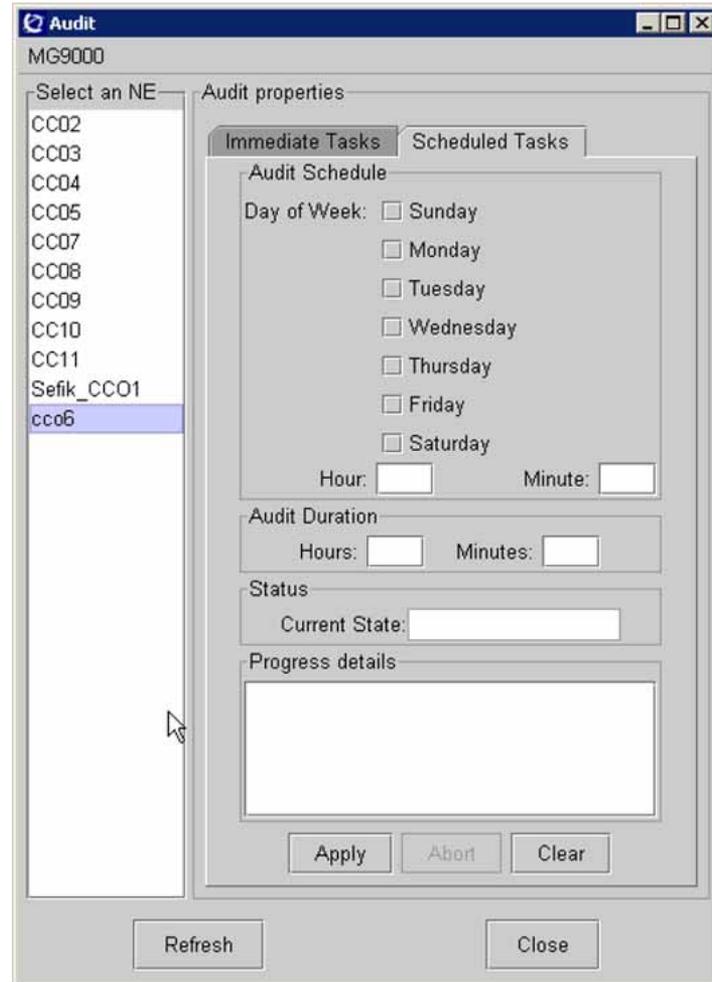
*The audit starts. You can monitor the status of the audit from the Current State field of the Status area. The Progress details area provides a log of the audit events including what was audited, the time of initiation and completion, and the reason for the audit.*

- c. Go to [step 6](#).

- 4** Click on the **Scheduled Tasks** tab.

*The Scheduled Tasks tab opens.*

**Audit View: Scheduled Tasks**



If a recurring audit is selected, select at least one day of the week and use the information in the following table to schedule a recurring audit.

Field	Description
Day of Week	The days of the week on which the audit should run.

Field	Description
Hour/Minutes	<p>The hour of the day on which the audit is to run.</p> <p>The audit scheduling subsystem assumes the MG 9000 Manager client and server machines are in the same time zone. Unexpected time shifts occur when the two machines are not in the same time zone. The following describes this behavior:</p> <ul style="list-style-type: none"> <li>• If the client is behind the server in time, the audit will run later than the time chosen in the GUI.</li> </ul> <p>For example, if the server is at EST and the client is at PST (-3 hours), an audit scheduled to run at 15:00 hrs will be run at 18:00 hrs on the server.</p> <ul style="list-style-type: none"> <li>• If the client is ahead of the server in time, the audit will run earlier than the time chosen in the GUI.</li> </ul> <p>For example, if the server is at PST and the client is at EST (+3 hours), an audit scheduled to run at 15:00 hrs will be run at 12:00 hrs on the server.</p>
Audit Duration	The maximum duration allowed for the selected audit. An audit duration must be greater than 30 minutes.
Status	The current state of the audit (Running, Stopped).
Progress details	Provides a log of the audit events including what was audited, the time of initiation and completion and the reason for the audit.

- 5 Click **Apply** to create the audit.

The progress of the audit will be displayed in the **Progress details** window of the **Audit** window.

- 6 This procedure is complete.

---

—End—

---

## Removing a scheduled audit

---

Step	Action
------	--------

---

### *At the MG 9000 Manager*

- 1 At the **Subnet View** from the **Configuration** menu, select **Audit NE**.  
*The Audit window appears.*  
**Note:** You can also access the Audit view from the NE desktop view. To do so, click the **Configuration** menu followed by NE Audit.
- 2 Select an NE from the **NE** list.
- 3 Click the **Scheduled Tasks** tab.
- 4 Click the **Abort** button.
- 5 This procedure is complete.

---

—End—

---

## Viewing the properties of an NE Audit

---

Step	Action
------	--------

---

### *At the MG 9000 Manager*

- 1 At the **Subnet View** from the **Configuration** menu, select **Audit NE**.  
*The Audit window appears.*  
**Note:** You can also access the Audit view from the NE desktop view. To do so, click the **Configuration** menu followed by NE Audit.
- 2 Select an NE from the **NE** list.
- 3 Select the tab (Immediate or Scheduled) for the audit type you wish to view.
- 4 This procedure is complete.

---

—End—

---

## Performing a routine exercise (REX) on intelligent cards

---

### When to use this procedure

Routine Exercise (REX) allows you to perform a diagnostic test on the inactive card of an intelligent pair of cards. REX is intended to diagnose latent faults in inactive (or standby) cards.

The REX GUI view on the MG 9000 Element Manager allows you to schedule and to monitor the progress of a REX test on a selected network element (NE). Using the GUI you can also

- add an NE for REX
- remove an NE for REX
- suspend REX on an NE
- resume REX on an NE

REX can be performed on the following types of cards:

- Digital Control Cards (DCC): SuperCore OC3 (SCO), SuperCore IMA (SCI), SuperCore Gigabit Ethernet (SCG)
- Internet Telephony Processor (ITP)
- Internet Telephony Extender (ITX)

### REX results

You can monitor the progress of REX in the Progress Details field of the REX GUI. Details also appear on the REX tab of NE Desktop View.

The REX routine generates the following logs:

- REX600. REX start or completed
- REX601. REX success or failure
- REX602. REX skipped

### Limitations

The following limitations apply to the REX function:

- REX is not supported on the following cards:
  - Access Bridge Interface (ABI) cards. ABI cards act in a master-slave relationship. SWACT is not possible on ABI cards.
  - DS1. DS1 cards adhere to a 1:N protection scheme, and thus are not REX capable.

- After performing a SWACT on ITP cards, you must wait at least 1 minute before you lock the newly inactive card.
- You must not perform REX tests on card pairs that exhibit CPU overload alarms, or cards subtending a card in the CPU overload state.
- REX cannot be executed if there are critical alarms present on the card pair.

### Description of REX NE GUI

The REX view has the following fields

#### REX NE GUI

Field	Description
Add button	Use the Add button to add an NE for REX.  After you press the Add button, a new panel opens that lists all of the NEs in a subnet. Select the NE for REX from this list.
Remove button	Use Remove button to remove a REX scheduled on a selected NE.  Select an NE from the NE list in the REX NE View. Press the Remove button to stop the REX.
Suspend button	Use the Suspend button to disable or suspend an NE for REX.  Select an NE from the NE list in the REX NE View. Press the Suspend button to suspend the REX.
Resume	Use the Resume button to continue the REX on an NE that had been suspended.  Select an NE from the NE list in the REX NE View. Press the Resume button to enable and resume the REX.
Select an NE to REX	This field lists all of the NEs in a subnet on which you can perform the REX.
REX Mode	REX has two modes: <ul style="list-style-type: none"> <li>• Without SWACT. Use this mode to start a REX on the inactive card of a card pair.</li> <li>• With SWACT. Use this mode to perform a REX on both cards of a card pair. The REX begins on the inactive card, followed by a SWACT on the active card. Thereafter, the newly inactive card undergoes the REX.</li> </ul>

Field	Description
Card Types	<p>You can choose from three types of cards:</p> <ul style="list-style-type: none"> <li>• DCC</li> <li>• ITP</li> <li>• ITX</li> </ul>
REX Schedule	<p>There are two scheduling options:</p> <ul style="list-style-type: none"> <li>• Run Immediately. Use this option to run the REX immediately. Select Apply to begin the REX. (Day of Week options are disabled.)</li> <li>• Day of Week</li> </ul> <p>Use this option to schedule a day, hour and minute on which to start the REX</p>
REX Duration	<p>Use this option to set the maximum duration (in hours and minutes), for the completion of the REX.</p> <p>If the duration of the REX exceeds the value you set, REX is skipped on that NE.</p>
REX Status	<p>The (non-editable) Current State field reports one of three states: Ready to Run, Running REX, and Completed REX.</p>
Progress details	<p>This text area displays the success or failure of the operations performed during REX on a selected NE. The operations performed during REX are</p> <ul style="list-style-type: none"> <li>• LOCK</li> <li>• UNLOCK</li> <li>• SWACT</li> <li>• Diagnose</li> </ul>

## Prerequisites

There are no prerequisites.

## Action

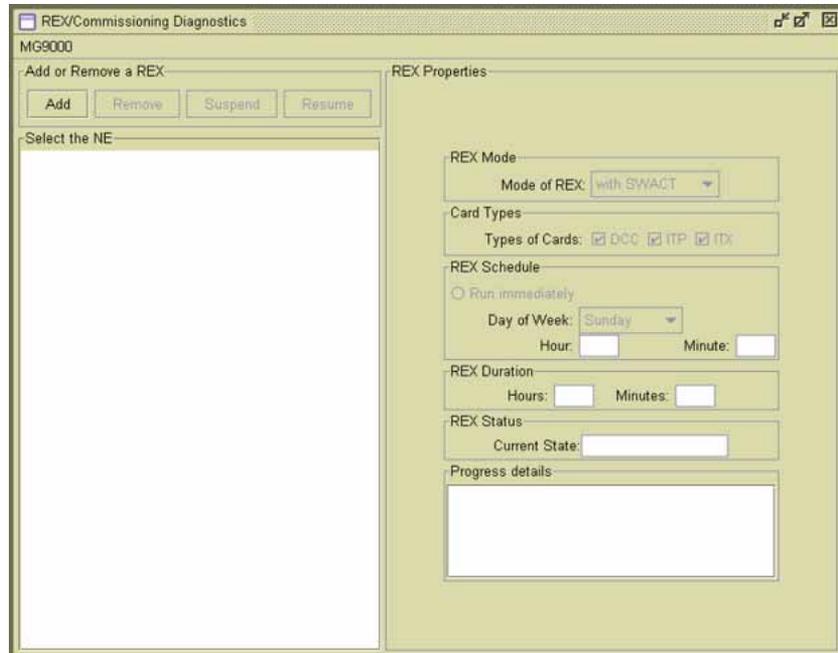
### Scheduling an NE for REX

Step	Action
------	--------

*At the MG 9000 Manager*

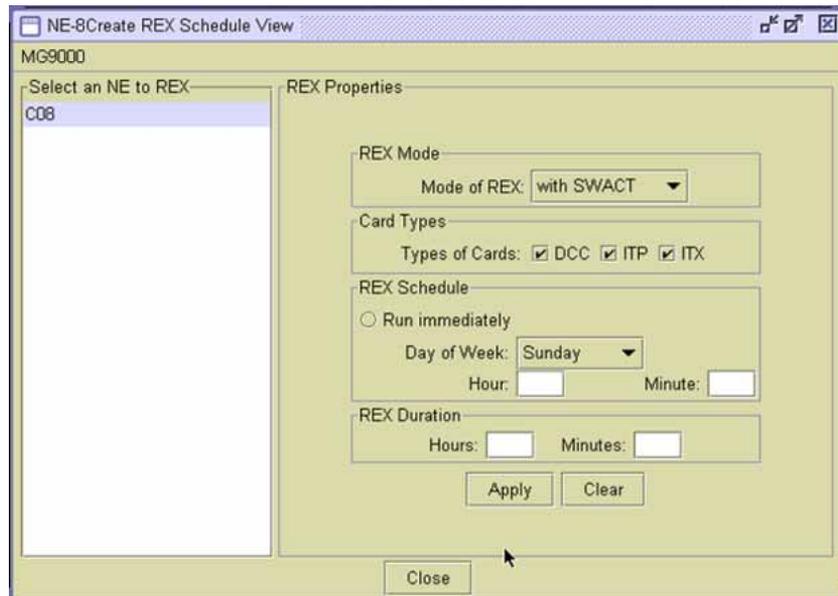
- 1 In the MG 9000 Manager Subnet View, select REX NE from the Configuration menu.

*The REX NE view appears.*



- 2 Select the Add button.

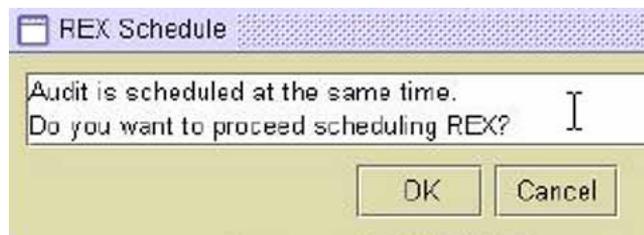
*The Create REX Schedule View appears that lists all of the available NEs in a subnet.*



- 3 Select the NE.
- 4 Select the mode for the REX.
- 5 Select the type of card for the REX.
- 6 Schedule the REX by selecting the Run Immediately or the Day of Week option.
- 7 Set the duration for the REX.
- 8 Press the Apply button.

*Your REX request is entered into the REX schedule. The Create REX Schedule view closes, and the system returns to the REX NE view. The REX NE View shows all of the scheduled REX routines.*

**Note:** If an audit has been scheduled for the same time, a warning box appears. Select either OK to proceed with the scheduled REX or Cancel to delete the scheduled REX. If you select OK, REX will be performed after the audit is completed and not at the scheduled time.



- 9 To monitor the progress or status of a REX on an NE, in the REX NE View, select an NE from the Select an NE list. To monitor the progress of a REX for a specific NE from the NE Desktop View, see Viewing the progress of a REX from the NE desktop view.  
*The status and progress details for that particular NE appear in the REX Properties area on the right side of the REX NE View.*
- 10 This procedure is complete.

---

—End—

---

## Removing an NE from the REX schedule

Step	Action
------	--------

	<i>At the MG 9000 Manager</i>
--	-------------------------------

- 1 In the MG 9000 Manager Subnet, select REX NE from the Configuration menu.  
*The REX NE view appears.*
- 2 Select the NE from the NE list.
- 3 Select the Remove button  
*The REX process for the selected NE is removed from the schedule.*
- 4 This procedure is complete.

---

—End—

---

You can use the desktop view for a specific NE to monitor the progress of a REX.

### Viewing the progress of a REX from the NE Desktop View

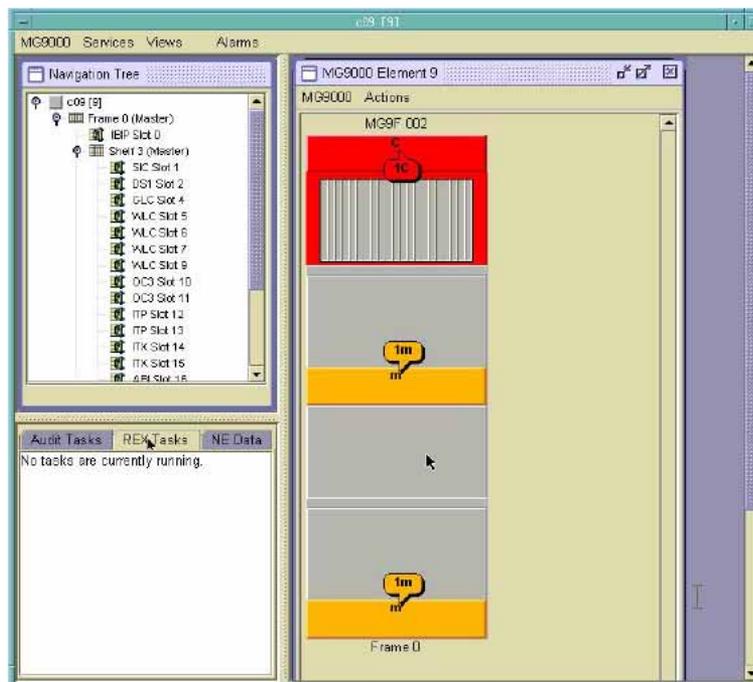
---

<b>Step</b>	<b>Action</b>
-------------	---------------

---

*At the MG 9000 Manager*

- 1 Click on MG 9000 in the subnet view.
- 2 From the NE desktop view, select REX NE from the Configuration menu.  
*The NE-specific desktop view opens.*



- 3 In the text area in the bottom left of the screen, select the REX Tasks tab.

*The status of the REX appears in the text box. The text reports the success or failure of an activity, and the status of a REX as LOCK, UNLOCK, SWACT or diagnose.*

- 4 This procedure is complete.

---

—End—

---

## Managing performance thresholds

### When to use this procedure

Growth of supported services and increased channel concentration on the MG 9000 requires additional system stability protection in the event of call processing overload. The MG 9000 supports performance thresholds that are used to raise and clear alarms. Use this procedure when it is necessary to provision performance thresholds after initial MG 9000 commissioning is complete for the following cards

- DCC (OC3, GigE, or DS1-IMA card)
- DS1
- ABI (DS-512)
- ITP
- ITX

**Note 1:** It is recommended that the factory configured default threshold settings be used.

**Note 2:** The values provisioned in the Performance Threshold tab impact when performance alarms are raised and cleared. These alarms appear at the Alarm Browser and are noted by OVLD800 to OVLD807 logs being output.

The performance threshold values are changed by accessing Actions->Manage Thresholds from any one of previously listed cards' Card View menu bar.

### Prerequisites

The user must have at least emsmtc permissions to make provisioned changes in the Thresholds View. Read only (emsro) and Services Provisioning (emssprov) users can access the view, but cannot make changes.

### Action

#### Managing performance thresholds

Step	Action
------	--------

<i>At the MG 9000 Manager</i>	
-------------------------------	--

- 1 From the **Subnet View**, double click on the **network element** icon for which performance thresholds are to be provisioned. The **Frame View** appears.
- 2 From the **Frame View** double click on the **target shelf**. The **Shelf View** appears.
- 3 From the **Shelf View**, double click on the **card** for which performance thresholds are to be provisioned. The **Card View** appears.
- 4 From the menu bar, select **Actions->Manage Thresholds**. The **Thresholds View** appears. Click on the **Performance Thresholds** tab. The following figure shows the Threshold View with the **Performance Thresholds** tab for a DCC card. On DS1 ABI, ITP, and ITX cards, the Threshold View displays only performance thresholds, since overload thresholds are not applicable.

Threshold View with Performance Thresholds tab selected

MG9000

Overload Thresholds

Performance Thresholds

OC3 Card: NE-3 Frame-0 Shelf-3 Slot-10

Raise CPU	850	Non-interval thresholds
Clear CPU	750	Non-interval thresholds
Interval CPU	1	Interval thresholds
Raise RAM	850	
Clear RAM	750	
Interval RAM	1	Interval thresholds
Raise Flash	850	
Clear Flash	750	
Interval Flash	1	
Raise Channel	850	
Clear Channel	750	
Interval Channel	1	

Apply

Refresh Close

5 Make any changes to the threshold values based on technical input from Nortel. The options are to raise, clear or interval for each threshold. The following criteria apply to the selections:

- raise/clear values have a range of integer values from 0 - 10000
- interval values have a range of integer values from 1-60

**Note:** Moving the cursor over the specific field displays the valid input ranges.

Click on **Apply** to submit the values. Select the **OK** button when the *warning message* appears.

6 This procedure is complete.

---

—End—

---

## Managing overload thresholds

### When to use this procedure

Growth of supported services and increased channel concentration on the MG 9000 requires additional system stability protection in the event of call processing overload. The MG 9000 supports overload thresholds that are used to raise and clear alarms. Use this procedure when it is necessary to provision overload thresholds after initial MG 9000 commissioning is complete. The overload thresholds are provisioned for the DCC cards (OC3, DS1-IMA, or GigE cards).

**Note 1:** It is recommended that the factory configured default threshold settings be used. These settings have a direct impact on call processing and any changes should be made only after contacting Nortel for support.

**Note 2:** When overload thresholds are crossed, overload faults are raised at the MG 9000 Alarm Browser and in log files and are denoted by OVLD800 to OVLD804. OMs associated with these MG 9000 Overload controls are collected and displayed in the MG 9000 Manager Performance Browser. Refer to *MG 9000 Performance Management*, NN10140-711

The threshold values are changed by accessing Actions->Manage Thresholds from OC3, DS1-IMA, or GigE Card View menu bar.

### Prerequisites

The user must have at least emsmtc permissions to make provisioning changes in the Thresholds View. Read only (emsro) and services provisioning (emssprov) users can still access the view but cannot make changes.

### Action

#### Managing overload thresholds

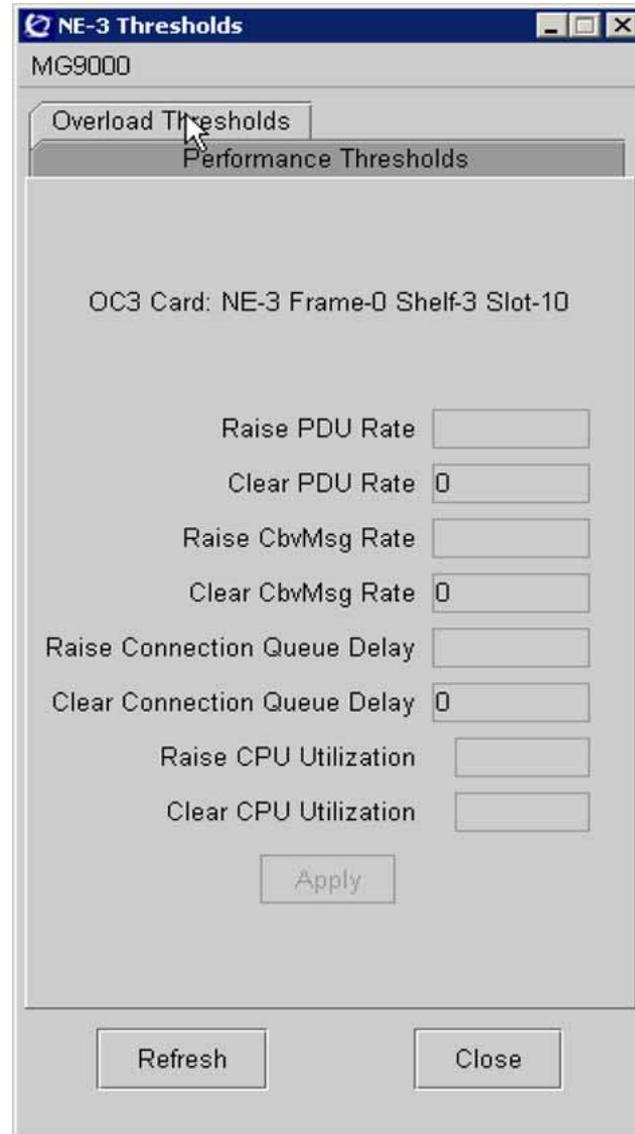
Step	Action
------	--------

*At the MG 9000 Manager*

- 1 From the **Subnet View**, double click on the **network element** icon for which overload thresholds are to be provisioned. The **Frame View** appears.
- 2 From the **Frame View** double click on the target shelf. The **Shelf View** appears.

- 3 From the **Shelf View**, double click on the OC3/DS1-IMA DCC card for which overload thresholds are to be provisioned. The **OC3/DS1-IMA Card View** appears.
- 4 From the menu bar, select **Actions->Manage** Thresholds. The **Thresholds View** appears. Click on the **Overload Thresholds** tab. The following figure shows the Threshold View with the **Overload Thresholds** tab.

Threshold View with Overload Thresholds tab selected



- 5 Make any changes to the threshold values based on technical input from Nortel. The options are to Raise and Clear each threshold. The following criteria apply to the selections:

- Raise PDU Rate, Raise CbvMsg Rate, and Raise Connection Queue Delay have an integer value range of 1 to 2147483647.
- Raise CPU Utilization has an integer value range of 1 to 10000.
- Clear PDU Rate and Clear CbvMsg Rate have an integer value range of 0 to 2147483647, which is at least 30 % less than the raise value.
- Clear Connection Queue Delay has an integer value range of 0 to 2147483647, which is at least 1000 % less than the raise value.
- Clear CPU Utilization has an integer value range of 1 to 10000, which is at least 30 % less than the raise value.

**Note:** Moving the cursor over the specific field displays the valid input ranges.

Click on **Apply** to submit the values.

**6** This procedure is complete.

---

—End—

---

---

## Changing MG 9000 Manager ESA data download properties

---

### When to use this procedure

The following procedures provides the steps to support ESA data download from the Core to the MG 9000 Manager and how to change the MG 9000 Manager ESA data download properties.

### Core configuration

The ESA data file will be downloaded from the Core using Secure Shell FTP (SSH FTP). Therefore it is important to ensure that enough TCP connections are configured in the Core for the SSH FTP Server sessions.

The maximum number of FTP session is controlled by the CM tuple in Table IPHOST in the CM. The CM tuple is usually the first tuple in the table. The tuple contains the following fields:

- NODENAME: Node name = CM
- CMINDEX: Index = 0
- TCPCONN: The total number of TCP connections allowed. This number must be greater than or equal to  $(FTPCLCON + FTPSVCON) \times 2$

where

- FTPCLCON is the maximum number of FTP client sessions allowed. SFT is not impacted by this value
- FTPSVCON is the maximum number of FTP server sessions allowed. Secure file transfer (SFT) shares this resource with other CM FTP users.

Care must be taken when determining the value of FTPSVCON. Other telnet applications may have been configured and the value of FTPSVCON should be incremented taking this into account.

If FTPSVCON is incremented, ensure that TCPCONN is large enough to support the total of FTPCLCON and FTPSVCON. Each FTP session will consume 2 TCP connections. This will be enforced by the IPHOST table control.

### Prerequisites

Ensure the CS 2000 Core Manager has the latest file set as part of the CS2E07 CS 2000 Core Manager load, for the package SDM\_BASE.fts for the File Transfer Service application. The minimum load is CS2E0007 6.1 19.78.0.0.

The following configuration activities must have occurred in the CS2000 Core to support ESA data download to the MG 9000 Manager. Procedures for configuring the CS2000 to support ESA data download are contained in *Communication Server 2000 Configuration Management*, NN10105-511, NN10188-511, NN10201-511, or NN10193-511.

- table LGRPINV must have tuples with GRPTYPE of S provisioned for MG 9000 VMGs
- table ESAPXLA updated to include special dialing codes for ESA
- table OFCENG, office parameter ESA\_GWDATA\_DEVICE must specify the device on the core where the ESA data is generated

For offices running the Core Billing Manager (CBM), the CBM software must be at the same release as the MG 9000 EM. For example, the MG 9000 EM SN09 software requires CBM load CBM0090.

### Limitations and restrictions

If an SFTP failure occurs between the MG 9000 Manager and MG 9000 during ESA download because of an SSH key mismatch, you must manually delete the entry for the node in `/data/mg9kem/hosts.auth` on the EM server.

### Action

Set up Secure Shell (SSH) authentication for the MG 9000 Manager to have the required access to the CS 2000 Core Manager for downloading the ESA data.

**Note:** The following procedure accommodates offices equipped with either the SDM or the CBM. The steps that you perform in the following procedure are determined by the configuration of your office.

### Setting up the SSH authentication

Step	Action
------	--------

**At the MG 9000 Manager CLI tool**

- |   |   |
|---|---|
| 1 | Configure the SDM IP and SDM User for this system by performing the following steps: <ol style="list-style-type: none"> <li>a. Log into the MG 9000 Manager server and su to root:               <pre>login: maint Password: &lt;maint password&gt; maint: su - root Password: &lt;root password&gt;</pre> </li> <li>b. Execute the following command:</li> </ol> |
|---|---|

```
# cli
```

- c. Select **Configuration**, then select **OAMP Application Configuration**.
  - d. Select **Configure SDM IP Address and User**.
  - e. Set the SDM IP to the correct IP address of the SDM.
  - f. Set the SDM user name to be "esouser"
  - g. Follow any on-screen instructions that are given.
- 2** If you are using the SDM, go to the next step. If you are using the Core Billing Manager (CBM), go to [step 6](#).
- 3** For the user, mgems on the MG 9000 Manager server, generate the SSH key pair needed for data transmission between the MG 9000 Manager and the SDM by performing the following steps:
- a. With superuser access, the mgems user generates the SSH key by typing:
 

```
#su - mgems
$ssh-keygen -t rsa
```
  - b. Accept the default location and enter an empty passphrase which creates the following key file:
 

```
/export/home/mgems/.ssh/id_rsa.pub
```
- 4** The key information contained in the file `/export/home/mgems/.ssh/id_rsa.pub` must be placed in the following file on the CS 2000 Core Manager: `/home/esouser/.ssh/authorized_keys2` by performing the following steps:
- a. Secure copy the `id_rsa.pub` file to the CS 2000 Core Manager by typing the following command:
 

```
$ scp /export/home/mgems/.ssh/id_rsa.pub
root@$SDM_IP:/home/esouser/tempkey
```

The system responds with  
Are you sure you want to continue connecting  
(yes/no)?
  - b. Type **Yes** to continue.
  - c. Enter the password of the root SDM user.
  - d. Securely append the public key to the authorized keys list on the SDM by typing

**Note:** The following command must be entered on one line exactly as shown.

```
$ ssh root@$SDM_IP "cat /home/esauser/tempkey >>
/home/esauser/.ssh/authorized_keys2"
```

e. Enter the password of the root SDM user when prompted for it.

5 Go to [step 7](#).

6 The key information contained in the file `/export/home/mgems/.ssh/id_rsa.pub` must be placed in the following file on the CBM: `/cbmdata/users/esauser/.ssh/authorized_keys2` by performing the following steps:

a. Secure copy the `id_rsa.pub` file to the CBM by typing the following command:

**Note:** The following command must be entered on one line exactly as shown.

```
$ scp /export/home/mgems/.ssh/id_rsa.pub
root@$SDM_IP:/cbmdata/users/esauser/tempkey
```

The system responds with

```
Are you sure you want to continue connecting
(yes/no)?
```

b. Type Yes to continue.

c. Enter the password of the root CBM user.

d. Securely append the public key to the authorized keys list on the CBM by typing the following command:

**Note:** Note: The following command must be entered on one line exactly as shown.

```
$ ssh root@$SDM_IP "cat /cbmdata/users/esauser/tempk
ey >> /cbmdata/users/esauser/.ssh/authorized_keys2 "
```

e. Enter the password of the root CBM user when prompted for it.

7 This procedure is complete.

---

—End—

---

## Changing ESA download properties

ESA properties must be set up correctly to download the right ESA data file from the Core at the right time. The XA-Core data collection is generated automatically on a daily basis on the time specified by `ESA_GWDATAUPD_HOUR` parameter in table `OFCENG`. The default value of this parameter is 6:00 AM. This data is saved in file `ESA_SYSTEM_SD$XML` on a device specified by Table `OFCENG` tuple `ESA_GWDATA_DEVICE`.

The default time when data is downloaded to the MG 9000 Manager is 6:00 AM. Nortel recommends that the default download time be changed immediately to some time after 6:00 AM, such as 6:30 or 7:00 AM.

**Note 1:** The download of the ESA data to the MG 9000 Manager must be synchronized to ensure all the required service order changes are captured. Using the default download time of 6:00 AM, changes will not be downloaded to the MG 9000 Manager or the MG 9000 for 24 hours after the changes are made in the Core.

**Note 2:** Ensure that the time the ESA data download occurs is not scheduled at the same time as the nightly audit, if a nightly audit is scheduled.

The following are the three data download properties that must be configured and their default values:

- the time that will be used for data downloads -  
`ESA.DataDownloadTime = 6:30 AM`
- the name of the device on the Core where the ESA data file will be stored -  
`ESA.DataDeviceName = /SFDEV`
- the name of the ESA data file -  
`ESA.DataFileName = ESA_SYSTEM_SD$XML`  
`ESA.DataFileNameUnix = ESA_SYSTEM_SD.XML`

**Note:** The `ESA.DataFileNameUnix` property is not editable. This is dynamically derived from the `ESA.DataFileName` property by the MG 9000 Manager software. The `ESA.DataFileName` on the Core must adhere to the following naming conventions:

- There can only be one \$ sign in the name separating the 'name' part from the 'extension' part. Refer to the default value for an example.
- No spaces are allowed in the file name.

Use the following procedure only if it is necessary to change the default values of the ESA properties.

---

## Changing ESA download properties

---

### Step Action

---

#### At the MG 9000 Manager server

1 Telnet into the MG 9000 Manager server.

2 To change directory, type  
`# cd /opt/nortel/mg9ksrv_08/bin`

3 To configure the server type

```
# ./mg9kserver config
```

The system responds

Main Configuration Menu

```
1) Change Distribution Policy
2) Change CS2M IP Address
3) Change Oracle IP Address
4) Change Debug Level for logs
5) Change Persistence settings
6) Change ESA data download settings
7) Change Imaging Server settings
8) Change EM Factory Sleep
9) Change OMC Settings
10) Display current settings
11) Exit from Main Menu
Please make a selection =>
```

4 Select 6.

The system responds:

ESA Configuration Menu

```
1) Change ESA data download time
2) Change ESA data device name
3) Change ESA data file name
4) Exit to Main Menu
Please make a selection =>
```

**Note:** Changes may take up to 60 seconds to take effect.

5 Select 1 to change the download time.

The system responds:

```
Please enter the new ESA data nightly download time ?
Default: [6:00 AM] =>
```

**Note:** The time must be entered in AM/PM format as shown.

An example input:

```
6:30 PM
```

The system responds:

```
ESA Configuration Menu
1) Change ESA data download time
2) Change ESA data device name
3) Change ESA data file name
4) Exit to Main Menu
Please make a selection =>
```

6 Select 2 to change the device name.

**Note:** The ESA data device must be a valid Core device such as SFDEV or a disk volume.

The system responds:

```
Please enter the new ESA data device name on the core ?
Default: [/SFDEV] =>
```

An example input:

```
/F02IMAGE
```

**Note:** When choosing the default or disk volume, the forward slash (/) is required.

The system responds:

```
ESA Configuration Menu
1) Change ESA data download time
2) Change ESA data device name
3) Change ESA data file name
4) Exit to Main Menu
Please make a selection =>
```

7 Select 3 to change the ESA data file name.

**Note:** The Core file name is hard coded as ESA\_SYSTEM\_SD\$XML.

The system responds:

```
Please enter the new ESA data file name on the core ?
Default: [ESA_SYSTEM_SD$XML] =>
```

An example input:

```
ESADATA$XML
```

The system responds:

```
Name of the ESA data file on the EM: ESADATA.XML
ESA Configuration Menu
1) Change ESA data download time
2) Change ESA data device name
3) Change ESA data file name
4) Exit to Main Menu
```

Please make a selection =>

**8** Select **4** to exit.

**4**

**Note:** Once completed, the new ESA data download properties will become effective on the future downloading of the ESA data.

**9** This procedure is complete.

---

—End—

---

---

## MG 9000 local craft interface

---

This section describes the local craft interface (LCI) which is used to install and commission the Carrier VoIP Media Gateway (MG 9000). Installation and commissioning activities are typically handled by Nortel or by operating company personnel using special documentation purchased from Nortel.

The LCI provides emergency MG 9000 management through a standard Web browser environment available on a 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 Data Communications Controller (DCC) card on the MG 9000.

**Note:** The LCI is to be used only 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.

Refer to the following MG 9000 documents for information on operation, configuration, and maintenance of the MG 9000 and the MG 9000 Manager:

- *MG 9000 Fault Management*, NN10074-911
- *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450
- *MG 9000 Configuration Management*, NN10096-511
- *MG 9000 Performance Management*, NN10140-711
- *MG 9000 Security and Administration*, NN10162-611
- *MG 9000 Basics*, NN10011-111

This chapter includes information on the following topics:

- ["LCI access" \(page 315\)](#)
- ["Launching the LCI from the MG 9000 Manager" \(page 320\)](#)
- ["LCI network element screen" \(page 325\)](#)
- ["LCI Connections view" \(page 329\)](#)

- "LCI Maintenance view" (page 347)

## LCI access

The LCI communicates to the MG 9000 shelf through an Ethernet port on the faceplate of the DCC card. A windows PC equipped with a Ethernet Network Interface Card (NIC) and Netscape Communicator Browser software Version 7.0 and up or Internet Explorer 5.5 and up is required. Versions of Netscape Communicator between 4.7 and 7.0 are not supported. An RJ-45 cross-over cable is required to connect the NIC on the PC to the RJ-45 port on the faceplate of the NTNY45AA/BA DCC card. A local PC is connected to the port and Netscape browser software is used to provide a GUI for performing basic functions on the cards equipped in the MG 9000 shelf and configuring the connections to the network and CS 2000. Use the DCC IP address to locate the LCI through the browser. HTTPS access is required.

**Note:** The LCI runs a heartbeat audit every 10 seconds. If no communication is received or is delayed for 30 seconds, the LCI is taken down. When the LCI is operating over a network, congestion may contribute to this delay. If the LCI connection is taken down, it must be restarted.

Set up the PC and connect to the LCI using the "LCI setup and access" procedure in *MG 9000 Security and Administration*, NN10162-611. After the connection and setup procedures are complete, login using the correct user name and password. The following figure shows the security screen requesting a user name and password.

### LCI security access



A successful login produces a screen display listing the LCI browser configuration requirements.

## LCI browser configuration

**MG 9000 Local Craft Interface**

**Configuration Requirements: NN=Netscape Navigator, IE=Internet Explorer**

1. [Netscape] Edit-->Preferences-->Appearance-->Fonts [Explorer] Tools-->Internet Options-->General-->Fonts	<ul style="list-style-type: none"> <li>• Fonts for Encoding/Fonts for: Western (NN4.7 &amp; NN7.0)</li> <li>• Variable Font =Times New Roman, Size =10 (NN4.7), Proportional: Serif, Size = 12, Serif: Times New Roman, Sans-serif: Arial (NN7.0)</li> <li>• Fixed Font/Monospace = Courier New, Size = 10 (NN4.7 &amp; NN7.0)</li> <li>• Select: use my default fonts, overriding document-specified fonts (NN4.7)</li> <li>• Uncheck: Allow documents to use other fonts (NN7.0)</li> <li>• Language Script: Latin Based, Web page font: Times New Roman, Plain text font: Courier New (IE5.5)</li> </ul>
2. [Netscape] Edit-->Preferences-->Advanced [Explorer] Tools-->Internet Options-->Advanced	<ul style="list-style-type: none"> <li>• Select: Automatically load images (NN4.7)</li> <li>• Select: Enable Java (NN4.7 &amp; NN7.0)</li> <li>• Select: Enable JavaScript (NN4.7)</li> <li>• Select: Enable style sheets/XSLT (NN4.7 &amp; NN7.0)</li> <li>• Select: Restore Defaults (IE5.5)</li> </ul>
3. [Netscape] Edit-->Preferences-->Advanced-->Cache [Explorer] Tools-->Internet Options-->General-->Temporary Internet Files-->Settings	<ul style="list-style-type: none"> <li>• Memory Cache =0 (NN4.7 &amp; NN7.0)</li> <li>• Disk Cache =0 (NN4.7 &amp; NN7.0), Amount of disk space to use :Set to minimum value (IE5.5)</li> <li>• Select: Document in cache is compared to document on network: Every time (NN4.7 &amp; NN7.0)</li> <li>• Check for newer versions of stored pages :Every visit to the page (IE5.5)</li> </ul>
4. General	<ul style="list-style-type: none"> <li>• If any toolbars are installed (like google toolbar, yahoo toolbar, etc.), ensure that the pop-up blocker is disabled on all of them</li> </ul>

**Click image below when complete:**



Configure the browser according to the setting **described** in the following table. When the settings are complete, click the Nortel logo to connect to the LCI interface.

## LCI Browser configuration

Menu path	Setting
[Netscape] Edit-->Preferences-->Appearance-->Fonts [Explorer] Tools-->Internet Options-->General-->Fonts	<ul style="list-style-type: none"> <li>• Fonts for Encoding/Fonts for: Western (NN4.7 &amp; NN7.0)</li> <li>• Variable Font =Times New Roman, Size = 10 (NN4.7), Proportional: Serif, Size = 12, Serif: Times New Roman, Sans-serif: Arial (NN7.0)</li> <li>• Fixed Font/Monospace = Courier New, Size = 10 (NN4.7 &amp; NN7.0)</li> <li>• Select: use my default fonts, overriding document-specified fonts (NN4.7)</li> <li>• Uncheck: Allow documents to use other fonts: (NN7.0)</li> </ul>

Menu path	Setting
	<ul style="list-style-type: none"> <li>Language Script: Latin Based, Web page font: Times New Roman, Plain text font: Courier New (IE5.5)</li> </ul>
[Netscape] Edit-->Preferences--> Advanced	<ul style="list-style-type: none"> <li>Select: Automatically load images (NN4.7)</li> </ul>
[Explorer] Tools-->Internet Options-->Advanced	<ul style="list-style-type: none"> <li>Select: Enable Java (NN4.7 &amp; NN7.0)</li> <li>Select: Enable JavaScript (NN4.7)</li> <li>Select: Enable style sheets/SXLT (NN4.7 &amp; NN7.0)</li> <li>Select: Restore Defaults (IE5.5)</li> </ul>
[Netscape] Edit-->Preferences--> Advanced-->Cache	<ul style="list-style-type: none"> <li>Memory Cache = 0 (NN4.7 &amp; NN7.0)</li> </ul>
[Explorer] Tools-->Internet Options-->General-->Temporary Internet Files-->Settings	<ul style="list-style-type: none"> <li>Disk Cache = 0 (NN4.7 &amp; NN7.0), Amount of disk space to use: Set to minimum value (IE5.5)</li> <li>Select: Document in cache is compared to document on network: Every time (NN4.7 &amp; NN7.0)</li> <li>Check for newer versions of stored pages: Every visit to the page (IE5.5)</li> </ul>
General	<p>If any toolbars are installed (such as, Google toolbar or Yahoo toolbar), ensure the pop-up blocker is disabled on all of them.</p>

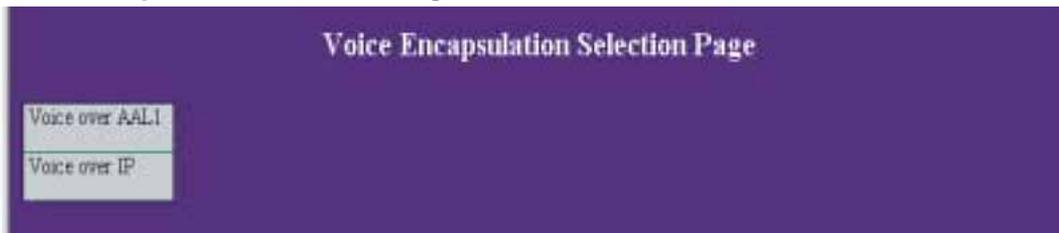
**Note:** Only one user login access is permitted on the LCI. If LCI access is networked, only one user may be logged in on an LCI port on a control shelf at any time.

If a pop-up window appears stating 'You must use the Active DCC', then the DCC card you have plugged into is not the active unit. The active unit will have the steady green light on the faceplate. Change the connection to the active DCC Card.

If the method over which the MG 9000 is providing voice services has not been selected, the Voice Encapsulation Selection Page appears as shown in the following figure. Choose from Voice over AAL1 (ATM) or Voice over IP (IP).

**Note:** If the MG 9000 is configured with Gigabit Ethernet (GigE) DCC cards, the following screen will not appear. The LCI will go directly into Voice over IP.

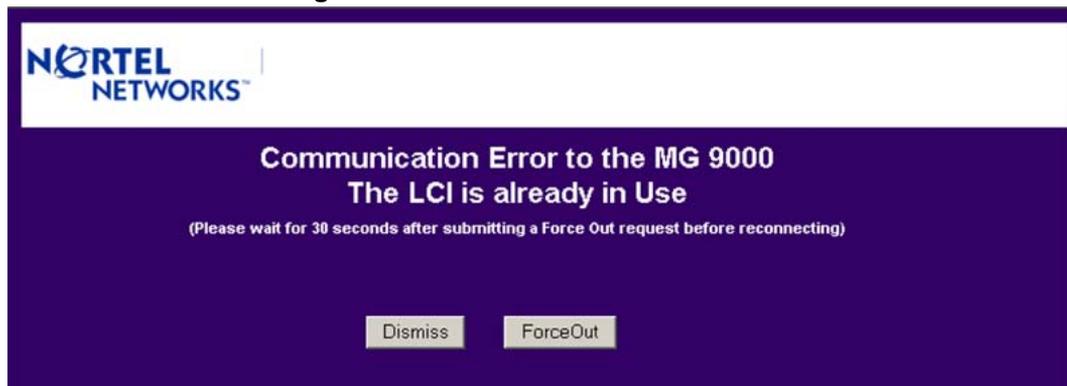
### Voice Encapsulation Selection Page



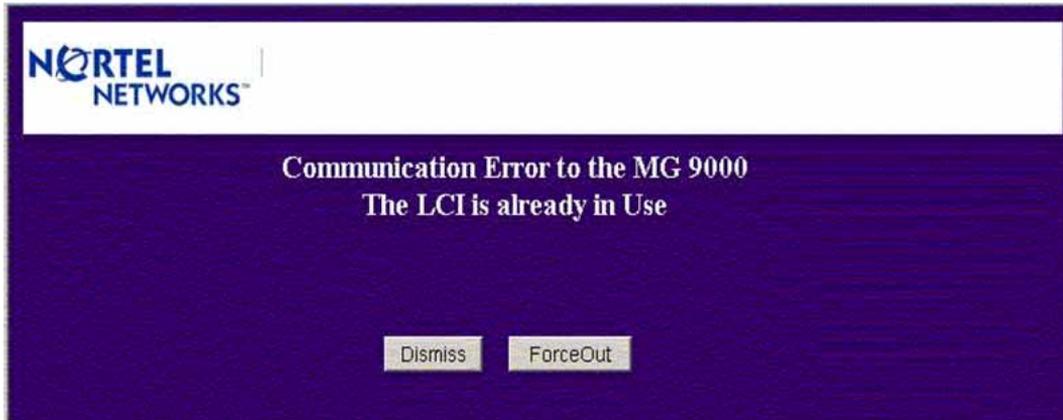
After the method is selected, a Network Element view appears which indicates the method of encapsulation chosen, which is described next.

When a user attempts to connect to the LCI, after entering the user name and password, the system performs an in use check. The system responds with the following message

### LCI in use check message



If a user is already connected to the LCI, and another user tries to connect to the same system, the LCI gives the second user an option to force out the first user. The following force-out message is received.

**LCI in use message**

When a user logs out of the LCI, wait 30 seconds before attempting to login again. This delay is used to cleanup data from the previous session and ensure a successful login. If another user tries to connect during this period, the LCI will behave the same as if a user is already connected by providing the LCI in use message seen in the previous figure.

When an intelligent card (DS1, ABI, DCC, ITP, or ITX) is restarted, a message appears in a pop-up window indicating the status of the restart and reporting the frame, shelf, and slot numbers.

When the connection between the MG 9000 and the MG 9000 Manager is not up, messages reporting the status of the connection to the user are visible at the LCI. If the system reports the same condition repeatedly, one message window will be repeatedly refreshed until the condition changes.

## Launching the LCI from the MG 9000 Manager

---

### When to use this procedure

Use the following procedure to launch the Local Craft Interface (LCI) from the MG 9000 Manager.

The LCI in this instance can be used in the case when a NE has lost communication with the MG 9000 Manager.

### Prerequisites

You must have emsadm privileges to perform this procedure.

### Limitations and restrictions

The following limitations and restrictions apply to this procedure:

- This procedure is valid for both discovered and undiscovered MG 9000 NEs.
  - Inband LCI launch is supported for software releases SN08, SN09, SN09FF and higher
  - Out of band LCI launch is supported only for software release SN09FF and higher.
- The MG 9000 Manager client must have a defined browser path in the OS environment. For Unix OS, the "PATH" environment must have a Netscape path defined. For Window OS, the default browser must be set to either Netscape or Internet Explorer.
- You must close any existing LCI windows on the MG 9000 Manager client before launching a session from MG 9000 Manager GUI.

**Note:** If a browser window is already open and you try to launch an LCI session (either inband or out of band), the http session will be established in the existing window. If you have already launched an LCI window, and if you try to launch a second LCI session, the MG 9000 Manager attempts to open the session in the existing LCI window. The LCI window properties and size cannot be controlled from MG 9000 Manager.

- When you choose to launch the LCI using the inband IP option, and if the inband address of the MG 9000 is allocated from a private co-LAN address space, a client located on the same co-LAN or a client which had been connected to the co-LAN through a VPN firewall will be able to launch the LCI session. Networking routing is very important while launching the LCI through inband IP.

**Note:** Check your network routing by using the `ping` and `tracert` commands. You can use either the command line or **Configuration > Tools** command from the subnet EM menu to access these utilities.

- LCI out of band access is only available if an Ethernet is connected at the face plate on the supercore and a valid out of band IP has been previously configured at LCI.
- If the LCI browser session returns a "404 not found" message, use the `ping` command to verify that the out of band address on MG 9000 is valid. The out of band address is the address in the URL shown on the browser screen when you launch the out of band LCI.

## Launching the LCI from the MG 9000 Manager

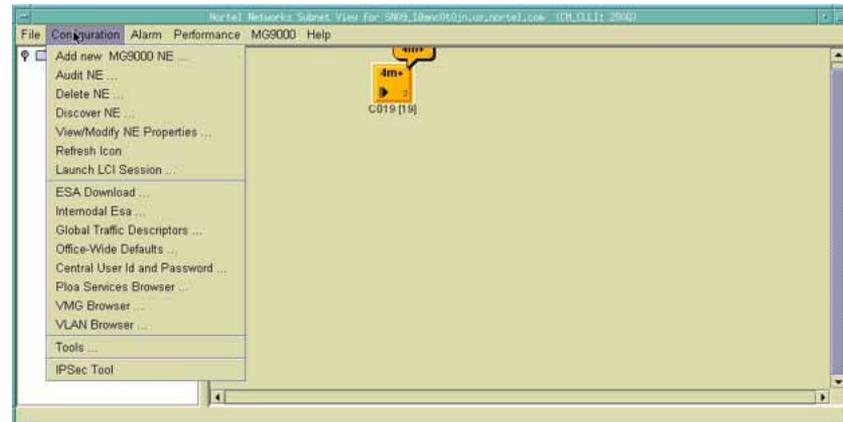
Step	Action
------	--------

*At the MG 9000 Manager*

- 1 From the MG 9000 Manager Subnet view, click on the NE for which you want to launch the LCI.
- 2 From the MG 9000 Manager Subnet view, select **Configuration**.

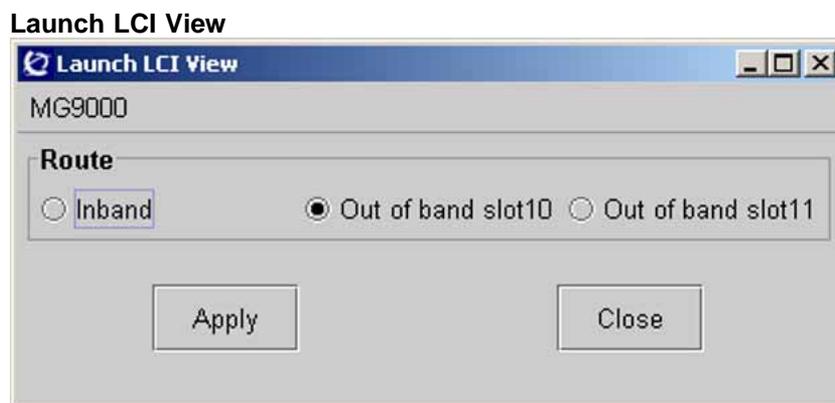
*The Configuration view appears:*

### Configuration menu



- 3 From the **Configuration** menu, choose **Launch LCI Session**.

*The Launch LCI View appears:*



- 4 Do one of the following actions depending on your network configuration and the software version you are using:

If you wish to use	Do
an out of band route	<a href="#">step 5</a>
an inbound route	<a href="#">step 6</a>

**Note:** Inband LCI launch is supported for software releases SN08, SN09, SN09FF and higher. Out of band LCI launch is supported only for software release SN09FF and higher.

- 5 Select the **Out of band** option for the side of the MG 9000 that is active, either slot 10 or 11, click **Apply**, then go to [step 7](#).

**Note:** If your attempt to launch the LCI through slot 10 is not successful because of inactivity of the DCC card, launch the LCI through slot 11.

- 6 Select **Inband** and click **Apply**.

- 7 The system asks you to confirm the operation:



8 Do one of the following actions:

If	Do
you wish to proceed	type " <b>accept</b> " and click <b>OK</b>
you wish to cancel this procedure	click <b>Cancel</b>

9 Do one of the following steps depending on the system response:

- If the system launches the default web browser and access to the LCI occurs. Go to [Step 11](#).
- If SNMP communication is inoperative, a communication failure error message appears:

**Example of LCI launch failure notification**



Go to [step 10](#).

- If an NE running pre-SN09FF software is discovered successfully and the communication channel is operative, an error message appears saying that the LCI launch operation is not supported for the software version running on the NE

**Example of unsupported LCI release notification**



Go to [step 10](#).

10 Click **OK** to exit.

- If you want to launch the LCI out of band, you must first establish SNMP communication with the MG 9000. Establish SNMP communication and return to the beginning of this procedure.

- Use inband communication. Repeat this procedure, but select **Inband** from the Launch LCI View.

**11** You have completed this procedure.

---

—End—

---

## LCI network element screen

The initial LCI screen presents a network element (NE) view of the MG 9000. The NE view provides the following functions:

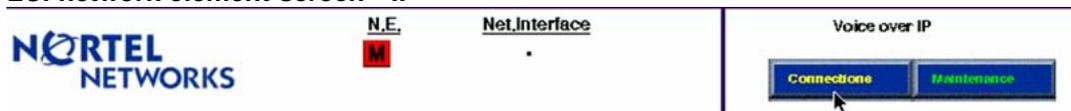
- access to the Connections menu
- access to the Maintenance menu
- MG 9000 alarm status

The following figure shows an example of the network element screen.

LCI network element screen - ATM



LCI network element screen - IP



The Connections menu is accessed by clicking on the Connections button in the banner and provides access to information necessary to add a newly configured MG 9000 network. Some common Connections menu tasks include the following actions:

- setting up connection to ATM network
- setting up call control connection
- setting up the OAMP connection between the MG 9000 and the MG 9000 Manager
- setting up ABI connection

The Maintenance menu is accessed by clicking on the Maintenance button in the banner and provides the ability to manage individual MG 9000 frames and shelves down to the card level. Some common Maintenance menu tasks include the following actions:

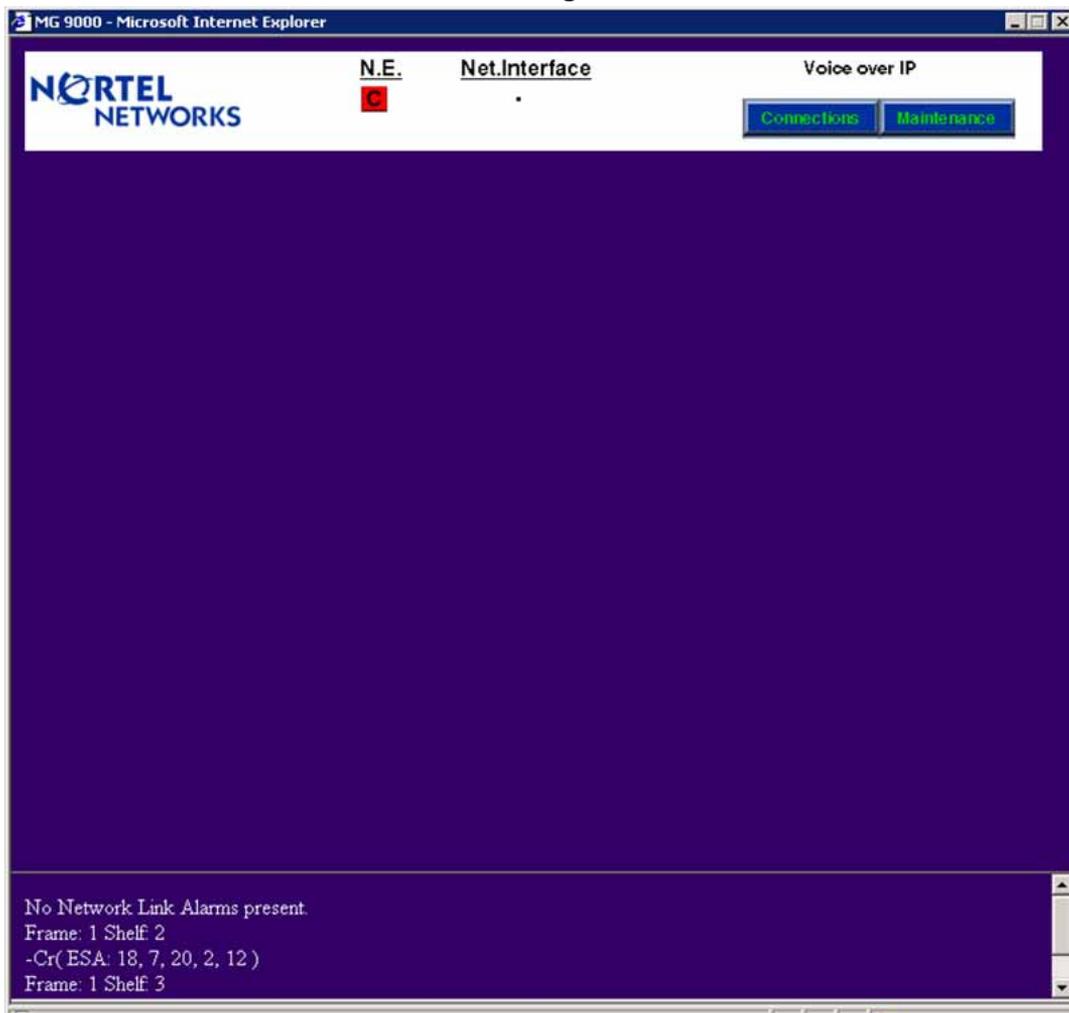
- perform a return to service (RTS)
- view the carriers (links in GigE)
- reload system cards
- run diagnostics
- monitor alarms

The network element screen displays the following alarm notifications that appear as light emitting diode (LED) icons on the screen:

- critical
- major
- minor

The following figure shows the NE screen and the accompanying message area at the bottom of the screen in response to clicking on either N.E. or Net.Interface in the banner. If alarms are present, they appear in the banner as C, M, or m and the severity of each alarm is listed in the bottom frame of the screen. If no alarms are present, a dot (.) is present in the banner. The following figure shows the message reporting that no network interface (link) alarms are present and identifies the location of the one NE alarm in the MG 9000.

#### Network element screen with alarms message



The message area shown at the bottom of the previous figure displays messages to the user and also acts as a message buffer, retaining the last message displayed during the LCI session. A new message overwrites the previous message.

The alarm notifications reflect the current state of the MG 9000 network element. These alarm displays appear on all LCI screens throughout all menus. If an LED next to an alarm appears lit, information regarding the alarm condition appears on demand by a mouse click on the alarm. During an alarm condition, a list of affected frames and shelves appears at the bottom of the screen. If multiple alarms apply, only the highest severity alarm for a particular shelf appears. The alarm notification serves as a warning and provides information to navigate to the problem area through the Maintenance menu.

Certain alarms are raised and appear under the NE banner but do not have corresponding alarms appear on the cards in the shelf screen. These alarms are

- virtual media gateway (VMG)
- emergency stand alone (ESA)
- stream control transmission protocol (SCTP)

Click on the NE in the banner and the alarm type, location, and severity information appear in the message area at the bottom of the screen.

The following are three examples of alarm messages seen in the message area:

- No carrier alarm and one minor node maintenance alarm. No VMG, ESA, or SCTP alarms are present.

```
No Network Carrier Alarms present.
Frame: 0 Shelf: 3 - Highest Alarm Severity for Node
Mtc: Mn
```

- No carrier alarm and no node maintenance alarm. One Critical VMG alarm, one Major ESA alarm, and one Minor SCTP alarm.

```
No Network Carrier Alarms present.
Frame: 0 Shelf: 3
-Cr( VMG: 12 ) -Mj( VMG: 12 ESA: 12) -Mn(SCTP: 21)
```

- No carrier alarm and no node maintenance alarm. One VMG alarm, no ESA alarm, and no SCTP alarm.

```
No Network Carrier Alarms present.
Frame: 0 Shelf: 3
-Cr( VMG: 12 )
```

The following figure shows one VMG alarm and no other alarms as listed above.

**Alarm information in message area**

The screenshot displays the Nortel Networks MG 9000 local craft interface. At the top, the Nortel Networks logo is on the left, and the text "N.E.", "Net.Interface", and "Voice over AAL1" is on the right. Below the logo, there are two buttons: "Connections" and "Maintenance".

The main area shows "Frame #1 Shelf #3 Selected" and a "select a shelf view below:" dropdown menu with "frame #1 shelf #3" selected. To the right of this is a vertical "FRAME" label. Below the dropdown is a table representing the shelf slots:

SIC									A	A						
PIO	MTA		LC	LC					DCC	DCC	ITP	ITP	ITX	ITX	LC	LC

An orange triangle points to the "ITP" slot in the second row. Below the table, the text "Alarm Info for Slot #12" is displayed. Underneath is a table with columns for "Severity", "Description", and "Time". The table is currently empty.

At the bottom of the interface, the text "Alarms query done" is displayed.

## LCI Connections view

The Connection View is where the basic connection information is configured to allow the MG 9000 to communicate to the ATM or IP network and CS 2000. In this section, the IP and ATM addressing information along with other connection-related data is entered for the network element.

Separate connections are configured for the ATM network, Call Control, OAMP, and ABI (if equipped). The Time of Day clock is also set from the Connections section. Selecting the Connections function box at the top of the screen produces the following options.

- "Connection to ATM network (voice over AAL1 only)" (page 330)
- "Call control connection" (page 332)
- "OAMP connection" (page 337)
- "ABI connection" (page 341)
- "Password change" (page 343)
- "RADIUS configuration" (page 344)
- "Time of day" (page 345)

After accessing a Connections menu item and it is necessary to return to the Main Page, click on the Connections button. This behavior is true throughout the LCI, to return to the previous menu, click on the menu item, card, frame or shelf which you entered.

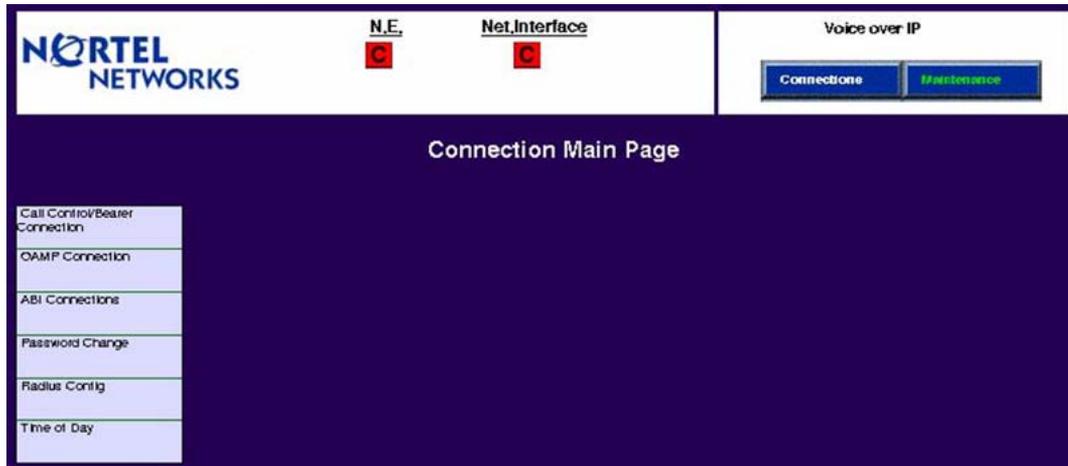
The following figure shows the LCI Connections Main Page for Voice over AAL1.

Connection Main Page - Voice over AAL1



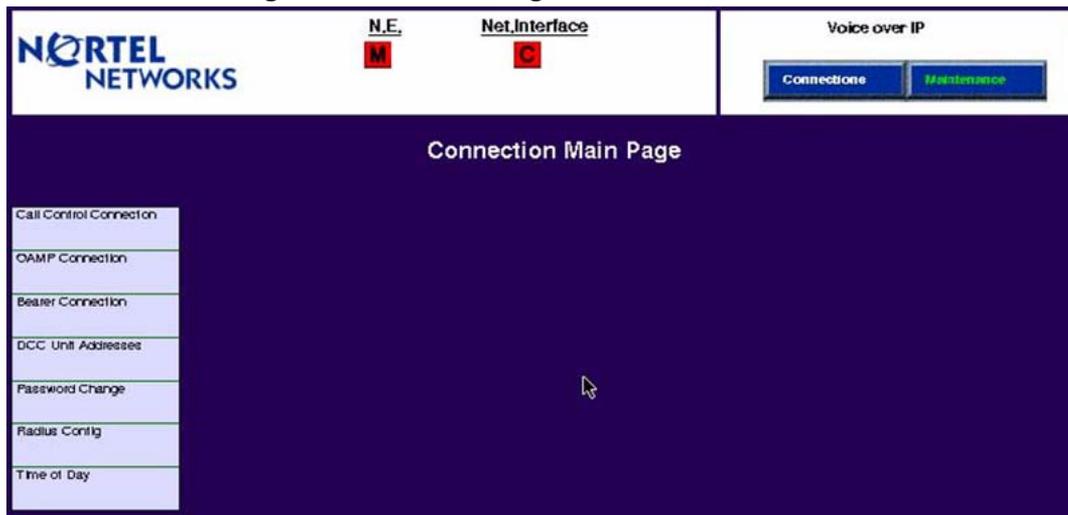
The following figure shows the Connection Main Page for Voice over IP.

**Connection Main Page - Voice over IP**



The following figure shows the Connections Main Page for Voice over IP when the MG 9000 is equipped with GigE DCC cards.

**Connection Main Page - Voice over IP, GigE**



**Connection to ATM network (voice over AAL1 only)**

The Connection to ATM network screen defines the location of the MG 9000 in the network.

## Connection to ATM Network screen

**NORTEL NETWORKS**      N.E.      Net.Interface      Voice over AAL1

Connections      Maintenance

### Connection to ATM Network

ILMI Status Enabled Disabled

---

SAAL Status      SAAL connection is ESTABLISHED      Query

---

UNI Version: uni4.0      Submit

Local Network Prefix: 39345678901234567890123A1

End System Identifier: 01999999      0000 - FFFF

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

Query All

At initial screen access, the LCI queries the server side for current settings of the following fields:

- ILMI Status
- SAAL Status
- UNI Version
- Local Network Prefix
- End System Identifier

**Note:** The Local Network Prefix value is automatically displayed in the associated boxes.

ILMI status has an LED Indicator that displays whether ILMI is enabled or disabled. This LED is updated after each Query. If Address registration is enabled, leaving the Local Network Prefix field blank and clicking "Submit" allows the network switch to automatically provide a network prefix.

The "Query All" button displays current values in the status boxes.

The following table describes the data fields displayed on the Connection to ATM Network screen.

#### Connection to ATM Network screen fields

Field	Description
ILMI status	Interim Local Management Information shares UNI management information between the MG 9000 as an ATM end system and the ATM switch.  The ILMI status is either enabled or disabled. If disabled, a 13 byte network prefix must be entered in the Local Network Prefix field. If enabled, the ATM network switch assigns the Local Network Prefix automatically.
SAAL Status	The LCI queries the Signalling ATM Adaptation Layer (SAAL) at screen access. A query button allows for an updated status after initial screen access.
UNI Version	The User-to-Network-Interface version represents the interface between the MG 9000 and the ATM switch.
Local Network Prefix	The local network prefix is the ATM end system address (AESA). An AESA is similar to an IP address and uniquely identifies the ATM endpoint within the global network. Routing and network management require this prefix configured into the ATM switch.
End System Identifier	The End System Identifier must be a unique number, (one that no other MG 9000 is using) which is converted to hexadecimal.

#### Call control connection

The Call Control Connection is used to assign the Subnet mask, Default Gateway, and Heartbeat Ping IP addresses supporting the MG 9000, in addition to the following specific fields based on solution:

- For Voice over AAL1, the Primary AESA to SC0 and Secondary AESA to SC1 address and Call Control Classical IP Over ATM (CIPOA) address.
- For Voice over IP, the VCC information and Traffic Parameters must be configured for the PVC configured between the MG 9000 and CallIP VLAN on the CS LAN.

The following figure shows the Call Control Connection screen for ATM solutions.

## Call Control Connection screen - Voice over AAL1

The screenshot shows the 'Call Control Connection' configuration screen for 'Voice over AAL1'. At the top left is the Nortel Networks logo. To its right, there are labels 'N.E.' and 'Net. Carrier' with a small red square icon. Further right, the text 'Voice over AAL1' is displayed above two buttons: 'Connections' and 'Maintenance'. The main title 'Call Control Connection' is centered. Below it, there are several input fields: 'SCO RESA' and 'SCI RESA' (both empty), 'Default Gateway' (containing '0.0.0.0'), 'Call Control CIPOR Address' (containing '0.0.0.0'), and 'Subnet Mask' (containing '0.0.0.0'). To the right of these fields are 'Conn status' indicators with 'up' and 'down' buttons. Below the 'Subnet Mask' field is a 'Heartbeat Ping IP (optional)' field. At the bottom center are 'Submit' and 'Query' buttons.

The Heartbeat Ping IP field is an optional field in both solution screens. If this field is provisioned, the MG 9000 will do Internet Control Message Protocol (ICMP) pings on the connection side and will attempt corrective action if the pings fail. This field also appears in the OAMP Connection and ABI Connection screens. Typically, the value is the same for each. Having this field in several screen gives the user the flexibility to enter different destinations, such as having call control messaging sent to one SAM21 and the OAMP messaging sent to another SAM21.

Use the following information to determine the heartbeat address to enter in the field based on the type of solution being configured.

- For Voice over AAL1, the recommended heartbeat address is the active Ethernet IP address of the shelf controller. Never use a unit or inactive address. Normally this address is the same for all connection types (OAMP, Call Control, and ABI).
- For Voice over IP, the recommended heartbeat address is the default Gateway for the connection.

**Note:** This address must be an address in the connection subnet.

The following figure shows the Call Control Connection screen for IP solutions.

## Call Control Connection screen - Voice over IP

**Note:** In the Call Control Connection screen for IP solutions, after a call control connection is established the VPI, VCI, PCR, SCR, MBS and CDVT fields become non-editable.

The following are the traffic parameter fields in the Voice over IP screen:

- PCR - peak cell rate
- SCR - sustainable cell rate
- MBS - maximum burst size
- CDVT - cell delay variation tolerance

The values for the traffic parameters are set to 0 when the screen is first displayed. Use the Default button to request default values for these fields.

**Note:** Since the calculation of these default values depends on the amount of available bandwidth, the carriers must be provisioned first. If not, 0's are returned and the following message is displayed: The Default Traffic Descriptors parameters cannot be determined. Please provision carriers.

The Traffic Parameters also appear in the OAMP Connection and ABI Connection screens. The values are different for each connection type.

**Note:** Consult with Nortel before entering values other than the default values.

When the MG 9000 is equipped with GigE DCC cards, the Call Control Connection screen contains the following fields:

#### Call Control Connection screen fields for VoIP solutions with GigE

Field	Description
Default Gateway	The IP address of the designated default router to create a route used when a more specific route is not available in the routing table.
Call Control Address	GigE IP address for call control signaling-related information. This address is used as the IESA IP address and obtains the MAC address of the default gateway.
Subnet Mask	A subnet mask is a series of numbers over an IP address used to simplify routing. An 8-bit binary mask of "1s" (decimal 255) tells the router to look at the number underneath the mask.
Heartbeat Ping IP	The Heartbeat ping IP field also appears in the OAMP and Call Control Connection screens. There is no ABI screen for GigE. Refer to the discussion of this field in the Call Control Connection screen.
VLAN ID	VLAN ID
VLAN name	VLAN name.
VLAN Peak Rate	Peak rate for the VLAN ID.
VLAN Priority Group	Indicates the four levels supported by the MG 9000. Select the Priority Group from the pull-down before selecting the Priority Value. The four supported Priority Groups are as follows: <ul style="list-style-type: none"> <li>• 7 (highest value, do not use since this is used for link integrity)</li> <li>• 6, 5</li> <li>• 4, 3</li> <li>• 2, 1, 0 (lowest)</li> </ul>
VLAN Priority Value	Indicates the Priority Value associated with each VLAN Priority Group. For example, Priority Group 0 will have Priority Values 0, 1, 2 associated with it. Select the Priority Value from the pull-down.
Slot 10 (11), Port number	Defaults to the network port if it is provisioned. If the network port has not been defined, a warning message appears in the connection screen.

Field	Description
Default button	<p>Allows the user to go back to default VLAN Peak Rate and VLAN Priority level at any time in the screen. Refer to "<a href="#">VLAN Peak Rate default values used on LCI screens</a>" (page 336) for default values.</p> <p><b>Note:</b> After the VLAN is created, the Priority value cannot be changed. The Default button can be used to display the default VLAN peak rate and priority setting.</p>
Submit button	<p>When the Submit button is clicked, only the Peak rate will be changed. No change will be made to the VLAN Priority. A message appears warning the user when an attempt is made to change the existing VLAN Priority value.</p>

The default values of VLAN are for the peak rate and Priority only. The following are the values for Peak Rate in bits/sec and the Priority by LCI screen

#### VLAN Peak Rate default values used on LCI screens

LCI screen	VLAN Peak Rate (bps)	VLAN Priority
Call Control Connection	4240000	4
OAMP Connection	1060000	2
Bearer Connection	548352000	6
DCC Unit Addresses	1060000	2

The following figure shows the Call Control Connection screen for a Voice over IP solution with GigE

Call Control Connection screen - GigE, voice over IP

**Call Control Connection**

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

Submit Query Default

OAMP connection

The OAMP Connection screen defines the MG 9000 connection to the MG 9000 Manager. The following figure shows the OAMP Connection screen for ATM solutions.

OAMP Connection screen - Voice over AAL1

**OAMP Connection**

SC0 AESA	<input type="text" value="39345678901234567890A4A4A400E0CF01"/>	Comm status	
SC1 AESA	<input type="text" value="39345678901234567890a4a4a400e0cf008"/>		
Default Gateway	<input type="text" value="47.142.105.193"/>		
IP Address of MG 9000 Element Manager	<input type="text" value="47.142.106.232"/>	IP Port of MG 9000 Element Manager	<input type="text" value="8002"/>
OAMP CIP0A Address	<input type="text" value="47.142.105.37"/>		
Subnet Mask	<input type="text" value="255.255.255.0"/>		
Preshared Key	<input type="password" value="*****"/>		
Confirm Preshared Key	<input type="password" value="*****"/>		
OAM Collector Server IP (optional)	<input type="text"/>	Heartbeat Ping IP (optional)	<input type="text"/>
Reestablish Communications to Element Manager	<input type="button" value="Comm.Reset"/>	<input type="checkbox"/> Force?	

Submit Query

The following figure shows the OAMP Connection screen for IP solutions.

**OAMP Connection screen - Voice over IP**

**OAMP Connection**

MG9000 Element Manager

IP Address: 47.142.92.98 Port: 8002

Default Gateway: 172.31.165.65

MG9000 IP Address: 172.31.165.66

Subnet Mask: 255.255.255.248

OAM Collector Server IP (optional):

Heartbeat Ping IP (optional):

Pre-shared Key: \*\*\*\*\*

Confirm Pre-shared 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   Force?

The following figure shows the OAMP Connection screen for an MG 9000 equipped with GigE DCC cards.

**OAMP Connection screen - GigE, voice over IP**

**OAMP Connection**

MG9000 Element Manager

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

OAM Collector Server IP (optional):

Subnet Mask: 255.255.255.248

Pre-shared Key: \*\*\*\*\*

Confirm Pre-shared Key: \*\*\*\*\*

**VLAN**

VLAN ID: 69

VLAN Name: oam

VLAN Peak rate (bps): 1080000

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   Force?

The following table describes the data fields displayed on the OAMP Connection screen.

#### OAMP Connection screen fields for AAL1 and VoIP solutions

Field	Description
SC0 AESA (Voice over AAL1 only)	The ATM address for the primary Switched Virtual Circuit (SVC) to the Service Application Module 21 (SAM21) shelf controller in the call server. The MG 9000 Manager connects to the SAM21 shelf controller through an Ethernet port. The Primary AESA is for the shelf controller card in slot 7.
SC1 AESA (Voice over AAL1 only)	The Secondary AESA is for the shelf controller card in slot 9.
IP Address	The IP network address assigned to the MG 9000 Manager.
IP Port	The IP port number assigned to the MG 9000 Manager. Ports are used to identify the ends of logical connections.
Default Gateway	The IP address of the designated default router to create a route used when a more specific route is not available in the routing table.
Subnet Mask	A subnet mask is a series of numbers over an IP address used to simplify routing. An 8-bit binary mask of "1s" (decimal 255) tells the router to look at the number underneath the mask.
OAMP address	For Voice over AAL1, this is the OAMP IP address for the in-band connection to the SAM21 Shelf Controller.  For Voice over IP, this is the OAMP IP address to the Media Gateway 7480/15000.  For GigE in Voice over IP, there are two OAMP address fields, Active OAMP IP and Inactive OAMP IP. These two IP addresses float between the two GigE cards depending on which one is active and inactive. The active OAMP IP will always be associated with the active card. The inactive OAMP IP will always be associated with the inactive card. The active OAMP IP must be used as the NE IP address when provisioning the node in the MG 9000 Manager.
Heartbeat Ping IP	The Heartbeat ping IP field also appears in the ABI Connection and Call Control Connection screens. Refer to the discussion of this field in the Call Control Connection screen
OM Collector Server IP (optional)	The IP address of the OM Collector server.

Field	Description
Virtual Channel Connection (Voice over IP only, not applicable to GigE)	The values for the traffic parameters (PCR, SCR, MBS, and CDVT) are set to 0 when the screen is first displayed. Use the Default button to request default values for these fields. Since the calculation of these default values depends on the amount of available bandwidth, the carriers must be provisioned first. If not, 0's are returned and the following message is displayed: The Default Traffic Descriptors parameters cannot be determined. Please provision carriers.
VLAN ID, VLAN name, VLAN Peak Rate, VLAN Priority Group, and VLAN Priority (Voice over IP with GigE only)	Refer to VLAN values and their explanation presented in association with the table " <a href="#">Call Control Connection screen fields for VoIP solutions with GigE</a> " (page 335).
Slot 10 (11), Port number	Defaults to the network port if it is provisioned. If the network port has not been defined, a warning message appears in the connection screen.
Preshared Key	NE Encryption Keys (Preshared Keys) are configured when the MG 9000 and MG 9000 Manager are upgraded to SN08. Preshared Keys are established to enable encryption of certain values passed between the MG 9000 and the MG 9000 Manager and to support functions such as software upgrade and ESA data download because communication is secured for these activities. For more information on Preshared Keys, refer to <i>MG 9000 Security and Administration</i> , NN10162-611.
Confirm Preshared Key	For user confirmation of Preshared Key.

Queries, through initial screen access and the Query button, display the server side field values in the text boxes.

The Comm Reset button provides the ability to send a manual cold start event to the MG 9000 Manager in situations where the MG 9000 Manager does not receive an automatic cold start.

## DCC Unit Addresses

The DCC Unit Addresses screen is used in an MG 9000 with GigE DCC cards to provide an IP address for each GigE card. This address is used for link integrity testing. The following options are available on this screen.

- Slot 10 (11) IP Addresses - IP addresses of each GigE card
- Slot 10 (11) Default Gateway - default gateway address of each GigE card
- Slot 10 (11) Subnet Mask - subnet mask of each GigE card
- VLAN ID, VLAN name, VLAN Peak Rate, VLAN Priority Group, and VLAN Priority - Refer to VLAN values and their explanation presented

in association with the table "Call Control Connection screen fields for VoIP solutions with GigE" (page 335).

- Slot 10 (11), Port number - defaults to the network port if it is provisioned. If the network port has not been defined, a warning message appears in the connection screen.

The following figure shows the DCC Unit Addresses screen for an MG 9000 equipped with GigE DCC cards

### DCC Unit Addresses

DCC Unit Addresses			
Slot10 IP Address	172.21.0.69	VLAN ID	68
Slot10 Default Gateway	172.21.0.65	VLAN Name	unit
Slot10 Subnet Mask	255.255.255.240	VLAN Peak rate (bps)	1060000
Slot11 IP Address	172.21.0.70	VLAN Priority Group	0
Slot11 Default Gateway	172.21.0.65	VLAN Priority	2
Slot11 Subnet Mask	255.255.255.240	Slot10,Port#	0
		Slot11,Port#	-
<input type="button" value="Submit"/> <input type="button" value="Query"/> <input type="button" value="Default"/>			

### ABI connection

The ABI Connection page allows the technician to assign the following for an ABI card

- the Primary and Secondary (ATM End System Addresses (AESAs) for the SC cards in the SAM 21 shelf
- the default gateway IP address
- the ABI CIPOA address
- the subnet mask
- the Heartbeat ping IP address. This field also appears in the OAMP Connection and Call Control Connection screens. Refer to the discussion of this field in the description of the "Call control connection" (page 332).

**Note:** The ABI Connection screen is available only for AAL1 and VoIP configurations. There is no ABI screen for GigE.

Refer to the tables in previous sections for explanations of the values for these fields. The following figure shows the ABI Connection screen for Voice over AAL1.

ABI Connection screen for Voice over AAL1

**ABI Connection**

SC0 AESA	39345678901234567890A4A4A400E0CF01	Conn status up down
SC1 AESA	39345678901234567890a4a4a400e0cf006	up down
Default Gateway	47.142.105.199	
ABI Channel Address	47.142.105.237	
Subnet Mask	255.255.255.0	Headbeat Ping IP (optional)

Submit Query

The following figure shows the ABI Connection screen for Voice over IP.

ABI Connection screen for Voice over IP

**ABI Connection**

Virtual Channel Connection

Default Gateway (optional)		Virtual Channel		Traffic Parameters
Headbeat Ping IP (optional)		Interface	16	PCR 0
Subnet Mask	0.0.0.0	VPI	18	SCR 0
		VCI	2044	MBS 0
				CDVT 0

Submit Query Default

For Voice over IP only, the values for the traffic descriptor (PCR, SCR, MBS, and CDVT) are set to 0 when the screen is first displayed. Use the Default button to request default values for these fields. Since the calculation of these default values depends on the amount of available bandwidth, the carriers must be provisioned first. If not, 0's are returned and the following message is displayed: The Default Traffic Descriptors parameters cannot be determined. Please provision carriers.

## Bearer Connection

The Bearer Connection screen is used in an MG 9000 with GigE DCC cards to identify the connection carrying all bearer traffic. The following options are available from the Bearer Connection screen:

- Default Gateway and Subnet Mask -
- Bearer IP - identifies the connection carrying all bearer traffic. The ABI and ITP bearer will be transmitted and received using this VLAN.
- VLAN ID, VLAN name, VLAN Peak Rate, VLAN Priority Group, and VLAN Priority - Refer to VLAN values and their explanation presented in association with the table ["Call Control Connection screen fields for VoIP solutions with GigE"](#) (page 335).

The following figure shows the Bearer Connection screen.

Bearer Connection screen - GigE, Voice over IP

The screenshot shows the 'Bearer Connection' configuration interface. It features a dark blue background with white text and input fields. The fields are arranged in two columns. The left column contains 'Default Gateway' (172.21.0.89), 'Bearer IP Address' (172.21.0.92), and 'Subnet Mask' (255.255.255.248). The right column contains 'VLAN ID' (71), 'VLAN Name' (Bearer), 'VLAN Peak rate (bps)' (548352000), 'VLAN Priority Group' (2), 'VLAN Priority' (6), 'Slot10.PortV' (0), and 'Slot11.PortV' (-). At the bottom, there are three buttons: 'Submit', 'Query', and 'Default'.

## Password change

The Password Change screen provides a means for changing the default password. This password is used for LCI and SFTP authentication. The following are the fields shown in the Password Change screen:

- Old Password - enter the existing password that is to be changed
- New Password - enter the new password
- Confirm Password - enter the new password again. If the password is entered incorrectly, an error message appears indicating the password change will not take effect.

**Note:** If the provisioned password is forgotten, contact Nortel GNPS for assistance.

Use the Submit button to send the data entered on the screen to the MG 9000 as a provisioning request. Results from the request are presented in the text area at the bottom of the LCI GUI screen.

The following figure shows the Password Change screen.

#### Password change screen



The screenshot shows the Password Change screen. At the top left is the Nortel Networks logo. To its right are the labels 'N.E.' and 'Net.Carrier' with a small orange 'm' icon. Further right is 'Voice over AAL1' and two buttons: 'Connections' and 'Maintenance'. The main title 'Password Change' is centered. Below it are three input fields labeled 'Old Password', 'New Password', and 'Confirm Password'. A 'Submit' button is at the bottom center.

#### RADIUS configuration

The RADIUS Configuration screen is used to set/query the RADIUS (IEMS) IP address which is used for user authentication. The RADIUS client of the MG 9000 includes software that collects user ids, passwords, and the source IP address. This information is passed on to the RADIUS server to track and log user's activity, including log out time. The following fields are available:

- Radius Server IP Address
- Radius Server Secret Key
- Reset button - used to reset Radius authentication from "central" to "local" authentication

## RADIUS Configuration screen

The screenshot shows a web-based configuration interface for RADIUS. It features a dark blue background with white text. The title 'RADIUS Configuration' is centered at the top. Below the title, there are two input fields: 'Radius Server IP Address' and 'Radius Server Secret Key'. At the bottom of the form, there are three buttons: 'Submit', 'Query', and 'Reset'.

## Time of day

The Time of Day command accesses the Set Time and Date screen which is used to set and query the MG 9000 system clock. The initial screen access, queries, and displays the current time and date. Fields in this screen provide the ability to

- enter the IP address for the Network Time Protocol (NTP) server and click on the Use Time Server box
- set the time and date if time server is not available

## Interactions with date and time settings

Changes to time and date values can impact call processing when IPSec with Digital Signatures has been deployed within your network. Specifically, if the changes fall outside of the validity period of the associated certificates, dependent IPSec secure associations that support call processing and OAM will fail to renew. For further details, consult the *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100, or contact your next level of support.



### CAUTION

#### Risk of communication disruption, loss of service, or outage.

Changing the system time and date can result in a call processing outage if your network IP Security (IPSec) configuration is enabled to use digital signature authentication. Consult *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100 for additional details, or contact your next level of support.

## Set Time and Date GUI

You access the Set Time and Date GUI by clicking the Time of Day link on the Connections main page.

## Set Time and Date screen

Click the **Query** button to display the current system time and date. Changes become active when you click the **Submit** button.

The data entered must fit into the ranges described in the following table, and must contain all numeric values. The hours entry requires a military format (hours 023). There is no checking for leap year or for invalid entries in months with less than 31 days.

The following table contains the Set Time and Date screen fields and ranges.

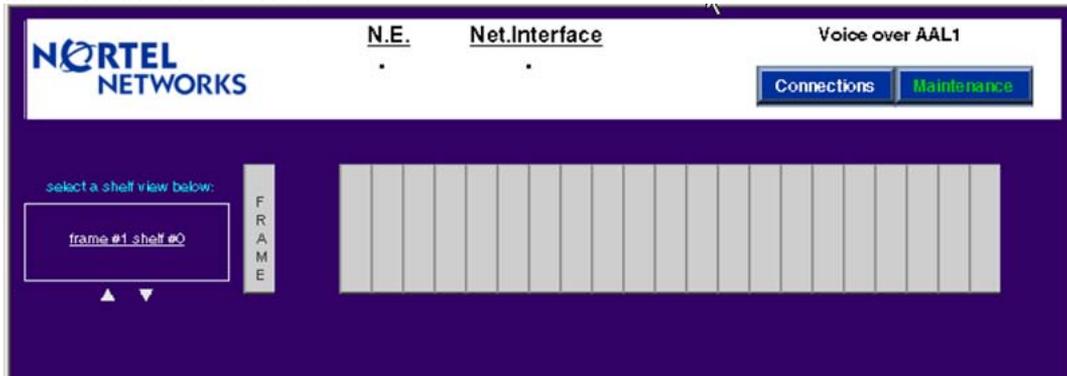
## Set Time and Date screen ranges

Field	Ranges
Year	2001 through 9999
Month	1 through 12
Day	1 through 31
Hours	0 through 23
Minutes	0 through 59
Seconds	0 through 59

## LCI Maintenance view

Selecting the Maintenance button at the top of the screen produces a shelf view with a frame selection box on the left. When first accessed, the view displays 21 empty slots. A list of available frames and shelves for selection is located on the left side of the screen. The full list is accessible through scroll arrows located immediately below the scroll window (in Internet Explorer) or through scroll bars (in Netscape Communicator). All subtending shelves connected to the master shelf are displayed. When performing activities that involve clicking on the Submit button in any of the maintenance screens, the results are displayed in the message frame at the bottom of the screen. When messages appear at the bottom, they will remain until replaced by another message. This message area acts as a message history buffer.

### Initial Maintenance View



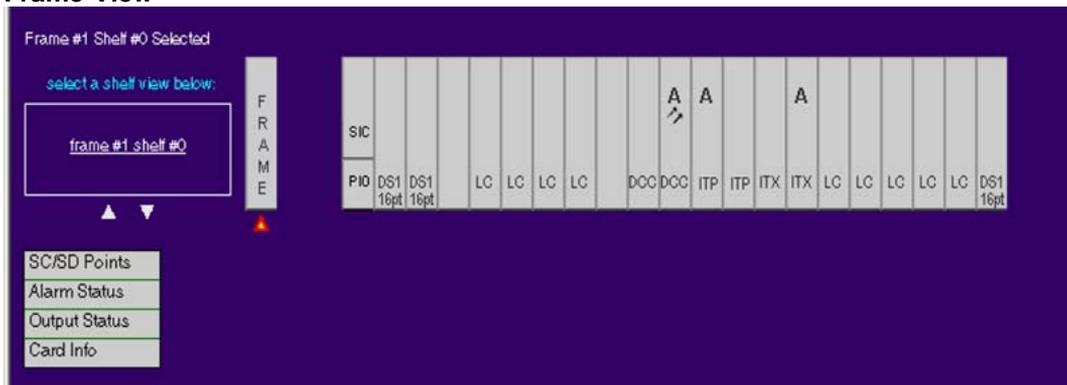
### Frame View

To view a frame, select a frame from the selection box on the left. Click on the Frame button and the following Frame Maintenance options appear:

- scan/signal distribution (SC/SD) Points
- Alarm Status
- Output Status
- Card Info

The following figure shows the frame menu options.

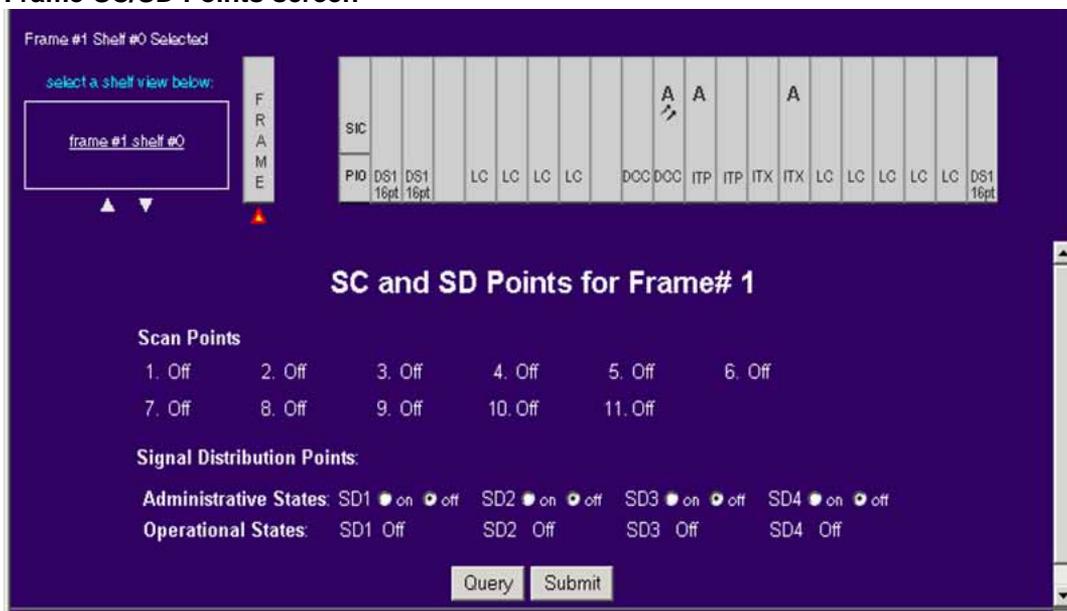
### Frame View



### SC/SD Points

The SC/SD Points option identifies the states of the Scan Points and allows the Administrative State of the Signal Distribution Points to be set. The following figure shows the SC/SD Points screen.

### Frame SC/SD Points screen



### Alarm Status

The Alarm Status option lists the alarm types and severities and their operational states. The following figure shows the Alarm Status screen.

**Frame Alarm Status**

Severity	Description	Operational state
Major	BIP Signal Battery Feed A1	Off
Major	BIP Signal Battery Feed A2	Off
Major	BIP Signal Battery Feed B1	Off
Major	BIP Signal Battery Feed B2	Off
Minor	BIP Talk Battery Filter Card A Presence	Off
Minor	BIP Talk Battery Filter Card B Presence	Off
Minor	BIP Talk Battery Filter Card A Fail	Off
Minor	BIP Talk Battery Filter Card B Fail	Off
NoAlarm	BIP Scan Point 1	Off
NoAlarm	BIP Scan Point 2	Off
NoAlarm	BIP Scan Point 3	Off
NoAlarm	BIP Scan Point 4	Off
NoAlarm	BIP Scan Point 5	Off
NoAlarm	BIP Scan Point 6	Off

**Output Status**

The Output status option lists the parameters for which an alarm or status condition will be raised, the severity and the operational state. The following figure shows the Output Status screen.

**Frame Output Status**

Severity	Description	Operational state
NoAlarm	BIP Signal Distribution Point 1	Off
NoAlarm	BIP Signal Distribution Point 2	Off
NoAlarm	BIP Signal Distribution Point 3	Off
NoAlarm	BIP Signal Distribution Point 4	Off
NoAlarm	BIP Visual Critical	On
NoAlarm	BIP Visual Major	Off
NoAlarm	BIP Visual Minor	On
NoAlarm	BIP Audible Critical	On
NoAlarm	BIP Audible Major	Off
NoAlarm	BIP Audible Minor	On
NoAlarm	BIP Alarm Cutoff LED	Off
NoAlarm	BIP Talk Battery Filter Card A LED	Off
NoAlarm	BIP Talk Battery Filter Card B LED	Off
NoAlarm	BIP Critical LED Bank	On

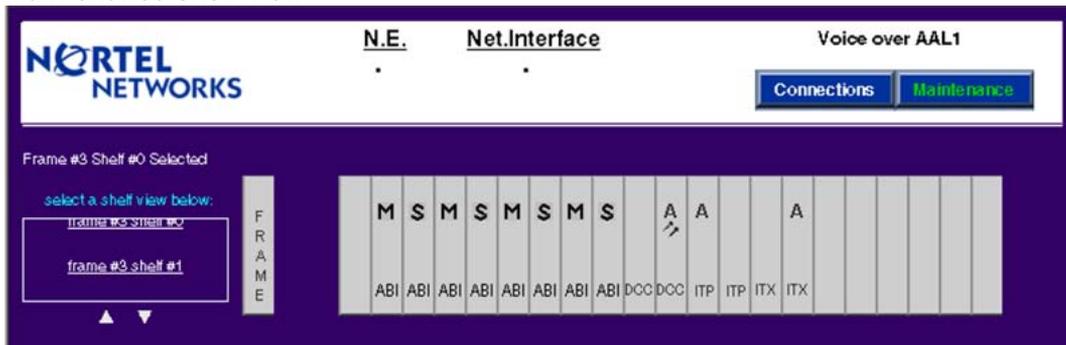
**Card Information**

The Card Information option identifies the Product Engineering Code (PEC) for the frame, the hardware revision, and any relevant software revision code.

**Shelf View**

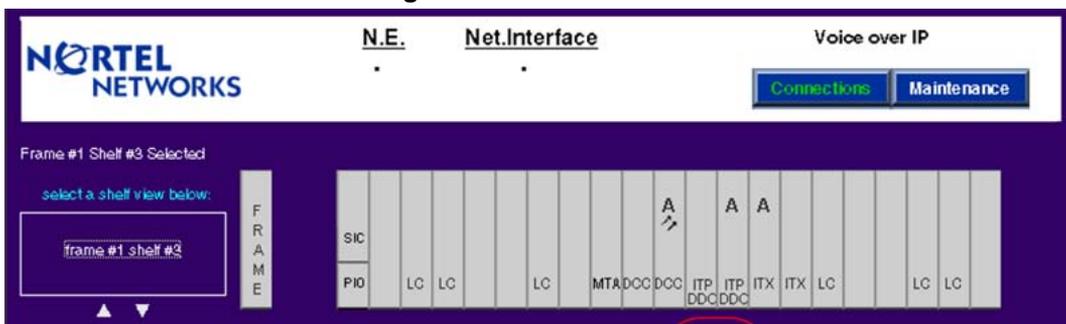
To select a shelf, move the cursor to a shelf location and click. After a selection has been made, the slots display the cards associated with the shelf selection.

**Maintenance shelf view**



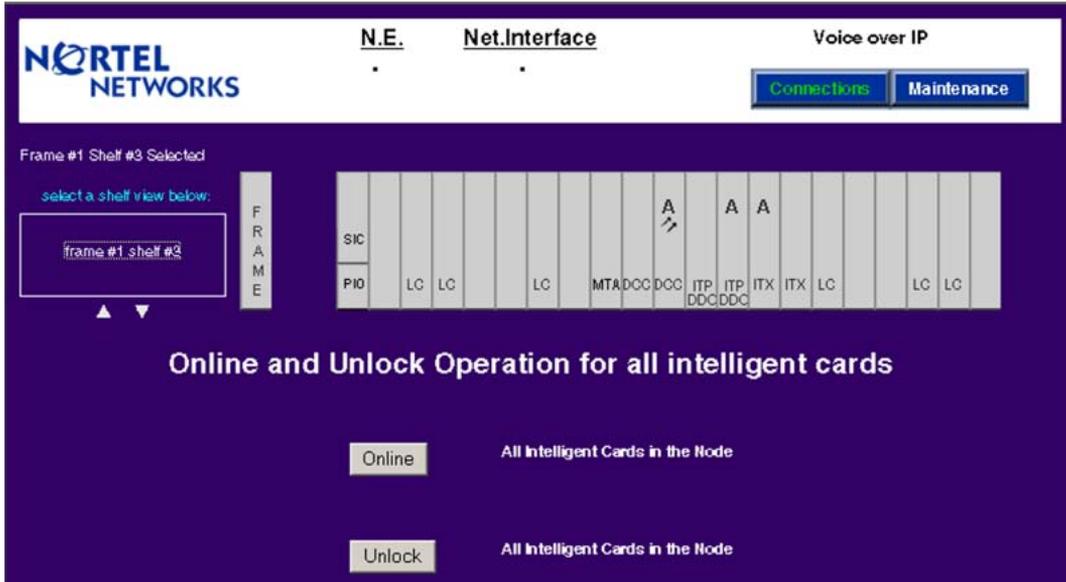
In an IP solution shelf view shown below, DDC appears below the ITP cards to indicate a daughter card is installed to support IP.

**Maintenance shelf view showing DDC under ITP card for IP solution**



When selecting the master shelf in a frame, the Online and Unlock screen appears. This screen provides buttons that enable the user to Online or Unlock all intelligent cards in the Node. These commands are typically used in an installation and commissioning scenario.

Maintenance shelf - Online and Unlock of intelligent cards in node



The shelf screen is dynamically updated as cards are added and de-provisioned. Cards are identified by the abbreviated card name. For example, DCC, DS1, ITX, and ITP. In addition to the card name, the screen also displays icons to indicate the following information regarding the card status:

- locked
- minor/major/critical (alarm)
- active carrier (active link for GigE)

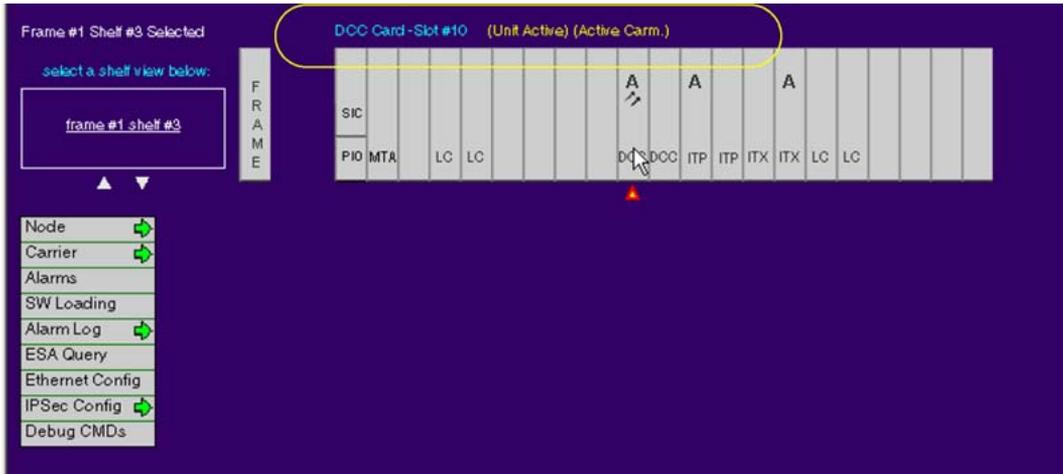
The following table lists the various icons seen on the cards which provide a high level view of the state of the card.

Icon	Description
	Card is locked
	Carrier is locked, only appears when the card is unlocked. For the DS1-IMA DCC card, this symbol indicates the IMA group is locked and only appears on the active IMA card. <b>Note 1:</b> The Carrier locked icon takes precedence over the Card locked icon. <b>Note 2:</b> For GigE, the carrier symbols map to link card symbols.

Icon	Description
	Critical alarm
	Major alarm
	Minor alarm
	Active card
	Active carrier
	Card or carrier is disabled
	Master ABI card
	Slave ABI card
	Carrier is enabled (red) LED
	Carrier is disabled (black) LED
	Card selected, appears below the card in the shelf view

To view the status and position of a card, in addition to the status icon, move the cursor over the card. Descriptive text appears above the card stating the card type, location, and status.

**Maintenance card status descriptive text**



To select a card, move the cursor on the card and click. Selecting a card produces a menu that displays the options available for that card. A separate set of maintenance menu options exists for each card type. A red triangle indicator appears underneath a selected card. The following figure shows the results of selecting a DCC card.

**Maintenance card selection menu**



The following table shows the cards and menu options available from the LCI maintenance screen.

#### Maintenance menu options

DS1	DCC (OC3)	DCC (DS1-IMA)	DCC (GigE)	ITP	ITX/ABI
Node <ul style="list-style-type: none"> <li>• Controls</li> <li>• Diags</li> <li>• Card Info</li> <li>• Sparing (not supported)</li> </ul>	Node <ul style="list-style-type: none"> <li>• Controls</li> <li>• Diags</li> <li>• Card Info</li> </ul>	Node <ul style="list-style-type: none"> <li>• Controls</li> <li>• Diags</li> <li>• Card Info</li> </ul>	Node <ul style="list-style-type: none"> <li>• Controls</li> <li>• Diags</li> <li>• Card Info</li> </ul>	Node <ul style="list-style-type: none"> <li>• Controls</li> <li>• Diags</li> <li>• Card Info</li> </ul>	Node <ul style="list-style-type: none"> <li>• Controls</li> <li>• Diags</li> <li>• Card Info</li> </ul>
Carrier <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> <li>• Status</li> <li>• Test</li> </ul>	Carrier <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> <li>• Status</li> <li>• Test</li> <li>• APS               <ul style="list-style-type: none"> <li>— Controls</li> <li>— Status</li> </ul> </li> </ul>	Carrier <ul style="list-style-type: none"> <li>• Provisioning               <ul style="list-style-type: none"> <li>— IMA Group/Links</li> <li>— DS1</li> </ul> </li> <li>• Controls               <ul style="list-style-type: none"> <li>— IMA Group/Links</li> <li>— DS1</li> </ul> </li> <li>• Status               <ul style="list-style-type: none"> <li>— IMA Group</li> <li>— IMA Link</li> <li>— DS1</li> </ul> </li> <li>• Test               <ul style="list-style-type: none"> <li>— IMA Group/Links</li> <li>— DS1</li> </ul> </li> </ul>	Link <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> <li>• Status</li> <li>• Test</li> <li>• Protection               <ul style="list-style-type: none"> <li>— Controls</li> <li>— Status</li> </ul> </li> </ul>		
Alarms	Alarms	Alarms	Alarms	Alarms	Alarms

DS1	DCC (OC3)	DCC (DS1-IMA)	DCC (GigE)	ITP	ITX/ABI
SW Loading	SW Loading	SW Loading	SW Loading	SW Loading	SW Loading
				Clock Sync <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> <li>• Status</li> <li>• Ref/Sig</li> </ul>	
	Alarm log <ul style="list-style-type: none"> <li>• Current</li> <li>• History</li> </ul>	Alarm log <ul style="list-style-type: none"> <li>• Current</li> <li>• History</li> </ul>	Alarm log <ul style="list-style-type: none"> <li>• Current</li> <li>• History</li> </ul>		
	ESA Query	ESA Query	ESA Query		
	Ethernet Config	Ethernet Config	Ethernet Config		
	IPsec Config <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> </ul>	IPsec Config <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> </ul>	IPsec Config <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> </ul>	IPsec Config <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> </ul>	IPsec Config (for ABI only) <ul style="list-style-type: none"> <li>• Provisioning</li> <li>• Controls</li> </ul>
	Debug CMDs	Debug CMDs	Debug CMDs		

This section includes information on the following topics:

- ["DS1 maintenance options" \(page 355\)](#)
- ["DCC Maintenance options" \(page 364\)](#)
- ["ITP maintenance options" \(page 410\)](#)
- ["ITX maintenance options" \(page 414\)](#)
- ["SIC maintenance options" \(page 414\)](#)
- ["ABI maintenance options" \(page 415\)](#)

## DS1 maintenance options

DS1 maintenance actions consist of the following options:

- node maintenance



The DS1 Node Control screen provides the following maintenance options:

### DS1 Node Control options

Control	Options
Configuration	<p>Online - allows the network to see and receive information from the card</p> <p>Offline - allows the network to see the card but not receive any information from the card</p> <p>Deprovision - used in conjunction with physically removing a card, removes the card from the network software. Removing a card without deprovisioning the card produces an alarm.</p> <p>Clear Config. Data - only used on the active DCC card. This action clears configuration data. When selecting this action, the LCI will instruct the user what actions to take.</p> <p>Force - used with the Clear Config. Data option</p>
Admin. State	<p>Lock (out of service)</p> <p>Unlock (return to service)</p> <p>Force (used with lock or unlock)</p>
Reload	<p>Restart Current</p> <p>Restart Flash Primary</p> <p>Restart Flash Backup</p>
Sparing	Not supported

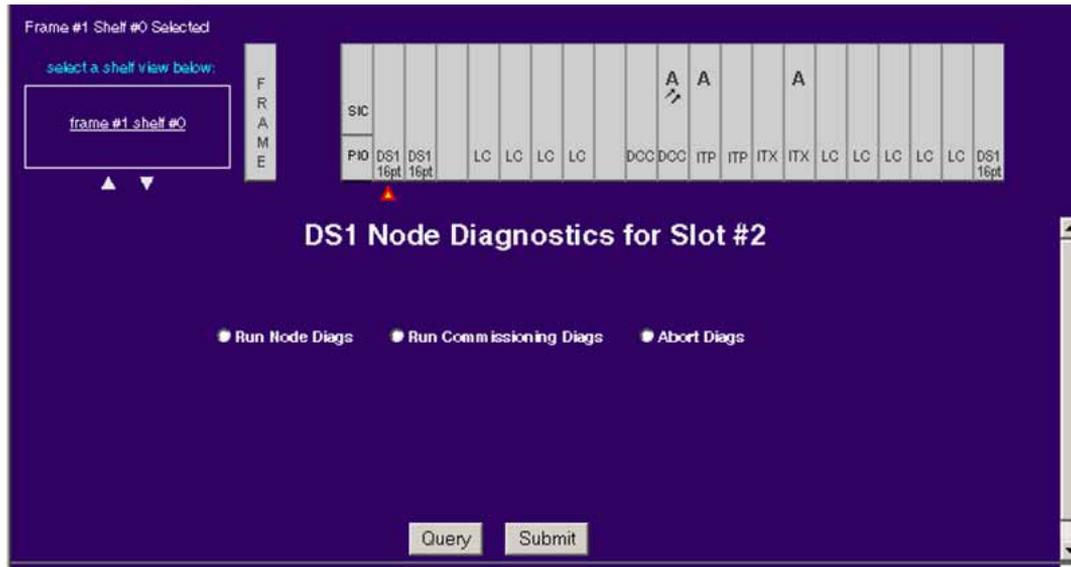
Each maintenance procedure requires selecting the appropriate action and clicking on the adjacent "submit" button.

The "Operation State" field shows the status of the card as either system enabled or system disabled. A red LED identifies the card's operational status. Status messages for submitted operations appear at the bottom of the screen.

### DS1 node diagnostics

The Node Diagnostics screen launches a request to run node level diagnostics for a selected card. The state of the card at the time of the request determines the diagnostic severity level. When accessed, the Node Diagnostics screen automatically performs an immediate query to determine if any diagnostics are currently running on the card. Only one set of diagnostics can run for a single card at a time. Multiple diagnostics, for multiple cards, can run simultaneously. The following figure shows a Node Control Diagnostics screen.

### DS1 Node Diagnostics screen



The Node Diagnostics screen offers three options:

- Run Node Diags
- Run Commissioning Diags
- Abort Node Diags

Each screen option becomes active through a Submit button. Status messages appear at the bottom of the screen during diagnostic testing.

The diagnostic results appear in a separate pop-up diagnostic response window when the tests have completed. The pop-up diagnostic response window appears with the first diagnostic result and continues to accumulate data for each card.

The diagnostic response window contains a print option button that allows printing the diagnostic results to either paper or to a file. The print option requires that the response window document be closed. Any responses received after the print option has been selected is captured in a later buffer.

The Abort Node Diags option allows operating company personnel to stop diagnostics while tests are underway.

### DS1 node card information

The Node Card Information screens displays the following hardware and software data for a selected card:

- product engineering code (PEC)

- hardware revision
- software revision
- restart load name
- restart flash load name

**DS1 carrier maintenance**

Carrier maintenance contains four separate options to manage the DS1 card at the DS0 carrier level.

- provisioning
- controls
- status
- test

To select an option, move the cursor to the option and click.

**DS1 carrier provisioning**

DS1 carrier provisioning displays the configuration data for the 16 ports of a selected DS1 card. The screen displays four ports with up and down arrows to navigate through all 16 ports. This screen is informational only and cannot modify the configurations. Modifications to DS1 carriers must be made through the MG 9000 Manager.

**DS1 Carrier Provisioning screen**

Frame #1 Shelf #0 Selected  
select a shelf view below:  
frame #1 shelf #0

SIC  
PI0 DS1 DS1 LC LC LC LC DCC DCC ITP ITP ITX ITX LC LC LC LC LC DS1  
16pt 16pt

**DS1 Carrier Provisioning Data for Slot #2**

Port	Line Type	Line Coding	Send Code	Loopback Config	Signal Mode	TX Clock Source	FDL Type	Line Length	Channelization
01	ESF	B&ZS	No Code	No Loop	None	thru Timing	ANSI	200m	Chann. Disabled
02	ESF	B&ZS	No Code	No Loop	None	thru Timing	ANSI	200m	Chann. Disabled
03	ESF	B&ZS	No Code	No Loop	None	thru Timing	ANSI	200m	Chann. Disabled
04	ESF	B&ZS	No Code	No Loop	None	thru Timing	ANSI	200m	Chann. Disabled

The following table describes the fields and options displayed on the DS1 carrier provisioning screen.

#### DS1 carrier provisioning screen options

Field	Options
Line Type	<ul style="list-style-type: none"> <li>• extended super frame (ESF)</li> <li>• super frame (SF)</li> <li>• user facility (UF)</li> </ul>
Line Coding	<ul style="list-style-type: none"> <li>• binary eight bit zero code (B8ZS)</li> <li>• alternate mark inversion (AMI)</li> <li>• zero code suppression (ZS)</li> </ul>
Send Code	<ul style="list-style-type: none"> <li>• no code</li> <li>• line code</li> <li>• payload</li> <li>• reset</li> <li>• quasi random signal</li> </ul>
Loopback Configuration	<ul style="list-style-type: none"> <li>• no loop</li> <li>• payload</li> <li>• line</li> <li>• inward terminal</li> <li>• dual</li> <li>• other</li> </ul>
Signal Mode	<ul style="list-style-type: none"> <li>• none</li> <li>• robbed bit</li> <li>• bit oriented</li> <li>• message oriented</li> <li>• other</li> </ul>
Transmit Clock Source	<ul style="list-style-type: none"> <li>• looping timing</li> <li>• local timing</li> <li>• thru timing</li> </ul>
Facilities Data Link (FDL) type	<ul style="list-style-type: none"> <li>• Att54016</li> <li>• none</li> <li>• ansiT1403</li> <li>• other</li> </ul>

Field	Options
Line Length	<ul style="list-style-type: none"> <li>655 meters</li> </ul>
Channelization	<ul style="list-style-type: none"> <li>channel disabled</li> <li>channel enabled DS0</li> <li>channel enabled DS1</li> </ul>

### DS1 carrier control

The DS1 carrier control screen defines administration (lock or unlock) and operation (online or offline) statuses for each carrier (port) on a DS1 card. In addition, all ports can be locked or set to online or offline by selecting the appropriate radio button and clicking on Submit All.

#### DS1 carrier control screen



Initial screen access automatically queries the administration and operation statuses for all 16 ports of the selected DS1 card. The Query button updates the carriers current status. DS1 carriers have a default status of locked and offline. Click on the Submit button to submit changes. Results are displayed in the message frame at the bottom of the screen.

The following table lists the DS1 carrier control option compatibilities. A carrier cannot have an unlock administration status with an offline operation status.

#### DS1 carrier control option compatibilities

Administration status	Operation status
lock	offline

Administration status	Operation status
lock	online
unlock	online

### DS1 carrier status

The DS1 carrier status screen detects error conditions relative to the individual ports of a selected card. Synchronous optical network (SONET) overhead adds end-to-end path level information to DS1 signals. Path level information contains SONET alarm defect status. A defect indicates a density of conditions, known as anomalies, that has reached a level where the ability to perform a function has been interrupted.

### DS1 carrier status screen

Frame #1 Shelf #0 Selected

select a shelf view below:

frame #1 shelf #0

FRAME

SIC	DS1 16pt	DS1 16pt	LC	LC	LC	LC	DCC DCC	DCC DCC	ITP	ITP	ITX	ITX	LC	LC	LC	LC	DS1 16pt

DS1 Carrier Status for Slot #2

Port#	LOF	LOS	AIS	RDI
Port 01	▲	▲	■	■
Port 02	▲	▲	■	■
Port 03	▲	▲	■	■
Port 04	▲	▲	■	■
Port 05	▲	▲	■	■
Port 06	▲	▲	■	■
Port 07	▲	▲	■	■
Port 08	▲	▲	■	■

Port#	LOF	LOS	AIS	RDI
Port 09	▲	▲	■	■
Port 10	▲	▲	■	■
Port 11	▲	▲	■	■
Port 12	▲	▲	■	■
Port 13	▲	▲	■	■
Port 14	▲	▲	■	■
Port 15	▲	▲	■	■
Port 16	▲	▲	■	■

The following table defines the defects displayed on the DS1 carrier status screen.

### DS1 carrier status defects

Defect	Explanation
AIS	Alarm indication signal. AIS generates to replace the normal traffic signal when it contains a defect condition. AIS prevents further downstream failures.
LOF	Loss of frame alignment. LOS occurs when an out of frame alignment (OOF) state exists for a specified time period.

Defect	Explanation
LOS	Loss of signal. LOS occurs when the synchronous signal (STS-N) level drops below a specified threshold.
RDI	Remote defect indication. A signal indicating the detection of a LOS, LOF, or AIS defect.

The DS1 carrier status screen automatically updates defect status every five seconds for all carriers. The following table shows the status indicators displayed for each defect.

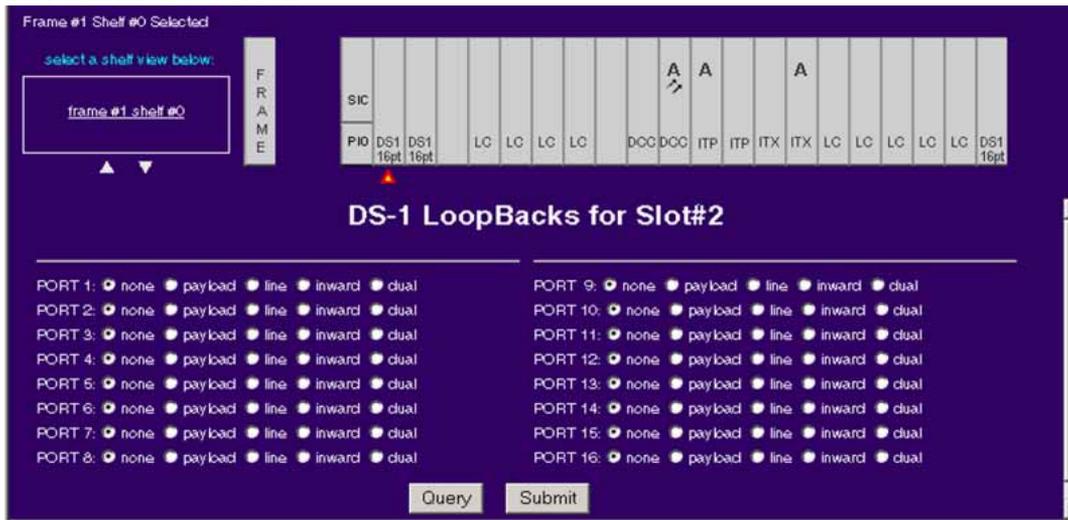
**DS1 carrier status indicators**

Symbol	Explanation
green square	A defect has not been detected for the carrier.
red triangle	A defect has been detected for the carrier.
empty square	The carrier is offline.

**DS1 carrier test**

The DS1 carrier test screen performs a set of loopback tests on the DS1 carrier links for a selected card. Loopback testing is a diagnostic method used to determine the integrity of a DS1 carrier. A transmit line loops back to a receive line either in the local device, along the line, or inside the remote device.

**DS1 carrier test screen**



The following table defines the loopback tests available from the DS1 test screen.

#### DS1 carrier loopback tests

Loopback Test	Explanation
Payload	The payload loopback loops the near end transmit to the near end receive. The loopback produces newly generated framing that may cause changes to the original received signal.
Line	The line loopback loops the received data back through the network. The signal returned toward the loopback source remains identical with no change in framing.
Inward	The inward loopback loops the near end transmit to the near end receive, but does not cause a change to framing.
Dual	The dual loopback performs the line and inward loopback tests at the same time.

Initially the DS1 carrier test screen displays the loopback testing status for all 16 ports on the selected DS1 card at the time of screen access. The Query button display updates the loopback status on demand. Each carrier is limited to a single loopback test at a time. Click on the Submit button to submit changes. Results are displayed in the message frame at the bottom of the screen.

#### DS1 alarms

The Alarms display screen is identical for all cards managed through the LCI. For a detailed description, see ["Alarm display" \(page 388\)](#).

#### DS1 software loading

The Software loading screen functionality is identical for all cards managed through the LCI. For a detailed description, see ["Software loading" \(page 388\)](#).

### DCC Maintenance options

DCC maintenance options consist of the following maintenance actions:

- Node maintenance
- carrier maintenance
- Alarm display
- Software loading
- alarm log
- ESA query
- Ethernet Config

- Debug CMDs

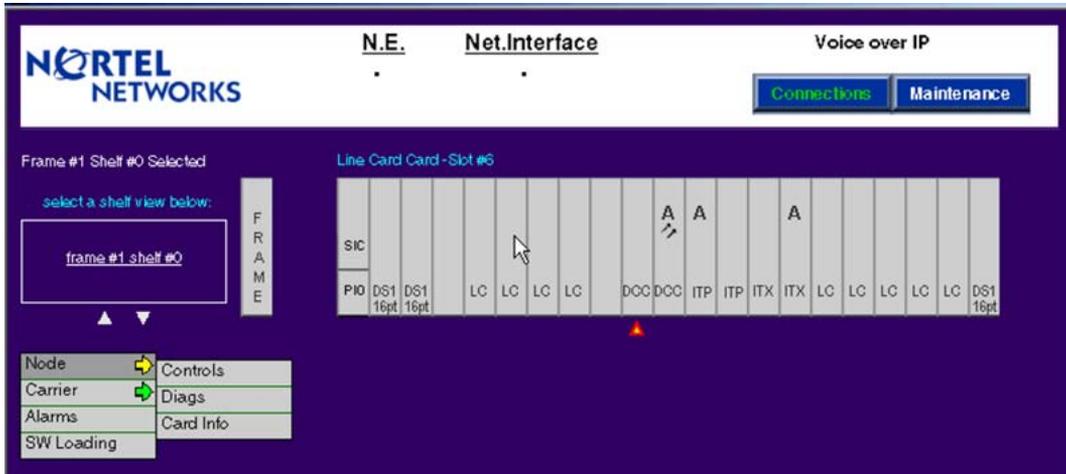
To select an option, move the cursor to the option and click.

**DCC node maintenance**

Node maintenance contains three separate options to manage the DCC card at the node level. The figure that follows shows the Node maintenance levels

- controls
- diagnostics
- card information

**DCC Node Maintenance levels**



**DCC node controls**

All node control screens, for all cards, provide configuration, administrative and restart options. The DCC Node Control screen provides the following maintenance options:

**DCC Node Control options**

Control	Options
Configuration	<ul style="list-style-type: none"> <li>Online</li> <li>Offline</li> <li>Deprovision</li> <li>Clear Config. Data</li> <li>Force</li> </ul>

Control	Options
Admin. State	Lock (out of service) Unlock (return to service) Force (used with lock or unlock)
Reload	Restart Current Restart Flash Primary Restart Flash Backup
Switch of Activity	Warm Switch of Activity Force

Click in the appropriate box or on the appropriate radio button to select the desired option then click on Submit adjacent to the option to begin the action.

The following figure shows the DCC Node Controls screen.

#### DCC Node Controls screen

The screenshot displays the DCC Node Controls interface for Slot #10. At the top, it shows the Nortel Networks logo and navigation options for 'Connections' and 'Maintenance'. The main area features a rack diagram with Slot #10 selected. Below the diagram, the 'DCC Node Controls for Slot #10' section includes several control groups:

- Operation State:** Enable (selected) / Disable
- Configuration Status:** Online (selected), Offline, Deprovision, Clear Config.Data, and a Force? checkbox.
- Admin State:** Lock (selected), Unlock, and a Force? checkbox.
- Reload:** Restart Current (selected), Restart Flash Primary, and Restart Flash Backup.
- Warm Switch of Activity:** Warm Switch of Activity (selected) and a Force? checkbox.

At the bottom, the status is shown as 'Procedural Status: Normal' and 'Availability Status: Normal', with a 'Query' button.

#### DCC node diagnostics

The Node Diagnostics screen functionality is identical for all cards managed through the LCI. For a detailed description, see "[DS1 node diagnostics](#)" (page 357) in the DS1 Maintenance section.

**DCC node card information**

The Node Card Information screen functionality is identical for all cards managed through the LCI. For a detailed description, see the DS1 Maintenance section.

**DCC carrier maintenance**

Carrier maintenance contains five separate options to manage the DCC card at the OC3 carrier level.

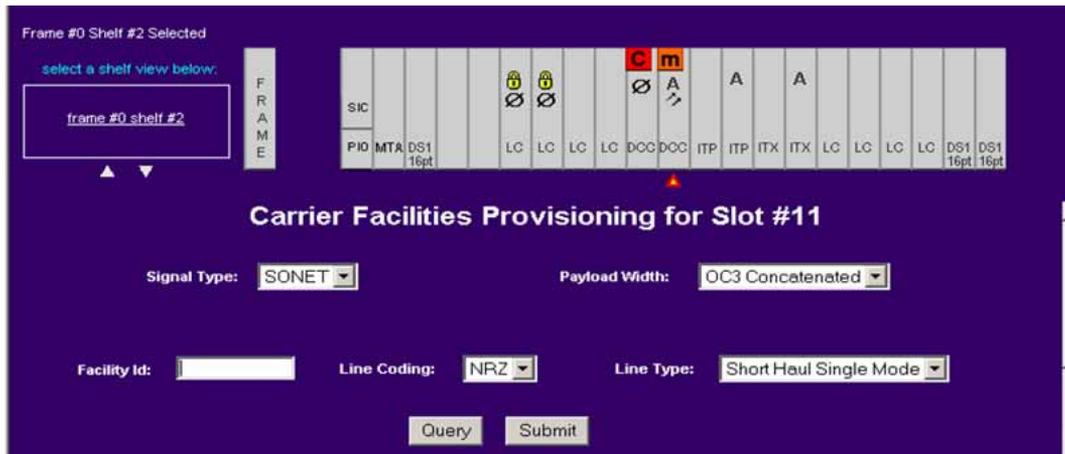
- provisioning
- controls
- status
- test
- APS

To select an option, move the cursor to the option and click.

**DCC provisioning**

DCC provisioning identifies OC3 carrier circuit characteristics maintained by the DCC card. Screen access automatically generates a query to the DCC. The Query button updates the carriers current status. The Submit button saves provisioning data. The carrier must be locked before attempting to save any provisioning data.

**DCC OC3 carrier provisioning screen**



The following table lists the OC3 carrier definition options available on the MG 9000.

#### DCC OC3 carrier provisioning definitions

Field	Options	Explanation
Signal Type	SONET SDH	Select the signaling type.
Payload Width	STM1 OC3 Concatenated OC3	STM1 is the default payload for SDH Non-channelized OC3 carrier Channelized OC3 carrier. When selected, this option enables the second section permitting selection of the payload and destination of the path
Line Coding	NRZ	Non Return to Zero (NRZ) line coding used for optical Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) signals.
Facility Id	Alphanumeric text string of up to 32 characters	Circuit identifier for the node's carrier
Line Type	Short haul single mode	The type of optical transport network.
Payload	DS3clearChannel	DS3 clearChannel (specific to channelized OC3, Payload width is OC3)
Destination	Network None	Identifies the active carrier paths when Network is selected (specific to channelized OC3, Payload width is OC3).

#### DCC carrier controls

The DCC OC3 carrier control screen defines administration (lock or unlock), configuration (online or offline) and laser statuses for the DCC card.

SONET automatic protection switching (APS) configures a pair of SONET lines for line redundancy so that the interface hardware automatically switches from a working line to a protection line, or vice versa within a defined period of time after a line failure.

**DCC OC3 carrier control screen for concatenated or SDH**



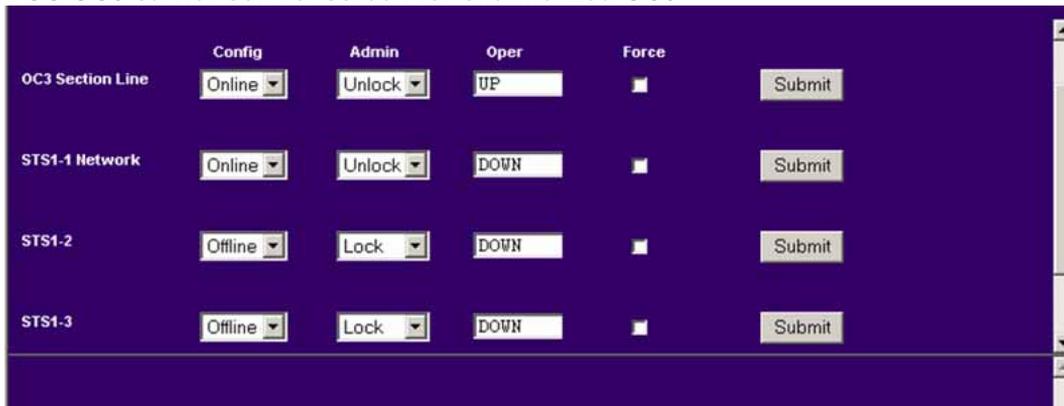
The Carrier Control screen provides the following maintenance options for a carrier in SDH or OC3 concatenated mode:

**DCC OC3c Carrier Control screen options**

Control	Option	Explanation
Laser	On	The laser option is an informational field indicating the OC3 carrier is on (in-service) or off (system busy).
	Off	
Administration	Unlock (return to service)	The administrative option to lock or unlock a card either places a card out of service (lock) or returns the card to service (unlock). The lock option can be used in conjunction with the "force" option.
	Lock (out of service)	
	Force (used with lock)	
Configuration	Online	The online option allows the network to see and receive information from the OC3 carrier.
	Offline	The offline option completely disables the carrier.

When the payload width of OC3 is selected, the OC3 carrier control screen appears as follow. This screen allows the user to select the payload and destination for the carrier path. This activity is performed during initial installation/commissioning activities.

**DCC OC3 carrier control screen for channelized OC3**



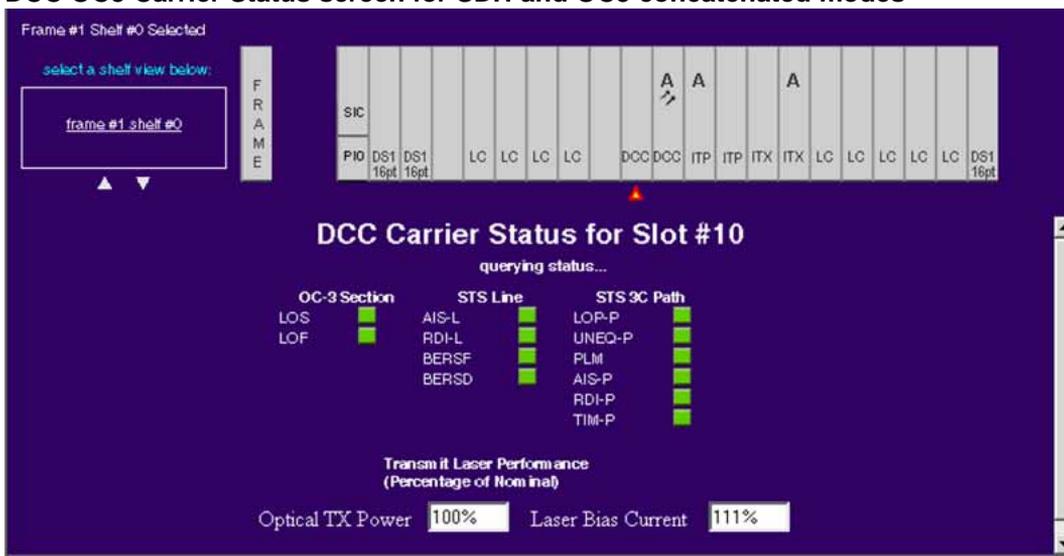
**DCC OC3 carrier status**

The DCC OC3 carrier screen displays the current carrier alarm status for the selected OC3 board. The following are the symbols that are displayed and their meaning:

- A green square indicates that no faults exist.
- A red triangle indicates an alarm condition exists.
- A blank display indicates the fault information could not be retrieved.

The following figure shows the DCC OC3 Carrier Status screen.

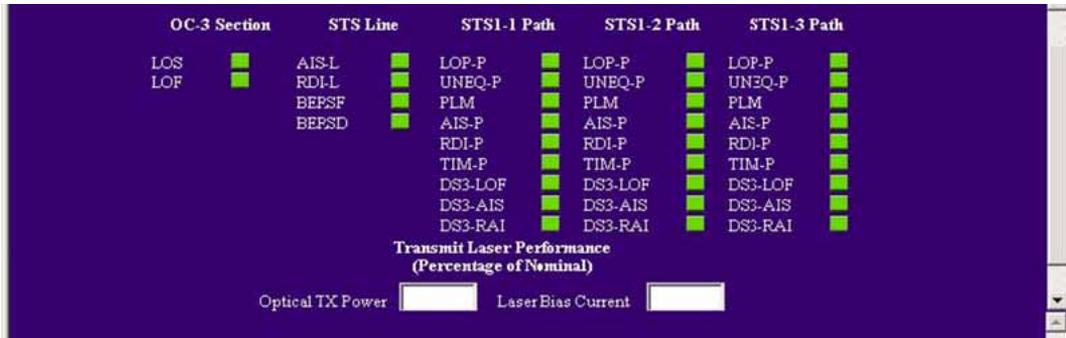
**DCC OC3 Carrier Status screen for SDH and OC3 concatenated modes**



Access to the screen automatically sends a query to the DCC card. After the initial query, the LCI automatically sends additional queries every 5 seconds. A message indicating "querying status..." displays on the screen whenever a query command has been issued.

The following figure shows the DCC OC3 Carrier Status screen for channelized OC3.

**DCC OC3 Carrier Status screen for OC3 channelized mode with DS3 payload**



The DCC carrier status screen contains the following maintenance options:

**DCC carrier status parameters**

Column	Alarm	Definition
OC3 Section	loss of signal (LOS)	LOS is raised when the synchronous signal (STS-N) level drops below a defined threshold. LOS causes could include a cut cable, excessive attenuation of the signal, or equipment fault.
	loss of frame (LOF) alignment	LOF state occurs when the OOF state exists for a specified time in milliseconds. LOF state clears when an in-frame condition exists continuously for a specified time in milliseconds.
STS Line	line alarm indication signal (AIS-L)	AIS-L is generated by section terminating equipment (STE) upon the detection of a loss of signal or loss of frame defect, or an equipment failure.
	line remote defect indication (RDI-L)	An RDI-L signal is returned to the transmitting line terminating equipment (LTE) upon detection of a loss of signal, loss of frame, or AIS-L defect. RDI-L was previously known as line FERF.
	bit error ratio signal fail (BERSF)	Bit error ratio is the ratio of the number of bit errors to the total number of bits transmitted in a given time interval. BERSF includes receiver failure and excessive BER.
	bit error ratio signal degradation (BERSD)	BERSD includes receiver degrade and moderate BER.

Column	Alarm	Definition
STS 3C Path	path loss of pointer (LOP-P)	An LOP-P defect is declared when either a valid pointer is not detected in eight consecutive frames, or when eight consecutive frames are detected with the New Data Flag set to "1001" without a valid concatenation indicator.
	path unequipped (UNEQ-P)	UNEQ-P occurs when a path connection is not provisioned (idle) the DCC signals the state by transmitting a Path signal label to indicate an unequipped path.
	payload label mismatch (PLM)	PLM indicates that a path is not correctly provisioned. A received signal label is considered mismatched if it does not equal either the locally provisioned value or the "equal equipped non-specific" value. Only in-service provisioned PTE can detect mismatched signal labels.
	path alarm indication signal (AIS-P)	AIS-P is defined as all "1s" in bytes H1-3 and the entire STS SPE.
	RDI-P	a signal returned to the transmitting STS path terminating equipment (PTE) upon detection of certain defects on the incoming path
	TIM-P	a mismatch has occurred between the expected and received path trace message. This applies to SDH only, though it is displayed on the DCC Carrier Status screen.
When a channelized OC3 is selected, the following alarm information appears for each STS-1 path in addition to the alarms seen for the STS-3C Path listed above.		
	DS3-LOF	Loss of frame on the DS3 payload
	DS3-AIS	Alarm indication signal for the DS3 payload
	DS3-RAI	Remote alarm indication for the DS3 payload

The Transmit Laser Performance portion of the OC3 Carrier Status screen provides two fields that report optical transmit power and laser bias current. These two values provide a view of the health of the transmit laser of the OC3 card. An explanation of the values and their interpretation is provided in "OC3 laser performance" in *MG 9000 Performance Management*, NN10140-711.

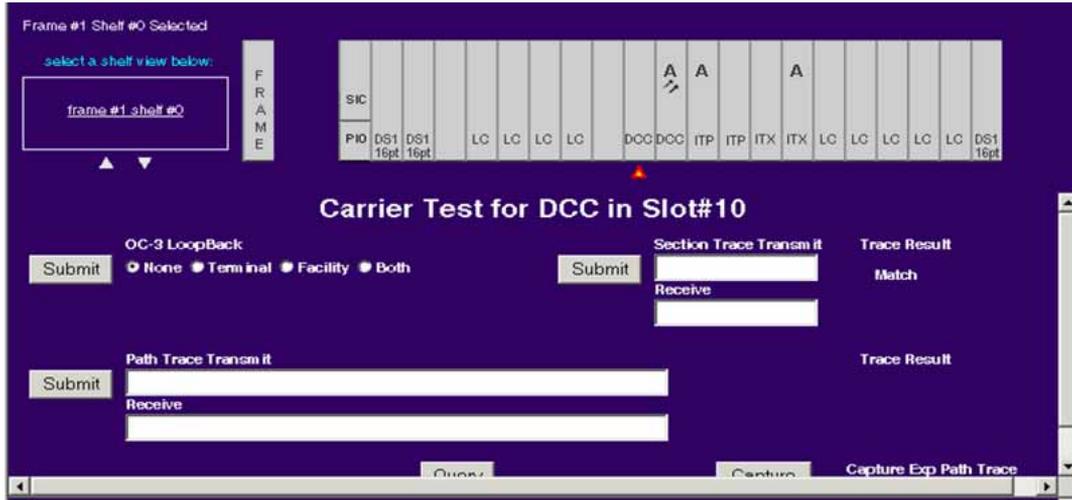
### DCC carrier test

The DCC carrier test screen sets and queries OC3 Loopbacks and submits test strings for the Section and Path trace tests. The LCI automatically sends a query to the OC3 when the screen is accessed. A Query button

also provides an on-demand query for updates. A Section or Path trace test produces an automatic query transmitted to the Section and Path trace data every 10 seconds. The trace tests identify locations of communication loss.

**Note:** The carrier must be locked before placing it in loopback.

**DCC carrier test**



The DCC carrier test screen contains the following maintenance options:

**DCC Carrier tests and options**

Test	Option	Explanation
OC3 LoopBack	none	clears a loopback test
	terminal	The signal from the transmit interface is looped back by connecting it to the receive interface.
	facility	The signal from the receive interface is looped back by connecting it to the transmit interface.
	both	Perform a terminal and a facility loopback test.
Section Trace	transmit	A character string up to 14 characters. A value of 0 clears the trace.
	receive	Not available.
Path Trace	transmit	A character string up to 62 characters. A value of 0 clears the trace. For SDH only, supports a 15 character string.

Test	Option	Explanation
	receive	Not available.
Capture Exp. Path Trace	none	Only used for SDH to clear Trace Identifier Mismatch - Path (TIM-P) alarms. The Path Trace Message (J1) received in the incoming STM-1 stream is compared against a 'saved' 16 byte string. If the two are different, a TIM-P alarm is raised. To clear the alarm, the incoming Path Trace Message (J1) is 'saved' so to create a match, clearing the alarm. This is normally performed at commissioning when the laser is first turned on.

### DCC APS controls

The Automatic protection switching (APS) Group Controls screen contains the options listed in the following table.

#### APS Group Controls

Option	Explanation
Protection channel	Select the protection channel to apply changes to the APS group.
Working channel	Select the working channel to apply changes to the APS group.
Clear lockout	Clears the APS lockout if the user has locked the carrier's ability to APS (the carrier subsystem will return to being able to switch as needed).
Lockout of protection	Disables Manual/Force Protection Switching features by locking out the protected (spare) carrier.
Manual Switch Protected to Working	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.
Forced Switch Protected to Working	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.

### DCC APS group status

The APS group status information is provided in this screen. The APS Group Status is shown in the following figure.

**APS Group Status**

Frame #1 Shelf #0 Selected  
select a shelf view below:  
frame #1 shelf #0

**APS Group Status**

APS Group Name	Group Status	SdBer Threshold	SfBer Threshold
APSGroup1	Enabled	10 <sup>-5</sup>	10 <sup>-3</sup>

APS Group Name	Chnl	Chnl Status				Sd	Sf	Ps	Last Prot Switch	Last Switch Cmd
		Sd	Sf	Lo	Sw					
APSGroup1	P	--	--	--	--	0	0	0	0	NoCmd
APSGroup1	W	--	--	--	--	0	0	0	0	NoCmd

The screen provides the following information for the APS group.

**APS Group status information**

Field	Description
APS Group Name	Name of the APS group
Group Status	Status of the APS group, enabled or disabled
Sd BER Threshold	Signal degrade (Sd) bit error rate (BER)
Sf BER Threshold	Signal fail (Sf) bit error rate
Chnl	Channel, protected (P) or working (W)
Chnl Status	Value of the following for each channel: <ul style="list-style-type: none"> <li>Sd - Signal Degrade condition exists</li> <li>Sf - Signal Fail condition exists</li> <li>Lo - lockout of Protection Switching</li> <li>Sw - Protection Switched</li> </ul>
Sd	Signal degrade count
Sf	Signal fail count
Ps	Protection switch count
Last Prot Switch	Time of last protection switch
Last Switch Cmd	The last command used to initiate a protection switch.

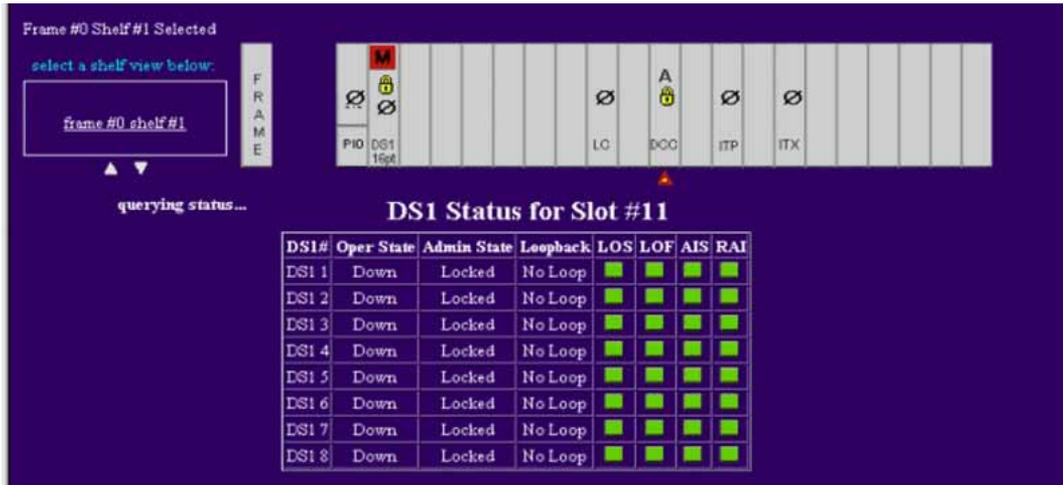
**DS-1 IMA**

When a DS1-IMA DCC card is installed, the DS1 IMA links can be managed using the LCI screens that are provided in this section. The DS1-IMA screens are accessed from the DCC Carrier Maintenance menu.

### DS1-IMA DS1 status

The DS1 Status screen identifies the status of DS1 IMA links and any error conditions that may exist. Refer to "DS1 carrier status" (page 362) for an explanation of the alarm status defects and indicators. The DS1 Status screen is shown in the following figure.

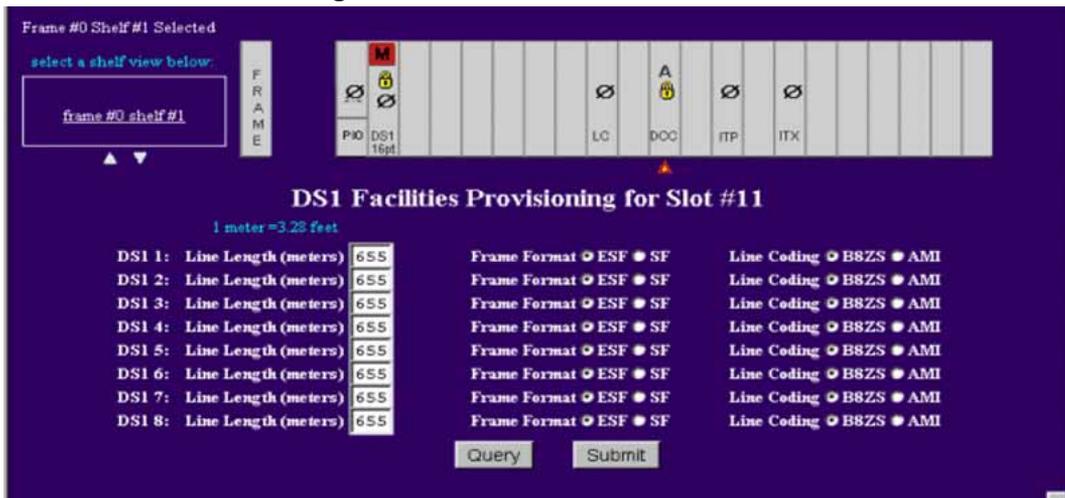
#### DS1 Status



### DS1-IMA DS1 facilities provisioning

Allows the line length, frame format and line coding to be provisioned. The following figure shows the DS1 Facilities Provisioning screen.

#### DS1 Facilities Provisioning



### DS1-IMA DS1 controls

The DS1 Controls screen allows the DS1-IMA links to set the state and status of the link, as shown in the following figure.

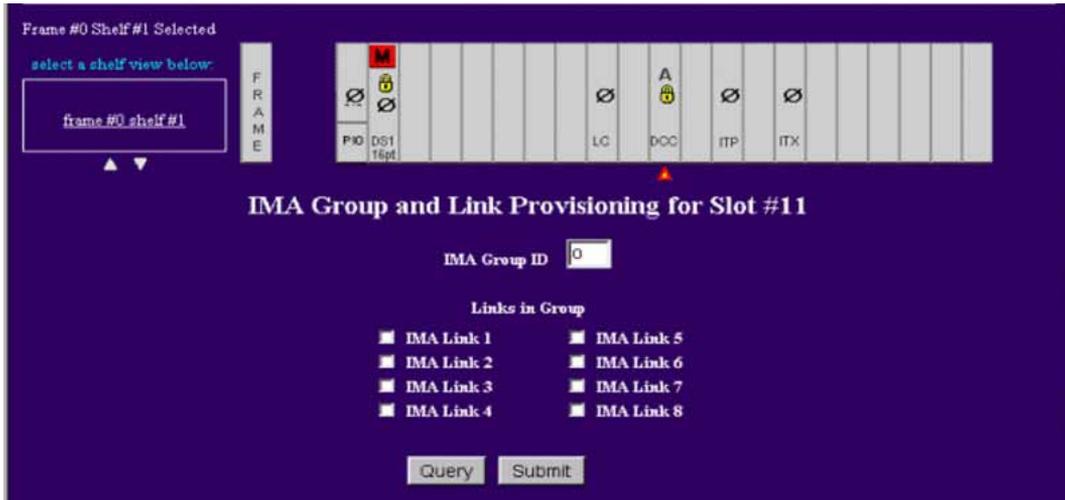
**DS1-IMA Controls**



**DS1-IMA group and link provisioning**

The DS1-IMA Group and Link Provisioning screen allows the user to provision the links that will be a part of an IMA group, as shown in the following figure.

**DS1-IMA Group and Link Provisioning**



**DS1-IMA link status**

The DS1-IMA Link Status screen reports the status of each link, failure conditions, and whether the link is in a group. The following figure shows this screen.

### IMA Link Status

Frame #0 Shelf #1 Selected  
select a shelf view below:  
frame #0 shelf #1

DS1IMA Card -Slot #11 (Card Locked) (Unit Active)

querying status...

#### IMA Link Status for Slot #11

IMA Link#	Oper State	Admin State	NE Transmit	NE Receive	FE Transmit	FE Receive	NE Failure Status	FE Failure Status
Link 01	Down	Locked	Not in Group	Not in Group	Not in Group	Not in Group	No Failure	No Failure
Link 02	Down	Locked	Not in Group	Not in Group	Not in Group	Not in Group	No Failure	No Failure
Link 03	Down	Locked	Not in Group	Not in Group	Not in Group	Not in Group	No Failure	No Failure
Link 04	Down	Locked	Not in Group	Not in Group	Not in Group	Not in Group	No Failure	No Failure
Link 05	Down	Locked	Not in Group	Not in Group	Not in Group	Not in Group	No Failure	No Failure
Link 06	Down	Locked	Not in Group	Not in Group	Not in Group	Not in Group	No Failure	No Failure
Link 07	Down	Locked	Not in Group	Not in Group	Not in Group	Not in Group	No Failure	No Failure
Link 08	Down	Locked	Not in Group	Not in Group	Not in Group	Not in Group	No Failure	No Failure

### DS1-IMA Group/Link test

The DS1-IMA Group/Link Test screen provides a test tool for testing an individual link and selecting the test pattern to be used when conducting the test. The test results are provided at the bottom of the screen.

### DS1-IMA Group/Link Test

Frame #0 Shelf #1 Selected  
select a shelf view below:  
frame #0 shelf #1

IMA Group/Link Test for DS1IMA in Slot#11

Test TX Link  Group Test Pattern

Test Pattern Control  Operating  Disabled

Link 1 Rx	Link 2 Rx	Link 3 Rx	Link 4 Rx	Link 5 Rx	Link 6 Rx	Link 7 Rx	Link 8 Rx
0	0	0	0	0	0	0	0
Pass							

Query Submit

### DS1-IMA group status

The DS1-IMA Group status screen reports the operational state, administrative state, near end and far end states, and failure status of the IMA group. The following figure shows the DS1-IMA Group Status screen.

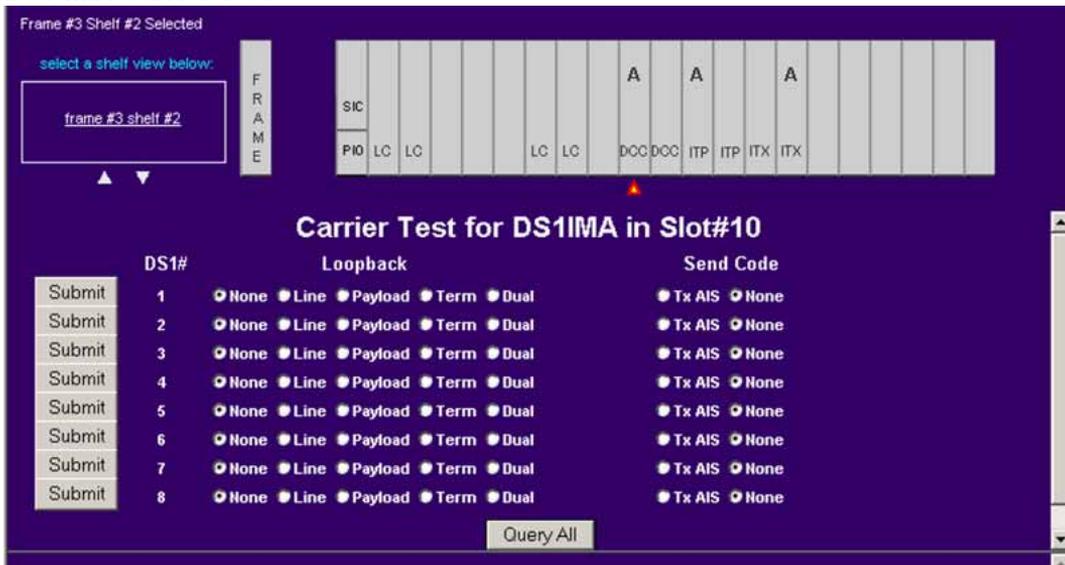
**DS1-IMA Group Status**



**DS1-IMA carrier test**

The DS1-IMA Carrier Test screen allows the user to select the link for a loopback test, the test type, and the send code. Click on Submit to begin the test on the selected link. The following figure shows the IMA Carrier Test screen.

**DS1-IMA Carrier Test**



**DS1-IMA Group/Link controls**

The DS1-IMA Group/Link Controls screen allows the user to enable or disable individual links or enable or disable the entire IMA group as shown in the following figure.

**Note:** Use of the Force option to disable the group is disruptive to traffic on the link.

### DS1-IMA Group/Link Controls



### Gigabit ethernet

GigE maintenance actions consist of the following options:

#### GigE provisioning

The link provisioning data submitted from the LCI are passed on to Link Maintenance. Data in the GigE network view element can also be queried using this screen. The following figure shows the GigE Provisioning screen.

### GigE Provisioning



The link parameters can be provisioned for only one link. The values are automatically apply to the other link.

### GigE Provisioning

Field	Option	Explanation
Link Type	PrimaryNI	Network Interface link. One per card.
TxRfi	Enable, Disable	If enabled, RFI will be sent for any major or critical alarm on the link.
RxRfi	Enable, Disable	If selected, receiving an RFI will result in a sparing activity.
MTU size	1600, 1900	This is a read-only field that displays the maximum transmittable unit
AutoNeg	Enable, Disable	Enable or disable auto-negotiation on a link.
Bandwidth (bits)		Identifies the bandwidth of the GigE link in bits per second. The default value is 1,000,000,000 which is the maximum value. This value may be changed to limit the output frame rate on the GigE link.
Local Adv.	Fdx, No-Pause	Full Duplex - No Pause is the only value currently supported.
Remote Adv.		This is a bit field that provides the advertised GigE link capability of the far end. The LCI gives a description of each bit when the field is clicked.

Field	Option	Explanation
Capability (bits)		This is a bit field that provides the GigE link capability of the MG 9000. The LCI gives a description of each bit when the field is clicked. This value can be compared with the Remote Advertised mentioned above.
AutoNeg Config	In Progress, Complete, Disabled	Gives the auto negotiation status of link.
Request AutoNeg button		To request auto-negotiation on link. AutoNeg should be enabled, and link should be on line and locked for auto-negotiation to work.

### GigE controls

The GigE Control screen defines administration (lock or unlock), configuration (online or offline) and laser statuses for the GigE card. When any of the four links are selected, the Admin and Configuration controls for that link will be displayed. However, only one link (any one of the available four) can be online and unlocked for SN08. The loopback can also be configured on the link and query the current status of the link from this screen.

The following figure shows the GigE Control screen.

**GigE control screen**



The GigE Control screen provides the following maintenance options for a GigE link.

**GigE Control screen options**

Control	Option	Explanation
Laser	On	The laser option is an informational field indicating the GigE link is on (in-service) or off (system busy).
	Off	
Administration	Unlock (return to service)	The administrative option to lock or unlock a card either places a card out of service (lock) or returns the card to service (unlock). The lock option can be used in conjunction with the "force" option.
	Lock (out of service)	
	Force (used with lock)	
Configuration	Online	The online option allows the network to see and receive information from the GigE link.
	Offline	The offline option completely disables the carrier.

**GigE status**

When Link->Status is selected, the GigE Status screen displays the current link alarm status for the selected GigE Card. The following are the symbols that are displayed and their meaning:

- A green square indicates that no faults exist.

- A red triangle indicates an alarm condition exists.
- A blank display indicates the fault information could not be retrieved.

The following figure shows the GigE Status screen.

**GigE Status screen**



Access to the screen automatically sends a query to the GigE card. After the initial query, the LCI automatically sends additional queries every 5 seconds. A message indicating "querying status..." displays on the screen whenever a query command has been issued.

The GigE Status screen contains the following maintenance options:

**GigE Status parameters**

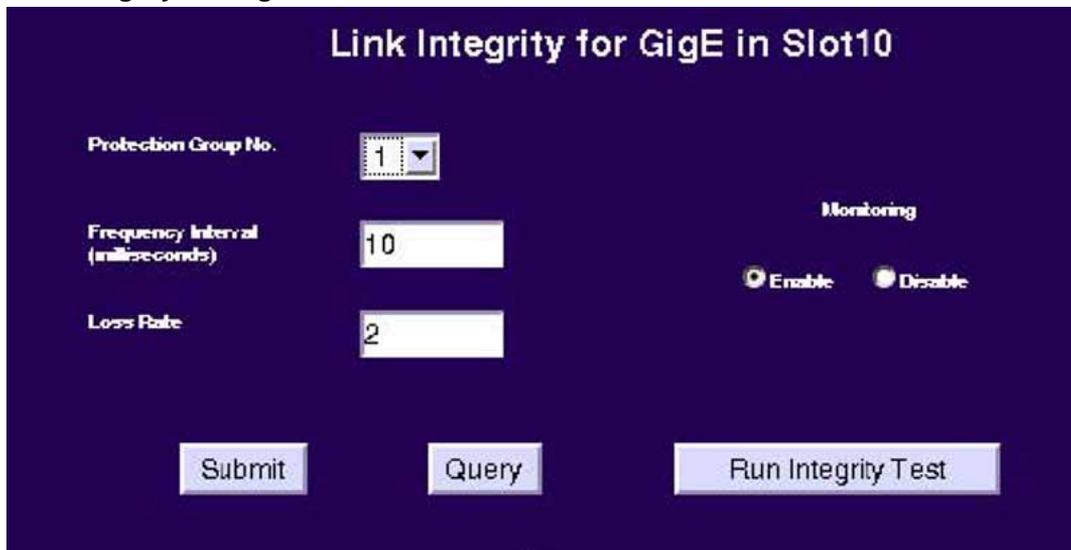
Alarm	Definition
Oper Stat	Operational status of link
Admin State	Admin status of link
Loopback	Loopback status
Loss of signal (LOS)	Loss of signal on link
RFI	Remote fault indication
TXF	Indicates transmission failure on link
TEM	Temperature high
POW	Voltage high
RxSD	Receive frames signal degraded
RxEER	Link receiving frames with excessive error ratio
TBC	Transmit bias current high
OPT	Transmit power high

Alarm	Definition
OPR	Receive power high
LINT	Link integrity test alarm
LKINT	Network failure alarm
AutoNeg	Indicates Auto-Negotiation status on link

**GigE link integrity test**

The GigE Link Integrity test screen. The user must first select the Protection Group from the pull down. The LCI automatically sends a query to the GigE when the screen is accessed. A Query button also provides an on-demand query for updates.

**Link Integrity for GigE**



The GigE Link Integrity test screen contains the following maintenance options:

**GigE Link Integrity tests and options**

Control	Option	Explanation
Run Integrity Test	N/A	Click on Run Integrity Test button. Results are displayed in the bottom pane.
Frequency Interval	N/A	Frequency of transmitting the heartbeat ping packet for the test. Should be greater than or equal to 10 ms.
Loss Rate	N/A	Loss rate for the test. Should be greater than or equal to one.
Monitoring	Enable, Disable	To enable or disable link monitoring.

Control	Option	Explanation
Query button	N/A	Displays the values previously set for Frequency, Loss Rate, and Monitoring. This does not display the results of the OOS Test.
Submit button	N/A	To set new values for Frequency Interval, Loss Rate, and Monitoring status.

### GigE protection control

Although each GigE DCC card supports up to four GigE ports, in SN08 only one port per card can be configured. There will be a one-to-one GigE link redundancy. In SN08, split mode protection scheme is not supported. Therefore, all failures result in a SWACT of the card to access the other fiber. This screen provides the interface for the LCI to set up the GigE link protection groups.

The GigE Link Protection Control screen contains the options listed in the following table.

### GigE Protection Controls

Field	Explanation
Group No	Group number of the protection group.
Group Type	Currently, only one-to-one protection is supported.
Working Link	The preferred link.
Protection Link	The link to switch to in case the working link fails.
Link Reversion	When reversion is enabled, the working link is always preferred and the system will SWACT to it when it is available.
Wait to Restore	If link reversion is on, this is the time period to wait after the working link becomes available, before reverting to it.
<b>Control</b>	
Create button	Used to create a protection group.
Modify button	Used to modify link reversion and wait to restore parameters for protection group.
Delete button	Used to delete a protection group with no associated link.
Associate button	Used to associate working and protection links to a group.
Disassociate button	Used to disassociate the links from a group.
Query button	Used to query the current link protection settings.

The following figure shows the GigE Link Protection Control screen.

**GigE Link Protection Control screen**



**GigE link protection status**

The GigE Link Protection Status information is provided in this screen (see the following figure).

**GigE Link Protection Status**



The screen provides the following information for the GigE.

**GigE Link Protection Status information**

Field	Description
Protection Group No	Group number of the protection groups.
Working Link	Slot and port number of the working (preferred) link.

Field	Description
Protection Link	Slot and port number of the protected (non-preferred) link.
Timestamp of the last protection switch	When the last protection switch occurred.
Prot. Status	Status of the protection group (which link is active).

### Alarm display

The Alarms screen displays the active alarms for a selected card. No maintenance activities can be performed at this screen.

#### Alarm information



The screen provides the following information for each alarm:

#### Alarm screen fields

Field	Explanation
Severity	The alarm severity as one of the following: <ul style="list-style-type: none"> <li>• Critical</li> <li>• Major</li> <li>• Minor</li> </ul>
Description	A description of the alarm type.
Time	The time that the alarm first occurred.

### Software loading

This screen loads current software to the selected board or queries and displays the current load status. To perform software loading using the LCI, the following conditions apply:

- the laptop PC must be connected directly to the Active DCC card
- 10-base addresses must be used, meaning the laptop must address the DCC card directly

- an FTP Daemon must be running on the laptop PC to act as the FTP server
- the software load file must be present locally on the PC
- the sFTP Daemon must be configured to accept requests from the following userid and password:
  - userid - admin
  - password - n0rtel
- if IPSec has been configured on the MG 9000, before loading, the IPSec policy must be set to On to allow a bypass during loading. After all loading is complete, the IPSec policy must be set to Off.

**Note:** Regardless of which software loading screen is used to toggle the IPSec policy, once it has been set on one screen the policy has been set for all card software loading screens. There is only one LCI control for software loading.

When a load request is submitted, a message appears near the bottom of the screen indicating that the request was successful. The loading process continues in the background after the message appears allowing access to other LCI screens. When the loading process has completed, a new window opens to provide notification that the load has finished. Query Load Information fields display the load information at the time of the query request. The query does not automatically update.

### Software Loading

**DCC Software Loading for Slot #10**

**Required Loading Information**

- IP Address to FTP Server: 10.0.0.2
- Load Name:

Browse... Load Clear Query

**Query Loading Information**

- Load Status: N/A
- Current Load Name: N/A
- Flash Primary Load Name: N/A
- Flash Backup Load Name: N/A

IPSec Policy to allow local Software download:  On  Off

Submit Query

The Clear button clears the IP address and Load Name text boxes.

The Software Loading screen provides the following information:

### Software Loading screen options

Task Heading	Field Option	Explanation
Required loading information	IP Address to FTP Server	Enter the IP address of the location storing the software load designated for download.
	Load Name	Enter the full path name of the load designated for download.
	IPSec Policy to allow local Software download	Values are On and Off. This implements an IPSec policy for 10.0.0.2. However, this setting is not associated with any existing fields or buttons on the software loading screen.
Query Loading Information	Load Status	Indicates whether the current load has been completed, or is still in progress
	Current Load Name	Identifies the current load in the DCC card.
	Flash Primary Load Name	Shows the full path name of the load in flash.
	Flash Backup Load Name	Shows the full path name of the load in RAM.

### Laptop setup for software loading

The following procedure provides step for setting up a PC (laptop or desktop) to support software loading.

**Note 1:** Read all the steps in this procedure first.

**Note 2:** Ensure Serv\_U FTP server software is loaded onto the PC before proceeding. Serv\_U is free FTP software available online at <http://www.rhinosoft.com/>.

### Setting up the PC for software loading

Step	Action
------	--------

#### At the LCI PC

- 1 Ensure the MG 9000 loads (ITP, ITX, ABI, DS1, SCO\*\_GZ) are available on CD (or other media device), or FTP the loads to the PC.
- 2 Start the Serv\_U FTP Server on the PC.
- 3 Setup the User and Home directory path as follows:
  - userid = admin (user directory path = D: or E: if loading from CD)

- password = n0rtel
  - home directory path = D: or E: if loading from CD (under user's Dir access)
- 4 Verify that Serv-U Server is running and the Domain is online. Ensure that user privileges are set to read/write.
  - 5 Connect an RJ45 cross-over cable to the active DCC card from the Ethernet port of the PC.
  - 6 Set the PC network configuration as follows:
    - a. From the Start menu select **Settings->Network Connections->Local Area Connections**. The **Local Area Connection Status** window appears.
    - b. Click on **Properties**. The **Local Area Connection Properties** window appears.
    - c. From the **list**, select **Internet Protocol (TCP/IP)**, then click **Properties** and enter the following values
      - IP address = 10.0.0.2
      - Subnet mask = 255.255.255.0
      - Gateway = 10.0.0.1
    - d. Restart the PC, if required.
    - e. Ping the MG 9000 to ensure the devices are communicating by typing the following from the Command Prompt (DOS):

```
C:\ ping 10.0.0.1 -t
```

**Note:** The MG 9000 has 10.0.0.1 address with SN08 dual homing feature.
  - 7 Launch the LCI screen, using the Netscape 7.0 or Explorer 5.5 browser, by typing the following in the address field:

```
https://10.0.0.1
```
  - 8 In the LCI, click on **Maintenance**, select the affected MG 9000 shelf, and click on the intelligent card on which the software is to be loaded.
  - 9 If IPSec has been configured on this MG 9000, in the **Software Loading** screen for the first target card, set the IPSec Policy to On to allow local Software download. Click **Submit**.

**Note 1:** Regardless of which software loading screen is used to toggle the IPSec policy, once it has be set on one screen the policy has been set for all card software loading screens.

**Note 2:** If IPsec has not been configured on this MG 9000, this step can be ignored.

- 10 In the **Software Loading** screen for the target card, enter the required loading information which includes the IP address of the FTP server and the load name and path.  
For example:
  - IP address to FTP server: 10.0.0.2
  - Load Name: E:\Loads\where ITPA08BQ\_GZ is the loadname
- 11 Click the **Load** button. From the **Serv\_U software** window, press **F5** to verify the connection. The MG 9000 image transfers as a software.bak file.
- 12 In the shelf view, click on the card being loaded and access the **Node->Controls maintenance** menu.
- 13 Click on the **Restart Flash Backup radio** button and click **Submit**. This action will boot the new load onto the MG 9000.
- 14 If the IPsec Policy was set to On in [step 9](#) to allow local Software download, set the IPsec Policy to Off. Click **Submit**
- 15 This procedure is complete.

---

—End—

---

## Alarm log

The SNMP Alarm Log History screen allows the technician to query and display the current SNMP alarms from the active DCC card by selecting Current from the Alarm log menu. The information provides a list of all the current events that occur on the node. To view the history of SNMP alarms, select History from the Alarm Log menu. The information displays a list of all the events that occurred to bring the node to its current state, which is useful for debugging. The following figures show the Alarm Log Current and History display screens,



- Admin Status - identifies if the VMG is presently active and in-service

The following figure shows the ESA Status screen

### ESA Status screen

The screenshot shows the 'ESA Status for VMGs on this Node' screen. At the top, it indicates 'Frame #0 Shelf #3 Selected' and provides a 'select a shelf view below:' dropdown menu with 'frame #0 shelf #3' selected. Below this is a rack diagram with columns for SIC and PID. The SIC row shows 'M', 'm', 'm', 'm' above 'A', 'A', 'A'. The PID row shows 'DCC', 'DCC', 'ITP', 'ITX', 'ITX', and 'DS1 16pt'. A red arrow points to the 'ITP' column. Below the rack diagram is a table with the following data:

Name	ESA	ESA Capable	Oper Status	Admin Status
SLOA011-0-3	Not in ESA	ESAcapable	Oos	Oos

**Note:** The ESA Status screen is an information only screen that gathers data only when the user enters the screen. To refresh the data displayed on the screen, re-enter the ESA Query tool.

### Ethernet configuration

This screen allows the technician to provision the Ethernet ports to a specified IP address. This allows remote access to the Ethernet port for FTP and LCI management.

The following fields appear in the Ethernet Configuration screen

- IP address - displays the provisioned address for the Ethernet port on the selected card or enter a new address for the port
- Subnet Mask - is used by network administrators to indicate how an IP address (host) is interpreted
- Default Gateway - defines the first hop in the routing of packets, where the first hop is the initial router to which the Ethernet is connected

The following figure shows the Ethernet Configuration screen.



- IKE Lifetime - specifies the lifetime for an IKE phase 1 Security Association

The lifetime determines how long the currently established security session will last. The IKE Security association defines the way in which two peers communicate and is then used to produce any number of IPSec security associations between peers. IKE Lifetime and IPSec Lifetime refer to the respective security association lifetimes. A security association exists only for the specified lifetime after which they are replaced with a new security association and the old one is removed from the database.

- IPSec Lifetime - specifies the lifetime for an IPSec Security Association
- Shared Key - specifies the pre-shared key used in the IKE establishment of a secure call control link. This is required for authentication. Enter a 20-120 alphanumeric character ASCII string.
- Confirm Shared Key - confirmation of the above shared key
- Authentication Method - allows users to select the authentication method: either Pre-Shared key or Digital Signatures.
- The LCI also displays alarms for digital certificates that are expired, invalid, or within 4 days of expiration. The procedures for clearing these alarms are described in *MG 9000 Fault Management*, NN10074-911, and *Nortel CVoIP IPSec Security Service Implementation Guide*, NN10453-100
- SSH Host Key Fingerprint - The field is populated only after a user queries the key. By selecting the Query button, the system displays the local SSH key for the node. This is a signature key. The EM is presented with this key when it tries to transfer files to the MG 9000. If the EM is unsure about the authenticity of the MG 9000 node, it will ask the user to verify the key that is displayed in the SSH Host Key Fingerprint field. In such a case, the EM displays a copy of the key that was presented to it by the node being verified. The user can compare the key with the value queried with the LCI. If the values match, the user can indicate that it is safe to proceed.

The following figure shows the OAMP IPSec Provisioning screen.

## OAMP IPsec Provisioning

Frame #0 Shelf #3 Selected

select a shelf view below:

frame\_#0\_shelf\_#3

FRAME

SIC

PIO LC LC LC LC ABI ABI MTADCC DCC ITP ITP ITX ITX

S M A A A

### OAMP IPsec Provisioning

Peer IP Address

Authentication Method

IKE Lifetime  Unit

IPSec Lifetime  Unit

Shared Key

Confirm Shared Key

---

SSH Host Key Fingerprint

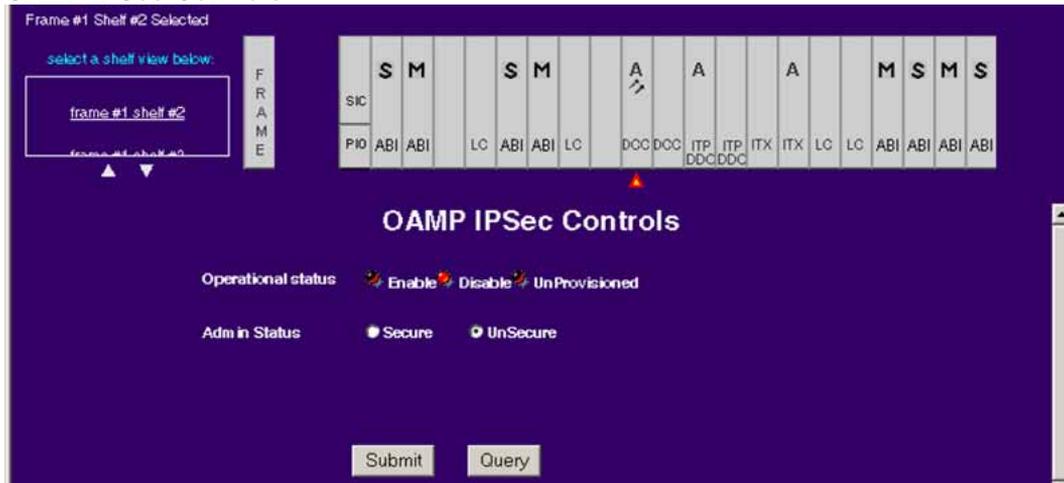
The OAMP IPsec Controls screen is used to set the Administrative status as Secure or Unsecure and to query the current security status. The following controls appear on this screen (for further details on usage, you must consult *Nortel CVoIP IPsec Security Service Implementation Guide*, NN10453-100):

**Note:** The security parameters cannot be reconfigured when IPsec is in a secure state.

- Operational status - indicates IPsec operational status
- Admin status - indicates if security is enabled

The following figure shows the OAMP IPsec Controls screen.

## OAMP IPsec Controls



## Debug commands

The Debugs Commands screen provides debugging commands used for system troubleshooting.

To use the debug commands, the user must perform the following steps:

Step	Action
------	--------

- Secure shell to the LCI debug port on the active DCC card (port 69).

**Note:** The SN07 release only supports running the debug commands on the active DCC card.

- Access debug port 69 by typing the following command string  
`> ssh -l admin -p 69 <IP_address>`
- Enter the login and password information:
  - login = admin
  - password = n0rtel

The following figure shows the system response.

```

47.142.82.159 - PuTTY
login as: admin
admin@47.142.82.159's password:
LCI Debug Command Port

<<<<<<<<<< Cmd 1 output start <<<<<<<<<<
/aer/listbuf - list avail AER buffers

  AAMBUF   APSBUF   ATMHAL   ATSSBUF  CARDLOG  CARMALM
  CARMBUF  CARMPM   DLINEMTC ERRORBUF HALBUF1  LBBUF
  LBBUF2   LCIBUF   LCLOG    LCSIM    LINEAUDT LINELOG
  LINEMTC  MRKTBUF  MTABUF   MTACARD  NMTCBUF  NMTCPRM
  SHFMGMT  SIGBUF   SIGPMBUF SLICLOG  SWINFO   TRAPINFO
  UPGBUF   WBBUF

Current Date and Time = 19:33:49.310 JANUARY 1, 1970
<<<<<<<<<< Cmd 1 output end <<<<<<<<<<

```

- 2      Navigate to the **Debug CMDs** screen off the **DCC card** menu.
- 3      Select the command number from the list of commands presented on the screen.
- 4      Enter the command number in the Commands field and If applicable, any parameters in the Parm (1-4) field(s).
- 5      Press **Submit**.
- 6      View the results which are sent to the secure shell session for viewing.

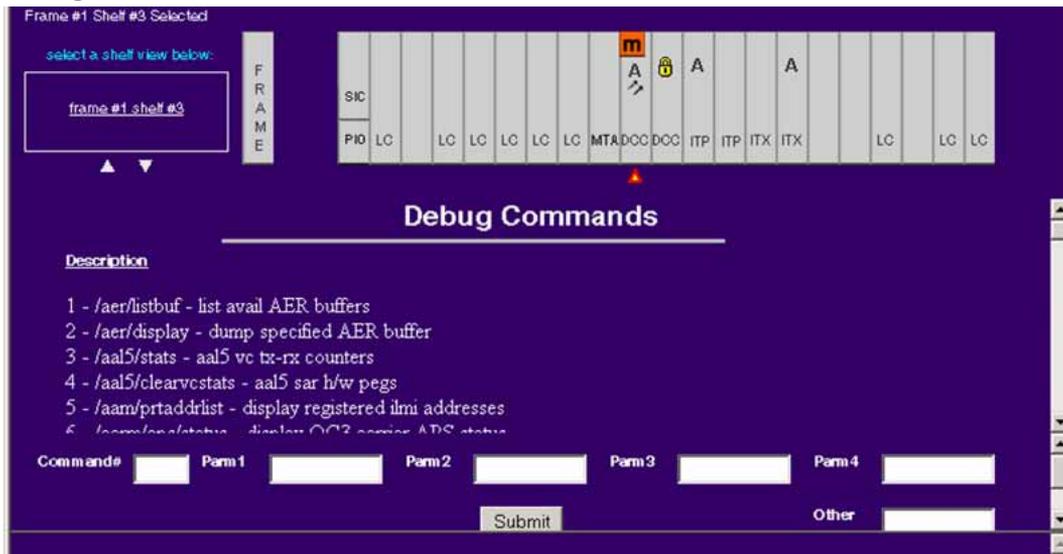
---

—End—

---

The following figure shows the Debug Commands screen.

## Debug Commands screen



The following table lists the available debug commands, the syntax, description, options/parameters and examples.

### Debug commands, syntax, description, and options

Debug command Syntax	Description Options/parameters and example
Command: /aal5/clearvcstats Syntax: /aal5/clearvcstats [-h]	Description: Clears (zeros) the per-virtual-circuit statistics for all virtual circuits.  Options/parameters: No command line options or parameters.
Command: /aal5/stats Syntax: /aal5/stats [-h]	Description: Obtains either Global or per-virtual-circuit statistics  Options/parameters: <ul style="list-style-type: none"> <li>stats g - to print Global statistics</li> <li>stats global - to print Global statistics</li> <li>stats interface vpi vci - to print Per-VC statistics for 1 VC</li> </ul>
Command: /aam/prtaddrlist Syntax: /aam/prtaddrlist -h	Description: Prints all entries in the ATM address list table  Options/parameters: No command line options or parameters.

Debug command Syntax	Description Options/parameters and example
<p>Command: /aer/display</p> <p>Syntax: /aer/display [-h] &lt;buffer_name/all&gt; [&lt;class_name&gt; [&lt;start_num&gt; [&lt;stop_num&gt;]]]</p>	<p>Description: Displays selected event reports.</p> <p>The buffer types ERRORBUF and TRAPINFO are used to log error conditions. Any events in these buffers warrant GNPS follow-up. All other buffer class are used for status/progress indications and the presence of logs in these buffers does not necessarily represent an error condition. For instance, the restorePersistence log shown below is a progress indication and does not indicate an error.</p> <p>Options/parameters:</p> <ul style="list-style-type: none"> <li>• &lt;buffer_name&gt;STRING - the name of a buffer type, as displayed by /aer/listbuf</li> <li>• &lt;class_name&gt;STRING. - the specific class of buffer, as display by /aer/listevent</li> <li>• &lt;start_num&gt;{0 TO 1000}</li> </ul> <p>&lt;stop_num&gt;{0 TO 1000}</p> <p>Example:</p> <pre>SCO [0 2 10] dSH&gt; /aer/display errorbuf No records SCO [0 2 10] dSH&gt; /aer/display aambuf INFO601 AAM JAN-01 00:00:24.960 restorePersistence called</pre>
<p>Command: /aer/listbuf</p> <p>Syntax: /aer/listbuf [-h]</p>	<p>Description: Lists all the AER buffer names in use on the card where it is executed.</p> <p>Options/parameters: No command line options or parameters.</p> <p>Example:</p> <pre>SCO [0 2 10] dSH&gt; /aer/listbuf AAMBUF ATMHAL ATMSSBUF CARDLOG CARMALM CARMBUF CARMPM DLINEMTC ERRORBUF HALBUF1 LBBUF LBBUF2 LCIBUF LCLOG LCSIM LINEAUDT LINELOG LINEMTC MRKTBUF MTABUF MTACARD NMTCBUF NMTCPRM RDPBUF SHFMGMT SIGBUF SIGPMBUF SLICLOG SWINFO TRAPINFO UPGBUF WBBUF</pre>
<p>Command: /carm/aps/status</p> <p>Syntax: /carm/aps/status [-h]</p>	<p>Description: Prints local and mate protection group status for the carrier on this card.</p> <p>Options/parameters: No command line options or parameters.</p>

Debug command Syntax	Description Options/parameters and example
Command: /carm/carrconfig/print Syntax: /carm/carrconfig/print[-h]	Description: Prints configuration data on the network carrier interfaces for the board on which it is executed.  Options/parameters: No command line options or parameters.
Command: /inet/ping Syntax: /inet/ping [-c count] [-s packetsize] [-l interval] host	Description: Sends ICMP ECHO_REQUEST packets to the specified network host. This is useful for verifying connectivity to gateway controller (GWC) and MG 9000 Manager.  If an OAMP inband connection has been established (this can be verified using the /wb/getconn command), pings to the MG 9000 Manager from the active DCC should be successful, as should pings to the shelf controller (SC0 CIPOA address for this MG 9000).  An ability to ping from the DCC to the SC but not to the MG 9000 Manager indicates an IP routing problem in the central office LAN and/or within the SC itself. An inability to ping from the DCC to the shelf controller when /wb/getconn indicates the OAMP CIPOA connection is available would tend to indicate a problem at the DCC or the shelf controller.  A ping to a GWC must be issued from the subtending ITP cards. (To access Dshell on subtending ITPs, use the /dshell/telnet command.) A subtending ITP may only ping the GWC address on which that ITP's VMG has been configured. Pings from the ITP to the GWC may be used to determine if network packet loss/delay (a possible cause of Megaco ALF alarms) is present.  Options/parameters: <ul style="list-style-type: none"> <li>• Count - number of ICMP ping requests to attempt (not necessary to use dshell access while the requests are in progress - so exercise caution in using this)</li> <li>• Packetsize - the size of the ECHO_REQUEST packets to use</li> <li>• Interval - the time to wait between ICMP ECHO_REQUEST packets</li> </ul>

Debug command Syntax	Description Options/parameters and example
	<ul style="list-style-type: none"> <li>Host - the IP address (in format xx.xx.xx.xx) to which the packets are sent</li> </ul> <p>Example:</p> <pre>SCO [0 0 11] dSH&gt; /snmp/getsnmip NVNodeNEIdentifier Payload: ===== NE Id.....= 11 NE Name.....= C411 NE TimeOfDay.= 2004-8-9,0:32:20 NE OamAesaSc0...= 39345678901234567890123aba00e0cf0 060f200' NE OamAesaSc1...= 39345678901234567890123aba00e0cf0 0612100' NE CcAesaSc0....= 39345678901234567890123ABA00E0CF0 060F200' NE CcAesaSc1....= 39345678901234567890123aba00e0cf0 0612100' NE DS512AesaSc0....= 39345678901234567890123aba00e0 cf0060f200' NE DS512AesaSc1....= 39345678901234567890123aba00e0 cf00612100' Transparent Items NE OamUemg Ip...= 10.32.0.70 NE OamUemg Mask.= 255.255.254.0 NE OamNextHop= 10.32.0.254 NE SnmIp....= 47.142.131.100 :: 8006 NE CcUemg Ip...= 10.32.0.80 NE CcUemg Mask.= 255.255.254.0 NE CcNextHop= 10.32.0.254 NE DS512Uemg Ip...= 10.32.0.90 NE DS512Uemg Mask.= 255.255.254.0 NE DS512NextHop= 10.32.0.254 SCO [0 0 11] dSH&gt; /inet/ping 10.32.0.254 10.32.0.254 is alive SCO [0 0 11] dSH&gt; /inet/ping 47.142.131.100 47.142.131.100 is alive</pre>

Debug command Syntax	Description Options/parameters and example
<p>Command: /inet/traceroute</p> <p>Syntax: /inet/traceroute [-adnruvAMOQ] [-w wait] [-S start_ttl] [-m max_ttl] [-p port#] [-q nqueries] [-g gateway] [-t tos] [-s src_addr] [-g router] host [data size]</p>	<p>Description: Traces packet route to a network host.</p> <p>This command can be useful in diagnosing connectivity problems to a central office host (usually the MG 9000 Manager if traceroute is being executed from the DCC, or the GWC if traceroute is being executed from an ITP/ABI)</p> <p>Options/parameters:</p> <ul style="list-style-type: none"> <li>• -a - Abort after 10 consecutive drops</li> <li>• -g - Use this gateway as an intermediate hop (uses LSRR)</li> <li>• -S - Set start TTL (default 1)</li> <li>• -m - Set maximum TTL (default 30)</li> <li>• -n - Report IP addresses only (not hostnames) ALWAYS ON</li> <li>• -p - Use an alternate UDP port</li> <li>• -q - Set the number of queries at each TTL (default 3)</li> <li>• -r - Set Don't Route option</li> <li>• -s - Set your source address</li> <li>• -t - Set the IP TOS field (default 0)</li> <li>• -u - Use microsecond timestamps</li> <li>• -v - Verbose</li> <li>• -w - Set timeout for replies (default 5 sec)</li> <li>• -A - Report AS# at each hop (from GRR)</li> <li>• -M - Do RFC1191 path MTU discovery</li> <li>• -O - Report owner at each hop (from DNS)</li> <li>• -P - Parallel probing</li> <li>• -Q - Report delay statistics at each hop (min/avg+-stddev/max) (ms)</li> <li>• -T - Terminator (line end terminator)</li> <li>• -U - Go to next hop on any success</li> </ul>

Debug command Syntax	Description Options/parameters and example
	<pre> Example: SCO [0 0 11] dSH&gt; /snmp/getsnmip NVNodeNEIdentifier Payload: ===== NE Id.....= 11 NE Name.....= C411 NE TimeOfDay.= 2004-8-9,0:32:20 NE OamAesaSc0...= 39345678901234567890123aba00e0cf0 060f200' NE OamAesaSc1...= 39345678901234567890123aba00e0cf0 0612100' NE CcAesaSc0....= 39345678901234567890123ABA00E0CF0 060F200' NE CcAesaSc1....= 39345678901234567890123aba00e0cf0 0612100' NE DS512AesaSc0....= 39345678901234567890123aba00e0 cf0060f200' NE DS512AesaSc1....= 39345678901234567890123aba00e0 cf00612100' Transparent Items NE OamUemg Ip...= 10.32.0.70 NE OamUemg Mask.= 255.255.254.0 NE OamNextHop= 10.32.0.254 NE SnmIp....= 47.142.131.100 :: 8006 NE CcUemg Ip...= 10.32.0.80 NE CcUemg Mask.= 255.255.254.0 NE CcNextHop= 10.32.0.254 NE DS512Uemg Ip...= 10.32.0.90 NE DS512Uemg Mask.= 255.255.254.0 NE DS512NextHop= 10.32.0.254 SCO [0 0 11] dSH&gt; /inet/traceroute 47.142.131.100 traceroute to 47.142.131.100 (47.142.131.100), 30 hops max, 40 byte packets 1 10.32.0.254 0 ms 0 ms 10 ms 2 172.20.240.3 0 ms 0 ms 0 ms 3 47.142.131.100 10 ms 0 ms 0 ms </pre>

Debug command Syntax	Description Options/parameters and example
<p>Command: /lanbuilder/prtconnlst</p> <p>Syntax: /lanbuilder/prtconnlst [-h] [all]</p>	<p>Description: Used to print the card to card connection list.</p> <p>Each MG 9000 has an internal IP network between the intelligent cards inserted into the MG 9000 shelves. This network is called the "lanbuilder" network, and uses the 192.168.0.0 subnet. Each card within the network receives a unique address within the 192.168.0.0 subnet based on it's shelf/frame/slot location.</p> <p>While these addresses can be calculated, the easiest way to see which address correspond to which cards on the internal network is to use the /lanbuilder/prtconnlst command. The output of this command shows the shelf/frame/slot for each intelligent card, and the address of the card. These internal addresses can be used to telnet to subtending cards from the DCC.</p> <p>/lanbuilder/prtconnlst can also be used to determine the health of the connections between cards. The simple form of the command gives only an up/down indication (or in the case of a subtending card, an N/A indication when there is no direct connection between the subtending card and the address). When the "all" parameter is added, additional debugging information is printed out.</p> <p>Options/parameters: [all] indicates that additional status information should be printed.</p> <p><b>Example:</b></p> <pre>SCO [0 2 10] dSH&gt; /lanbuilder/prtconnlst CONNECTION LIST ===== Frame   Shelf Slot  Card      ip          Succ Fail   ConnId ConnState ===== 0       2       10      OC3        192.168.192.74 0       0       0        up 0       2       11      OC3        192.168.192.75 3       29      39        up 0       2       12      ITP        192.168.128.76 0       3       37        up 0       2       13      ITP        192.168.128.77 0       6       38        up 0       2       14      ITX        192.168.128.78 1       0       34        up</pre>

Debug command Syntax	Description				Options/parameters and example
	0	2	15	ITX	192.168.128.79
	0	4	36	up	
<b>Example:</b>					
SCO [0 2 10] dSH> /lanbuilder/prtconnlst all					
wyaReceived_ = True					
lbInitComplete_ = True					
rdpConTo10_ = False					
rdpConTo11_ = True					
CONNECTION LIST					
=====					
Frame	Shelf	Slot	Card	ip	Succ
Fail	ConnId	ConnState			
=====					
0	2	10	OC3	192.168.192.74	
0	0	0	up		
Fr:0 Sh:2 Sl:10 Ip:192.168.192.74 cardType:OC3					
vccCipoaIsSetUp_ = False wyaAcked_ = True					
wyaResends_ = 0					
msgUp_ = False nonRDPmsgUp_ = False					
rdpConnPtr_ = 0x0					
0	2	11	OC3	192.168.192.75	
3	29	39	up		
Fr:0 Sh:2 Sl:11 Ip:192.168.192.75 cardType:OC3					
vccCipoaIsSetUp_ = True wyaAcked_ =					
True wyaResends_ = 0					
msgUp_ = True nonRDPmsgUp_ = False					
rdpConnPtr_ = 0x6782e98					
0	2	12	ITP	192.168.128.76	
0	3	37	up		
Fr:0 Sh:2 Sl:12 Ip:192.168.128.76 cardType:ITP					
vccCipoaIsSetUp_ = True wyaAcked_ =					
True wyaResends_ = 1					
msgUp_ = True nonRDPmsgUp_ = False					
rdpConnPtr_ = 0x67cc8c8					
0	2	13	ITP	192.168.128.77	
0	6	38	up		
Fr:0 Sh:2 Sl:13 Ip:192.168.128.77 cardType:ITP					
vccCipoaIsSetUp_ = True wyaAcked_ =					
True wyaResends_ = 1					
msgUp_ = True nonRDPmsgUp_ = False					
rdpConnPtr_ = 0x67c1990					
0	2	14	ITX	192.168.128.78	
1	0	34	up		
Fr:0 Sh:2 Sl:14 Ip:192.168.128.78 cardType:ITX					
vccCipoaIsSetUp_ = True wyaAcked_ =					
True wyaResends_ = 0					

Debug command Syntax	Description Options/parameters and example
	<pre> msgUp_                = True      nonRDPmsgUp_ = False rdpConnPtr_          = 0x6817278 0      2      15      ITX      192.168.128.79 0      4      36      up Fr:0 Sh:2 Sl:15 Ip:192.168.128.79 cardType:ITX vccCipoaIsSetUp_    = True      wyaAcked_      = True      wyaResends_ = 1 msgUp_                = True      nonRDPmsgUp_ = False rdpConnPtr_          = 0x67e13b8 </pre>
<p>Command: /snmp/getsnmip</p> <p>Syntax: /snmp/getsnmip [-h]</p>	<p>Description: Displays inband (wan builder) configuration and external addressing for the MG 9000 subnets.</p> <p>Options/parameters: No command line options or parameters.</p>
<p>Command:</p> <p>/snmp/getsnmip</p> <p>(contd)</p>	<p>Example:</p> <pre> SCO [0 0 11] dSH&gt; /snmp/getsnmip NVNodeNEIdentifier Payload: ===== NE Id.....= 11 NE Name.....= C411 NE TimeOfDay.= 2004-8-9,0:32:20 NE OamAesaSc0...= 39345678901234567890123aba00e0cf0 060f200' NE OamAesaSc1...= 39345678901234567890123aba00e0cf0 0612100' NE CcAesaSc0....= 39345678901234567890123ABA00E0CF0 060F200' NE CcAesaSc1....= 39345678901234567890123aba00e0cf0 0612100' NE DS512AesaSc0....= 39345678901234567890123aba00e0 cf0060f200' NE DS512AesaSc1....= 39345678901234567890123aba00e0 cf00612100' Transparent Items NE OamUemg Ip...= 10.32.0.70 NE OamUemg Mask.= 255.255.254.0 NE OamNextHop= 10.32.0.254 NE SnmIp....= 47.142.131.100 :: 8006 NE CcUemg Ip...= 10.32.0.80 NE CcUemg Mask.= 255.255.254.0 NE CcNextHop= 10.32.0.254 NE DS512Uemg Ip...= 10.32.0.90 NE DS512Uemg Mask.= 255.255.254.0 NE DS512NextHop= 10.32.0.254 </pre>

Debug command Syntax	Description Options/parameters and example
<p>Command: /wb/cause</p> <p>Syntax: /wb/cause[-h]</p> <p><b>Example:</b></p> <pre>SCO [0 0 11] dSH&gt; /wb/cause OAMP Connection... SVC to SC0 is currently Connected -- cause code 0 - NA SVC to SC1 is currently Connected -- cause code 0 - NA Call Control Connection... SVC to SC0 is currently Connected -- cause code 0 - NA SVC to SC1 is currently Connected -- cause code 0 - NA DS512 Connection... SVC to SC0 is currently Connected -- cause code 0 - NA SVC to SC1 is currently Connected -- cause code 0 - NA</pre>	<p>Description: Displays the release cause codes for the inband (wanbuilder0 messaging links).</p> <p>Options/parameters: No command line options or parameters.</p>
<p>Command: /wb/getconn</p> <p>Syntax: /wb/getconn [all]</p> <p><b>Example:</b></p> <pre>SCO [0 0 11] dSH&gt; /wb/getconn OAM connection... Primary has been Connected to SC 1. Primary Vpi, Vci = 0, 1648. Secondary has been Connected to SC 0. Secondary Vpi, Vci = 0, 1649. Call Control connection... Primary has been Connected to SC 1. Primary Vpi, Vci = 0, 1650. Secondary has been Connected to SC 0. Secondary Vpi, Vci = 0, 1651. DS512 connection... Primary has been Connected to SC 1. Primary Vpi, Vci = 0, 1646. Secondary has been Connected to SC 0. Secondary Vpi, Vci = 0, 1647.</pre>	<p>Description: Displays connection information for the inband (wan builder) messaging links.</p> <p>Options/parameters: [all] The All option displays more detailed information</p>

## ITP maintenance options

ITP maintenance options consist of the following maintenance actions:

- node maintenance
- alarm display
- software loading
- clock synchronization maintenance
- IPsec Config

To select an option, move the cursor to the option and click.

The node, alarm and software screen functionality is identical for all cards managed through the LCI. For a detailed description, see "[DS1 node maintenance](#)" (page 356) and "[DCC node maintenance](#)" (page 365). The VMG IPsec Config screen is similar to that of the DCC. For more information, refer to "[IPsec configuration](#)" (page 395).

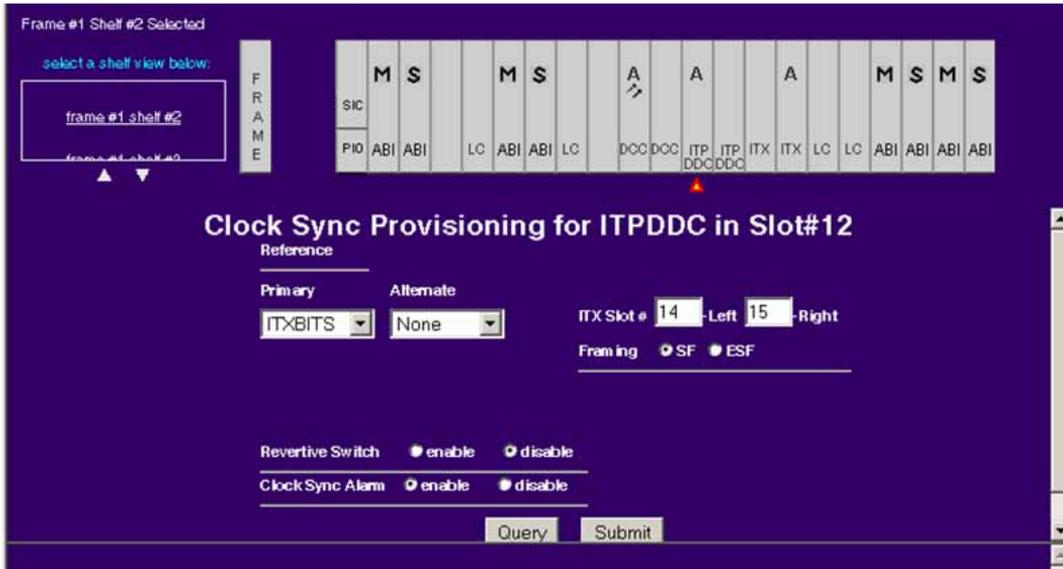
## Clock sync provisioning

The Clock Sync Provisioning screen defines the system timing mode for the network element. The screen provides three timing mode options:

- network (not supported on an MG 9000 with GigE DCC cards)
- ITX building integrated timing system (ITXBITS)
- DCCBITS
- DCC Synchronization Supply Unit (DCCSSU), only supported with the NTNY45FA GigE DCC card using 2048 kHz interfaces (used in international solutions only)

The Network selection indicates the clock sync derives the timing reference from the upstream network connection. The MG 9000 accepts an external BITS DS1 input signal, referenced to a Stratum timing source that is Stratum-3 or better. The external timing signal is a DS1 BITS supplied clock. The ITP card receives the BITS reference signal card through an 8 KHz signal transmitted over the MG 9000 backplane.

**ITP Clock Sync Provisioning screen**



The ITXBITS selection requires at least one ITX card provisioned to serve as the BITS timing reference source. If only one ITX is provisioned, set the slot number fields to the same value. Set the upper ITX slot field to the left most ITX being used for BITS distribution. Set the lower slot field to the right most ITX being used for BITS distribution.

If DCCBITS or ITXBITS was selected, select the format encoding method, SF (superframe) or ESF (extended superframe).

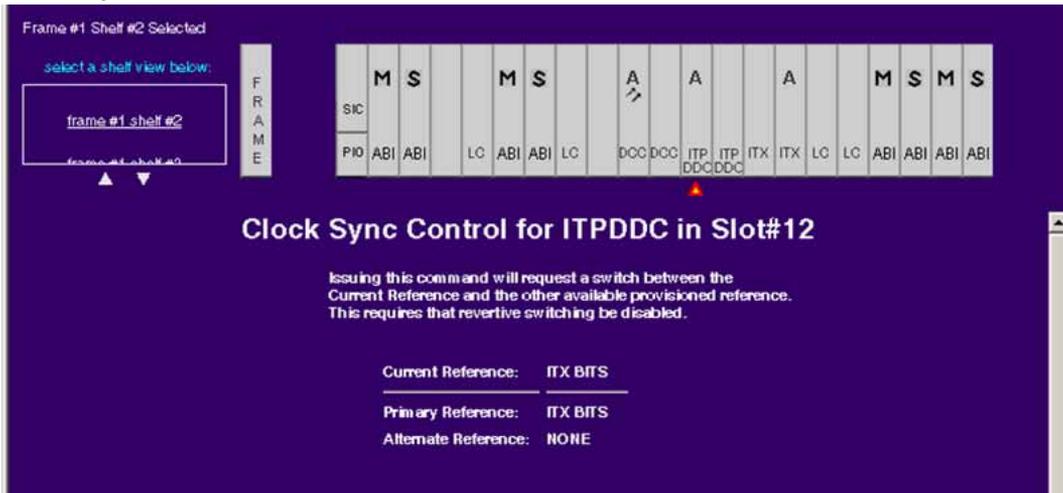
The reference switching default option is non-revertive.

To enable clock sync alarms, select the Enable radio button.

**Clock sync control**

The Clock Sync Control screen queries the current clock reference and allows the option to set the clock reference to either ITP0 or ITP1.

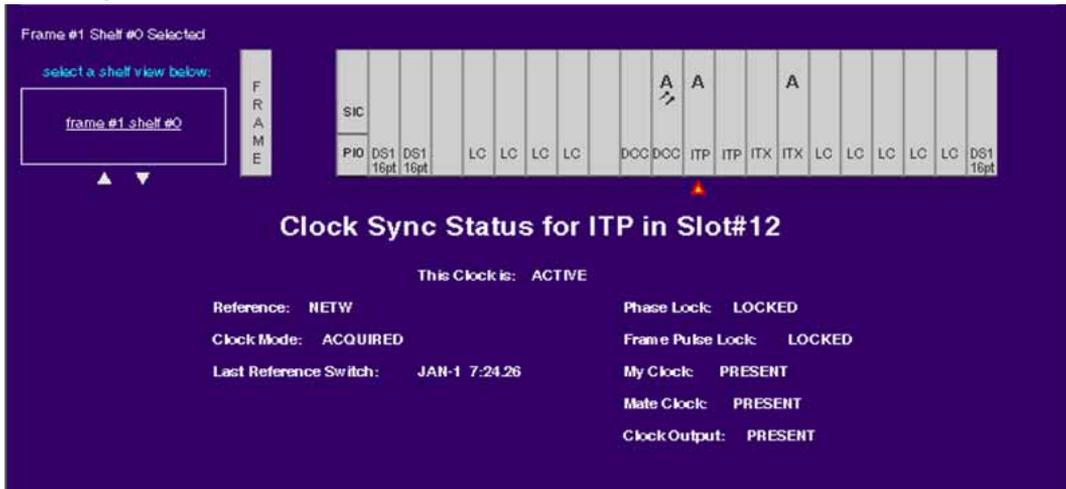
**Clock Sync Control screen**



**Clock sync status**

The Clock Sync Status screen contains information regarding the condition of the system clock and the selected ITP reference. The information appearing on the screen automatically updates every 10 seconds.

**Clock Sync Status**



The following table lists the fields and status options displayed on the Clock Sync Status screen.

#### Clock Sync Status options

Field	Status Options
Reference	<ul style="list-style-type: none"> <li>• DCCBITS</li> <li>• NETW</li> <li>• ITXBITS</li> <li>• DCCSSU (supported on GigE only)</li> <li>• None</li> </ul>
Clock Mode	<ul style="list-style-type: none"> <li>• Normal</li> <li>• Acquiring (a transient condition)</li> <li>• Acquired</li> <li>• Hold Over</li> <li>• Free Run</li> </ul>
Last Reference Switch	month, dd:hh:mm:ss
Phase Lock	<ul style="list-style-type: none"> <li>• Locked</li> <li>• Not locked</li> </ul>
Frame Pulse Lock	<ul style="list-style-type: none"> <li>• Locked</li> <li>• Not locked</li> </ul>
My Clock	<ul style="list-style-type: none"> <li>• Present</li> <li>• Missing/Failed</li> </ul>
Mate Clock	<ul style="list-style-type: none"> <li>• Present</li> <li>• Missing/Failed</li> </ul>
Clock Output	<ul style="list-style-type: none"> <li>• Present</li> <li>• Missing/Failed</li> </ul>

#### Clock sync reference/timing signal

The Reference/Timing Signal screen identifies the active clock sync reference and the timing signal source used by the MG 9000. The following figure shows the Reference/Timing Signal screen.

### Clock Sync Reference/Timing Signal screen

Frame #1 Shelf #2 Selected

select a shelf view below:

frame #1 shelf #2

FRAME

M S M S A A A M S M S

SIC

PIO ABI ABI LC ABI ABI LC DCC DCC ITP ITP ITX ITX LC LC ABI ABI ABI ABI

Sync Reference /Timing Signal for ITP in slot # 12

Sync Reference				
ID	Status	LOS Count	OOF Count	Fail Reason
ITXBITS_0	inactive	0	0	none
ITXBITS_1	active	0	0	none
DCCBITS_0	unused	0	0	none
DCCBITS_1	unused	0	0	none

Timing Signal				
ID	Status	LOS Count	LOF Count	Fail Reason
ITXBITS_A0	inactive	6	0	none
ITXBITS_B0	unused	6	0	none
ITXBITS_A1	active	5	0	none
ITXBITS_B1	unused	5	0	none

### ITX maintenance options

ITX maintenance options consist of the following maintenance actions:

- node maintenance
- alarm display
- software loading

To select an option, move the cursor to the option and click.

The node, alarm and software screen functionality is identical for all cards managed through the LCI. For a detailed description, see ["DS1 node maintenance"](#) (page 356) and ["DCC node maintenance"](#) (page 365).

### SIC maintenance options

Shelf interface card/power input-output card (SIC/PIO) maintenance options consist of the following maintenance actions:

- alarm status
- output status
- card info

To select an option, move the cursor to the option and click.

The card info screen functionality is identical for all cards managed through the LCI. For a detailed description, see ["DS1 node maintenance"](#) (page 356) and ["DCC node maintenance"](#) (page 365).

The card output status reports the alarm that is output based on the operational state of the SIC card.

The alarm status screen identifies the alarms that can be output by type and the operational state that raises the alarm.

### ABI maintenance options

Access Bridging Interface (ABI) card, (also known as the DS512 card) maintenance options consist of the following maintenance actions:

- node maintenance
- alarm display
- software loading

To select an option, move the cursor to the option and click.

The node, alarm and software screen functionality is identical for all cards managed through the LCI. For a detailed description, see "[DS1 node maintenance](#)" (page 356) and "[DCC node maintenance](#)" (page 365).

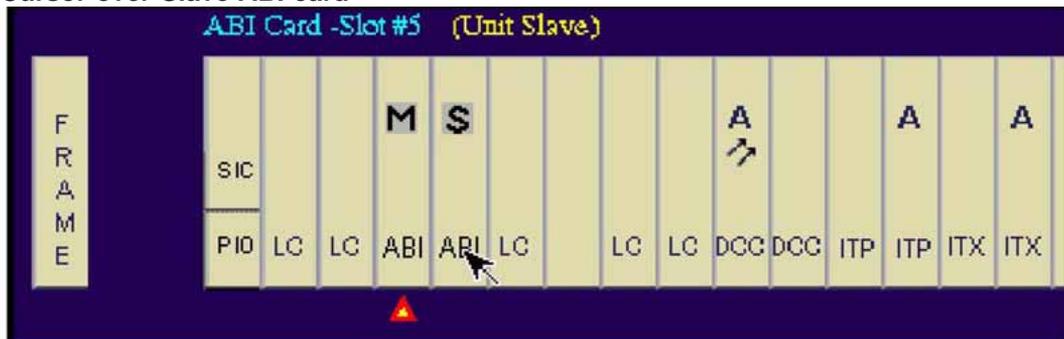
The following figure shows the Master ABI card selected. Moving the mouse cursor over the card causes (Unit Master) to appear above the shelf view.

Master ABI card selected and cursor over Master card



The following figure shows the mouse cursor over the Slave card which causes (Unit Slave) to appear above the shelf view.

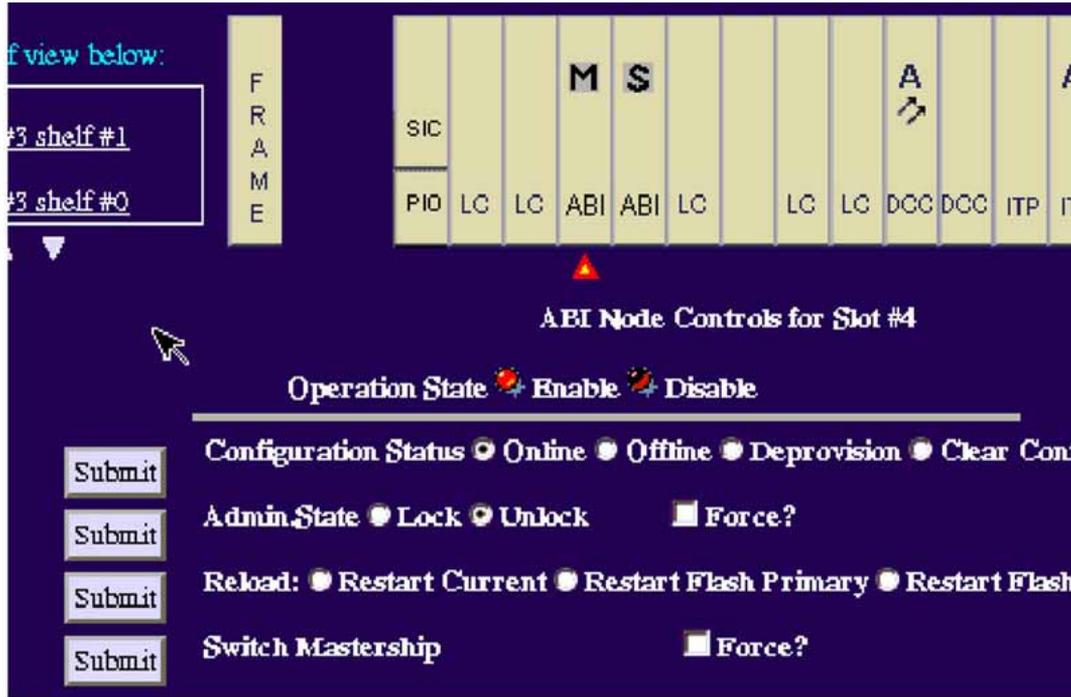
Cursor over Slave ABI card



### ABI node controls

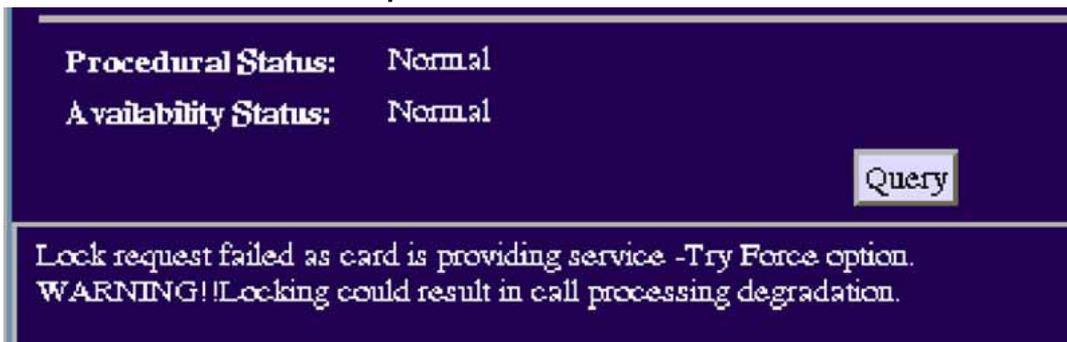
The node control screen for the ABI card is similar to all other cards. However, the ABI card uses Switch Mastership instead of Warm Switch of Activity. The following figure shows an example of a Node Control screen for an ABI card.

ABI Node Control screen showing the Switch Mastership control



At the bottom of the node control screen, the command responses appear. The following figure shows the response when a normal lock is attempted on the selected Slave ABI card.

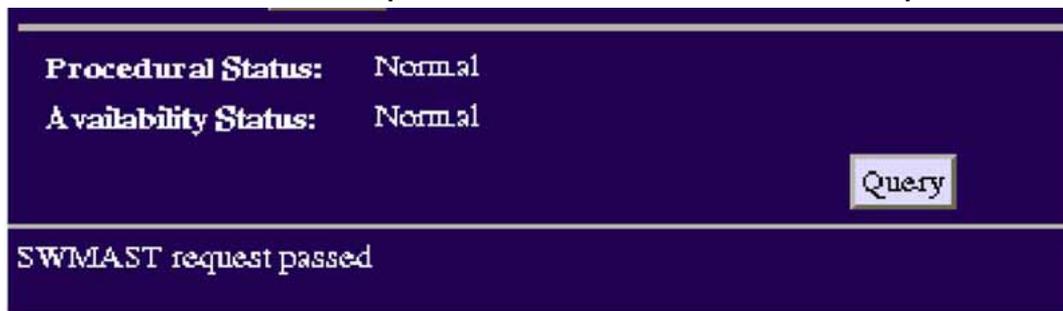
ABI Node Control screen - response to Normal lock on Slave ABI



The following figure shows the response when a normal lock is attempted on the selected Slave ABI card.

**ABI Node Control screen - response to Switch of Mastership on Slave ABI**

The following figure shows the response when a Switch Mastership was successful.

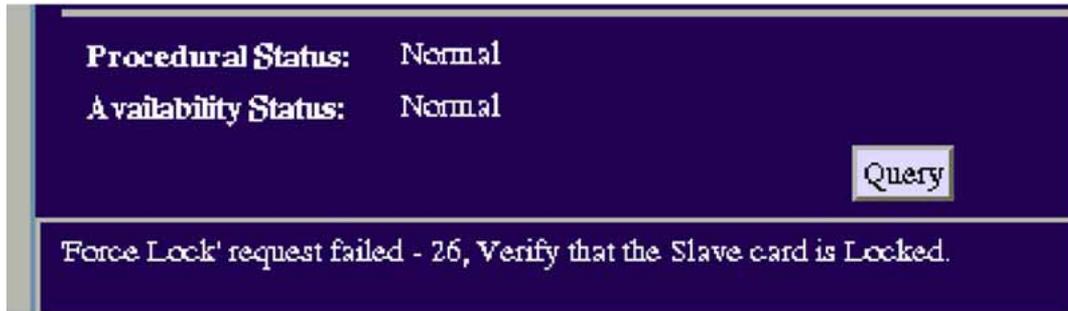
**ABI Node Control screen - response to successful Switch of Mastership**

The following conditions and messages may appear

- Request failure message on Normal Lock of Master ABI card while the Slave ABI card is unlocked
- Request failure message on Force Lock of Master ABI card while the Slave ABI card is unlocked
- Request failure message on Normal Lock of Master ABI card while the Slave ABI card is disabled
- Request failure message on Force Lock of Master ABI card while the Slave ABI card is disabled
- Warning message on Force Lock of Master ABI card while Slave ABI card is locked

The following figure shows the response to a successful Force Lock of the Master ABI.

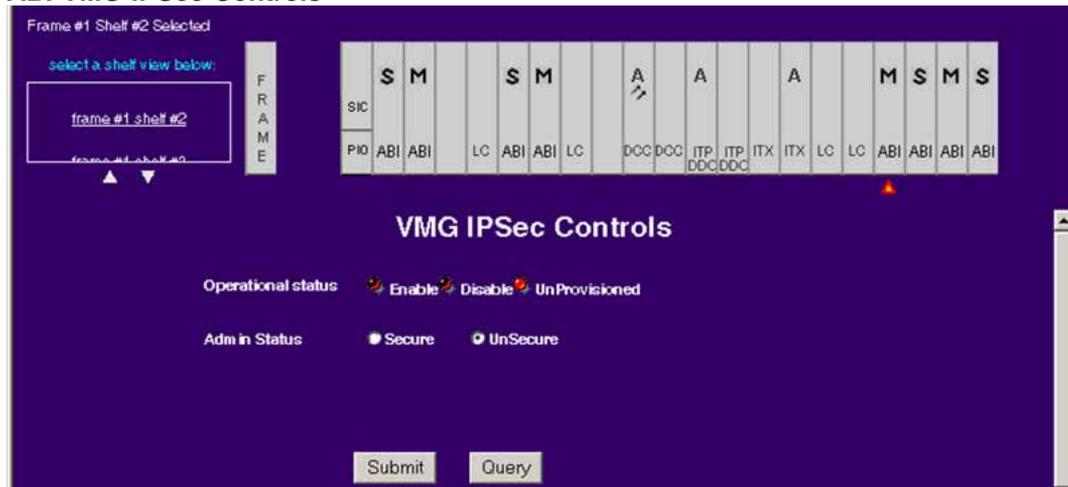
**ABI Node Control screen - response to a Force Lock of the Master ABI**



**ABI IPsec**

The ABI VMG IPsec Config screen is similar to that of the DCC. For more information, refer to "IPsec configuration" (page 395).

**ABI VMG IPsec Controls**





## Upgrading software in MG 9000 cards

---

This section provides an overview of upgrading software in MG 9000 cards.

The MG 9000 Manager provides tools for upgrading software in MG 9000 cards to upgrade the software in the following intelligent cards in the MG 9000:

- data control card (DCC)
  - OC3
  - DS1-IMA
  - Gigabit Ethernet (GigE)
- Internet telephony extender (ITX) card
- Internet telephony processor (ITP) card
- DS-512 Access Bridging Interface (ABI) card
- DS1 card (not used in UA-IP solution)
- metallic test access (MTA) card
- x digital subscriber line (xDSL) card

The Software Upgrade Wizard supports the following two types of upgrades:

- complete upgrade
- download only

The following cards use the Software Upgrade Wizard only when a complete upgrade is selected from the MG Upgrade Wizard:

- MTA card
- xDSL card
- GLC12 CA
- GLC32 BA

Otherwise, each card must have the software downloaded into it individually using the Software Download tool accessed from the card view for each card. The software download procedures for these cards are provided later in this document.

The software upgrade consists of the following four steps:

1. Configure - The configuration parameters are entered in a Card Upgrade Wizard or MG Upgrade Wizard described later.

2. Download - The MG 9000 is requested to download the software load to a card or cards based in the parameters configured in the previous step. The load is downloaded and stored in flash memory.
3. Apply - The software load is installed. A restart is performed in the card.
4. Accept - The new installed load is made the primary load. The user can no longer revert to the old load unless a complete downgrade is performed.

An additional Abort step can be used to abort an upgrade in progress and revert back to the old load.

**Note:** Software upgrade of cards in the MG 9000 must be performed in the following order: DS1, ABI, ITP, ITX, DCC.

The two ways to perform a software upgrade are as follows:

- with user interaction - The user must enter separate commands to perform the download, apply, and accept steps.
- without user interaction - The user enters a single command to perform the download, apply, and accept steps.

### Upgrade version rules

The software upgrade application requires the following version order when an upgrade is performed to a load with the same version or to higher version load.

- DS1 or ABI
- ITP
- ITX
- DCC

**Note 1:** When it is necessary to downgrade to SN08 or SN09 from SN09FF, perform procedure "Downgrading the MG 9000 and MG 9000 Manager from SN09FF to SN08 or SN09" in *Nortel Carrier Voice over IP Upgrades and Patches*, NN10440-450.

**Note 2:** During a downgrade, attempting to downgrade cards to a version lower than the DCC card is not supported.

Upgrades - The supported upgrade path for the MG 9000 is from SN08 or SN09 to SN09FF for the UA-IP solution and from SN08 or SN09 to SN09FF for the UA-AAL1 solution.

Downgrades - The supported downgrade path for the MG 9000 is from SN09FF to SN08 or SN09 for UA-AAL1 and SN09FF to SN08 or SN09 for UA-IP.

## Software Upgrade View

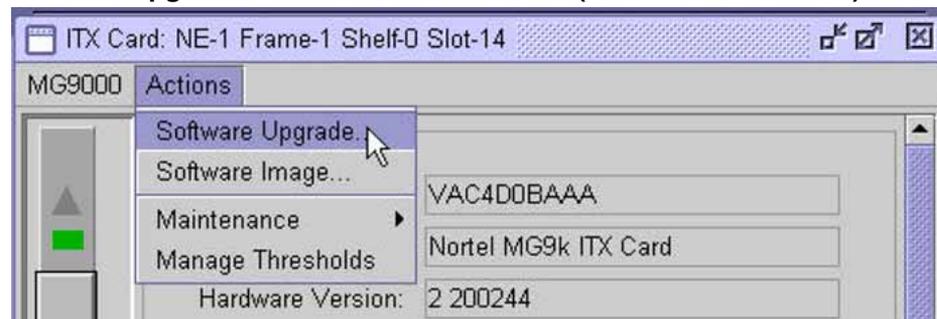
This section provides an overview of the Software Upgrade tool in the MG 9000 Manager.

The software upgrade is performed using the Software Upgrade tool. The Software Upgrade tool is accessed from the MG 9000 Manager. When accessed, the Software Upgrade View appears. The Software Upgrade view is accessed from the following:

- Card View - for upgrading a single card, protection group, or all cards of the same type
- Frame View - for upgrading multiple card types

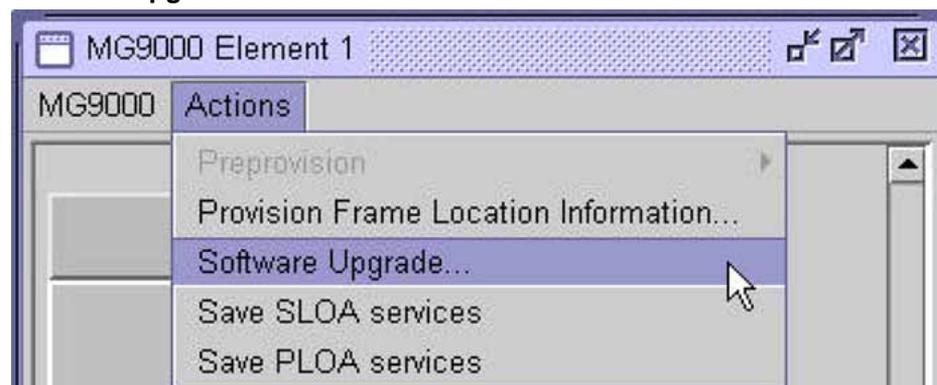
The following figure shows Software Upgrade accessed from the Actions pull-down menu from the Card View

**Software upgrade accessed from Card View (ITX Card view shown)**



The following figure shows Software Upgrade accessed from the Actions pull-down menu from the Frame View.

**Software upgrade accessed from Frame View**



The Software Upgrade view contains the following four panels

- Upgrade Originator panel - displays the name and number of the MG 9000 where the upgrade is taking place and the location of the view from which the upgrade command was invoked. In addition, The Originator field indicates whether the upgrade is being controlled from the GUI or the CLUI.
- Upgrade State - displays text fields with information about an upgrade in progress which includes the status and the action being performed or just completed. The action and upgrade type fields are updated when the upgrade request is confirmed. The upgrade status is updated as upgrade steps are performed.
- Upgrade Type Data - displays data used to perform the upgrade. The text fields in this panel are updated when the configure step is completed. When the upgrade is for a single card type, protection group, or single card it includes text fields for the cards being upgraded, the load server, the user identifier that is used to access the load server, and the full path to the load name. The text field upgrading indicates the cards being upgraded as follows
  - For a single card upgrade, this field displays the location of the card being upgraded.
  - For an active/inactive pair of mate cards, the shelf location followed by the two slot numbers is displayed.
  - For a card type upgrade, the card type being upgraded is indicated.
- Upgrade Instructions & Results - displays the results of an upgrade step and instructions for the next step to perform

Seven buttons are provided in the lower area of the view to enable the user to perform commands. The buttons are described in the following table.

#### Software Upgrade View buttons and descriptions

Button	Description
History	This button creates a new view that shows the upgrade history for the given MG 9000. Refer to " <a href="#">Upgrade history</a> " (page 462).
Refresh	This button updates the Software Upgrade View.

Button	Description
<upgrade step>	<p>This is the second button from the left. This button is used to perform an upgrade step. It changes its label depending on the next step to be performed. It is greyed out when the step is no longer valid. The labels assumed by this button are described as follows:</p> <ul style="list-style-type: none"> <li>• Configure - The upgrade step button is set to this label when the view is first created, and after an abort is completed. <ul style="list-style-type: none"> <li>— When pressed on the Software Upgrade accessed from the Card View, the Card Upgrade Wizard is created.</li> <li>— When pressed on the Software Upgrade accessed from the Frame View, the Upgrade Type Selection panel is created.</li> </ul> <p>See "<a href="#">Upgrade Wizard overview</a>" (page 429). If another user is performing a software upgrade, a message is output indicating the tool is in use and the Configure button is disabled.</p> </li> <li>• Upgrade - The Upgrade step button appears when an upgrade without user interaction is chosen. This step accomplishes the actions described in the following three buttons that appear when user interaction is selected.</li> </ul> <p>The following labels appear when user interaction is selected:</p> <ul style="list-style-type: none"> <li>• Download (not applicable to the Software Upgrade accessed from the Frame View) - The upgrade step button is set to this label when the upgrade wizard finishes the configuration for an upgrade with user interaction. When pressed, the MG 9000 is requested to perform a download. The parameters provided by the upgrade wizard are sent to the MG 9000 in the download request.</li> <li>• Apply (not applicable to the Software Upgrade accessed from the Frame View) - The upgrade step button is set to this label when the MG 9000 completes the download</li> </ul>

Button	Description
	<p>step successfully. When this button is pressed the MG 9000 is requested to apply the load to the card previously downloaded.</p> <ul style="list-style-type: none"> <li>Accept (not applicable to the Software Upgrade accessed from the Frame View) - The upgrade step button is set to this label when the MG9000 completes the apply step successfully. When this button is pressed, the MG 9000 is requested to accept this load as the primary load.</li> </ul>
Version List	View all versions of the cards.
Abort	<p>This button is used to request the MG 9000 perform an abort. The button is enabled when an upgrade without user interaction is executed, and when the download step for an upgrade with user interaction is performed. It remains enabled until an abort is initiated or the accept step of the upgrade is initiated. In certain situations, such as when a fault on a card cannot be corrected, the MG 9000 cannot abort and revert back to the old loads. If the abort fails and there is no other way to stop the upgrade, use the Reset Upgrade System command located on the MG9000 History view (refer to "Upgrade history" (page 462)).</p>
Close	<p>This button is used to close this view. It is disabled while the upgrade is in progress. The button is enabled when an accept or an abort step is completed. An upgrade view can also be closed by the Close command in the window menu. A Close command is also provided in the MG 9000 menu. For the last two cases the Close command is not disabled when an upgrade is in progress.</p>
Retry	<p>This button is enabled only if a step in the upgrade process fails. Retry is used to continue an upgrade action from the place where it stopped after the customer has corrected the problem.</p>

The following figure shows the Software Upgrade View accessed from the Card View.

**Software Upgrade View accessed from Card View**

MG 9000 Software Upgrade Element: 1

MG9000

**Upgrade Originator**

MG 9000 Name: VOIP10 1

Originating View: GUI: ITX Card: NE-1 Frame-1 Shelf0 Slot-14

**Upgrade State:**

Upgrade Status: Waiting for Configure

Upgrade Action:

Upgrade Type:

**Upgrade Type Data:**

Upgrading:

Load Server:

Load Server User Id:

Load:

**Upgrade Instructions & Results:**

Press Configure to invoke the Upgrade Configuration Wizard.  
Or press Version List to see all the versions of the cards.  
Or press History to see the results of previous upgrades.

History Refresh Configure Version List Abort Retry Close

When performing an upgrade of multiple card types, from the Frame View of the MG 9000 to be upgraded, select Actions->Software Upgrade. The Software Upgrade View accessed from the Frame View appears as shown in the following figure.

**Software Upgrade View accessed from Frame View**

MG 9000 Software Upgrade Element: 1

MG9000

**Upgrade Originator**

MG 9000 Name: VOIP10 1

Originating View: GUI: MG9000 Element 1

**Upgrade State:**

Upgrade Status: Waiting for Configure.

Upgrade Action:

Upgrade Type:

**Upgrade Type Data:**

Upgrading:

Load Server:

Load Server User Id:

Load:

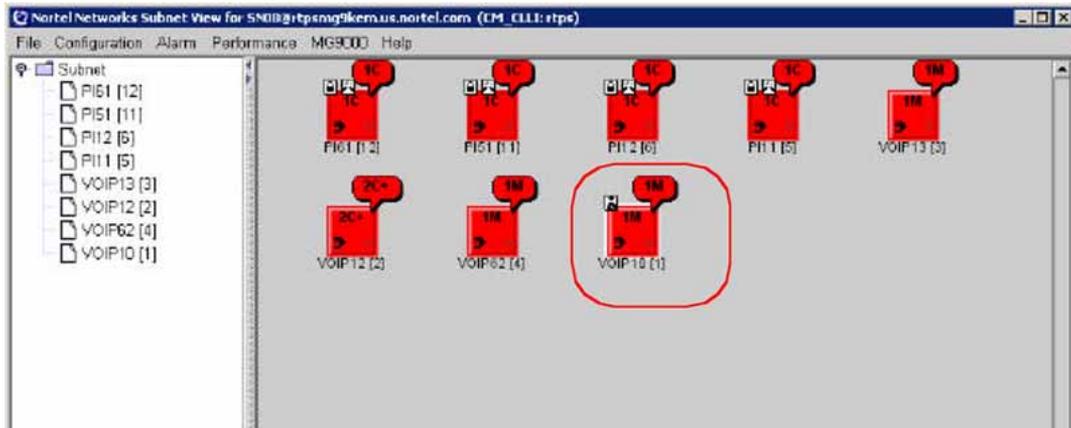
**Upgrade Instructions & Results:**

Press Configure to invoke the Upgrade Configuration Wizard.  
Or press Version List to see all the versions of the cards.  
Or press History to see the results of previous upgrades.

History Refresh Configure Version List Abort Retry Close

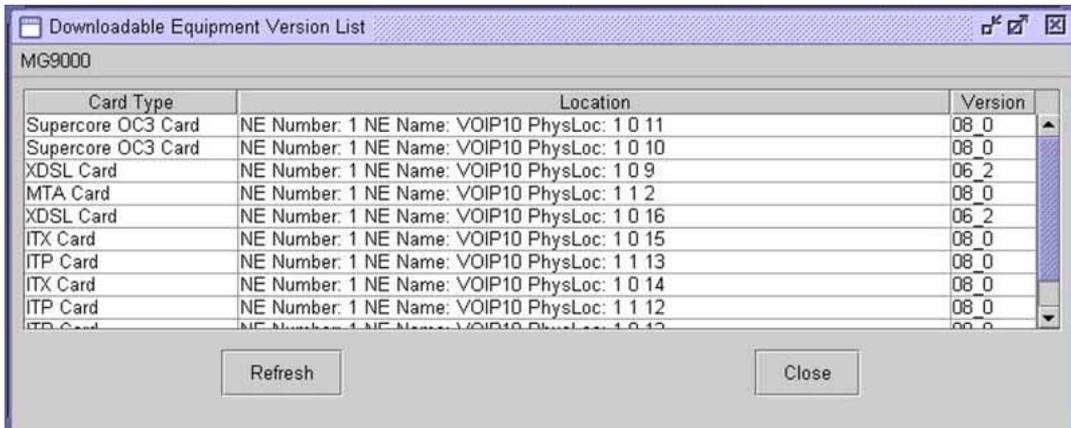
The following figure shows the Subnet View with the download icon on top of the MG 9000 on which a software download is in progress. The download icon also appears at the card and shelf views. The icon remains until the upgrade is complete or an abort completes.

**Subnet View showing download icon**



The following figure shows the version list that appears in response to selecting the Version List button on the Software Upgrade View. The version list shows all common cards on the selected MG 9000 and the software version of the loads in the card.

**Version list**



## Upgrade Wizard overview

This section provides an overview of the upgrade wizard which is accessed from the Software Upgrade View.

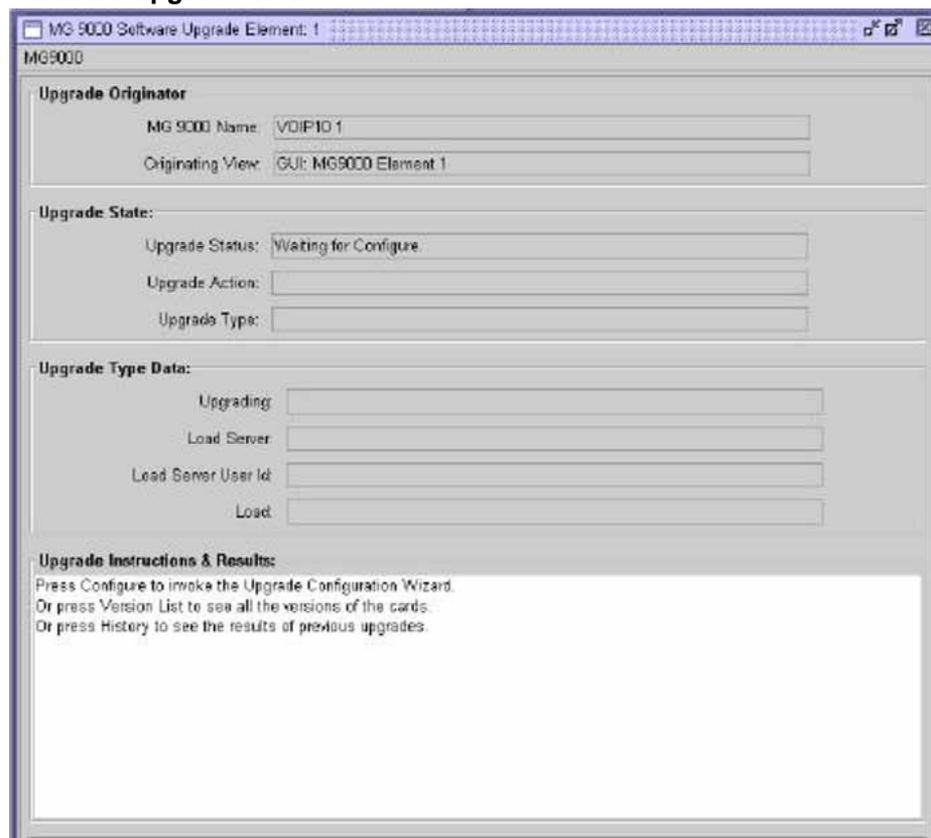
The Software Upgrade View contains the following text fields:

- MG 9000 Name - provides the name and number of the MG 9000 selected for upgrade
- Originating view - provides the frame view of the MG 9000 view from which the software upgrade request has been originated
- Upgrade status - is set to Waiting for Configure

**Note:** All other fields are blank and then updated when the configuration step is completed and the Configure button is enabled. The user is instructed to perform the Configure step in the Upgrade Instructions & Results texts area.

The following figure shows the Software Upgrade View.

### Software Upgrade View



MG 9000 Software Upgrade Element: 1

MG9000

**Upgrade Originator**

MG 9000 Name: VOIP101

Originating View: GUI: MG9000 Element 1

**Upgrade State:**

Upgrade Status: Waiting for Configure

Upgrade Action:

Upgrade Type:

**Upgrade Type Data:**

Upgrading:

Load Server:

Load Server User Id:

Load:

**Upgrade Instructions & Results:**

Press Configure to invoke the Upgrade Configuration Wizard.  
Or press Version List to see all the versions of the cards.  
Or press History to see the results of previous upgrades.

After the user clicks Configure, the Upgrade Wizard appears. The upgrade wizard is available in two forms, Card Upgrade Wizard and MG Upgrade Wizard, depending on how it was accessed. These two forms are described in the sections that follow.

## Overview of Card Upgrade Wizard

This section provides an overview of the Card Upgrade Wizard. The Card Upgrade Wizard is accessed from the individual card view by selecting Actions->Software Upgrade from the menu bar and clicking on Configure in the Software Upgrade View.

The Upgrade Wizard consists of four panels. Each panel is a step in the Card Upgrade Wizard and all four steps are discussed in the following sections.

### Select the upgrade type: Step 1

Step 1 allows the user to specify the upgrade type by clicking the pull-down menu. The following three upgrade types are available:

- upgrade this card - upgrade the individual card from which this panel was launched
- protection group - upgrade the card from which this panel was launched and its redundant mate (though this option is available in the Card upgrade wizard, it is recommended that upgrades of a protection group be performed using the "[Overview of MG Upgrade Wizard](#)" (page 433)).
- all cards of this type - upgrade all cards of the selected type in the MG 9000 (though this option is available in the Card upgrade wizard, it is recommended that upgrades of all card of a given type be performed using the "[Overview of MG Upgrade Wizard](#)" (page 433)).

The upgrade procedures for protection group and all card type upgrades are similar to the upgrade procedures for single card upgrades. The difference are:

- upgrading of multiple cards instead of a single card with upgrade icon appearing on all cards being upgraded
- Swact occurs without user intervention as part of the upgrade

The following figure shows step 1 of the Card Upgrade Wizard.

**Card Upgrade Wizard: Step 1**
**Select a load server: Step 2**

Step 2 allows the user to enter a load server IP address, a userid and password to be used to access the load server. The last six entries for the server IP address are remembered. The user can select between the last six entries or enter a new one. The user is not allowed to move to the next panel until all the entries on this panel are completed with valid data. If the entered IP address, userid, or password are not valid, an error message appears and the user must correct the entry for the upgrade process to proceed to the next step.

The following figure shows step 2 of the Card Upgrade Wizard.

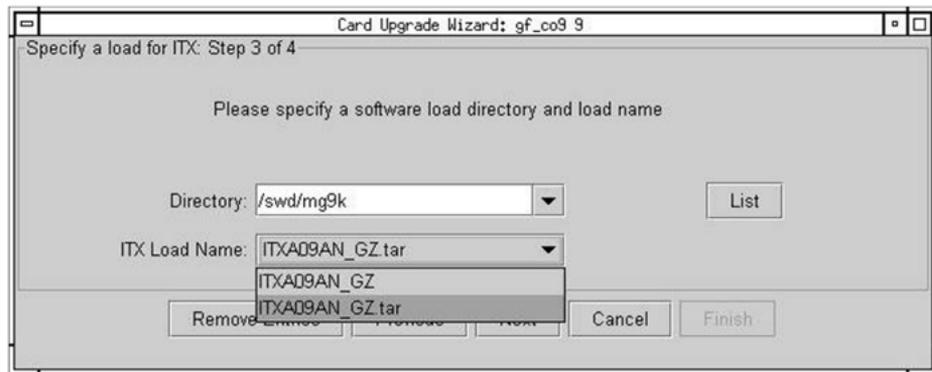
**Card Upgrade Wizard: Step 2**
**Specify a load: Step 3**

Step 3 allows the user to enter the directory and load name to be used for the upgrade. If the entered directory is incorrect, a message appears to inform the user and the directory must be corrected for the upgrade to proceed.

Click the List button to retrieve the files from the load server and the combo box is populated with MG 9000 patched image (PI) file names (identified by the .tar extension on the filename). Choose a file from the list.

The following figure shows step 3 of the Card Upgrade Wizard.

#### Card Upgrade Wizard: Step 3

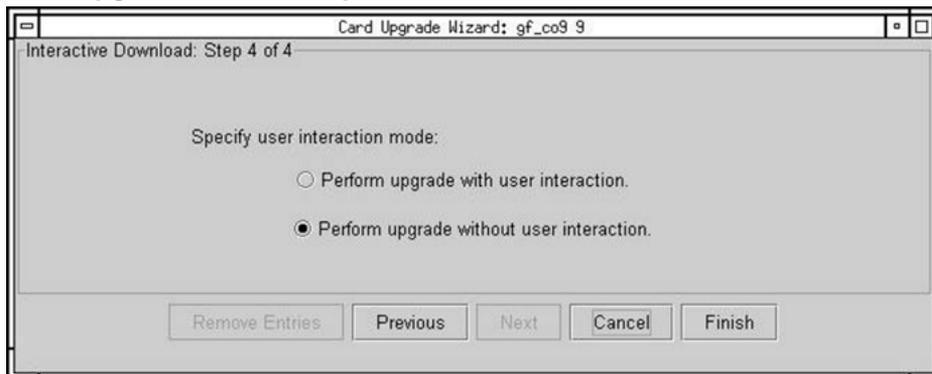


#### Specify user interaction mode: Step 4

Step 4 prompts for the user to select between performing the upgrade with user interaction or without user interaction.

The following figure shows step 4 of the Card Upgrade Wizard with interactive download selected.

#### Card Upgrade Wizard: Step 4



The two types of user interaction upgrades are as follows:

- Perform upgrade without user interaction - This mode is recommended. When the user selects this mode and clicks Finish, the system responds with an Upgrade button on the Software Upgrade View. After the user clicks Upgrade, the system continues with the successful completion of each action. The next action automatically executes without any input needed from the user. If an error occurs, the upgrade stops and the user must click Abort. Error messages will be output. Refer to "[Software upgrade errors and problem resolution](#)" (page 439) for information on responding to errors.

- Perform upgrade with user interaction - In this mode, the system responds with a Download button on the Software Upgrade View. The system then prompts for an Apply followed by an Accept. Refer to "[Software upgrade errors and problem resolution](#)" (page 439) for information on responding to errors.

**Note 1:** If a Protection group or All cards of this type upgrade is selected, during the Download action/phase of the upgrade, only one designated card gets the new software from the load server. All other cards involved with the upgrade get the new software from that card.

**Note 2:** If a Protection group or All cards of this type upgrade is selected, during an upgrade, a controlled, non-user requested Swact occurs. The system raises redundancy notifications as normal while Apply action is occurring; only an encountered error terminates its progress.

The user interaction is as follows:

- Apply - After the system successfully completes the Download, the system prompts the user to click Apply. Apply causes the card to restart. After the restart has completed, the card executes the new, upgraded software. An automatic SWACT and restart of the mate occurs as part of the Apply action. (Not applicable to single card upgrades.)
- Accept - After the system successfully completes the Apply the system prompts the user to click Accept. Accept causes the card to complete its upgrade activity, which takes a few seconds. The system notifies the user when the Accept is completed. Exit the upgrade view by pressing Close. Verify the upgrade is complete by viewing History.

After the user clicks Finish, the Upgrade Wizard disappears and the Software Upgrade View prompts the user to click Download (with user interaction) or Upgrade (without user interaction) to start the upgrade process. Upgrade progress is reported in the Upgrade Instructions & Results window of the Software Upgrade View.

## Overview of MG Upgrade Wizard

This section provides an overview of the MG Upgrade Wizard. The MG Upgrade Wizard is accessed from the Frame View by selecting Actions->Software Upgrade from the menu bar and clicking Configure in the Software Upgrade View.

The upgrade wizard consists of multiple steps (panels), depending on the actions chosen in step 1. Each panel is a step in the MG Upgrade Wizard and all steps are discussed in the following sections.

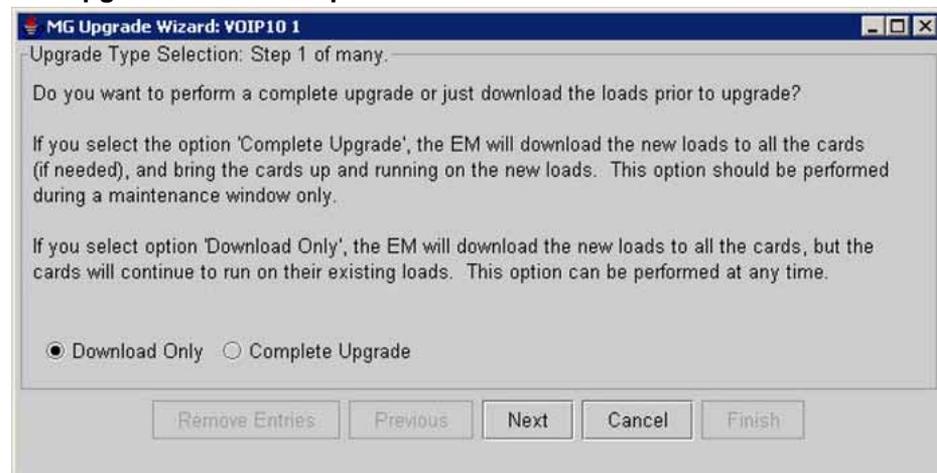
### Select the upgrade type: Step 1

Step 1 allows the user to select the upgrade type: complete upgrade or just download the loads prior to an upgrade. As noted in the GUI, select

- Complete Upgrade - the MG 9000 Manager downloads the loads to all the cards, if needed, and brings the cards up and running on the new loads. This option should be performed during a maintenance window only.
- Download Only - the MG 9000 Manager downloads the loads to all the cards but the cards continue to run on their existing loads. This option can be performed at any time.

The following figure shows step 1 of the MG Upgrade Wizard

#### MG Upgrade Wizard: Step 1

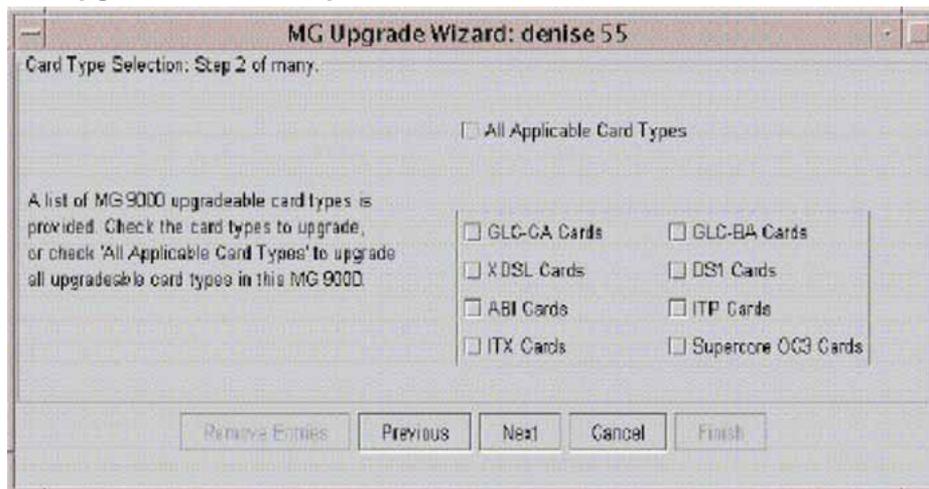


### Select the card type: Step 2

Step 2 allows the user to specify All Card Types, one card type, or multiple card types. The MG Upgrade Wizard upgrades the software in all cards of the selected type.

The following figure shows step 2 of the MG Upgrade Wizard with multiple cards selected.

## MG Upgrade Wizard: Step 2



The MG Upgrade Wizard contains a list of card types available to be upgraded on the given MG 9000. One or more card types can be selected for upgrade. The user can also select all the card types on a given MG 9000 by selecting All Card Types. This panel enables or disables the check boxes for GLC-BA, GLC-CA, MTA and xDSL card types based on the user's selection in the Upgrade Type Selection Type, step 1.

**Note:** The selections GLC-BA Cards and GLC-CA Cards in the Upgrade Wizard are not used during an upgrade of other MG 9000 cards. The other MG 9000 cards must already be upgraded prior to any upgrade of the Field Programmable Gate Array software load in the GLC cards. The FPGA software load is to be upgraded only if there is a new release of the FPGA to address a field issue.

## Select a load server: Step 3

Step 3 allows the user to enter a load server IP address, a userid and password to be used to access the load server. The last six entries for the server IP address are remembered. The user can select between the last six entries or enter a new one. A user is not allowed to move to the next panel until all the entries on this panel are completed with valid data.

The following figure shows step 3 of the MG Upgrade Wizard.

**MG Upgrade Wizard: Step 3**
**Specify a load: Step 4**

Step 4 allows the user to enter the directory and load name to be used for the upgrade. Like the Card Upgrade Wizard discussed earlier, if the entered directory is incorrect, a message appears to inform the user and the directory must be corrected for the upgrade to proceed.

The following figure shows step 4 of the MG Upgrade Wizard.

**MG Upgrade Wizard, Step 4**

Click the List button to retrieve the files from the load server and the combo box is populated with PI file names (identified by the .tar extension on the filename). Choose a file from the list.

This step will continue to increment until the loads are specified for each card type that is part of the upgrade. When the load for last card in the upgrade is specified, click Finish. The load names entered for the selected card types are checked for version range validity (refer to "Upgrade version rules" (page 421)).

## Completion of configuration steps

When the configuration steps are completed, the MG Upgrade Wizard is closed and the third pane in the Software Upgrade view is modified to display the upgrade data for all the card types selected for upgrade. The MG 9000 can upgrade only one card type at a time, so the MG 9000 Manager automatically schedules the upgrade for the selected card types in sequence. The third pane contains the card type for which the upgrade is in progress in the MG 9000.

The third pane also contains a tabbed panel with a tab for each card type selected for upgrade. Each tabbed entry contains the load server, the user identifier, and the full path load name for that card type. The card type being upgraded is on the top of the tabbed pane.

## Limitations

The following limitations apply to upgrading GLC, MTA, and xDSL cards:

- Upgrade the FPGA configuration load in the NTNY53BA GLC32 or NTNY53CA GLC12 card only when it is recommended by Nortel to resolve a field issue. The FPGA load upgrade process is not used for routine software download activities.
- Prior to upgrading MTA or xDSL cards, the MG 9000 Manager verifies all the cards are in an unlocked/enabled state. If any card is not in the correct state, the MG 9000 Manager will not perform the upgrade.
- To upgrade MTA and xDSL cards, the MG 9000 Manager locks the card, downloads the load to the card, and then unlocks the card. The order in which the MG 9000 Manager upgrades xDSL cards cannot be specified as part of the upgrade.
- The lock request of an XDSL card fails if the card has an active call. If the lock request fails for a given xDSL card, the MG 9000 Manager notes the failure and attempts to upgrade the remaining xDSL cards. Once the MG 9000 Manager has upgraded the remaining xDSL cards, the MG 9000 Manager halts the upgrade process. The MG 9000 Manager reports that some of the xDSL cards cannot be upgraded.
- If the download or unlock of any MTA or xDSL card fails, the MG 9000 Manager immediately halts the upgrade process.

- If an MTA or xDSL card already has the load file specified in the upgrade request, the MG 9000 Manager considers the card already upgraded and moves on to the next card to upgrade.
- When upgrading xDSL cards, the MG 9000 Manager can upgrade only those cards with supported hardware. If a given xDSL card does not have a CLEI code of VA1AAAAAA, the MG 9000 Manager skips that card and moves on to the next card to upgrade.
- If the user aborts an upgrade while the MG 9000 Manager is upgrading the xDSL cards, the MG 9000 Manager returns all cards to an unlocked state. However, the MG 9000 Manager will not roll back the loads on any of the cards. For instance, assume the user is upgrading all five xDSL cards on a given node. Assume the user aborts the upgrade after the first two cards have upgraded and a third card is in the process of upgrading. The MG 9000 Manager halts the upgrade process after the third card completes its upgrade. In the end, three xDSL cards are running the new load and two xDSL cards are running the old load.

When a user begins the upgrade, the MG 9000 Manager stops the database. The database will not restart until the upgrade process completes.

## Software upgrade errors and problem resolution

The following table lists the potential errors that arise at various steps in the MG 9000 software upgrade process, the cause, and recovery actions.

### MG 9000 software upgrade errors and problem resolution

Error type	Possible cause	Recovery action
<b>Upgrade provisioning errors</b>		
Invalid file type	This error is received if the card type selected is invalid for the load file name provided. Every load file name has the card type embedded within it.	Ensure the load file name is valid for the card type to be provisioned, then try again.
Invalid Version	This error is received if the version number embedded within the load file name is invalid for this gateway. For example, if it is only valid to upgrade to versions 5 or 6 and the loadfile name contains version 8, an error is displayed.	Ensure the load file name version is valid for the attempted upgrade, then try again.
Invalid State	This card is locked or active.	<p>If this card is active and does have a mate, the request will be denied. First Swact/Spare the card to its mate and continue.</p> <p>If this card is inactive, but locked, first unlock the card and continue.</p>
<b>Download errors</b>		
FTP server related	<ul style="list-style-type: none"> <li>incorrectSDM loadfile/path permissions</li> <li>floating IP configuration error</li> <li>network connection failure identified during the provisioning activity</li> <li>Preshared keys between the MG 9000 and the MG 9000 Manager do not match</li> </ul>	<p>Abort the upgrade. Check provisioned data for validity and provision another upgrade. For the SSH host key mismatch error, do one of the following procedures:</p> <p>For pre-SN09FF gateways, remove the SSH keys on the MG 9000:</p> <ul style="list-style-type: none"> <li>1. Go to the MG 9000 Local Craft Interface (LCI) on the active DCC card.</li> <li>2. Click <b>Maintenance</b>. Select the Active DCC card, and select <b>Debug Cmds</b>.</li> <li>3. Enter command number 6 (/keymgmt/clrsshclientkeys) to clear the SSH keys from the MG 9000.</li> </ul>

Error type	Possible cause	Recovery action
	<ul style="list-style-type: none"> <li>SSH host key mismatch between the gateway and the SDM/CBM</li> </ul>	<p>For SN09FF gateways, do the following steps:</p> <ul style="list-style-type: none"> <li>1. At the MG 9000 Manager, from the NE desktop view menu bar, select <b>Services &gt; Load Server SSH Authentication</b>.</li> <li>2. Enter the load server (SDM/CBM) IP address and click <b>Apply</b>.</li> <li>3. If validation is successful, a dialog box appears with a SSH validation is complete message. If validation fails because of an SSH key mismatch or the MG 9000 does not have keys cached for the server, a fingerprint icon appears with an Accept or Reject option.</li> <li>4. If you click <b>Accept</b>, the MG 9000 will distribute the new SSH keys to all the cards in the network element, and when complete, an SSH validation complete message appears. If you click <b>Reject</b>, the MG 9000 discards the new SSH keys. The existing SSH key cache is not changed. If you entered an incorrect load server (SDM/CBM) IP address, an SSH validation failed message appears.</li> </ul>
Corrupt File	<ul style="list-style-type: none"> <li>an incompatible load file provisioned for this card. For instance, if the card type is ITP, the load file name must include ITP. The same is true for other cards.</li> <li>insufficient memory for an image file</li> </ul>	<p>Abort the upgrade.</p> <ul style="list-style-type: none"> <li>For the incompatible load file error, check the file name type and provision another upgrade.</li> <li>For the insufficient memory error, go to dshell and do a filesys/finfo and look at the freespace on the volume. It should be about three times the size of the image file.</li> </ul>
Node Not Responding	The card is undergoing a maintenance operation or is in an otherwise invalid state (such as, restarting) or is not running.	Go to the Card View and verify the card status. If the card status appears correct, the error is possibly due to a longer than expected communication delay. Abort the upgrade and try again
Flash exhaust	There is insufficient flash memory to allow the download of the software to the card.	Contact Nortel for assistance to restore space on the flash memory.
<b>Apply errors</b>		

Error type	Possible cause	Recovery action
State	If this card is Active, an Apply will fail if this card has a mate.	Abort the upgrade. Cause a redundancy action (Swact or Spare) to occur. This card was possibly Inactive during the provisioning of the upgrade. A card is no longer Active when a redundancy action occurs.
Node Not Responding	This card is undergoing a maintenance operation, is in an otherwise invalid state (such as, restarting) or is not running.	Go to the Card View and verify the card status, if the card status appears correct the error is possible due to a longer than expected communication delay. Abort this upgrade and try again.
SwactDataSync Multi-Node Only	Mate cards in a protection group are NOT in data sync; a required Swact has failed or will not be executed	<p>Go to the Card View and lock the card, then go to the Card View for the Inactive mate and unlock the card. The unlock action will cause a restart (since they are not in data sync).</p> <p>Once the Inactive card has completed its restart, attempt to Abort.</p> <p><b>Note:</b> If after multiple tries data sync is not achieved, contact Nortel for further guidance. Additional upgrades are not possible until this problem is resolved.</p>
SwactMateState Multi-Node Only	For reasons other than not in DataSync, the Active card refuses to give up activity (possibly due to faults on the inActive card).	<p>Determine what the fault state or problem with the inActive card is and correct it.</p> <p>Once the inActive card is in a valid state, attempt to Abort.</p> <p><b>Note:</b> If you cannot correct the error, contact Nortel for further guidance. Additional upgrades are not possible until this problem is resolved.</p>
SwactMateUnavail Multi-Node Only	A communication problem exists between the Inactive and the Active cards. A Swact is not allowed.	<p>Resolve the communication problem.</p> <p>Once the Inactive card is in a valid state, attempt to Abort.</p> <p><b>Note:</b> If you cannot correct the error, contact Nortel for further guidance. Additional upgrades are not possible until this problem is resolved.</p>

Error type	Possible cause	Recovery action
SwactError  Multi-Node Only	A generic error associated with a Swact request, but enough information cannot be obtained for the Upgrade subsystem to identify the cause.	Contact your maintenance administrator to identify and resolve the problem.  Once the card(s) are in a valid state, attempt to Abort.  <b>Note:</b> If you cannot correct the error, contact Nortel for further guidance. Additional upgrades are not possible until this problem is resolved.
Generic <b>Accept errors</b>	See the previous entry.	Contact Nortel.
Node Not Responding	The card is undergoing a maintenance operation, is in an otherwise invalid state (such as restarting) or is not running.	Go to the Card View and verify the card status. If the card status appears correct the error is possibly due to a longer than expected communication delay. Abort the upgrade and try again.
GENERIC <b>Abort errors</b>	See the previous entry.	Contact Nortel.
Node Not Responding	The card is undergoing a maintenance operation, is in an otherwise invalid state (such as restarting) or is not running.	Go to the Card View and verify the card status. If the card status appears correct, the error is possibly due to a longer than expected communication delay. Abort this upgrade and try again.
SwactDataSync	Mate cards in a protection group are NOT in data sync; a required Swact has failed or will not be executed	Go to the Card View and lock, then go to the Card View for the inActive mate and unlock the card. The unlock action will cause a restart (since they are not in data sync).  Once the inActive card has completed its restart, attempt to Abort.  <b>Note:</b> If after multiple tries data sync is not achieved, contact Nortel for further guidance. Additional upgrades are not possible until this problem is resolved.

Error type	Possible cause	Recovery action
SwactMateState	For reasons other than not in DataSync, the Active card refuses to give up activity (possibly due to faults on the Inactive card).	<p>Determine the fault state or problem with the inActive card and correct it.</p> <p>Once the Inactive card is in a valid state, attempt to Abort.</p> <p><b>Note:</b> If you cannot correct the error, contact Nortel for further guidance. Additional upgrades are not possible until this problem is resolved.</p>
SwactMateUnavailable	There is a communication problem between the Inactive and Active cards. A Swact is not allowed.	<p>Resolve the communications issue.</p> <p>Once the Inactive card is in a valid state, attempt to Abort.</p> <p><b>Note:</b> If you cannot correct the error, contact Nortel for further guidance. Additional upgrades are not possible until this problem is resolved.</p>
SwactError	This is a generic error associated with a Swact request, but enough information cannot be obtained for the Upgrade subsystem to identify the cause.	<p>Contact your maintenance administrator to identify and resolve the problem.</p> <p>Once the card(s) are in a valid state, attempt to Abort.</p> <p><b>Note:</b> If you cannot correct the error, contact Nortel for further guidance. Additional upgrades are not possible until this problem is resolved.</p>
GENERIC	See the previous entry.	Contact Nortel.

## Card upgrade with user intervention

### When to use this procedure

Use this procedure when to upgrade a single card or a protection group in an MG 9000. This procedure provides the steps to perform a software upgrade in a DCC, ITP, ITX, ABI, or DS1 card with user interaction.

### Prerequisites

Clear all alarms on the card to be upgraded before proceeding with the upgrade process.

### Action

#### Card upgrade with user intervention

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 From the Subnet View, select the network element (NE) containing the card to be upgraded. Double-click the NE icon and the Frame View appears.
- 2 Double-click the shelf containing the card and the Shelf View appears.
- 3 Double-click the card to be upgraded and the Card View appears.
- 4 If performing a single card upgrade, from the Card View of the card selected for upgrade, lock the card by changing the Administrative state to Lock from the Administrative state pull-down menu.
- 5 From the Card View of the card selected for upgrade, select Actions->Software Upgrade from the menu bar.
- 6 The Software Upgrade view appears as described in "[Software Upgrade View](#)" (page 422).

There are four possible messages in the Card Upgrade View at the time it appears:

- If a previous user closed the view before an abort was completed, the abort is possibly still in progress. An indication to wait until the abort is completed is displayed. In this case, the Configure button is disabled. Either wait for the abort to complete or close the view.

A message will appear notifying when the abort is completed, and the Configure button is enabled.

- Another user is performing an upgrade on a card on the same MG 9000. In this case, the user can close the view or abort the upgrade in process and start a new upgrade.
  - If no upgrade activity is in progress on the selected MG 9000, the user is prompted to press the Configure button to start the upgrade.
  - If the floating IP address has not been provisioned, the system prompts you to provision it. After the floating IP address is provisioned, continue with the procedure.
- 7 Press the Configure button to start the Upgrade wizard. The upgrade wizard is created as described in "[Upgrade Wizard overview](#)" (page 429).
  - 8 Enter the parameters in the first three panels as described in "[Upgrade Wizard overview](#)" (page 429).
  - 9 Select Perform Upgrade with user interaction in the last panel. Press Finish to completed the configuration. The user is returned to the Card Upgrade View. The following figure shows the Upgrade View with the system prompting the user to press the Download button.

**Software Upgrade View**

MG9000

**Upgrade Originator**

MG 9000 Name: PL7 7

Originating View: OC3 Card: NE-7 Frame-1 Shelf-0 Slot-10

**Upgrade State:**

Upgrade Status: Configure step completed.

Upgrade Action: Configure

Upgrade Type: Single Node

**Upgrade Type Data:**

Upgrading: OC3 Card: NE-7 Frame-1 Shelf-0 Slot-10

Load Server: 47.142.84.205

Load Server User Id: anonymous

Load: mg9k\_loads/SN06\_02/SCOA06ET\_2\_GZ

**Upgrade Instructions & Results:**

Press Configure to invoke the Upgrade Configuration Wizard.  
 Or press Version List to see all the versions of the cards.  
 Or press History to see the results of previous upgrades.  
 Configuration Completed.

Press Download Button to start upgrade with user interaction.

History Refresh Download Version List Abort Close

- 10** Press Download to request the MG 9000 to perform the download step. When the download is complete, the results are displayed in the result area of the Software Upgrade View as follows:
- The download step was successful. The step button changes to Apply. The user is prompted to perform the Apply step
  - The download step failed. An indication of the failure is indicated. Possible cause of failure could be:
    - communication problems between the GUI client and the mid-tier layer, between the mid tier layer and the MG 9000 Manager, between the MG 9000 Manager and the MG 9000.

- invalid configuration parameters. The user could abort the upgrade. When the upgrade is aborted, the step button changes back to Upgrade.
- 11** Press the Apply button for the MG 9000 to perform the apply step. When the apply is completed the results are displayed in the result area of the card upgrade view as follows:
- The Apply step was successful. The step button changes to Accept. Go to [step 12](#).
  - The Apply step failed. An indication of the failure is indicated. Possible cause of failure could be:
    - communication problems between the GUI client and the mid-tier layer, between the mid tier layer and the MG 9000 Manager, between the MG 9000 Manager and the MG 9000. The user must abort the upgrade. After that it could configure again or close.
    - card is locked (during protection group upgrade) or involved in a maintenance activity. The system prompts to unlock or wait until the maintenance activity is completed. Press Apply again.
- 12** Press Accept to complete the upgrade. The Accept and Abort buttons are disabled. When the Accept is completed, the results are displayed in the result area of the card upgrade view as follows:
- The accept step was successful. Close the Upgrade View.
  - The accept step failed. An indication of the failure is indicated. Possible cause of failure could be communication problems between the MG 9000 Manager client and the mid-tier server, between the mid-tier server and the master server, between the master server and the MG 9000. Abort the upgrade. Abort the upgrade by pressing the Abort button to cancel the remainder of the upgrade. Configure again or close.
- 13** When the accept is completed, close the upgrade view. Apply patches. Refer to "Applying patches using the NPM" procedure in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450 for patching procedures.
- 14** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Card upgrade without user intervention

### When to use this procedure

Use this procedure to upgrade the software in a single card without user intervention. This procedure provides the steps to perform a software upgrade in a single DCC, ITP, ITX, ABI, or DS1 card without user interaction.

**Note:** This procedure applies to single card upgrades only, not multiple card upgrades.

### Prerequisites

Clear all alarms on the card to be upgraded before proceeding with the upgrade process.

### Action

#### Card upgrade without user intervention

Step	Action
------	--------

*At the MG 9000 Manager*

- |   |  |
|---|--|
| 1 | From the Subnet View, select the network element (NE) containing the card to be upgraded. Double-click the NE icon and the Frame View appears.   |
| 2 | Double-click the shelf containing the card and the Shelf View appears.   |
| 3 | Double-click the card to be upgraded and the Card View appears.  |
| 4 | If performing a single card upgrade, from the Card View of the card selected for upgrade, lock the card by changing the Administrative state to Lock from the Administrative state pull-down menu. |
| 5 | From the Card View of the card selected for upgrade, select Actions->Software Upgrade from the menu bar  |
| 6 | The Software Upgrade view is described in " <a href="#">Software Upgrade View</a> " (page 422). The Software Upgrade View appears as shown in the following figure.                                |

## Software Upgrade View

MG 9000 Software Upgrade Element: 1

MG9000

**Upgrade Originator**

MG 9000 Name:

Originating View:

**Upgrade State:**

Upgrade Status:

Upgrade Action:

Upgrade Type:

**Upgrade Type Data:**

Upgrading:

Load Server:

Load Server User Id:

Load:

**Upgrade Instructions & Results:**

Press Configure to invoke the Upgrade Configuration Wizard.  
 Or press Version List to see all the versions of the cards.  
 Or press History to see the results of previous upgrades.

History Refresh Configure Version List Abort Close

Four possible messages are displayed by the Software Upgrade View. The messages indicate the following:

- If a previous user closed the view before an abort was completed, the abort may still be in progress. An indication to wait until the abort is completed is displayed. In this case, the Configure button is disabled. Either wait for the abort to complete or close the view.

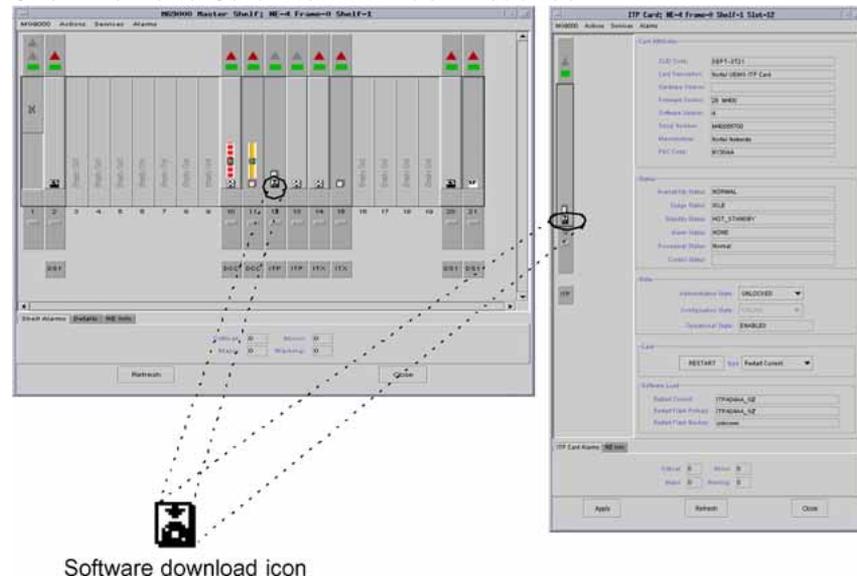
A message appears notifying when the abort is complete, and the Configure button is enabled.

- Another user is performing an upgrade on a card on the same MG 9000. In this case, the user can close the view or abort the upgrade in process and start a new upgrade.

- If no upgrade activity is in progress on the selected MG 9000, the user is prompted to press the Configure button to start the upgrade.
  - Select Upgrade to continue with the upgrade without user interaction. If the floating IP address has not been provisioned the user is prompted to provision it. After that, continue with the upgrade procedure.
- 7 Press the Configure button to start the Upgrade wizard. The Card Upgrade Wizard appears. See "[Upgrade Wizard overview](#)" (page 429).
  - 8 Enter the parameters in the first three panels as described in "[Upgrade Wizard overview](#)" (page 429).
  - 9 Select Perform Upgrade without user interaction in the last panel. Press Finish to complete the configuration.
  - 10 Click the Upgrade button to begin the upgrade process
  - 11 Messages indicating the progress of the upgrade, download, apply, and accept steps are displayed. If a step fails, a message is displayed indicating the reason. The user can abort and perform the configure step again or close the view.

The download icon appears in the Shelf View and the Card View. The icon remains until the upgrade is completed or aborted.

#### Shelf View and Card View with download icon



- 12 When the accept is completed, close the upgrade view. Apply patches. Refer to procedure "[Applying patches using the NPM](#)"

in *Nortel Carrier Voice over IP Network Upgrades and Patches*, NN10440-450 for patching procedures.

- 13 If problems occur, abort the upgrade by pressing the Abort button to cancel the remainder of the upgrade.
- 14 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## MG prep download

### When to use this procedure

Use the following procedure to pre-download software loads to multiple cards and protection groups without user intervention. If you select the "Download Only" option, the system downloads the software to the cards, but it does not upgrade them. The cards continue to run on their existing loads until the new software is activated.

This procedure can be performed at any time to save time during maintenance windows. When all of the cards have been prep downloaded, they can be upgraded during a maintenance window, which will activate the pre-downloaded software.

This procedure provides the steps to perform a software upgrade in DCC, ITP, ITX, ABI, and DS1 cards without any requirement for user interaction.

### Prerequisites

The Download Only option will automatically perform a pre-check on the flash memory to verify that the card has the required flash memory capacity. If a failure occurs, the system generates a Flash exhaust software error. For further details, refer to ["Software upgrade errors and problem resolution" \(page 439\)](#) to address the issue.

### Action

#### MG prep download

Step	Action
------	--------

##### *At the MG 9000 Manager*

- 1 At the Frame View of the MG 9000 selected for upgrade, click the Actions menu.
- 2 At the Actions menu, select Software Upgrade. The MG 9000 Software Upgrade view is created as described in ["Software Upgrade View" \(page 422\)](#).
- 3 Check the Upgrade Originator pane in the MG 9000 Software Upgrade View to ensure the MG 9000 Name and Originating View (NE number) represent the MG 9000 to be upgraded.
- 4 Press the Configure button to start the MG Upgrade wizard. The Upgrade Type Selection, Step 1 appears. Choose Download Only. Next, the MG Upgrade Wizard, Card Type Selection, Step 2 appears.

- 5 Select the card types to upgrade or select all card types by selecting All Applicable Card Types. A check appears in the corresponding box next to the selection.
- 6 Enter the load server information. Use the following table to determine the next step.

If upgrading	Do
only one card type	<a href="#">step 7</a>
multiple card types	<a href="#">step 8</a>

- 7 In the MG Upgrade Wizard, specify a load, the load directory, and the load name. The upgrade now begins. Go to [step 9](#).
- 8 In the MG Upgrade Wizard, specify a load, the load directory, and the load name for the card type (such as, SCOA09AZ\_1\_GZ.tar). The system repeats this step in succession for each card type in the following order: DS1, ABI, ITP, ITX, and DCC. The load names are checked for version range validity.

When the MG Upgrade Wizard closes, the MG 9000 Software Upgrade View appears showing the Upgrade Type Data panel. This panel displays the upgrade data for all the card types selected for upgrade. The panel also reports the card type for which the upgrade is in progress in the MG 9000. Go to [step 9](#).

**Note:** The MG 9000 upgrades one card type at a time. The MG 9000 Manager schedules the upgrade for the selected card types in sequence.

- 9 This procedure is complete.

---

—End—

---

## MG upgrades

### When to use this procedure

Use the following procedure to upgrade the software in multiple cards and protection groups without user intervention. This procedure provides the steps to perform a software upgrade in DCC, ITP, ITX, ABI, and DS1 cards without user interaction.

### Prerequisites

Clear all alarms on the cards to be upgraded before proceeding with the upgrade process.

### Action

#### MG upgrades

Step	Action
------	--------

*At the MG 9000 Manager*

- 1 At the Frame View of the MG 9000 selected for upgrade click the Actions menu.
- 2 At the Actions menu select Software Upgrade. The MG 9000 Software Upgrade view is created as described in "[Software Upgrade View](#)" (page 422).
- 3 Check the Upgrade Originator pane in the MG 9000 Software Upgrade View to ensure the MG 9000 Name and Originating View (NE number) represent the MG 9000 to be upgraded.
- 4 Press the Configure button to start the MG Upgrade wizard. The Upgrade Type Selection, Step 1 appears. Choose Complete Upgrade. Next, the MG Upgrade Wizard, Card Type Selection, Step 2 appears.
- 5 Select the card types to upgrade or select all card types by selecting All Applicable Card Types. A check appears in the appropriate box next to the selection.
- 6 Enter the load server information. Use the following table to determine the next step.

If upgrading	Do
only one card type	<a href="#">step 7</a>
multiple card types	<a href="#">step 8</a>

- 7 In the MG Upgrade Wizard, Specify a load, specify the load directory and load name. The upgrade now begins. Go to [step 10](#).
- 8 In the MG Upgrade Wizard, Specify a load, specify the load directory and load name for the card type (such as, SCOA09AZ\_1\_GZ.tar). The system repeats this step in succession for each card type in the following order: DS1, ABI, ITP, ITX, and DCC. The load names are checked for version range validity.  
  
When the MG Upgrade Wizard closes, the MG 9000 Software Upgrade View appears with the Upgrade Type Data panel updated to display the upgrade data for all the card types selected for upgrade and reports the card type for which the upgrade is in progress in the MG 9000. Go to [step 10](#).  
  
**Note:** The MG 9000 upgrades one card type at a time. The MG 9000 Manager schedules the upgrade for the selected card types in sequence.
- 9 Click the Upgrade button to begin the upgrade process.
- 10 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Downloading software into the MTA card

### When to use this procedure

Use this procedure to update software onto an MTA card. The Software Download Manager menu option provides access to a Software Download Manager window.

### Prerequisites

None

### Action

#### Downloading software into the MTA card

Step	Action
<i>At the MG 9000 Manager</i>	
1	At the Subnet View, double-click the MG 9000 that has the MTA card to which software is to be downloaded. The Frame View appears.
2	At the Frame View, double-click the shelf in which the MTA card resides. The Shelf View appears.
3	At the Shelf View, double-click the slot in which the MTA card resides. The card view appears.
4	Select the Locked option for the Administrative Status in the Status box. The card must be Locked prior to requesting a download.
5	From the MTA Card View menu level, select Actions->Software Download Manager.
6	Enter data in the fields as follows: <ul style="list-style-type: none"> <li>• File Path - the path and name of the file on the load server to be downloaded to the card (/mg9k/&lt;loadname&gt;)</li> <li>• IP address - the file location (IP address)</li> <li>• Server userName - the login name for the server where load resides</li> <li>• Server password - the password for the server where load resides</li> <li>• Select Force Download if forced download is required. The Force option is needed only when the card must be reloaded with the same load that already exists on the card.</li> </ul>

- 7 Select the Download button at the bottom of the Software Download Manager window.

Once the download is complete, the Load Status field indicates if the download was successful, and the software load being used by the card is displayed under Restart Current in the Software Load pane.

**Note:** After the software download is performed, a message appears stating that the MTA card is restarted.

Perform the download again, since the MTA card has a Primary and Backup load. When a download is performed, the Primary load becomes the Backup load and the new load becomes the Primary load. Performing the download twice makes the new load the Primary and the Backup load and guarantees the current load is the new load.

- 8 After the second download is complete, from the MTA Card View set the Administrative Status of the MTA card to Unlocked by selecting the Unlocked option in the Status box.
- 9 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Downloading software into the xDSL card

### When to use this procedure

Use this procedure to download updated software onto an xDSL card. The Software Download Manager menu option provides access to a Software Download Manager window.

### Prerequisites

Perform this activity during periods of low traffic.

### Action

#### Downloading software into the xDSL card

Step	Action
<i>At the MG 9000 Manager</i>	
1	At the Subnet View, double-click the MG 9000 that has the xDSL card to which software is to be downloaded. The Frame View appears.
2	At the Frame View, double-click the shelf in which the xDSL card resides. The Shelf View appears.
3	At the Shelf View, double-click the slot in which the xDSL card resides. The card view appears.
4	Select the Locked option for the Administrative Status in the Status box. The card must be Locked prior to requesting a download.
5	From the xDSL Card View menu level, select Actions->Software Download Manager.
6	Enter data in the fields as follows: <ul style="list-style-type: none"> <li>• File Path - the path and name of the file to be downloaded to the card (/mg9k/&lt;loadname&gt;)</li> </ul> <p style="text-align: center;"><b>Note:</b> In certain offices, the file path is /swd/mg9k/</p> <ul style="list-style-type: none"> <li>• IP address - the file location (IP address)</li> <li>• Server userName - the login name for the server where load resides</li> <li>• Server password - the password for the server where load resides</li> </ul>

- Select Force Download if forced download is required. The force option is needed only when the card must be reloaded with the same load that already exists on the card.
- 7 Select the Download button at the bottom of the Software Download Manager window. When the download begins the download icon appears on the card.  
  
Once the download is complete, the download icon disappears and the initialization icon appears. Once initialization is complete, the icon disappears and the software load used in the card is displayed in the Software Load section of the Card View.
  - 8 If necessary, repeat [step 3](#) through [step 7](#) for all xDSL cards in the MG 9000 network element that must be upgraded. Otherwise skip this step.
  - 9 Unlock the card that was locked in [step 4](#).
  - 10 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Downloading software into the GLC cards

### When to use this procedure

Use this procedure to download an updated Field Programmable Gate Array (FPGA) configuration load into the following Global line cards

- NTNY53BA (GLC32)
- NTNY53CA (GLC12)

**Note:** Use this procedure only when it is recommended by Nortel to download an updated FPGA configuration load to resolve a field issue. This procedure is not to be used for routine software download activities.

The Software Download Manager menu option provides access to a Software Download Manager window.

### Prerequisites

Perform this activity only when recommended by Nortel and during periods of low traffic.

### Action

#### Downloading software into the GLC card

Step	Action
<i>At the MG 9000 Manager</i>	
1	At the Subnet View, double-click the MG 9000 that has the GLC card to which software is to be downloaded. The Frame View appears.
2	At the Frame View, double-click the shelf in which the GLC card resides. The Shelf View appears.
3	At the Shelf View, double-click the slot in which the GLC card resides. The card view appears.
4	Select the Locked option for the Administrative Status in the Status box. The card must be Locked prior to requesting a download.
5	From the GLC Card View menu level, select Actions->Software Download Manager.
6	Enter data in the fields as follows: <ul style="list-style-type: none"> <li>• File Path - the path and name of the file to be downloaded to the card (/mg9k/&lt;loadname&gt;)</li> </ul>

**Note:** In certain offices, the file path is /swd/mg9k/

- Server IP - the file location (IP address)
- Server userName - the login name for the server where load resides
- Server password - the password for the server where load resides
- Select Force Download if forced download is required. The force option is needed only when the card must be reloaded with the same load that already exists on the card.

**7** Select the Download button at the bottom of the Software Download Manager window. When the download begins the download icon appears on the card.

Once the download is complete, the download icon disappears and the initialization icon appears. Once initialization is complete, the icon disappears and the FPGA configuration load used in the card is displayed in the Configuration Load section of the Card View.

**8** If necessary, repeat steps [step 3](#) through [step 7](#) for all GLC cards in the MG 9000 network element that must be upgraded. Otherwise skip this step.

**9** Unlock the card that was locked in step [step 4](#).

**10** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

## Upgrade history

---

The Upgrade History is a view that is accessed from the Software Upgrade View that reads information about upgrades performed on an MG 9000. The Upgrade History contains:

- the time the upgrade was performed
- the type of upgrade
- the card on which the upgrade was performed
- the full path of the load name
- the final status

All the entries' status are completed or aborted. The last entry can have a different status since an upgrade is in progress.

An entry is created in the Upgrade History when the user attempts to image a card.

The Software Upgrade History windows shows the following message at the bottom of the window: Upgrade history is not maintained for any MTA and xDSL cards that may be present in the NE.

The following buttons are provided in the Upgrade History:

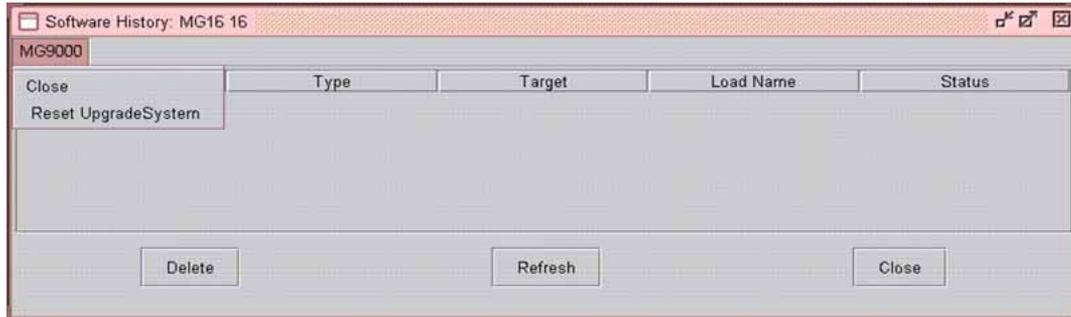
- Delete - deletes a history entry. An attempt to delete an entry for an upgrade in progress will fail.
- Refresh - updates the view with the latest data since the view is not dynamically updated
- Close - exits the Upgrade History view

From the menu bar, the following MG 9000 items are available

- Close - exits the Upgrade History view
- Reset Upgrade System - resets the upgrade system back to idle (that is, the upgrade process is abandoned where it is). This action can leave the cards in a mixed state, and the loads in the cards will not be reverted back to the original loads. Clear the card fault or replace the faulty card and try the upgrade again.

The following figure shows the Reset Upgrade System command.

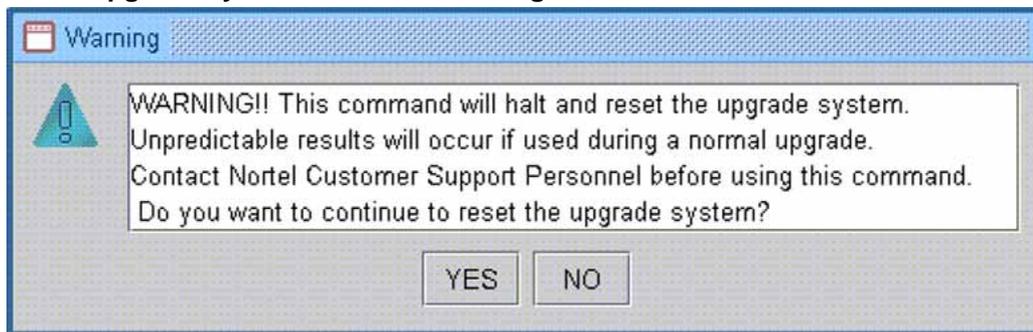
### Reset Upgrade System command



The Reset Upgrade System command requires emsadm permission and is considered a drastic step. Do not use this command unless directed to do so by Nortel customer support.

The following figure shows the warning message that appears when the Reset Upgrade System command is used.

### Reset Upgrade System command warning



The following figure shows the History View.

Software upgrade History view

Software Upgrade History: PL6 1				
MG9000				
Upgrade Time	Upgrade Type	Upgrade Target	Load Name	Upgrade Status
Thu Jan 04 02:34:01 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 11	h:\mg5\ot:ads\CC3\mg_17\0002...	Upgrade completed successfully.
Thu Jan 04 01:48:02 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 12	h:\mg5\ot:ads\DS*1,emg_17\DS*0...	Upgrade aborted.
Thu Jan 04 01:39:45 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 12	h:\mg5\ot:ads\?Jemg_17\AT*004...	Upgrade completed successfully.
Thu Jan 04 02:40:05 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 12	h:\mg5\ot:ads\DS*1,emg_17\DS*0...	Upgrade aborted.
Thu Jan 04 02:24:42 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 15	h:\mg5\ot:ads\?Jemg_17\AT*004...	Upgrade completed successfully.
Thu Jan 04 00:30:15 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 12	h:\mg5\ot:ads\?Jemg_17\AT*004...	Upgrade aborted.
Thu Jan 04 01:13:04 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 12	h:\mg5\ot:ads\DS*1,emg_17\DS*0...	Upgrade aborted.
Thu Jan 04 01:15:35 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 12	h:\mg5\ot:ads\DS*1,emg_17\DS*0...	Upgrade aborted.
Thu Jan 04 00:49:52 EST..	Engine 4:de	NE Number: 1 Node Name: P_6 PhysLoc: 0 1 12	h:\mg5\ot:ads\?Jemg_17\AT*004...	Upgrade aborted.



Carrier VoIP

## MG 9000 Configuration Management

Copyright © 2006, Nortel Networks  
All Rights Reserved.

Publication: NN10096-511  
Document status: Standard  
Document version: 09.02  
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to [www.nortel.com/documentfeedback](http://www.nortel.com/documentfeedback).

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

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

