

NN10255-111

Succession Multimedia Xchange

# Succession MX SIP PRI Gateway

## Basics

Standard Succession MX 1.1 (01.02) July 2003

---





# Overview

## How this chapter is organized

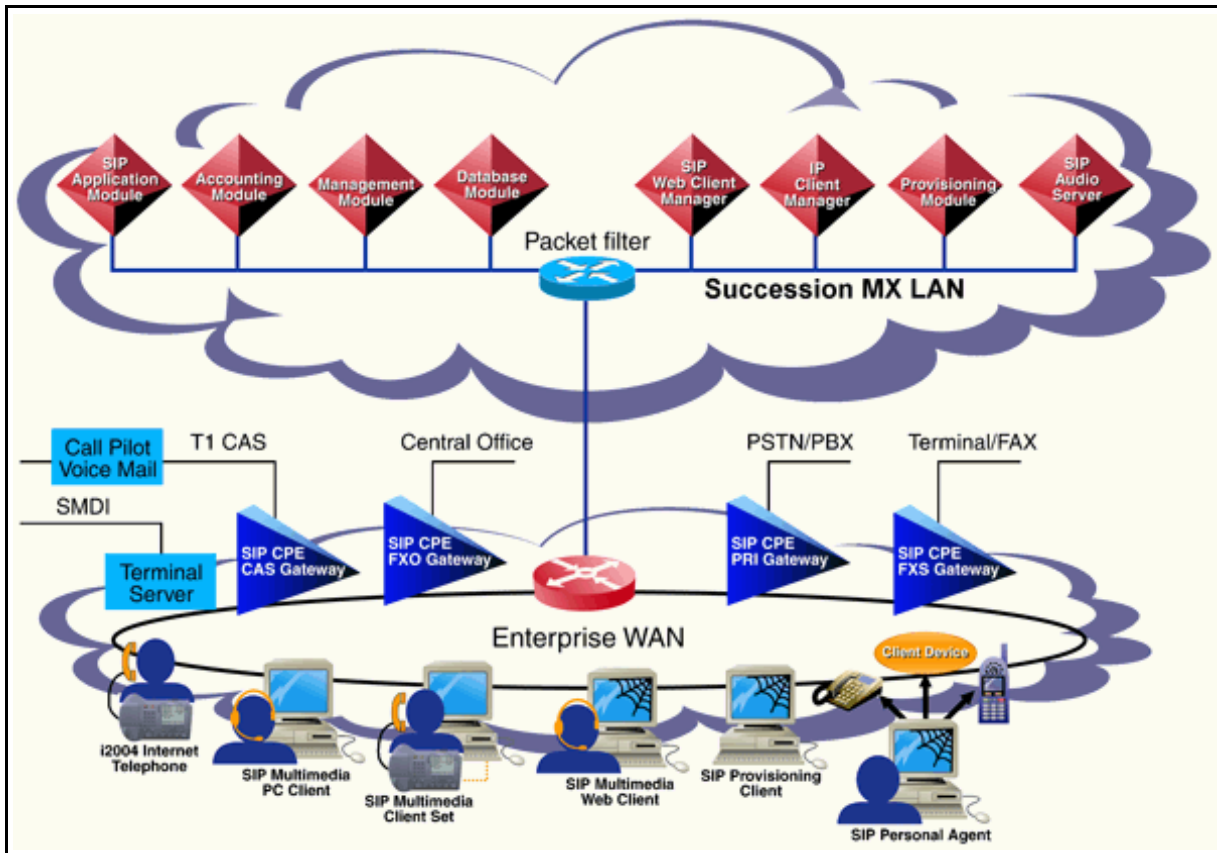
This chapter is organized as follows:

- “Overview” on page 3
  - Carrier and trunk group relationship
  - Call processing support
- “Hardware” on page 7
- “Software” on page 15
- “Supported services” on page 16
- “OAM&P strategy” on page 17

## Overview

The SIP PRI Gateway is a SIP-enabled media server, one of several gateways available for use with the Succession Multimedia Xchange (MX). This document deals exclusively with the Nortel Networks SIP PRI Gateway. For a list of other gateways that interwork with this platform, please see the *Succession MX Basics* document. For more information about those other gateways, please see the manufacturers' documentation.

The SIP PRI Gateway acts as a signaling and media gateway between a SIP Voice Over IP domain and a system using the ISDN Primary Rate Interface (PRI/Q.931), typically a PBX or PSTN switch. Figure 1, “Network overview,” gives an overview of the network configuration. The following sections provide more details about the SIP PRI Gateway.

**Figure 1 Network overview**

The Succession MX is a data-network-oriented, IP-based voice communications solution. The SIP PRI Gateway is responsible for the conversion of packet-based voice streams to circuit-based voice streams.

For PRI-to-SIP calls, the SIP PRI Gateway does not have the responsibility of finding the user. Instead, the SIP PRI Gateway sends a request to the provisioned SIP Application Module. Then the SIP Application Module attempts to route the call to an endpoint specified by a query of the user in the database. That endpoint can be any type of SIP node, end-user client, or gateway.

When the system attempts a SIP call to a user in the PRI domain, the SIP Application Module invokes Telephony routing. Basically, Telephony routing involves determining which gateway and trunk group the SIP message goes to. Telephony routing allows the SIP Application Module to manipulate digits, match the number to an entry in the internal mapping tables, and then send the call to a particular gateway. The manipulated number is part of the URL.

The SIP PRI Gateway application connects endpoints in a packet network to TDM endpoints that are accessed over TDM trunks on T1 or E1 carrier spans. PRI trunk groups must be created and maintained in the SIP PRI Gateway for this purpose and serve as the TDM bearer containers.

The principal TDM resources used in SIP PRI Gateway call processing are trunk group TDM endpoints. Trunk groups are supported by carriers, which, in turn, are supported by hardware interfaces.

Table 1, "Supported PRI variants," lists the supported PRI variants.

**Table 1 Supported PRI variants**

Variant	Specification
AT&T 4ESS (AT4)	TR 41459 (August 1995), PRI
AT&T 5ESS10 (E10)	AT&T 235-900-342 (January 1996): PRI
Northern Telecom DMS-100 (DMS)	NIS A211-1 release 6 (BCS 36): PRI
Bellcore National 2 (NI2)	SR-3887 (November 1996): PRI
ETSI	ETS 300 102-1 (December 1990) + Addendum ETS300 103-1/A2 (October 1993)
Japanese PRI	NTT INS 1500

**Note:** The supported countries for ETSI are Spain (Europe) and Australia.

### Carrier and trunk group relationship

The T1 is a serial line used mainly in North America that relays DS1 information frames at a rate of 1.544 Mbps. In Europe, the E1 line, which is similar to the T1, relays E1 information frames at a rate of 2.048 Mbps. T1 and E1 lines are commonly known as *carriers*. Both DS1 and E1 frames can carry smaller units of multiplexed transmission, called "DS0 frames." A DS0 frame represents 64 kbps of information, the standard bit rate of a digital telephone channel (PCM voice encoding) carrying a single conversation. A DS0 is also known as a *trunk*. A T1 line can accommodate 24 DS0s, while an E1 line can accommodate 32 DS0s. The overhead, that is, bits used in addition to the data payload for signaling and fault detection, is greater on the E1 line.

Each CG6000C media card acts as a timing “slave” to the far-end switch. This means that the card relies on the equipment at the other end of the T1 or E1 to provide the timing for synchronization. The CG6000C card uses the top T1 connection, port 1, as the primary clock source. The card uses port 2 as the fallback clock source if the primary clock source is not available, for example, if the carrier signal is not present.

The PRI application uses T1 or E1 carriers to host its DS0 trunks. PRI trunks are organized into trunk groups that are, in turn, associated with specific signaling protocols, features, and routing treatment. PRI trunk groups are defined around a D-signaling channel associated with a group of B channels (23 for T1 and 30 for E1). Thus, a PRI trunk group must contain at least a single DS0 channel used as the D-signaling channel and some number of DS0s acting as B channels. The following configuration rules are applied to the SIP PRI trunk groups and carriers:

- The D-signaling channel (channel 17 for E1, channel 24 for T1) is on the same carrier used for the trunk group’s B channels.
- PRI trunk groups cannot span more than a single carrier.
- The number of B-channel DS0s used in a trunk group cannot exceed the number of DS0s available in a carrier span.
- There may be no more than one PRI trunk group for each carrier.

### **Call processing support**

The SIP PRI Gateway is associated with one or more SIP Application Modules. The SIP Application Modules route SIP requests to the gateway (SIP-to-PRI calls) and service SIP requests from the gateway (PRI-to-SIP calls).

In a SIP-to-PRI call, the SIP PRI Gateway receives a SIP request for a new session. The message specifies an outgoing call over the PRI trunk group identified in the message. The SIP PRI Gateway selects an available B-channel endpoint from the PRI trunk group. This endpoint is then marked as unavailable until the completion of the call. If no B-channel endpoints are available for a new call, the SIP PRI Gateway rejects the call, indicating that no circuits are available.

PRI-to-SIP call requests received at the SIP PRI Gateway include the B-channel ID that the far end has selected. The SIP PRI Gateway marks this endpoint as unavailable until the completion of the call. If no B-channel endpoints are available for a new call, then the SIP PRI Gateway rejects the call, indicating that no circuits are available. Service providers should configure the far end to select the B channel for incoming PRI calls in ascending order, from lowest to highest B channel ID value, to reduce glare.

### Codec negotiation

The SIP PRI Gateway performs codec negotiation between various Voice over IP codecs. Codec is a compression scheme for audio data. Codec negotiation can be performed during call set up, mid-call, call transfer, and call retrieve. End-user benefits of codec negotiation include bandwidth preservation and increased voice quality.

Codec negotiation is performed as outlined in RFC23261 SIP: Session Initiation Protocol. The SIP PRI Gateway supports the codecs listed in Table 2, "Supported codecs." The Packetization column lists the transmission rates in milliseconds supported by each codec.

**Table 2 Supported codecs**

Codecs	Packetization
G.711 mu-law (PCMU)	10,20,30,40,50,60
G.711 a-law (PCMA)	10,20,30,40,50,60
G723.1	30,60
G.729a	10,20,30,40,50,60

### Hardware



The SIP PRI Gateway runs on a Motorola 8216T SAM16 chassis. The chassis provides the basic operating environment (such as power, backplane, cooling, and mounting slots) required to house compact, PCI-based, single-board computers.

The Motorola 8216T SAM16 chassis is configured as two independent processing systems and two separate domains (domains are the partitioned, left or right halves of the chassis) on each half shelf. Each system/domain or half-shelf is an independent processing system representing one SIP PRI Gateway or one SIP Audio Server. The chassis can support 552 T1 DS0s or 720 E1 DS0s for each half shelf. Service providers can add half shelves as needed to scale up.



Table 3, "Hardware requirements for the SIP PRI Gateway," lists the required SIP PRI Gateway hardware.

**Table 3 Hardware requirements for the SIP PRI Gateway**

Name	Detailed description
<p><b>Motorola 8216T SAM16 chassis</b></p> 	<p>The Chassis kit for each half shelf consists of the following:</p> <ul style="list-style-type: none"> <li>• Common Packfill kit</li> <li>• CPV5370 700MHZ, 1 GB Pentium II CPU</li> <li>• CPV5370 80MM Transition Module</li> <li>• PMC SCSI Controller</li> <li>• PIM SCSI Module</li> <li>• 36 GB SCSI HD drive chassis mounted</li> <li>• 40X SCSI CD-ROM Dr</li> <li>• Peripheral cards</li> <li>• 1 NMS CG6000 IP Telephony Card*</li> <li>• 1 NMS CG6000 Rear Input/Output (I/O) Card*</li> <li>• Optional: 6 total NMS CG6000 cards on each half shelf*</li> </ul> <p>* 4 ports on each card</p>
<p><b>Raritan KVM Switch</b></p> 	
<p><b>Keyboard / Monitor/Mouse</b></p>	<p><b>Note:</b> New purchases of systems that require a Motorola chassis will not be getting a monitor, keyboard, or mouse. Users of DC configurations will also not receive the power inverter. Customers must provide them separately. Most work on the Motorola chassis can be done through the System Management Console or PCAnywhere.</p>



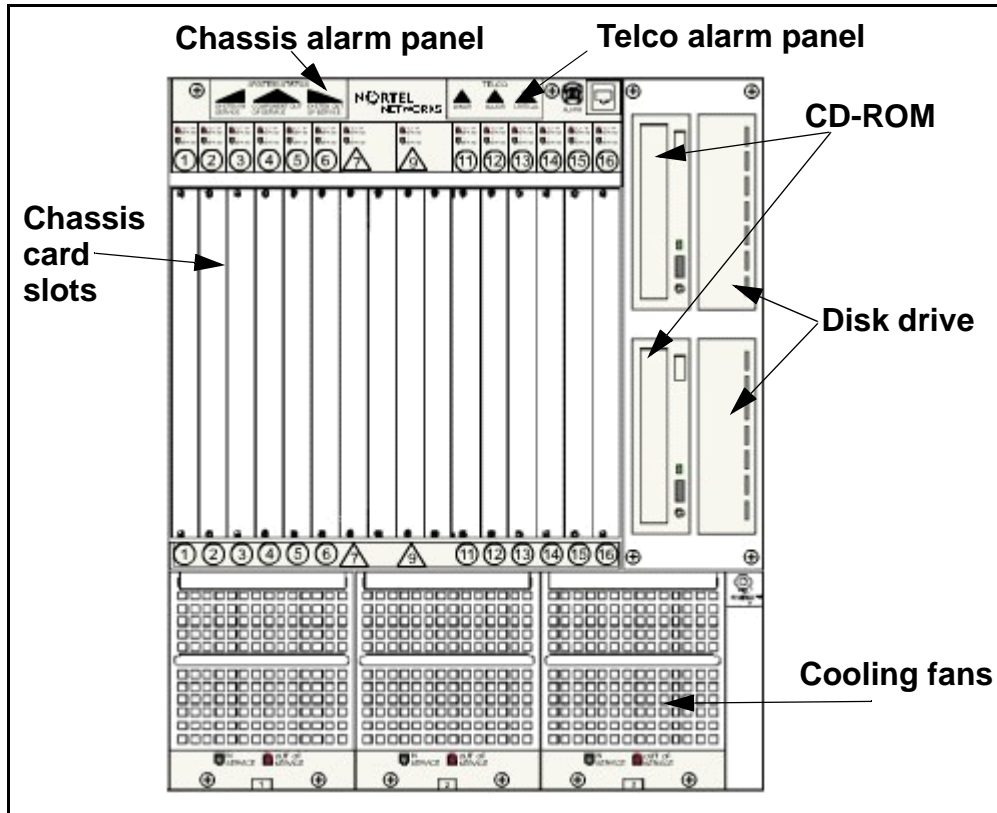
**Note:** Note that the NMS (Natural Micro Systems) cards are physically keyed (with red and blue keys) to only fit the backplane of the Motorola 8216T SAM16 chassis. They are not compatible with other CPX8216 models.

The HSC provides the services necessary to hot swap (remove and replace) the Host CPU and I/O cards in the opposite domain without powering down the chassis. The HSC in the left domain controls the right domain. The HSC card in the right domain controls the left domain.

**CAUTION**

If you remove the Host CPU, that half shelf will reboot and drop all calls.

The Motorola 8216T SAM16 chassis, when supported by the software components, uses its separate processors and I/O domains as a dual-host system. Each half of the Motorola 8216T SAM16 chassis can be an independent SIP PRI Gateway (or SIP Audio Server).

**Figure 2 Chassis diagram (Motorola 8216T SAM16 chassis)**

The SAM16 chassis contains a total of 16 slots. The slots are divided into two independent domains. Each domain consists of 8 slots. The only information passed between the domains are hardware alarms. The software sends the alarms to the left domain to light up the chassis alarms. When provisioned, each domain contains the following types of cards:

- Two system controller cards (Host CPU and HSC) control the operations for the domain.
- Up to six Input/Output (I/O) cards provide the interface to the network.

The Host Central Processing Unit (CPU) card controls the overall operations for the domain by performing the following:

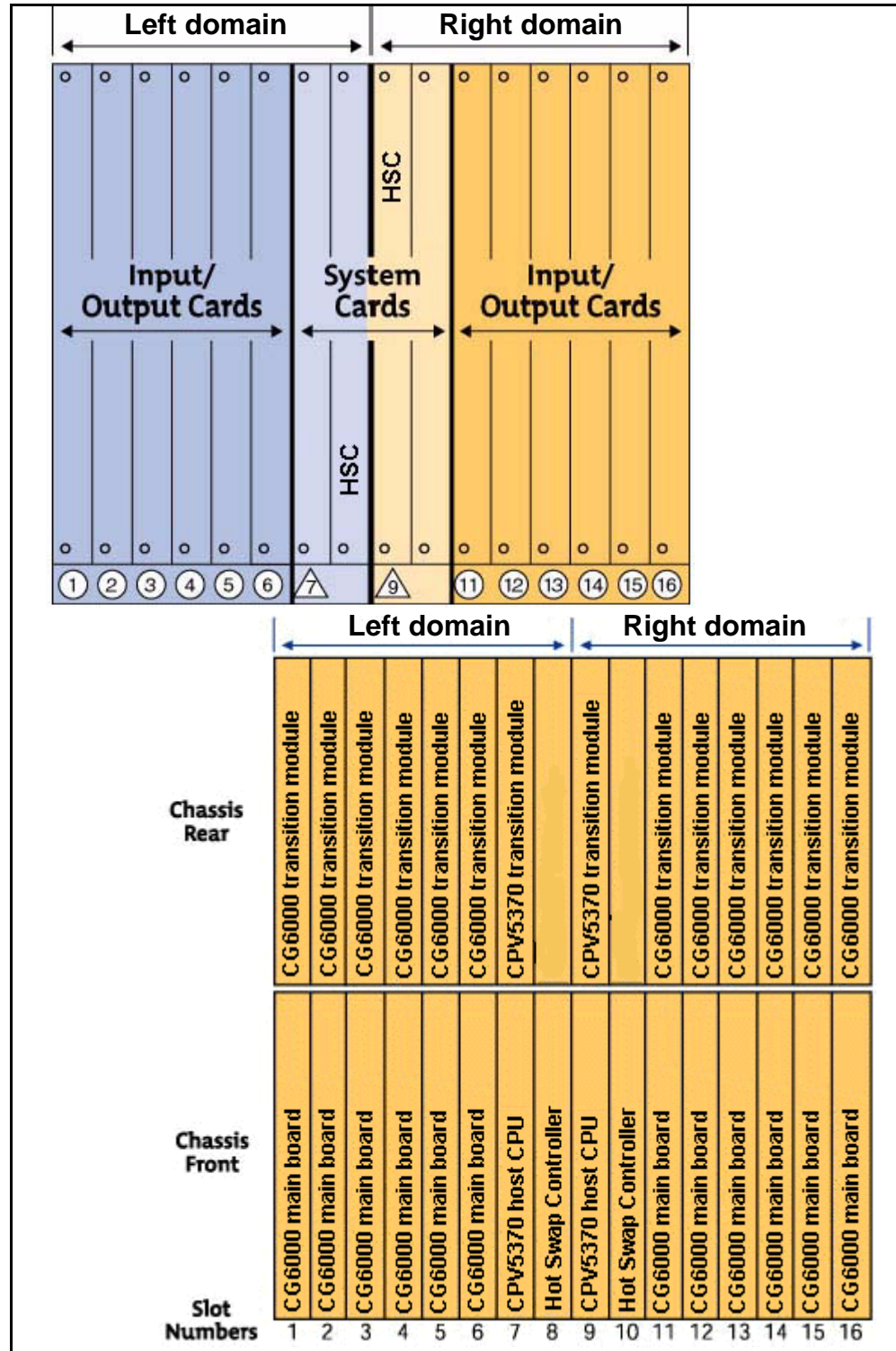
- processes requests from other network nodes
- manages the resources for the domain

When configured for a SIP PRI Gateway, each CG6000C I/O card performs the following functions:

- provides connectivity to the private network through Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) media streaming capability
- converts packet-based voice streams to/from circuit-based voice streams

Figure 3, “Motorola 8216T SAM16 cards,” shows a front view of the card slots. Notice the slots are numbered from left to right.

Figure 3 Motorola 8216T SAM16 cards



The **Telco alarm panel** located at the top of the Motorola 8216T SAM16 chassis contains LEDs arranged in three groups: System Status indicators; Telco alarm indicators; and card slot status indicators. The System Status indicators and the card slot status indicators are not operational. The Telco alarm indicators, located in the upper-right corner of the alarm panel (see Figure 2 “Chassis diagram (Motorola 8216T SAM16 chassis),” on page 10), are operational. These LEDs are activated in response to Critical, Major, and Minor system alarms raised in both domains of the chassis. If a system alarm is raised either in a single domain, or in both domains, of a chassis, the appropriate Telco alarm indicator on the panel is activated. The color scheme for the Telco alarm indicators is shown in Table 4.

**Table 4 Telco Alarm Indicators**

LED	Color
No alarm	Lights are off
Minor	Yellow
Major	Red
Critical	Red

The SIP PRI Gateway can be deployed in pairs of systems (domains) on a single chassis. However, if you are only configuring half a chassis, use the left half (when viewed from the front of the chassis), or "A" domain. This configuration ensures that the system alarms can activate the appropriate Telco alarm LEDs on the CX8216T chassis alarm panel.

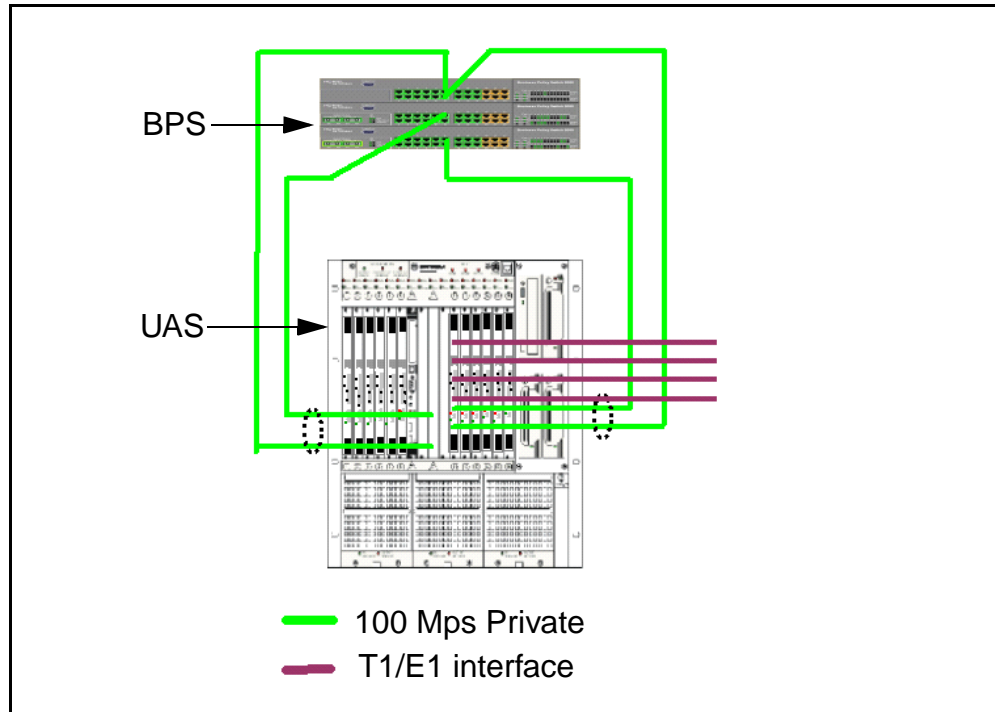
The SIP PRI Gateway can be configured in either a DC or an AC cabinet. In a DC configuration only, the CPX8216T chassis alarm panel is cabled to the breaker interface panel located at the top of the cabinet. This enables the alarm indicators on the breaker interface panel to be activated when alarms are activated on the alarm panel of any of the Motorola 8216T SAM16 chassis provisioned in the cabinet.

### Hardware redundancy

A SIP PRI Gateway consists of two half-shelves managed by two independent Host Controllers. Each Host Controller manages a half-shelf of up to six media traffic processing cards (or resource cards). Each card has two Ethernet connections to the network. For redundancy, these connections are connected to two separate BPS2000 switches. Dual network interfaces prevent a failed BPS2000

switch from taking the card out of service. See Figure 4, “Network connections,” for a diagram of the network connections.

**Figure 4 Network connections**



The Host Controller failure only impacts the media cards it manages. The rest of the cards in the chassis will continue to operate normally. To ensure that the engineered service capacity will not be degraded due to a single host outage, you can provision the system on an N + 1 basis. For more information, see the chapter “Security and Administration” on page 93 in this document.

There are redundant links connecting Host Controllers (CPV 5370) to separate BPS 2000s. If one of the links goes down, the controller continues to operate through the redundant link. (An ethernet link is considered failed by the media card only if no electrical voltage is present on the link. If a layer 2 failure occurs, but the physical layer is still active and voltage is present, the media card will not detect this as a failure.) Each media processing card has its own network connections for media flows.

Should a media processing card or its network connections fail, only that card will be taken out of the service. The existing media sessions are lost for that card. The rest of media processing cards continue to function normally.

## Software

The Nortel Networks Global Server serves as the base software layer platform for the SIP PRI Gateway. Global Server currently supports Windows 2000 as the operating system. The Global Server software is loaded onto the disk drive of the SIP PRI Gateway chassis domain to be used by the Host Central Processing (CPU) card.

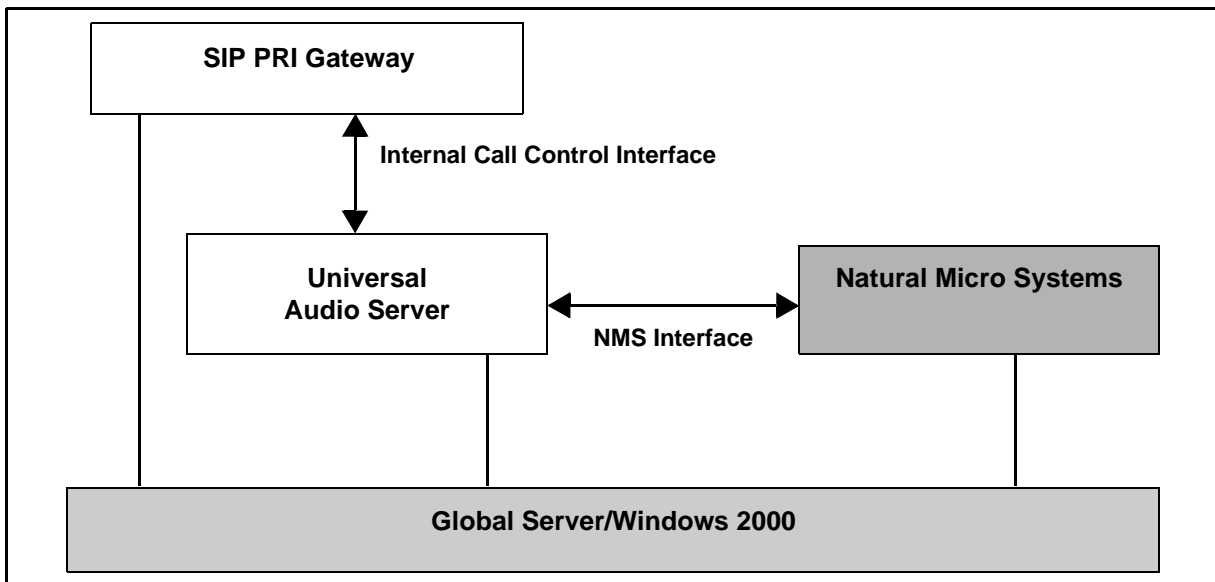
Each domain in the SAM16 chassis can contain up to six Input/Output (I/O) cards. Each Input/Output (I/O) card contains Natural Micro Systems (NMS) software. NMS software is preloaded on each card by the manufacturer.

The Universal Audio Server (UAS) base software is downloaded onto each Host CPU card. The UAS software communicates with the NMS software. NMS software controls all of the I/O card resources. UAS software communicates with the NMS software to request the appropriate I/O card resources.

SIP PRI Gateway software is installed onto each Host CPU card after installation of the UAS base software. SIP PRI Gateway software provides the SIP and gateway functionality.

See Figure 5, "SIP PRI Gateway software configuration," for a diagrammatic view of the software configuration.

**Figure 5 SIP PRI Gateway software configuration**





## Supported services

The SIP PRI Gateway is responsible for

- Signaling conversion: converting SIP to PRI and PRI to SIP
- Media Stream conversion: converting packet-based voice streams to and from circuit-based voice streams

The SIP PRI Gateway supports the following call types. For more information about header mappings, see “Mapping tables” on page A135:

- SIP to PRI
- PRI to SIP
- PRI to PRI

These call types require a PBX or PSTN terminal and a SIP terminal to place calls through the gateway. The gateway connects the VoIP and TDM domains in a call context.

The SIP PRI Gateway provides the following services for calls involving PRI:

- Basic call (For more information on basic calls, see the *MCP Basics* document.)
- Hold/Retrieve: Once the client puts the call on hold, the SIP PRI Gateway stops sending media to that client until the call is retrieved.
- Call transfers (caller or callee, if on a SIP-based access client)
- Call redirection
- Codec negotiation
- Call Rejection on Nodal Authentication Request
- Calling party name and number delivery to SIP (this is PRI-variant dependent)
- DTMF outpulsing toward PBX/PSTN (*no DTMF detection; Military DTMF digits A-D are currently not supported*)
- ISDN trunk group selection based on request URI data
- location-based ringback for the PRI originating agent to hear while the SIP side is alerting

The term *ringback* refers to the signaling tone that indicates to the caller's access client that the called party is being alerted (ringing). Ringback is provided by the last switch that is the closest to the point of termination. The SIP PRI Gateway is the last switch in a

PRI-to-SIP call. The SIP PRI Gateway provides ringback toward the PSTN during call setup.

- ANSI and ETSI PRI variant support
- Japanese PRI variant support
- parameter mapping between SIP and PRI protocols
- mapping between SIP error codes and PRI cause values
- PRACK (Provisional Response Acknowledge message)
- Programmable Real-Time Protocol (RTP) Type of Service (ToS) setting to control Quality of Service (QoS)
- Long-call service: a mechanism used to detect and release resources from abandoned calls

### OAM&P strategy

The Management Module manages the OAM&P functions for the SIP PRI Gateway. For additional information, refer to the *Succession MX Management Module Basics* and the *Succession MX System Management Console Basics* documents and the *Security and Administration* chapter in this document.





# Upgrades

## How this chapter is organized

This chapter is organized as follows:

- “Overview” on page 19
- “Maintenance release (UAS06MR\_MJ) update” on page 19
- “Software update procedure” on page 20
- “Update failures” on page 27
- “OAM&P strategy” on page 27

## Overview

This section describes the update strategies for the SIP PRI Gateway. Updates have the following characteristics:

- They introduce new functionality across many components without affecting network stability.
- If a server update fails, you have a choice of rolling it back or not. It does not roll back automatically.

Screen shots in this document are representative of what you may see, but may not be the same for individual service providers due to the particular configuration shown.

## Maintenance release (UAS06MR\_MJ) update

### *at the System Management Console*

- 1 Remove any version of UAS06MR\_MG1, UAS06MR\_MG2, UAS06MR\_MG3 and UAS06MR\_MH before installing UAS06MR\_MJ.
- 2 To uninstall:
  - a Go to *Add/Remove* applications under the Control Panel and locate UAS06MR\_M(x).
  - b Choose **Remove** to uninstall the UAS06MR\_M(x).

- c Follow the *uninstall* screen instruction to uninstall.
  - d Reboot.
- 3 To install the UAS06MR\_MJ patch:
  - a On the System Management Console, make sure to delete the old UAS patches under components for the server.
  - b On the System Management Console, under **Components** for the server, select the **ADD** menu.
  - c Select **BaseSoftware**.
  - d Select the *uasmtcload-mj* latest build and click **Apply**.
  - e On the UAS-based machine go to  
D:\IMS\uasmtcload-mj\winnt\setup.exe.
  - f Run the setup.exe and follow the screen prompts.
  - g Reboot when prompted.

### Software update procedure

Perform a SIP PRI Gateway maintenance load update from the System Management Console. The following procedure enables you to perform an update.

**Note:** When upgrading from 1.1 to 1.1 FP1 you must upgrade from 1.1.4 build 297 to 1.1.5 build 326. After the upgrade to build 326 is complete, you may then update to any load of FP1.



#### CAUTION

No remote access sessions (telnet, ftp) should be in progress on a unit that is being updated.



#### CAUTION

Under no circumstances should the locking key on the system hard drive be turned while the system is operational. Turning this key while the system is operational can result in false error condition reporting by the system.

## Procedure 1 Updating the uasload procedure

### ATTENTION

The server will be unavailable during the update. Existing calls will lose voice path and no new calls will be established.

### At the System Management Console

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP PRI Gateway bullet.

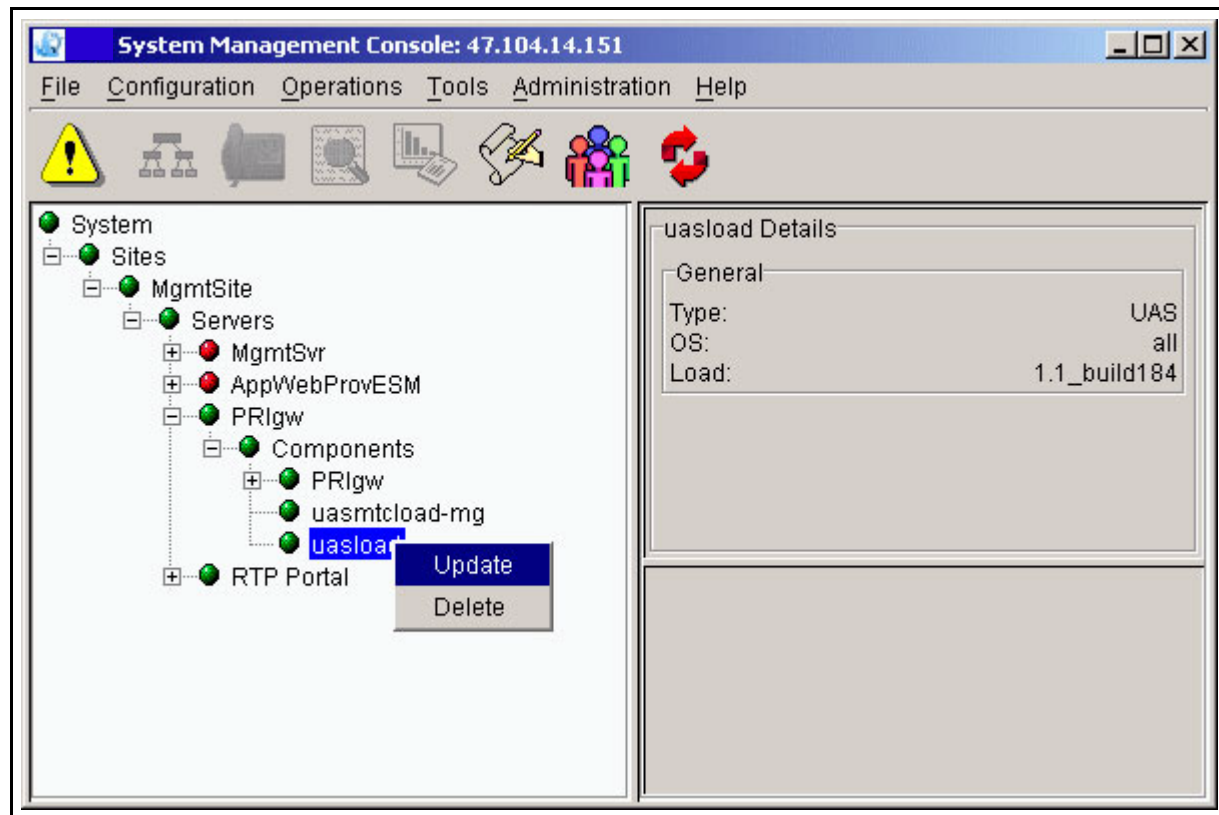
**Note:** The name of the SIP PRI Gateway is the name assigned to it during deployment, in this particular example, **PRlgw**.

- 2 Right-click on the SIP PRI Gateway bullet, **PRlgw**.
- 3 Right-click on **uasload**.

Figure 1 Selecting the uasload bullet

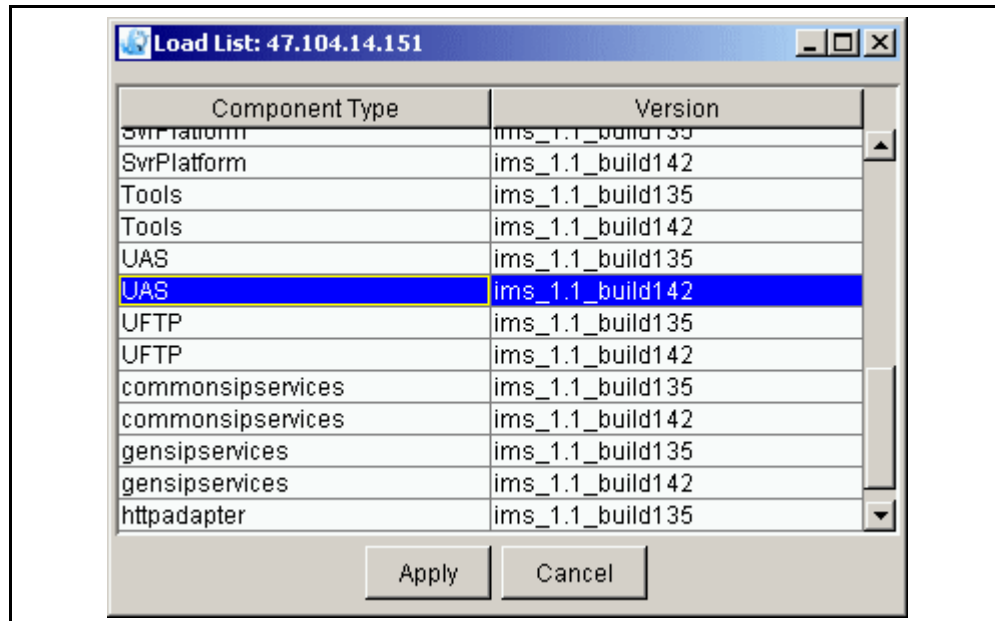


- 4 Select **Update**.

**Figure 2 Selecting the Update function**

- 5 When the Load List window appears, select the UAS Maintenance load you need.



**Figure 3 Selecting the uasload from the list**

- 6 Select the **Apply** button.  
The uasload is downloaded to the target node.
- 7 After the software load deployment is complete, log into the system.
- 8 Connect to the node that you are updating.
- 9 Install the new software load by double-clicking  
**D: IMS\uasload\WINNT\setup.exe.**  
  
**Note:** If you are adding a new maintenance load from the UAS, for example, uasmtcload-mg as shown in Figure 2, "Selecting the Update function," then the path would be d:\ims\uasmtcload-mg\WINNT\setup.exe. The subdirectory name would change to match the name of the UAS maintenance software load being deployed. For example, then, the next release might be d:\ims\uasmtcload-mh\WINNT\setup.exe.
- 10 An installation Wizard appears. Follow the steps in the Wizard.
- 11 If prompted to reboot, do so.

## Procedure 2 Performing the SIP PRI Gateway software update

### ATTENTION

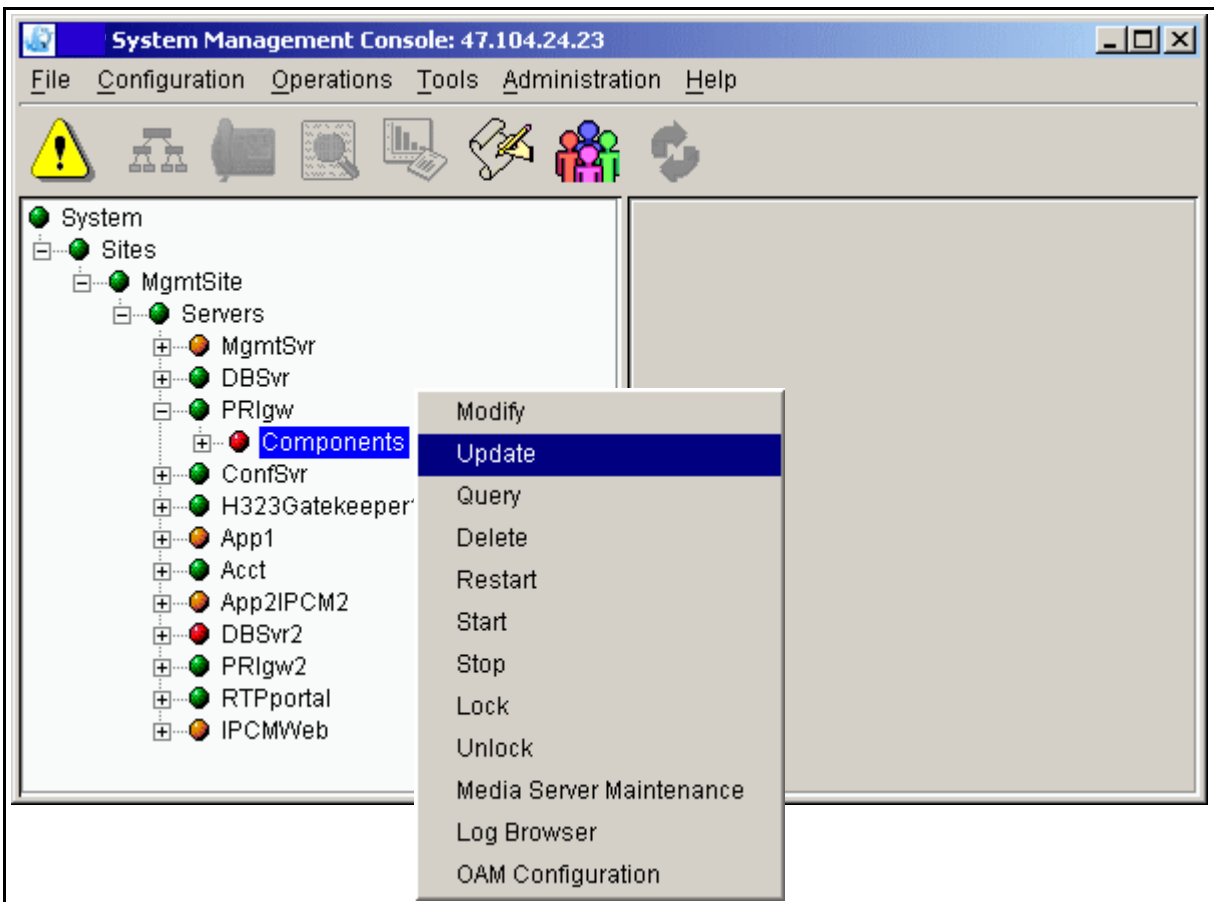
The server will be unavailable during the update. Existing calls will lose voice path and no new calls will be established.

### at the System Management Console

- 1 A load can be either up-versioned or down-versioned. In either case, updating a load from one version to another results in stopping and deleting the previously added version, adding the new version and auto-launching the new version.

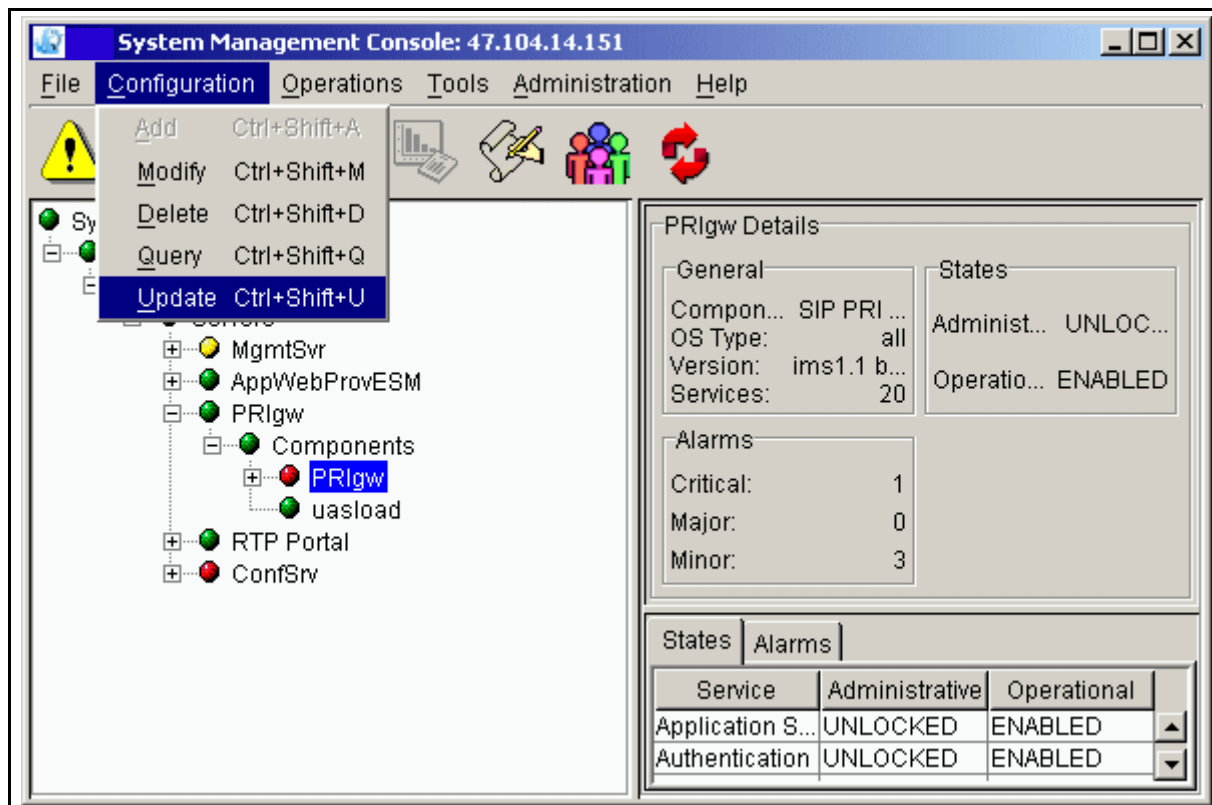
Using the following example, from the Management Console, navigate to **Components**, as shown. Right-click on **Components** and select **Update** from the pop-up menu.

Figure 4 Updating the SIP PRI Gateway from the menu tree



You can also launch the update from the pull-down Configuration menu, as shown.

**Figure 5 Updating the SIP PRI Gateway from the pull-down menu**



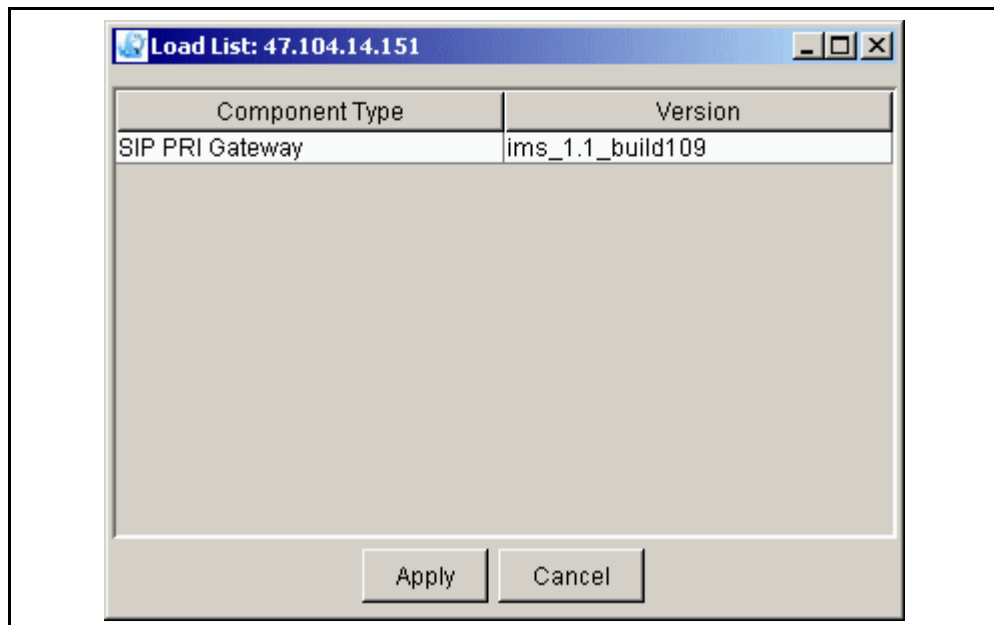
- 2 Select the **Update** command. The following window appears.

**Figure 6 The update window, retrieving the load list**



- 3 You can only do an update from one version to another. Therefore, the window only shows loads that have the same name as the load being updated. Select the version you want to update.

**Figure 7 Load list for updating**



- 4 The console displays the differences between the configuration data of the old version and the configuration data of the updated version by highlighting the tab(s). On the configuration window, modify any configuration values you need.
- 5 *When you have finished making your changes*, click on the **Apply** button. The load list changes automatically. The alarm clears when the server comes back up.

### Update failures

If an update fails, wait for the Information Dialog box requesting a revert confirmation. Click **Yes** to revert to the previous load.

### OAM&P strategy

The Management Module manages the OAM&P functions for the SIP PRI Gateway. For additional information, refer to the *Succession MX Management Module Basics* and the *Succession MX System Management Console Basics*.





# Fault management

## How this chapter is organized

The procedures in this section are organized as follows:

- “Term definitions” on page 30
- “Interpreting software errors” on page 30
- “Clearing alarms” on page 33
  - “Clearing the UAS128 alarm (Failure of T1/E1 carrier)” on page 33
  - “Clearing the UAS746 (LRM\_MEM\_C [81923]) alarm” on page 33
  - “Clearing the UAS748 (LRM\_DISK\_C [81925]) alarm” on page 33
  - “Clearing the UAS939 (CG6000 card failure) alarm” on page 34
- “Repairing hardware failures” on page 35
  - “Clearing the Motorola 5370 Ethernet connection failure” on page 35
  - “Clearing the NMS CG6000 Ethernet connection failure” on page 35
  - “Clearing the Motorola 5370 card failure” on page 35
  - “Clearing the NMS CG6000 card failure” on page 35
  - “Clearing the NMS T1/E1 carrier failure” on page 36
- “Replacing a CPV5370 Processor card” on page 37
- “Replacing a Hot Swap Controller card” on page 40
- “Replacing a CG6000 card through a hot swap” on page 41

See the *Succession MX System Management Console Basics* for more information about logs and alarms that pertain to the SIP PRI Gateway.



## Term definitions

The procedures in this document use the following terms in the steps:

- **lock force** - administratively locks the SIP PRI Gateway node immediately, which causes all active calls associated with the node to be dropped immediately
- **lock graceful** - administratively locks the SIP PRI Gateway node after stable calls using the node have been completed
- **unlock** - returns the SIP PRI Gateway node to service if no other conditions exist that prevent it from coming back into service
- **reboot** - reboots the SIP PRI Gateway hardware
- **restart** - restarts the SIP PRI Gateway software
- **administrative state** - the state that can be changed through the System Management Console to enable maintenance activity to be performed. These states include:
  - **locked**
  - **unlocked**
- **operational state** - the state that describes the current operational status of the node. These states include:
  - **enabled** - the node is capable of handling traffic
  - **disabled** - the node is out of service

## Interpreting software errors

The following tables detail the possible software error scenarios a user may encounter in an alarm situation.

**Table 1 Interpreting the 45058 DCHNL\_IN\_SERVICE error**

Field	Description
Message	"TGID %d is in service"
EventType	information
Probable cause	The D-Channel is in service and callp signaling (from the PRI side) is now possible.
Corrective action	No action, for information only

**Table 2 Interpreting the 45059 DCHNL\_NOT\_IN\_SERVICE error**

Field	Description
Message	"TGID %d is NOT in service"
EventType	error
Probable cause	Could not establish the D-Channel for this trunk group.
Corrective action	Lock the trunk group. Then Unlock the trunk Group. If the D-channel does not show in-service, check configuration and the status of the far-end D-channel.

**Table 3 Interpreting the 45060 B\_CHNL\_CONFLICT error**

Field	Description
Message	"Rejected an incoming (PBX) call the requested B-Channel %d is not available"
EventType	information
Probable cause	A channel that is already in use was requested for an additional call setup.
Corrective action	If no call is actually on this channel and problem persists, <b>lock force</b> this channel. Then unlock the channel.

**Table 4 Interpreting the 45061 B\_CONTEXT\_UNAVAILABLE error**

Field	Description
Message	"Rejected an incoming (PBX) call the requested B-Channel %d is not provisioned"
EventType	error
Probable cause	A call that was requested to be set up on a channel is not provisioned.
Corrective action	Check provisioning to make sure all channels were provisioned for this trunk group.

**Table 5 Interpreting the 45062 D\_CONTEXT\_UNAVAILABLE error**

Field	Description
Message	"D-Channel context is not available for TGID: %d"
EventType	error
Probable cause	The NMS context for the D-channel is not accessible.
Corrective action	Lock the trunk group. Unlock the trunk group. If the problem persists, restart the gateway.

**Table 6 Interpreting the 45063 NMS\_ERROR\_EVENT error**

Field	Description
Message	"NMS reported error cause of %d, diagnostic code is %d "
EventType	error
Probable cause	NMS software reported an internal error.
Corrective action	If problem persists, restart the gateway.

**Table 7 Interpreting the 45064 SETUP\_NOTIFICATION\_ERROR error**

Field	Description
Message	"Did not send a notify signal to call server to report a PRI origination on TGID %d"
EventType	error
Probable cause	Incoming setup was not reported to the SIP Application Module.
Corrective action	If the problem persists, lock force and unlock this channel. If problem persists, restart the gateway.

## Clearing alarms

### Procedure 1 Clearing the UAS128 alarm (Failure of T1/E1 carrier)

#### *At the frame*

- 1 If a trunk goes out of service due to a bad cable or lost carrier, then the error is detected and new calls are routed to the next available trunk. The next available trunk is defined by the alias and domain sent by the SIP Application Module in the request URI. Due to a *no carrier* error, all existing calls lose voice path and are taken down when the user hangs up.

The NMS CG6000 cards contain four T1/E1 ports. Lost carriers can be the result of a pulled cable or bad cable, or loss of the far-end connection. The T1/E1 trunk is placed in the LOCKED state. All channels associated with this card are placed in an OUT-OF-SERVICE state. All active calls on this trunk are dropped and all resources associated with this card are placed in OUT-OF-SERVICE state to prevent any future calls from trying to use this card. A UAS128 alarm with severity = CRITICAL is raised to indicate the problem.

To clear the alarm, restore the carrier. Trunks are restored to their pre-failure state. See "Clearing the NMS T1/E1 carrier failure" on page 36.

### Procedure 2 Clearing the UAS746 (LRM\_MEM\_C [81923]) alarm

#### *At the frame*

- 1 When this alarm appears, you will see the message = "[mem\_usage\_high\_critical] Memory usage critical. (<percent>% used)". The probable cause of this alarm is that the system is out of memory.

To clear this alarm, free some non-used memory. The alarm will clear when memory usage no longer exceeds the critical limit. One example of non-used memory is old debug logs. These are located in c:\uas\etc\callpdebug and d:\ims\prigw\log\ImsPRIGWC.

### Procedure 3 Clearing the UAS748 (LRM\_DISK\_C [81925]) alarm

#### *At the frame*

- 1 When this alarm appears, you will see the message = "[disk\_usage\_critical] File system %s usage critical. (<percent>% used)". The probable cause of this alarm is a

storage capacity problem, partially caused by the debug logs being turned on.

To clear this alarm, turn off debug logging. The alarm will clear when the disk usage no longer exceeds critical limit.

- a To turn off debug logging for UAS, enter the following command: **"uasdebugstatus disable all"**.
- b Do a carriage return, then enter **"callp resetdebug"**.
- c Do a carriage return, then delete old debug logs. See Procedure 2, "Clearing the UAS746 (LRM\_MEM\_C [81923]) alarm," for more information about clearing disk space.

#### **Procedure 4 Clearing the UAS939 (CG6000 card failure) alarm**

##### ***At the frame***

- 1 A card failure results when the card is removed from the system. All of the calls using that card are released. The card is no longer used for subsequent calls. A UAS939 alarm with severity = MAJOR is raised to indicate the problem.

To clear the alarm,

- a Lock the card.
- b Pull and replace the card (hot swap). See "Replacing a CG6000 card through a hot swap" on page 41 for specific instructions.
- c Unlock the card.
- d Restart the SIP PRI Gateway.
- e If the problem continues, contact your support team.

## Repairing hardware failures

Use the following procedures to recover from hardware failures.

### Procedure 5 Clearing the Motorola 5370 Ethernet connection failure

#### *At the frame*

- 1 The host card is configured with two fault-tolerant ports. If one port fails then all signaling is routed over the other port. Alarm UAS158 appears. When both ports fail, the SIP Application Module cannot communicate with the gateway and route advances the call to the next route after performing SIP retransmission. All existing calls remain active.

Restore the network connection. See "Clearing the Motorola 5370 Ethernet connection failure" on page 35.

### Procedure 6 Clearing the NMS CG6000 Ethernet connection failure

#### *At the frame*

- 1 The NMS cards are configured with two 100 base-T ethernet connections (ports). If one port fails then all signaling is routed over the other port and a UAS923 alarm with severity = MINOR is raised. If both ports fail, a UAS923 alarm with severity = CRITICAL is raised. The card is out of service at that point. All ISDN call attempts to the SIP PRI Gateway with this failed host card fail since communication to the SIP Application Module is lost. All existing calls remain active.

Restore the network connection.

### Procedure 7 Clearing the Motorola 5370 card failure

#### *At the frame*

- 1 If the Motorola 5370 card fails, replace it. See "Replacing a CPV5370 Processor card" on page 37.
- 2 Restart the server.

### Procedure 8 Clearing the NMS CG6000 card failure

#### *At the frame*

- 1 If an NMS CG6000 card is not responding, then all SIP calls that terminate to that card receive a SIP 480 Temporarily Unavailable response. It is up to the SIP Application Module to route the call to another device for completion. Due to card failure, all existing

calls lose voice path and are released when the users hang up. The UAS939 alarm with severity = MAJOR is raised.

If the alias and domain match, the SIP PRI Gateway can choose another card or the SIP Application Module can choose another route (and gateway). See Table 11, "Sample Trunk Group entries," for setup examples.

Replace the NMS CG6000 card. See "Replacing a CG6000 card through a hot swap" on page 41.

## Procedure 9 Clearing the NMS T1/E1 carrier failure

### *at the frame*

- 1 If the T1/E1 carrier connection on an NMS CG6000 card fails, the UAS128 alarm with severity = CRITICAL is raised. All the existing calls using those trunk groups are dropped. Calls associated with the domain for which that trunk group was configured will be processed if there are other trunk groups configured for the same domain. Consider the following scenario where there are two trunk groups configured in the system:

Trunk Group ID	Alias	Domain
1	trkgrp1	nortel.com
2	trkgrp1	telco.com

Trunk Group with Trunk Group ID = 1 detaches from the card. After this occurs, the SIP-to-PRI call with the following request URI is not established, since there are no trunk groups with domain nortel.com: INVITE  
sip:test@nortel.com;maddr=47.104.22.198;user=phone;  
norteldevice=pri;norteltrkgrp=trkgrp1

The SIP PRI Gateway responds with:

480 Temporary Unavailable (No Circuits Available).

The SIP Application Module can choose another route.

If there is another trunk with matching alias and domain, the SIP PRI Gateway chooses that one.

When the T1/E1 carrier is re-established, the trunk groups return to the state they were in before the extraction/failure. If a trunk group was in-service before the extraction/failure, then new call establishment will be available on that trunk group again.

- 2 Restore the carrier. See "Maintaining the SIP PRI Gateway Carrier and Trunk Group" on page 107.



## Replacing a CPV5370 Processor card



### **WARNING** Static electricity damage

While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.



### **CAUTION** Possible equipment damage

Use care when inserting and removing cards from the shelf. Ensure that the spiral gasket on the edge of the card faceplate is not loose; otherwise, it could become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

**Figure 1 Loose spiral gasket**



### ***At the System Management Console main screen***

- 1 Navigate to the Maintenance window as shown in “Accessing

the Maintenance window” on page 98.

- 2 Click the **Change** button, located in the States pane.  
A Change Administrative State window appears.
- 3 If you want to forcefully lock the SIP PRI Gateway, select the **Lock Force** radio button.  
If you want to gracefully lock the SIP PRI Gateway, select the **Lock Graceful** radio button.
- 4 Click **OK**.
- 5 Ensure that the new Administrative State is **locked**.
- 6 Shut down the system:  
Select **Start -> Shut Down**
- 7 On the Shut Down Windows screen, select **Shut down this computer**. When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do not turn off power to the computer.
- 8 Locate the CPV5370 card. If the node is located in the left domain, the card will be in slot 7; if the node is located on the right domain, the card will be in slot 9.
  - a Determine whether you are replacing only the front module, replacing only the rear module, or replacing both the front and the rear modules.

If	Do
you are replacing only the front module	step b through n
you are replacing only the rear module	step d through n
you are replacing both the front and the rear module	step i through n

- b Remove the front module (Loosen the screws that secure the modules in the slots with a Phillips head screwdriver, and unlock the lock latches to remove the modules.).
- c Insert the new front module, lock the lock latches on the module and tighten the screws that secure the module in the shelf. The node reboots when you insert the modules into the shelf.
- d Disconnect the network interface cables, KVM, SCSI cable, and connections from the rear transition module.

- e** Remove both front and rear modules, in that order (Loosen the screws that secure the modules in the slots with a Phillips head screwdriver, and unlock the lock latches to remove the modules.).
  - f** Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.
  - g** Insert the front module that you removed in step **e**. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.
  - h** Reconnect the cables disconnected in step **d**. The node reboots when you insert the modules into the shelf.
  - i** Disconnect the network interface cables, KVM, SCSI cable, and connections from the rear transition module.
  - j** Remove both front and rear modules, in that order (Loosen the screws that secure the modules in the slots with a Phillips head screwdriver, and unlock the lock latches to remove the modules.).
  - k** Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.
  - l** Insert the new front module. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.
  - m** Reconnect the cables disconnected in step **i**.
  - n** Restart the system.
- 9** Click the **Change** button located in the States pane.  
A Change Administrative State window appears.
- 10** Click **OK**.
- 11** Ensure that the New Administrative State is **Unlocked**.
- 12** You have completed this procedure.

## Replacing a Hot Swap Controller card

This procedure enables you to replace a Hot Swap Controller card.



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

While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.



### **CAUTION** **Possible equipment damage**

Use care when inserting and removing cards from the shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit. See Figure 1, "Loose spiral gasket," on page 37.

### ***At the System Management Console main screen***

- 1 Navigate to the Maintenance window as shown in "Accessing the Maintenance window" on page 98.
- 2 Click the **Change** button, located in the States pane.  
A Change Administrative State window appears.
- 3 If you want to forcefully lock the SIP PRI Gateway, select the **Lock Force** radio button.  
If you want to gracefully lock the SIP PRI Gateway, select the **Lock Graceful** radio button.
- 4 Click **OK**.
- 5 Ensure that the New Administrative State is **Locked**.

### ***At the system console (Windows desktop interface) connected to the domain containing the card being replaced:***

- 6 Shut down the system by selecting  
**Start -> Shut Down**

- 7 On the Shut Down Windows screen, select **Shut down this computer**. When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do not turn off power to the computer.
- 8 Locate the Hot Swap Controller card. The Hot Swap Controller cards reside in the domain of the chassis opposite from the domain that they control. Thus, the Hot Swap Controller for the left domain resides in slot 10; the Hot Swap Controller for the right domain resides in slot 8.
  - a Remove the Hot Swap Controller card (Loosen the screws that secure the modules in the slots with a Phillips head screwdriver, and unlock the lock latches to remove the modules.).

**Note:** There is no rear transition module for this card.
  - b Insert the new Hot Swap Controller card. (After the new card has been inserted into the card slot, lock the lock latches, and tighten the screws that secure the card in the shelf.)
- 9 Restart the system.

***At the System Management Console main screen:***

- 10 Click the **Change** button, located in the States pane.  
A Change Administrative State window appears.
- 11 Click **OK**.
- 12 Ensure that the New Administrative State is **Unlocked**.
- 13 You have completed this procedure.

**Replacing a CG6000 card through a hot swap**

This procedure enables you to replace a faulty CG6000 card set in an in-service unit. You can either perform

- a **graceful** extraction by first locking the card at the maintenance GUI and removing the card from the slot, raising a UAS939 alarm with severity = MAJOR
- a **surprise** extraction by forcefully removing the card from the slot, raising a UAS936 alarm with severity = MAJOR (raised for general card failure)

All existing calls using the trunk groups associated with that card are dropped. Calls are processed if you have configured other cards to handle other trunk groups configured for the same domain. For

example, consider the following scenario where there are two cards configured in the system:

Card number	Trunk Group ID	Alias	Domain
1	1	trkgrp1	nortel.com
1	2	trkgrp1	telcom.com
2	2	trkgrp2	telcom.com
2	2	trkgrp3	telcom.com

Card number 1 is removed. The SIP-to-PRI call with the following request URI is NOT established, since there are no trunk groups with domain nortel.com: INVITE

```
sip:test@nortel.com;maddr=47.104.22.198;user=phone;norteldevice=pri;norteltrkgrp=trkgrp1 .
```

The SIP PRI Gateway responds with: 480 Temporary Unavailable (No Circuits Available). The SIP-to-PRI call with the following request URI is established, since card 2 has two trunk groups with domain telco.com: INVITE

```
sip:test@telco.com;maddr=47.104.22.198;user=phone;norteldevice=pri;norteltrkgrp=trkgrp1
```

For graceful extractions, when the card is re-inserted and unlocked from the maintenance window, the trunk groups return to the state they were in before the extraction. If the trunk group was in-service before the extraction, then new call establishment will be available on that trunk group again.

For surprise extractions and failures, when the card is re-inserted, you need to restart call processing to re-initialize and return the card to service.

**Note:** You cannot hot swap the innermost CG6000 card set in the node. This card set acts as the clock master.



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

While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.



**CAUTION**  
**Possible equipment damage**

Use care when inserting and removing cards from the shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit. See Figure 1, "Loose spiral gasket," on page 37.

***At the System Management Console***

- 1 Using "Locking or unlocking a trunk group or a trunk" on page 109, perform a **force** or **graceful lock** on all the trunk groups associated with the CG6000 card being replaced.
- 2 Using "Locking or unlocking an interface card (CG6000), carrier, or channel" on page 101, perform a **force** or **graceful lock** on the CG6000 card being replaced.
- 3 Replace, move, remove, or add the CG6000 card(s) by performing the following steps:

- a** Determine the steps to follow based on the card configuration action you are performing.

<b>If</b>	<b>Do</b>
you are replacing only a front module	step b through m
you are replacing only a rear module	step f through m
you are replacing both a front module and a rear module	step j through m

- b** Remove the front module by performing the following steps:

- i** With a Phillips head screwdriver, loosen the screws that secure the module in the slot.
- ii** Unlock the lower lock latch on the module. When you unlock the lower lock latch, the blue light located at the bottom of the module faceplate will light.
- iii**



**WARNING**

Both the blue light and the red light must be lit before you can remove the module.

When the red “out of service” light located above the module on the alarm panel also lights, it is safe to remove the module from the card slot. Unlock the upper lock latch on the module and remove the module from the slot.

- c** Insert the new front module, lock the lock latches on the card and tighten the screws that secure the card in the shelf.
- d** Go to step 4.
- e** Remove the front module by performing the following steps:
  - i** With a Phillips head screwdriver, loosen the screws that secure the module in the slot.
  - ii** Unlock the lower lock latch on the module. When you unlock the lower lock latch, the blue light located at the bottom of the module faceplate will light.



iii

**WARNING**

Both the blue light and the red light must be lit before you can remove the module.

When the red “out of service” light located above the module on the alarm panel also lights, it is safe to remove the module from the card slot. Unlock the upper lock latch on the module and remove the module from the slot.

- f Remove the rear module by performing the following steps:
  - i With a Phillips head screwdriver, loosen the screws that secure the module in the slot.
  - ii Unlock the lock latches on the module.
  - iii Remove the module from the card slot.
- g Insert the new rear module, lock the lock latches, and tighten the screws that secure the module in the shelf.
- h Insert the front module that you removed in step e. Lock the lock latches on the card and tighten the screws that secure the card in the shelf.
- i Go to step 4.
- j Remove the front module by performing the following steps:
  - i With a Phillips head screwdriver, loosen the screws that secure the module in the slot.
  - ii Unlock the lower lock latch on the module. When you unlock the lower lock latch, the blue light located at the bottom of the module faceplate will light.

iii

**WARNING**

Both the blue light and the red light must be lit before you can remove the module.

When the red “out of service” light located above the module on the alarm panel also lights, it is safe to remove the module from the card slot. Unlock the upper lock latch on the module and remove the module from the slot.

- k** Remove the rear module by performing the following steps:
    - i** With a Phillips head screwdriver, loosen the screws that secure the module in the slot.
    - ii** Unlock the lock latches on the module.
    - iii** Remove the module from the card slot.
  - l** Insert the new rear module, lock the lock latches, and tighten the screws that secure the module in the shelf.
  - m** Insert the new front module. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.
- 4** Using the procedure “Locking or unlocking an interface card (CG6000), carrier, or channel” on page 101, unlock the CG6000 card that was just replaced.
- 5** Using the procedure “Locking or unlocking a trunk group or a trunk” on page 109, unlock of all the trunk groups associated with the CG6000 card that was just replaced.
- 6** You have completed this procedure.



# Configuration management

## How this chapter is organized

This chapter is organized as follows:

- “Overview” on page 47
- “Configuration procedures” on page 48
- “Changing SIP PRI Gateway configuration” on page 80

## Overview

The SIP PRI Gateway is deployed and configured using the System Management Console. Changes to system parameters are also made through the System Management Console. For more information, refer to the *Succession MX Management Module Basics* and the *Succession MX System Management Console Basics*.

This chapter describes the configurable parameters affecting operation of the SIP PRI Gateway and the procedures for configuration required at the service provider premises.

Screen shots in this document are representative of what you may see, but may not be the same for individual service providers due to the particular configuration shown.

## Configuration procedures



### CAUTION

Before making any changes to the base configuration, consult your support team.

This section contains the following procedures:

- “Adding the UAS load base software” on page 48
- “At the System Management Console” on page 50
- “Configuring the tabs” on page 54

Before adding the component, make sure that the UAS base software has been installed.

### Adding the UAS load base software

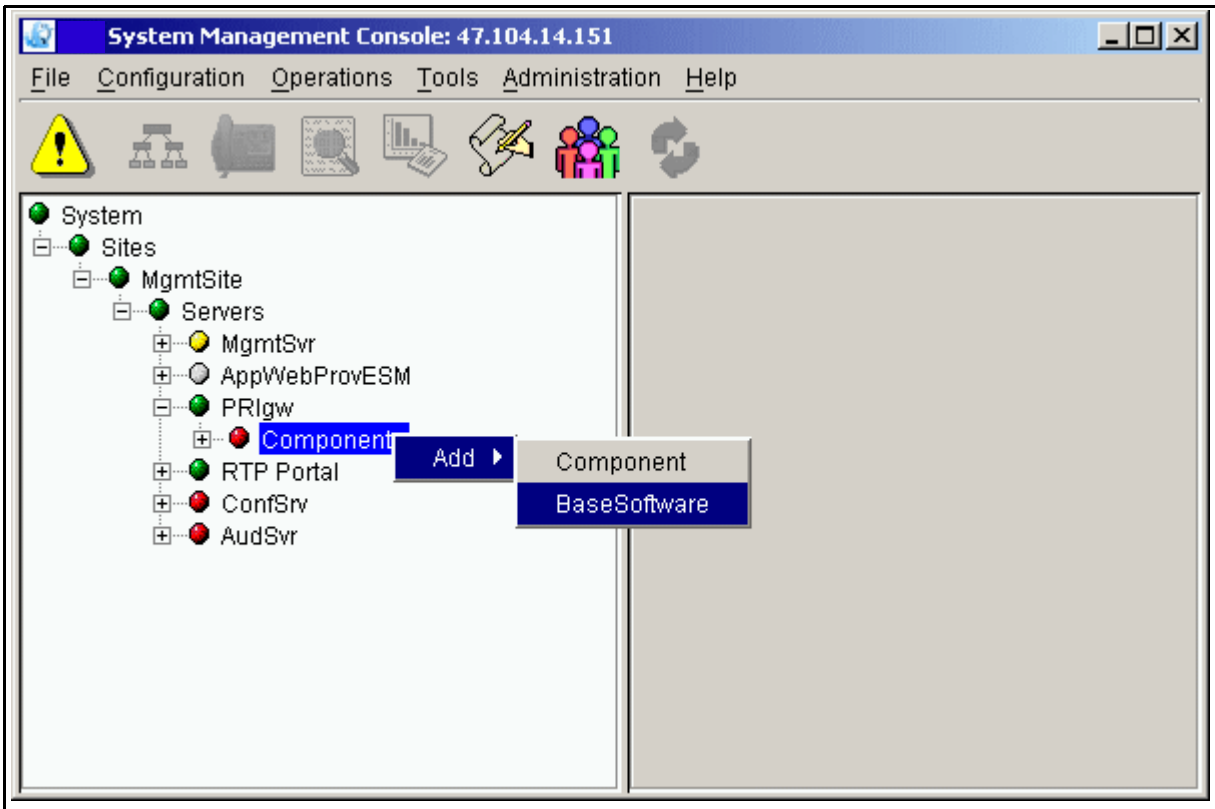
#### *at your workstation*

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP PRI Gateway bullet, as shown in Figure 1, “Adding Base Software.”

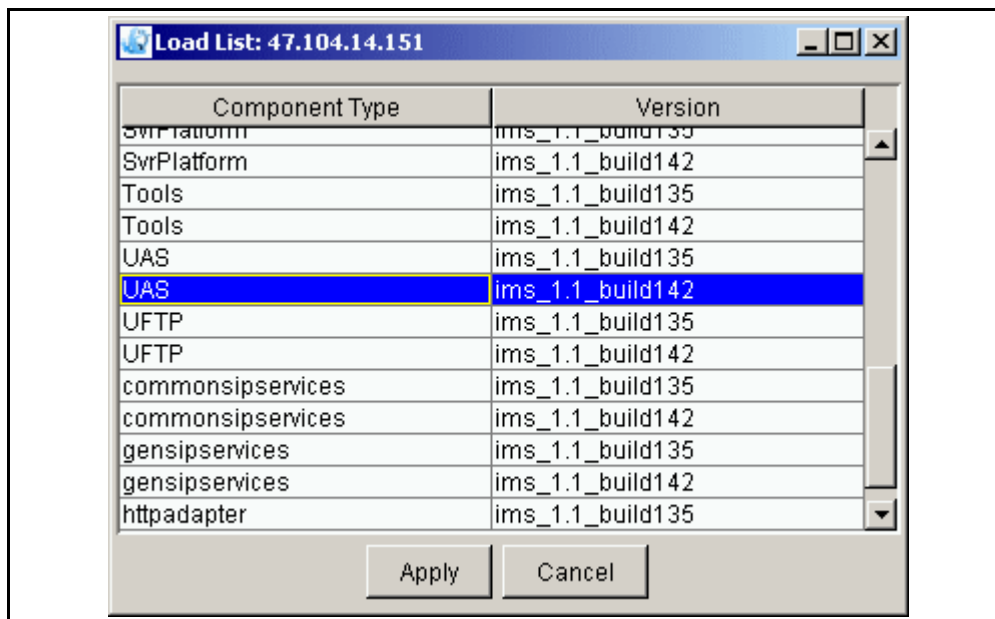
**Note:** The name of the SIP PRI Gateway is the name assigned to it during deployment, in this particular example, **PRlgw**.

- 2 Navigate to the gateway server that was installed at deployment. Right click on **Components**.

Select **Add->BaseSoftware**, as shown in the following figure.

**Figure 1 Adding Base Software**

3 Select the UAS load as shown in the following figure.

**Figure 2 Selecting the correct load**

- 4 Click the **Apply** button. The uasload is downloaded to the target SIP PRI Gateway node.
- 5 After the uasload download is complete, log into the system.
- 6 Connect to the node that you are upgrading.
- 7 Install the new software load by double-clicking **D: \IMS\uasload\WINNT\Setup.exe**.
- 8 An installation Wizard appears. Follow the steps in the Wizard.
- 9 If prompted to reboot, do so.

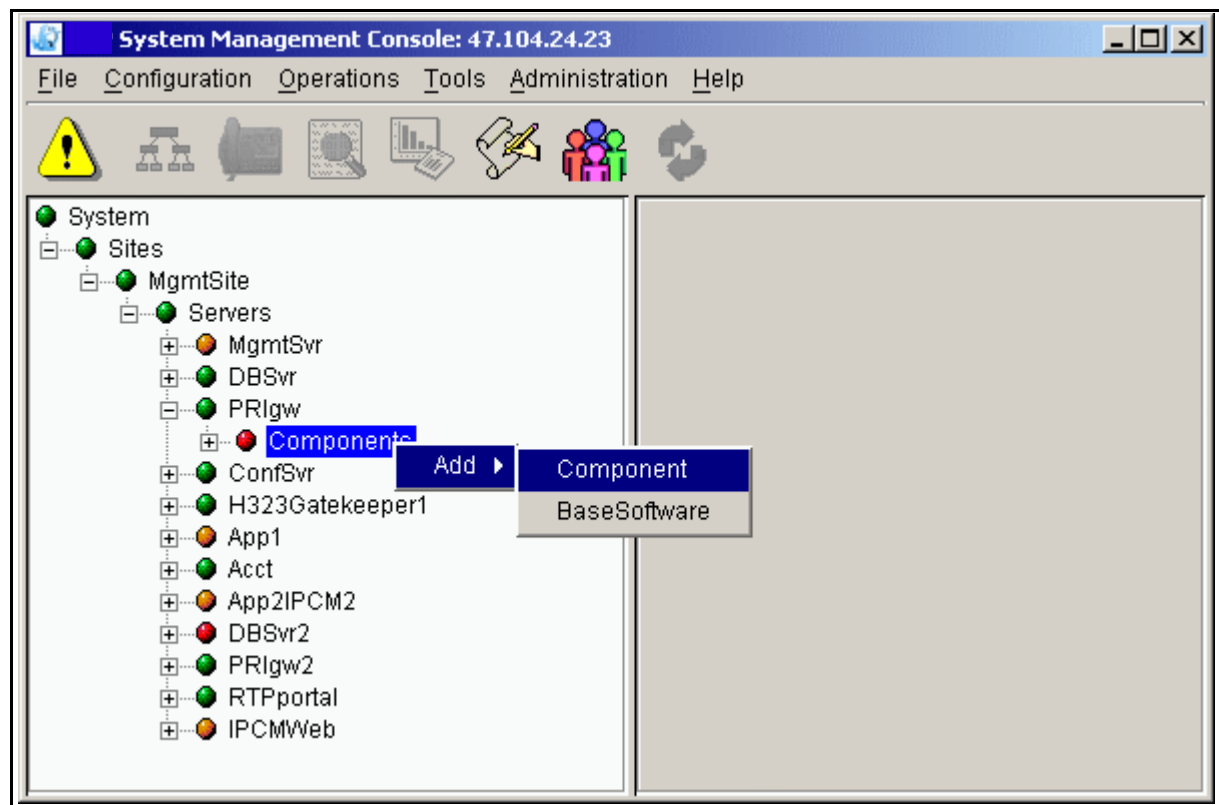
### Adding a component

Use the following procedure to add a SIP PRI Gateway component. The example shown assumes that the server on which the SIP PRI Gateway will be deployed has already been configured. For example, Figure 3, "Adding the component," shows the SIP PRI Gateway being deployed onto the previously configured server **PRlgw**.

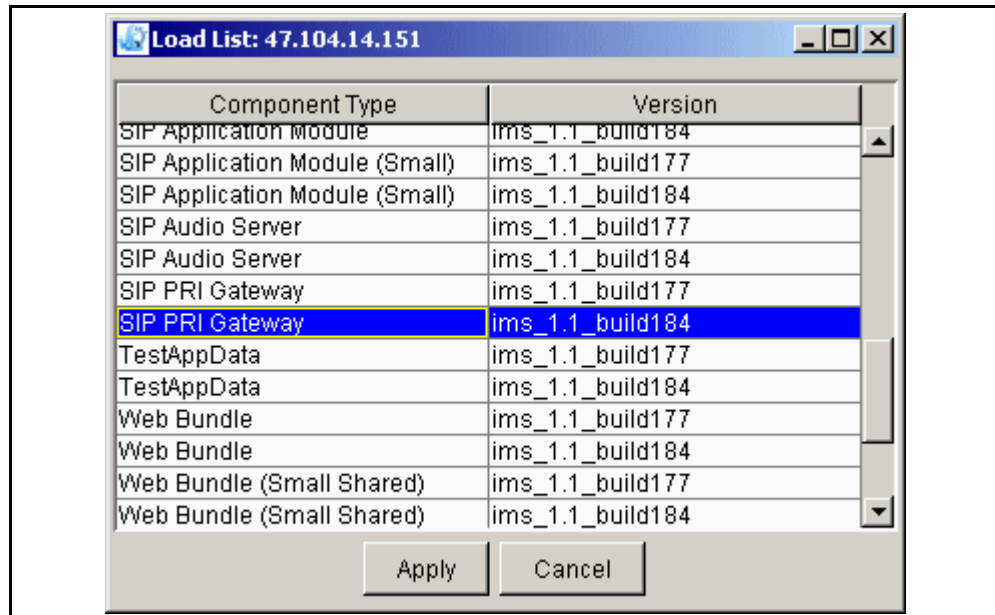
For the procedure for adding a server, refer to the *Succession MX System Management Console Basics* document.

### At the System Management Console

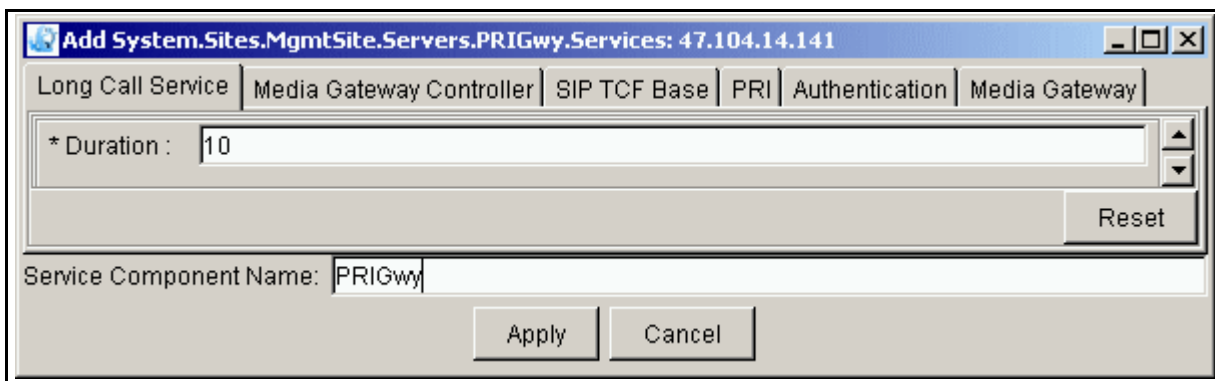
- 1 To add the SIP PRI Gateway component, right-click on **Components** under the server **PRIGwy** and select **Add->Component** as shown in Figure 3, "Adding the component."

**Figure 3 Adding the component**

- 2 The window shown in Figure 4, "Selecting the SIP PRI Gateway load," appears. There may or may not be multiple software loads for you to choose from. Select the SIP PRI Gateway load you want and click on the **Apply** button.

**Figure 4 Selecting the SIP PRI Gateway load**

- 3 The configuration window appears. Once the configuration window appears, enter a label with a maximum of six characters in the Service Component Name field at the bottom. This name must be unique among the components. The following figure shows an example with the name **PRIGwy** entered in the Service Component Name field.

**Figure 5 Example window with Service Component Name added**

4

**ATTENTION**

DO NOT click on **Apply** until you have FINISHED filling in the fields that you need.

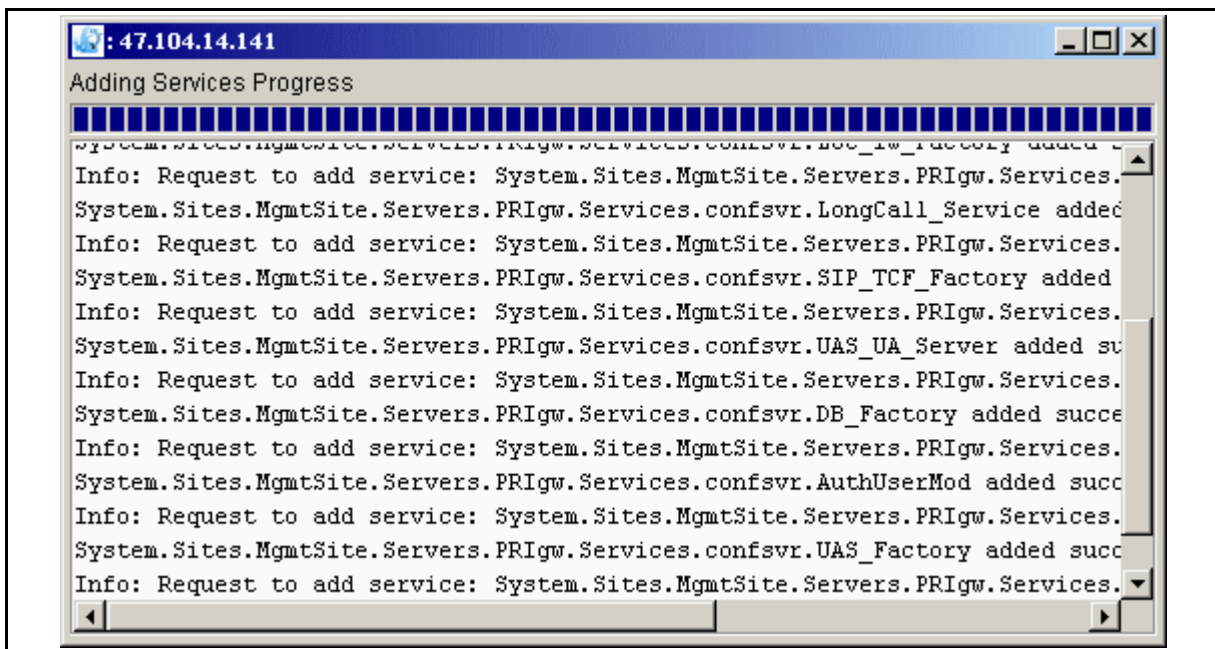


Note that there are a number of different tabs representing the configurable services that the SIP PRI Gateway requires. The following section in this chapter describes each tab in detail and provide guidance on how to configure the tabs. Many of the fields already contain default values, and administrators can leave most of these default values alone.

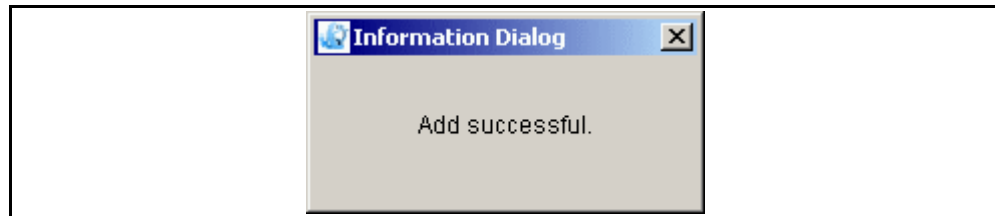
**Note:** The parameters with asterisks (\*) are mandatory. The grayed-out fields are for information only and cannot be changed.

After you click the **Apply** button, the System Manager begins the deployment of the SIP PRI Gateway software. The Adding Services Progress dialog box appears as shown in Figure 6, “Adding Services Progress dialog box.”

**Figure 6 Adding Services Progress dialog box**



If the deployment is successful, an “Add successful” box appears, as shown in Figure 7, “The Add successful dialog box.”

**Figure 7 The Add successful dialog box****ATTENTION**

When the system has finished initializing and becomes usable, the critical alarm disappears. See the *Succession MX System Management Console Basics* document.

**Configuring the tabs**

The following sections describe how to configure the tabs in detail.

**ATTENTION**

DO NOT click on **Apply** until you have FINISHED filling in the fields that you need.

**Configuring the Long Call Service tab**

Click on the Long Call Service tab and fill in the field as appropriate. The Long Call Service tab allows the service provider to set the length of time between endpoint audits. The Long Call Service detects abandoned calls and releases the resources used by such calls.

**Figure 8 The Long Call Service tab**

Add System.Sites.MgmtSite.Servers.PRIGwy.Services: 47.104.14.141  
 Long Call Service | Media Gateway Controller | SIP TCF Base | PRI | Authentication | Media Gateway  
 \* Duration : 10  
 Reset  
 Service Component Name: PRIGwy  
 Apply Cancel

**Table 1 Long Call Service tab field descriptions**

Field	Value	Description
Duration	Type=integer Range=1-60 minutes Default=10	This field indicates the length of time in minutes between endpoint audits. This field is used to detect abandoned calls. A value of zero deactivates it. The recommended value is 10 (minutes). If it detects an abandoned call leg, the resources will be released for that leg.

**Completing the Authentication tab**

Click on the Authentication tab and fill in the fields as appropriate. This tab enables the software to authenticate the proxies (or nodes) in the network that are authorized to request a conference. The SIP PRI Gateway processes the request (or message) if it is from an unauthorized (non-trusted) node. The Authentication tab enables or disables authentication for requests and sets additional authentication information.

**Figure 9 The Authentication tab**

Add System.Sites.MgmtSite.Servers.PRIGwy.Services: 47.104.14.141  
 Long Call Service | Media Gateway Controller | SIP TCF Base | PRI | **Authentication** | Media Gateway

Methods to Authorize :   
 Realm :   
 \* Private Key :   
 \* Nonce Interval : 600000  
 Authorized SIP Nodes : 60.60.60.150:5060  
 \* Nodal Auth : ☐

Reset

Service Component Name: PRIGwy

Apply Cancel

**Table 2 Authentication tab field descriptions (Sheet 1 of 2)**

Field	Value	Description
Methods to Authorize	Type=string Default=blank	This field is not used by the SIP PRI Gateway.
Realm	Type=string Range=0-256 characters Default=none	This field is not used by the SIP PRI Gateway.
Private Key	Type=string Range=0-256 characters Default=none	This field is not used by the SIP PRI Gateway.
Nonce Interval	Type=integer Range=10000- 600000 milliseconds Default=600000	The software uses this field to determine how long to wait (in milliseconds) for a response to a challenge with a specific nonce value before generating a new nonce value.

**Table 2 Authentication tab field descriptions (Sheet 2 of 2)**

Field	Value	Description
Authorized SIP Nodes	Type=string Range=0-2000 characters Default=none	This is a list of valid proxies (SIP Application Modules) from which the SIP PRI Gateway can accept Invites. If an Invite is received from another proxy, a 305 - "Use Proxy" message is sent back to tell the client to use one of the proxies in the list.
Nodal Auth.	Type=checkbox Default=checked	When checked, this field only allows messages from the SIP Application Module(s) listed in the Authorized SIP Nodes field to be accepted. If the field is not checked, the software accepts requests from any SIP Application Module.

**Completing the SIP TCF Base tab**

The SIP TCF Base provides support for the SIP protocol. The SIP PRI Gateway is one of several components that use the SIP TCF Base. Click on the tab and fill in the fields as appropriate. This field contains all the configuration data, such as the number of hops and timers, pertaining to the SIP protocol. The SIP TCF Base tab includes information regarding the transport IP addresses/ports, timers, number of redirects, and retransmission, among other items. Modifications to the SIP TCF Base tab require that the SIP TCF Base be locked.

**Figure 10 The SIP TCF Base tab**

Add System.Sites.MgmtSite.Servers.PRIGwy.Services: 47.104.14.141  
 Long Call Service | Media Gateway Controller | **SIP TCF Base** | PRI | Authentication | Media Gateway

\* Transport Config : UDP=0.0.0.0:5060:optional;TCP=0.0.0.0:5060:optional  
 \* Retransmission Off : ☐  
 \* Invite Timer : 128000  
 \* Application Type : user\_agent  
 \* Time Transaction : ☒  
 \* Add Defaults : ☒  
 \* Check Mandatory Headers : ☐  
 \* Maximum Number of Redirections : 5  
 \* Initial Maximum Hop Value : 20

Reset

Service Component Name: PRIGwy

Apply Cancel

**Table 3 SIP TCF Base tab field descriptions (Sheet 1 of 2)**

Field	Value	Description
Transport Config	Type=string Default=UDP=0.0.0.0:5060:optional;TCP=0.0.0.0:5060:optional	This field specifies the transport, IP addresses, and ports. Transports can appear more than once. Replace 0.0.0.0 with the private IP Address of the SIP PRI Gateway.
Retransmission Off	Type=checkbox Default=unchecked (false)	If this box is unchecked, SIP retransmission for unreliable transports is enabled. This is a read-only field.
Invite Timer	Type=integer Range=120000 to 3600000 milliseconds Default=128000	This controls the maximum time in milliseconds to wait for an INVITE to receive a Final Response, after receiving a provisional Response. Nortel Networks recommends that you use the default.

**Table 3 SIP TCF Base tab field descriptions (Sheet 2 of 2)**

Field	Value	Description
Application Type	Type=string Range=callstate_server, stateful_server, stateless_server, or user_agent Default=user_agent	This read-only field indicates that the SIP PRI Gateway is a "user-agent" type of SIP server.
Time Transaction	Type=checkbox Default=checked (true)	If checked, this read-only field specifies whether the SIP transactions should be timed.
Add Defaults	Type=checkbox Default=checked	If checked, this field allows the software to fill in missing mandatory headers with default values in the SDP message bodies. Nortel Networks recommends that the box be checked.
Check Mandatory Headers	Type=checkbox Default=unchecked	Controls whether the Mandatory SDP headers are checked for presence in the SDP messages. Nortel Networks recommends that the box not be checked.
Maximum Number of Redirections	Type=integer Range=3-10 characters Default=5	This is the maximum number of redirections allowed before the SIP PRI Gateway drops the request.
Initial Maximum Hop Value	Type=integer Range=5-50 characters Default=20	This is the maximum number of hops allowed before the SIP PRI Gateway drops the request.

### Configuring the Media Gateway Controller tab

Click on the Media Gateway tab and fill in the fields as appropriate. This service configures and controls communication with the Application Server.

**Figure 11 The Media Gateway Controller tab**

**Table 4 Media Gateway Controller tab field descriptions**

Field	Value	Description
Gateway ID	Type=string Range=1-20 characters Default=GW1	This field contains the Gateway server ID appended to the User Agent header delivered in all Invites originated from the Gateway.
Gateway User-Agent Header	Type=string Range=1-20 characters Default=SIP PRI Gateway	This field contains the User Agent name used in the User Agent header delivered in all Invites originated from the Gateway.
Application Server	Type=string Range=1-250 characters Default=0.0.0.0:5060	This field contains the ordered list of SIP Application Modules. Up to ten server IPs:ports may be listed, separated by a +. Use the private IP address.

### Configuring the Media Gateway tab

Click on the Media Gateway tab and fill in the fields as appropriate. All the configuration pertaining to the base UAS software is provided here. Basically, this tab contains all the media card configuration and SNMP configuration (used for polling alarms and OMs from base UAS software).



**Figure 12 The Media Gateway tab, General subfield**

Add System.Sites.MgmtSite.Servers.PRIGWY.Services: 47.104.14.141

Long Call Service | Media Gateway Controller | SIP TCF Base | PRI | Authentication | Media Gateway

General | SNMP | Media Cards | View Trunk Groups

\* Host Card Type: 5370 ☐ \* Use Existing Data

\* RTP Base Port: 30000 \* NTP Server IP Address

\* Toneset: France \* Alarm Synchronization Interval

\* Slot Number: 9 (dropdown menu showing 7, 9)

Reset

Service Component Name: PRIGWY

Apply Cancel

**Table 5 Media Gateway tab, General subfield descriptions (Sheet 1 of 2)**

Field	Value	Description
Host Card Type	Type=dropdown menu Range=5370 Default= 5370	This read-only field contains the host card type.
RTP Base Port	Type=string Default=30000 Range=1024-63094 characters	This field contains the base number of ports for the RTP stream. Nortel Networks recommends that you use the default.
Toneset	Type=string	This field is not used for the SIP PRI Gateway.

**Table 5 Media Gateway tab, General subfield descriptions (Sheet 2 of 2)**

Field	Value	Description
Slot Number	Type=string Range=7, 9 Default=9	This field contains the number of the physical slot on which the CPV5370 host card is installed. If the node is located in the left domain, the card will be in slot 7. If the node is located in the right domain, the card will be in slot 9.
Use Existing Data	Type=checkbox Default=unchecked	If checked, the software uses the existing configuration data on the SIP PRI Gateway. If unchecked, the existing data is not used. Nortel Networks recommends that this be checked when you do an update.
NTP Server IP Address	Type=string Range=7-15 characters Default=0.0.0.0	This logical IP address of the Network Time Protocol (NTP) server is the same as the private IP address of the Management Module. The software uses the NTP server so that all the clock timers on all the nodes are in sync.
Alarm Synchronization Interval	Type=integer Range=30000-60000 0 milliseconds Default=180000	This field contains the time interval in milliseconds after which alarms from the SIP PRI Gateway will be retrieved.

**Configuring the Media Gateway, SNMP sub-tab** Click on the Media Gateway, SNMP sub-tab, and fill in the fields as appropriate.

**Figure 13 The Media Gateway, SNMP sub-tab**

**Add System.Sites.MgmtSite.Servers.PRIGWY.Services: 47.104.14.141**

Long Call Service | Media Gateway Controller | SIP TCF Base | PRI | Authentication | Media Gateway

General | **SNMP** | Media Cards | View Trunk Groups

**SNMP Version 2C User**

\* Read Only Name: public

\* Read/Write Name: admin

**Trap Destination**

\* IP Address: 0.0.0.0

\* UDP Port: 162

Reset

Service Component Name: PRIGWY

Apply Cancel

**Table 6 Media Gateway, SNMP sub-tab field descriptions (Sheet 1 of 2)**

Field	Value	Description
Read Only Name	Type=string Default=public	This is a read-only field.
Read/Write Name	Type=string Default=admin	This is a read-only field.

**Table 6 Media Gateway, SNMP sub-tab field descriptions (Sheet 2 of 2)**

Field	Value	Description
IP Address	Type=string Range=7-15 characters Default=0.0.0.0	This field contains the private IP address of the SIP PRI Gateway to which the software sends all the SNMP traps containing alarms and logs.
UDP Port	Type=integer Default=162	This is a read-only field indicating that SNMP traps will be sent to Port 162.

**Completing the Media Gateway, Media Cards sub-tab** Use the values in the table for each card you want to configure on your system. You need to know the following configuration of the PRI Gateway Server machine:

- the number of media cards, their type (T1/E1), and the slots associated with those cards and other properties as listed on the panel
- the number of trunk groups that are associated with each media card and the port on the media card

Before adding a trunk group associated with a media card, configure all the properties on the screen shown above correctly, then click on the **Add** button. After you add a trunk group, you cannot modify some of the properties for that media card.

**Figure 14 The Media Gateway, Media Cards sub-tab**

The screenshot shows a configuration window titled "Add System Sites Mgmt Site Servers PRI Gwy Services: 47.104.14.141". The "Media Gateway" tab is selected, and the "Media Cards" sub-tab is active. The configuration is for "Card 11".

**Media Card Present:** ☒ (checked)

**\* IP Address:** 47.249.48.20

**\* Subnet Mask:** 255.255.255.128

**\* Router IP Address:** 47.249.48.20

**\* BCT Support:** DISABLED

**\* Protocol Variant:** DMS

**\* Signal Type:** PRI

**\* Card Type:** T1

**\* CRCMF:** OFF

**\* Impedance:** OSX1

**\* Frame Type:** ESF

**\* ISDN Flag:** YES

**\* Line Code:** B8ZS

**\* Compression Mode:** MU-LAW

**Carrier Configuration:**

Port	Line Length
Port 1	PMT 100
Port 2	PMT 100
Port 3	PMT 100
Port 4	PMT 100

**Trunk Groups:**

Tru...	Trunk Grou...	Domain	SubDom...	Voicema...	Meridian Fl...	Messaging T...	Term Ty...	Numb...	Numb...	D-C...	D-C...	D-C...	Card	Port

Service Component Name: PRI Gwy

Buttons: Apply, Cancel, Reset

**Table 7 Media Gateway, Media Cards sub-tab field descriptions (Sheet 1 of 3)**

Field	Value	Description
Media Card Present	Type=checkbox Default=unchecked	Check this box only if a media card is installed in any of these slots (Card 11, 12, and so on, in the example shown in Figure 14).
IP Address	Type=string Range=7-15 characters Default=0.0.0.0	This field contains the IP address of this particular media card.
Subnet Mask	Type=string Range=7-15 characters Default=255.255.255.128	This field contains the subnet mask associated with the card.
Router IP Address	Type=string Range=7-15 characters Default=0.0.0.0	This field contains the router associated with the card.
BCT Support	Type=pulldown menu Range=DISABLED, ENABLED Default=DISABLED	This field does not support the SIP PRI Gateway.

**Table 7 Media Gateway, Media Cards sub-tab field descriptions (Sheet 2 of 3)**

Field	Value	Description
Protocol Variant	<p>Type=pulldown menu  Range=(T1) 4ESS, 5E10, DMS, NI2, NTT,  Default=(T1) DMS</p> <p>Range= (E1) FTVN6, AUSTEL1, KOREA, HONGKONG, TAIWAN, ETSI_Aus, ETSI_Aut, ETSI_Bel, ETSI_Chn, ETSI_Den, ETSI_Fin, ETSI_Ger, ETSI_Grc, ETSI_Icl, ETSI_Ire, ETSI_Ita, ETSI_Lie, ETSI_Lux, ETSI_Net, ETSI_Nor, ETSI_Por, ETSI_Rus, ETSI_Sin, ETSI_Spn, ETSI_Swe, ETSI_Swi, ETSI_Gbr, QSIG  Default=(E1) FTVN6 (France)</p>	<p>This field specifies the trunk group PRI signaling protocol variant. This is a read-only field if there are trunk groups already defined. You cannot change the Protocol Variant unless you delete all the trunk groups from the card; then you can use the pull-down menu to select. If you haven't provisioned any trunk groups yet, this field can be changed.</p>
Signal Type	<p>Type=pulldown menu  Range=PRI  Default=PRI</p>	<p>This field specifies the type of signaling that must be supported on the carrier.</p>
CRCMF	<p>Type=pulldown menu  Range=ON, OFF  Default=(T1) OFF  Default=(E1) ON</p>	<p>This field indicates whether the cyclical redundancy checking is used. Typical deployments have CRC off, but this actually depends on how the far end has its T1 or E1 span configured. Nortel Networks recommends that CRC be OFF.</p>
Frame Type	<p>Type=pulldown menu  Range=(T1) ESF, D4  Default=(T1) ESF</p> <p>Range=(E1) CEPT  Default=(E1) CEPT</p>	<p>This field specifies the frame formatting used on the carrier. Either ESF or D4 is valid; however, the typical deployment is ESF. D4 is not typically used in newer deployments.</p>

**Table 7 Media Gateway, Media Cards sub-tab field descriptions (Sheet 3 of 3)**

Field	Value	Description
ISDN Flag	Type=pulldown menu Range=YES, NO Default=YES	This field specifies whether or not a PRI D-channel exists on the carrier. Much like Signal Type, this deals with whether this T1 trunk has a signaling channel on it or not. Set this field to YES.
Card Type	Type=pulldown menu Range=T1, E1 Default=T1	This field specifies the carrier type for the trunk group as either T1 or E1.
Impedance	Type=pulldown menu Range=(T1) DSX1 Default=(T1) DSX1  Range=(E1) E75, E120 Default=(E1) E120	This field specifies the type of cable being used for the physical carrier connection. There is only one choice for T1 cards. For E1 cards there are two choices: 75 and 120 ohm. Coaxial cable terminations use 75 and twisted pair terminations use 120.
Line Code	Type=pulldown menu Range=(T1) B8ZS Default=(T1) B8ZS  Range=(E1) HDB3 Default=(E1) HDB3	This field specifies the density maintenance method being used on the carrier line to maintain a clear channel transmission.
Compression Mode	Type=pulldown menu Range=MU-LAW, A-LAW Default=MU-LAW	This field specifies the G.711 compression mode being used on the card carriers.

Click on any of the PMT buttons to modify or configure performance thresholds. The following screen appears. Fill in the fields as appropriate.

**Figure 15 Modifying the Performance Thresholds**

15-Minute Thresholds		24-Hour Thresholds	
Controlled Slip Seconds	1	Controlled Slip Seconds	4
Errored Seconds	65	Errored Seconds	648
Severely Errored Seconds	10	Severely Errored Seconds	100
Severely Errored Framing Seconds	2	Severely Errored Framing Seconds	17
Unavailable Seconds	10	Unavailable Seconds	10
Line Code Violations	13340	Line Code Violations	133400

Accept Cancel

**Table 8 Media Gateway, Media Card sub-tab, PMT field descriptions (Sheet 1 of 2)**

Field	Value	Description
<i>15-Minute Thresholds</i>		
Controlled Slip Seconds	Type=integer Range=0-32767 characters Default=1	This field specifies the 15-minute threshold for controlled slip seconds; in other words, by entering <b>1</b> , you are allowing 1 slip in a 15-minute period before reporting an alarm.
Errored Seconds	Type=integer Range=0-32767 characters Default=65	This field specifies the 15-minute threshold for errored seconds.
Severely Errored Seconds	Type=integer Range=0-32767 characters Default=10	This field specifies the 15-minute threshold for severely errored seconds.
Severely Errored Framing Seconds	Type=integer Range=0-32767 characters Default=2	This field specifies the 15-minute threshold for severely errored framing seconds.



**Table 8 Media Gateway, Media Card sub-tab, PMT field descriptions (Sheet 2 of 2)**

Field	Value	Description
Unavailable Seconds	Type=integer Range=0-32767 characters Default=10	This field specifies the 15-minute threshold for unavailable seconds.
Line Code Violations	Type=integer Range=0-32767 characters Default=13340	This field specifies the 15-minute threshold for line code violations.
<i>24-Hour Thresholds</i>		
Controlled Slip Seconds	Type=integer Range=1-2147483647 characters Default=4	This field specifies the 24-hour threshold for controlled slip seconds.
Errored Seconds	Type=integer Range=1-2147483647 characters Default=648	This field specifies the 24-hour threshold for errored seconds.
Severely Errored Seconds	Type=integer Range=1-2147483647 characters Default=100	This field specifies the 24-hour threshold for severely errored seconds.
Severely Errored Framing Seconds	Type=integer Range=1-2147483647 characters Default=17	This field specifies the 24-hour threshold for severely errored framing seconds.
Unavailable Seconds	Type=integer Range=1-2147483647 characters Default=10	This field specifies the 24-hour threshold for unavailable seconds.
Line Code Violations	Type=integer Range=1-2147483647 characters Default=133400	This field specifies the 24-hour threshold for line-code violations.

**Completing the Media Gateway, Media Cards section, trunk group subsection**

To best understand the logic behind the configuration of the media card trunk group subsection, refer to “Configuring the Add Trunk Group dialog box” on page 83 before filling in the Add Trunk Group dialog box.

## Procedure 1 Adding a trunk group

### at the *Media Gateway* tab, *System Management Console*

- 1 To add a trunk group, select the **Add** button at the bottom of the Trunk Group section, as shown.

**Figure 16 The Media Gateway, Media Cards sub-tab, trunk group subsection**

The screenshot shows a configuration window titled "Add System.Sites.MgmtSite.Servers.PRIGw2.Services: 47.104.14.151". The "Media Gateway" tab is selected, and the "Media Cards" sub-tab is active. The window is divided into two main sections: "Media Card Present" and "Trunk Groups".

**Media Card Present Section:**

- ☒ **Media Card Present**
- \* IP Address: 60.60.60.112
- \* Subnet Mask: 255.255.255.128
- \* Router IP Address: 60.60.60.112
- \* BCT Support: DISABLED
- \* Protocol Variant: DMS
- \* Signal Type: PRI
- \* CRMF: OFF
- \* Frame Type: ESF
- \* ISDN Flag: YES
- \* Card Type: T1
- \* Impedance: DSX1
- \* Line Code: B8ZS
- \* Compression Mode: MU-LAW

**Carrier Configuration Section:**

Port	Line Length
Port 1	PMT 100
Port 2	PMT 100
Port 3	PMT 100
Port 4	PMT 100

**Trunk Groups Section:**

Tru...	Trunk Gro...	Domain	SubDo...	Voicem...	Meridian ...	Messaging ...	Term T...	Numberin...	Nu...	D-...	D-...	D-C...	Card	Port

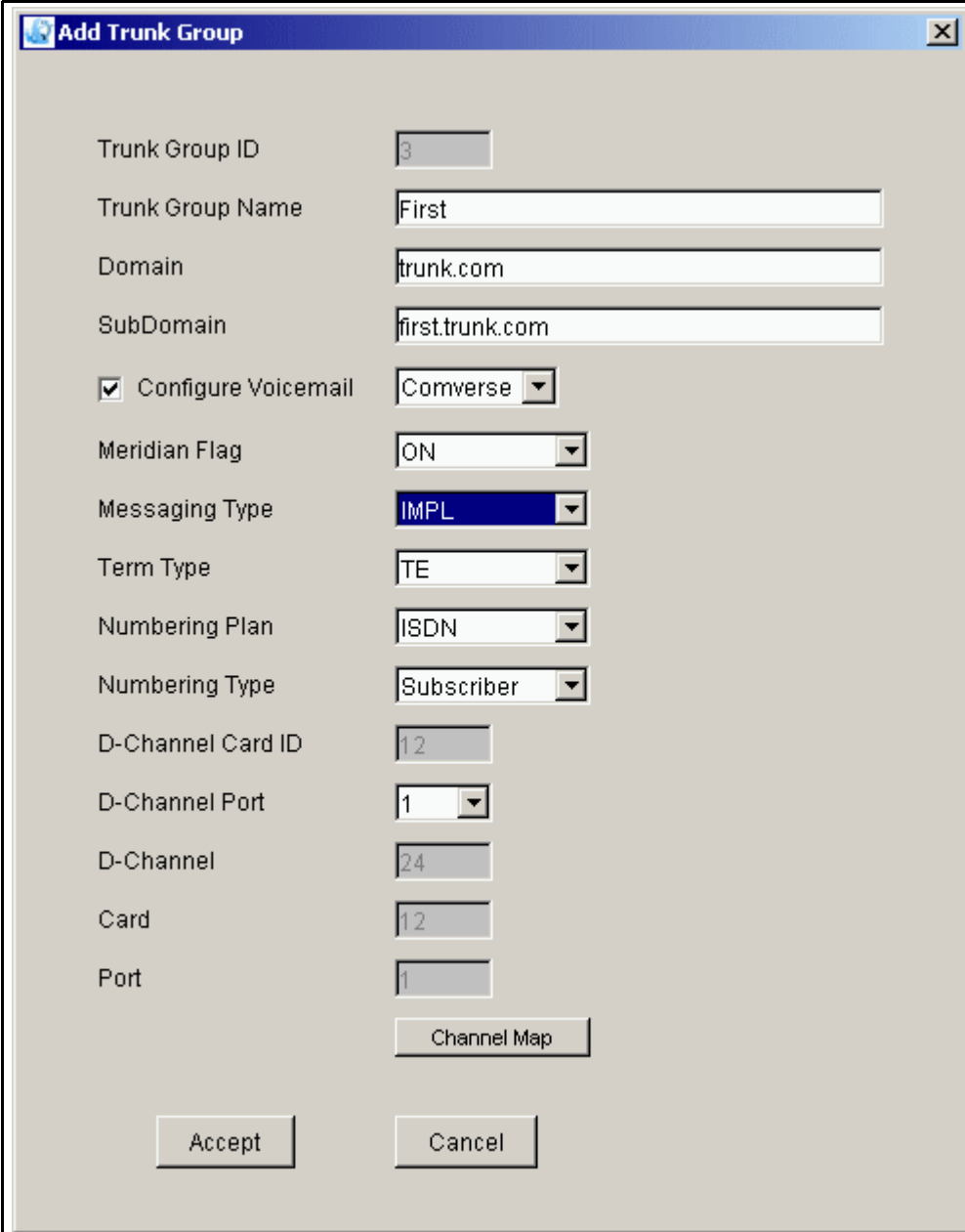
Buttons: Add, Modify, Delete, View, Reset

Service Component Name: PRIGw2

Buttons: Apply, Cancel

- 2 Enter data into the pop-up window (see Figure 17, "The Media Gateway, Media Cards sub-tab, Add Trunk Group dialog box"). Table 9, "Media Gateway, Media Cards sub-tab, trunk group subsection field descriptions," shows the field descriptions for the fields that appear in this window.

**Figure 17 The Media Gateway, Media Cards sub-tab, Add Trunk Group dialog box**



The image shows a Windows-style dialog box titled "Add Trunk Group". It contains several input fields and dropdown menus for configuring a trunk group. The fields are arranged in a vertical list on the left, with their corresponding input controls on the right. At the bottom, there are "Accept" and "Cancel" buttons, and a "Channel Map" button is located above the "Accept" button.

Field	Value
Trunk Group ID	3
Trunk Group Name	First
Domain	trunk.com
SubDomain	first.trunk.com
<input checked="" type="checkbox"/> Configure Voicemail	Comverse
Meridian Flag	ON
Messaging Type	IMPL
Term Type	TE
Numbering Plan	ISDN
Numbering Type	Subscriber
D-Channel Card ID	12
D-Channel Port	1
D-Channel	24
Card	12
Port	1

Channel Map

Accept Cancel

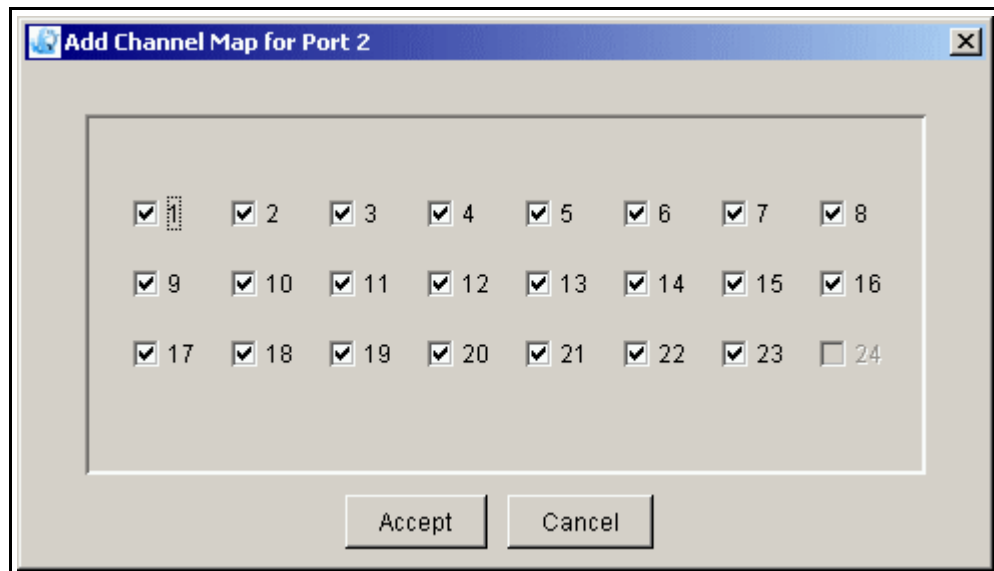
**Table 9 Media Gateway, Media Cards sub-tab, trunk group subsection field descriptions (Sheet 1 of 2)**

Field	Value	Description
Trunk Group ID	Type=integer	This is a read-only field. This number identifies the individual trunk group in the list that appears in the configuration screen.
Trunk Group Name	Type=string Range=0-39 printable characters, no white spaces allowed Default=blank	This field contains the descriptive name that identifies a group of B-channels on a carrier.
Domain	Type=string Range=0-39 printable characters, no white spaces allowed Default=blank	This field identifies the trunk group carrier owner.
SubDomain	Type=string Range=0-39 printable characters, no white spaces allowed Default=blank	This field indicates the subdomain associated with the trunk group carrier. The subdomain must be fully qualified (in other words, containing both the subdomain and domain).
Configure Voicemail	Type=checkbox Range if checked=Comverse, Other Default=unchecked	Check this box only if this specific T1 or E1 span is connected to a voicemail system.
Meridian Flag	Type=dropdown menu Range=OFF, ON Default=OFF	This field specifies whether the peer switch to which the PRI trunk group is connected is a Meridian switch or not. OFF means the switch is not connected; ON means the switch is connected.
Messaging Type	Type=dropdown menu Range=IMPL, EXPL Default=IMPL	This field specifies if the D-channel messaging is explicit or implicit to the PRI trunk group.
Term Type	Type=dropdown menu Range=TE, NT Default=TE	This field specifies if the carrier ISDN termination is TE (terminal equipment) or NT (network termination).

**Table 9 Media Gateway, Media Cards sub-tab, trunk group subsection field descriptions (Sheet 2 of 2)**

Field	Value	Description
Numbering Plan	Type=dropdown menu Range=Private, Unknown, ISDN, Telephone, Data, TElex, National Default=Unknown	This field specifies the numbering plan used for the trunk group.
Numbering Type	Type=dropdown menu Range=Unknown, Subscriber, International, National, Local, Abbreviated, Net_SPF Default=Unknown	This field specifies the numbering type used for the trunk group.
D-Channel Card ID	Type=integer	This read-only field shows the location of the PRI trunk group D-channel carrier TDM adapter interface card.
D-Channel Port	Type=dropdown menu Range=1, 2, 3, 4 Default=1	This field shows the local port location of the PRI trunk group D-channel carrier on the TDM adapter interface card.
D-Channel	Type=integer	This read-only field shows the carrier channel selected to be the D signaling channel for the trunk group. It is 24 for T1, 16 for E1.
Card	Type=integer	This read-only field shows the slot location of the trunk group carrier TDM adapter interface card.
Port	Type=integer	This read-only field shows the local port location of the trunk group carrier on the TDM adapter interface card.
Channel Map	Type=radio button	Click on this button to enable or disable specific B-channels for this trunk group carrier.

- 3 When you click on the Channel Map button, you will see the following pop-up box. You can select or deselect specific B channels, then click on the **Accept** button or **Cancel**. Uncheck the boxes only if that specific B-channel is out of service.

**Figure 18 Channel Map selection box**

- 4 You can now click on the **Accept** button to add the newly configured trunk group, or **Cancel**. If you click on **Accept**, you will see the trunk group appear as shown in Figure 19, "The Media Gateway tab with new trunk added."

**Figure 19 The Media Gateway tab with new trunk added**

**Add System.Sites.MgmtSite.Servers.PRIGw2.Services: 47.104.14.151**

SIP TCF Base | Media Gateway Controller | PRI | Long Call Service | Authentication | Media Gateway

IP Address: 60.60.60.112 | Signal type: PRI | Card type: 1

\* Subnet Mask: 255.255.255.128 | \* CRCMF: OFF | \* Impedance: DSX1

\* Router IP Address: 60.60.60.112 | \* Frame Type: ESF | \* Line Code: B8ZS

\* BCT Support: DISABLED | \* ISDN Flag: YES | \* Compression Mode: MU-LAW

\* Protocol Variant: DMS

Trunk Groups

Tru...	Trunk Gro...	Domain	SubDo...	Voicem...	Meridian ...	Messaging ...	Term T...	Numb...
1	First	trunk.com	first.trun...	Comverse	ON	IMPL	TE	ISDN
2	subRich	nortel.co...	rich.nort...	Comverse	ON	IMPL	TE	Private

Add Modify

Reset

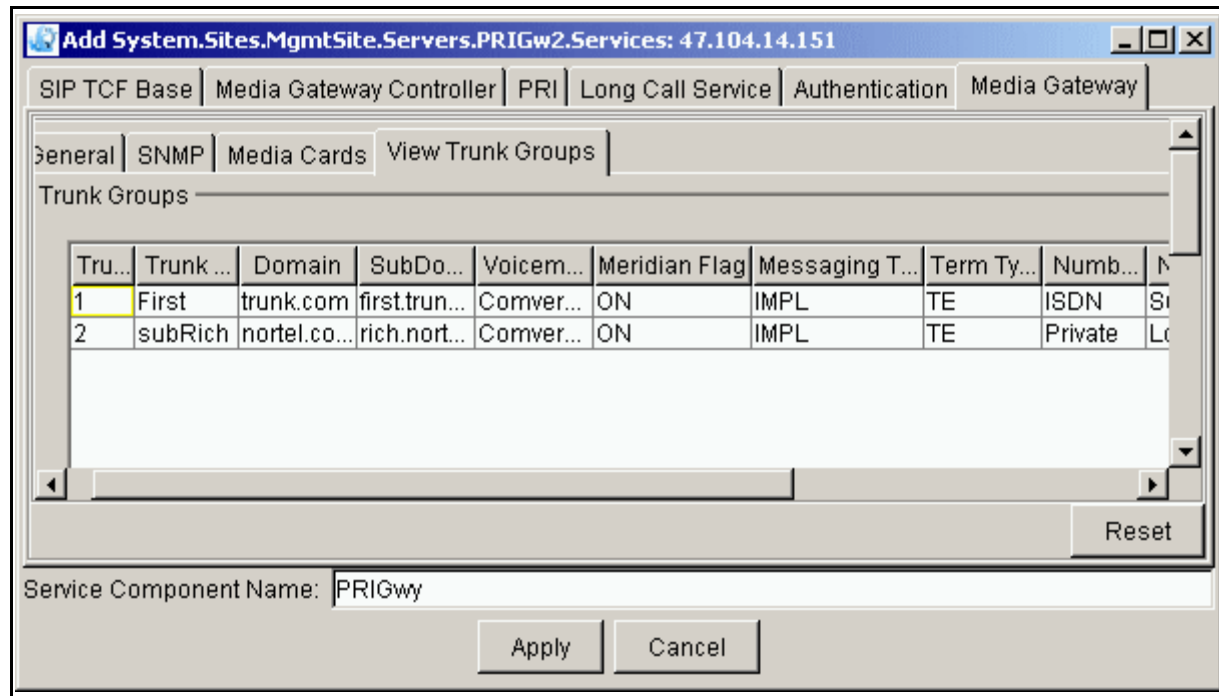
Service Component Name: PRIGwy

Apply Cancel

**Viewing the Media Gateway, View Trunk Groups sub-tab**

Click on View Trunk Groups to view the configured trunk groups.

**Figure 20 The Media Gateway, View Trunk Groups sub-tab**





## Configuring the PRI tab

Click on the PRI tab and fill in the fields as appropriate.

**Figure 21 The PRI tab**

**Add System.Sites.MgmtSite.Servers.PRIGWY.Services: 47.104.14.141**

Long Call Service | Media Gateway Controller | SIP TCF Base | **PRI** | Authentication | Media Gateway

\* Gateway IP Addr : 0.0.0.0

\* Gateway Domain : domain.com

\* DTMF Digits Enabled : ☒

\* RTP Type of Service : 184

\* PRI Default Calling Party : 5550000

\* Calling Party Num Handling : actualParty

\* Restricted-User Default Name : Unknown\_User

\* Restricted-User Default Number : Unknown\_Number

\* SIP Default User Name : Unknown

\* Codec Preference : PCMU,PCMA,G729,G723

\* SDP Session Name : Unknown Session

\* Trunk Group Alias Token : nortelTrkGrp

\* Default Trunk Domain : domain.com

\* Num of Trunk Retries : 2

Reset

Service Component Name: PRIGWY

Apply Cancel

**Table 10 PRI tab field descriptions (Sheet 1 of 3)**

Field	Value	Description
Gateway IP Addr	Type=string Range=1-15 characters Default=0.0.0.0	This field contains the private IP address of the SIP PRI Gateway.
Gateway Domain	Type=string Range=1-64 characters Default=domain.com	This field contains the gateway domain address in the format: HostName.PrimaryDNSSuffix (example: DallasGW.us.nortel.com). You can find this address by going to the C:\ prompt, then typing <b>nslookup &lt;IP GW&gt;</b> .

**Table 10 PRI tab field descriptions (Sheet 2 of 3)**

Field	Value	Description
DTMF Digits Enabled	Type=checkbox Default=checked	Check this field to enable the SIP PRI Gateway to generate DTMF tones on behalf of the SIP clients.
RTP Type of Service	Type=integer Range=0-184 characters Default=184	This field specifies the priority of the RTP packets throughout the network.
PRI Default Calling Party	Type=integer Range=1-999999999999 characters Default=5550000	This field indicates the default phone number for the outgoing Calling Party Number Information Element. Use is controlled by the Calling Party Num Handling field.
Calling Party Num Handling	Type=string Range=fixed, numericOnly, actualParty Default=actualParty	This field specifies the population of the outgoing PRI Calling Party Number. If the choice is <b>fixed</b> , then the software uses the PRI Default Calling Party field. If the choice is <b>numericOnly</b> , the software uses the default. If the choice is <b>actualParty</b> , the software uses the whatever value is in the SIP signal. If the number contains alphanumeric digits, the software uses whatever value is contained in the SIP signal.
Restricted-User Default Name	Type=string Range=1-20 characters Default=Unknown_User	This field is used to populate the FROM header when the PRI signaling indicates the calling party information is restricted.
Restricted-User Default Number	Type=string Range=1-20 characters Default=Unknown_Number	This field is used to populate the FROM header when the PRI signaling indicates the calling party information is restricted.
SIP Default User Name	Type=string Range=1-32 characters Default=Unknown	This field is used to populate a user name in the FROM header when the PRI call does not provide calling party information.
Codec Preference	Type=string Range=PCMU, PCMA, G729, G723 Default=PCMU, PCMA, G729, G723	This field indicates the supported Gateway codecs in order of preference. Specify one or more comma-separated codecs.

**Table 10 PRI tab field descriptions (Sheet 3 of 3)**

Field	Value	Description
SDP Session Name	Type=string Range=1-20 characters Default=Unknown Session	This field indicates the name that appears in the SDP Session Name attribute of SIP messages.
Trunk Group Alias Token	Type=string Range=1-20 characters Default=nortelTrkGrp	This field indicates the parameter token used in the Request URI to specify the PRI trunk.
Default Trunk Domain	Type=string Range=1-32 characters Default=domain.com	This field indicates the default domain to use when a domain is not configured for the trunk being used.
Num of Trunk Retries	Type=integer Range=0-9 characters Default=2	This field indicates the number of times to try a new trunk member when a request is denied.

## Changing SIP PRI Gateway configuration

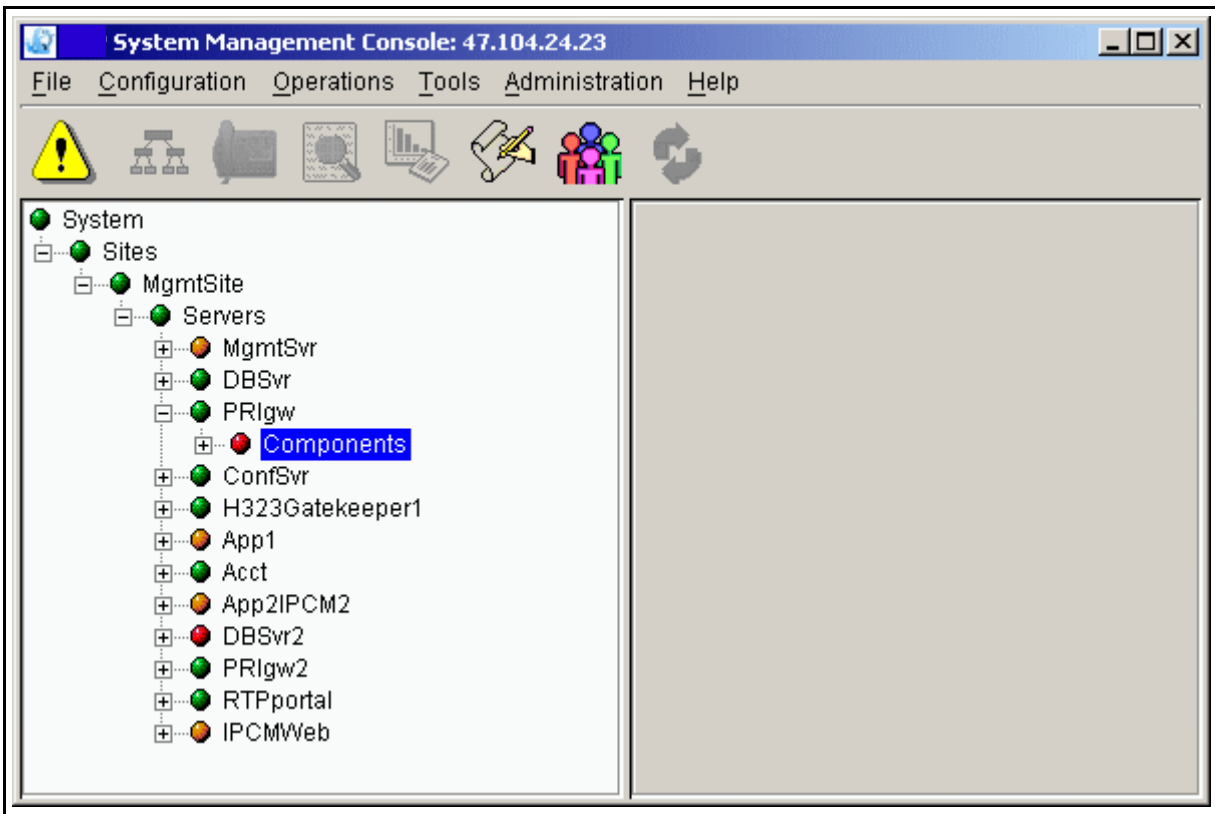
### ATTENTION

The SIP PRI Gateway does not process any calls at this time. During this process, you will see a critical alarm. Before you change any tab, you must lock it.

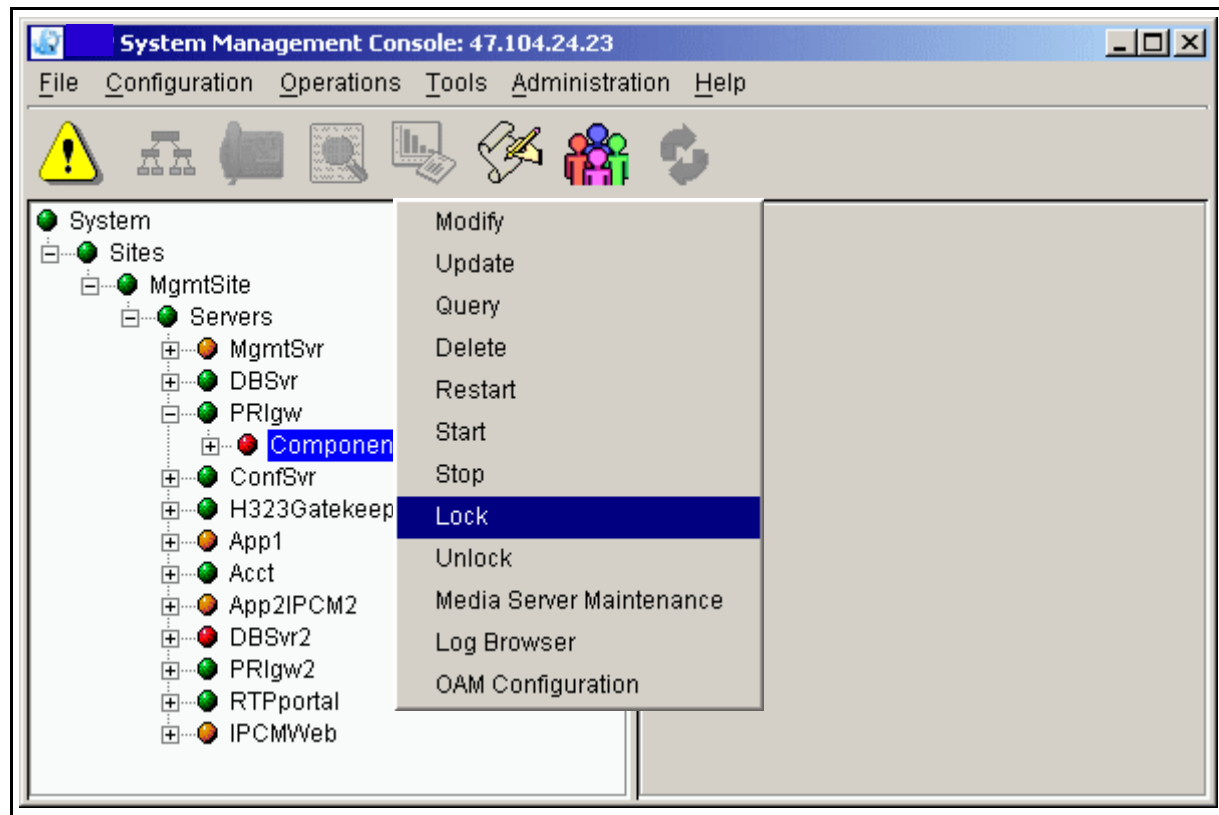
### At the System Management Console

- 1 Navigate through the system hierarchy tree located in the left panel as shown in Figure 22, "Navigation path."

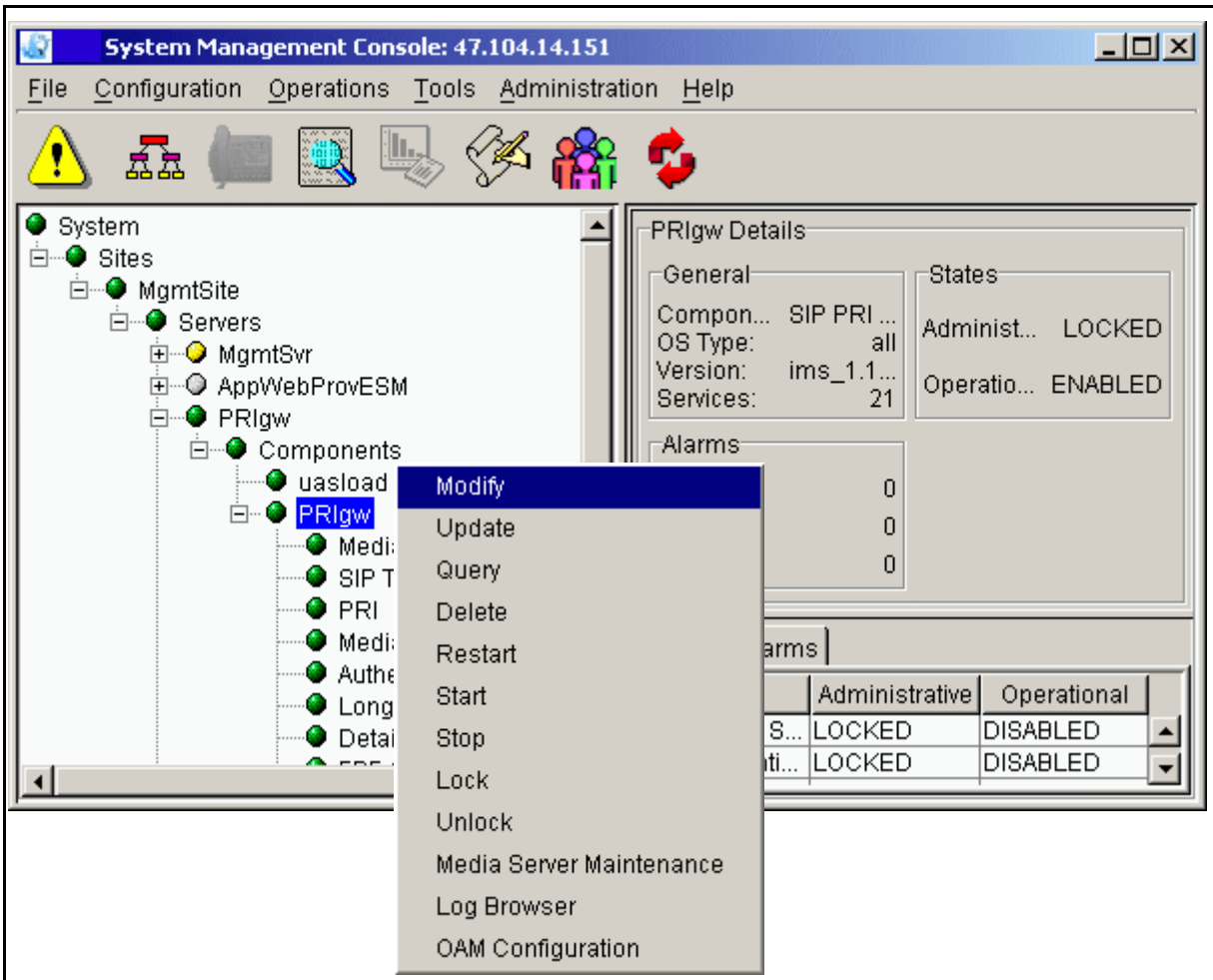
Figure 22 Navigation path



- 2 Right-click on the SIP PRI Gateway bullet (**PRIgw** in the example).
- 3 Select **Lock** in the pop-up menu that appears.

**Figure 23 Locking the PRIgw component**

- 4 Right-click the SIP PRI Gateway bullet again.
- 5 Select **Modify**, as shown.

**Figure 24 Modify menu**

The tabs appear.

- 6 Select the tab you want to modify.
- 7 Change the information as needed.
- 8 Click **Apply**, located at the bottom of the window. The software restarts automatically after you hit the **Apply** button.

If the deployment is not successful, re-examine the configuration tabs and verify that all 0.0.0.0 IP addresses have been replaced with the correct IP address. Verify other non-default parameters for accuracy. After the SIP PRI Gateway initializes, the services

will be unlocked and enabled. If they are locked or disabled, bring up the alarm browser to find any alarms.

#### ATTENTION

When the system has finished initializing and becomes usable, the critical alarm disappears. See the *Succession MX System Management Console Basics* document for more information.

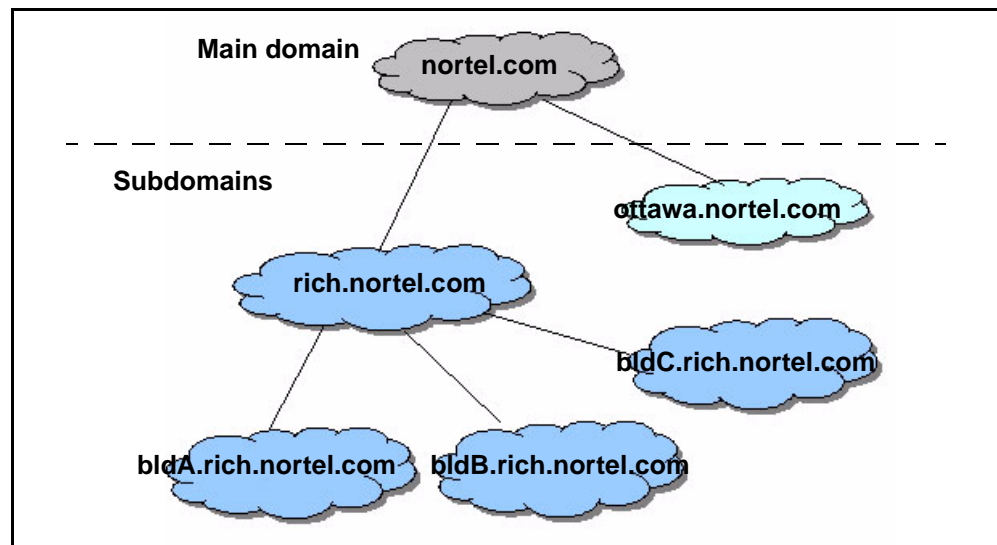
## Additional configuration details

### Configuring the Add Trunk Group dialog box

This example illustrates how to complete the Add Trunk Group dialog box. Figure 25, "Routing example," shows how the SIP PRI Gateway uses the datafill in this section to route calls through domains and subdomains. In this example, the SIP PRI Gateway has the following connections to the network components:

- one trunk group (T1) to nortel.com
- one trunk group (T1) to rich.nortel.com
- one trunk group (T1) each to bldA.rich.nortel.com, bldB.rich.nortel.com, bldC.rich.nortel.com
- four trunk groups (T1) to ottawa.nortel.com

**Figure 25 Routing example**



In this case, you could enter the information into the Add Trunk Group dialog box as follows:

**Table 11 Sample Trunk Group entries**

TGID	Alias	Domain	Subdomain	Card	Port
1	parent	nortel.com		0	0
2	subRich	nortel.com	rich.nortel.com	0	1
7	subOttawa1	nortel.com	ottawa.nortel.com	1	2
8	subOttawa1	nortel.com	ottawa.nortel.com	1	3
9	subOttawa2	nortel.com	ottawa.nortel.com	2	0
10		nortel.com	ottawa.nortel.com	2	1

For *SIP-to-PRI* trunk selections, based on the incoming request URI from the SIP Application Server, the SIP PRI Gateway uses the following logic to select a trunk:

- If the URI contains both trunk group name and domain,
  - The SIP PRI Gateway compares the incoming domain from the request URI with the subdomain listed for each trunk in the tab. If there is no subdomain, the software uses the listed domain.
  - If a single trunk matches both alias and domain, then the SIP PRI Gateway selects that trunk. If there is more than one match, the SIP PRI Gateway selects the first trunk that matches.
- If the URI contains only a domain,
  - The SIP PRI Gateway compares the incoming domain from the request URI with the subdomain listed for each trunk in the tab. If there is no subdomain, the software uses the listed domain.
  - The SIP PRI Gateway selects the first trunk it finds that matches the domain.
- if the URI contains only an alias, the SIP PRI Gateway selects the first trunk it finds that matches the alias, regardless of domain.



See Table 12, “Examples of SIP-to-PRI trunk selection,” for more specific examples of datafill.

**Table 12 Examples of SIP-to-PRI trunk selection (Sheet 1 of 2)**

URI type	Selection process	Selected trunk group
<b>URI containing both a trunk group name and domain</b>		
INVITE SIP:5551234@nortel.com;user=phone;norteldevice=pri;norteltrkgp= parent	The SIP PRI Gateway selects the first trunk with available resources that contains the alias <i>parent</i> and domain <i>Nortel.com</i> .	Trunk Group ID: 1 Alias: parent Domain: nortel.com
INVITE SIP:5551234@rich.nortel.com;user=phone;norteldevice=pri;norteltrkgp=subRich	The SIP PRI Gateway selects the first trunk with available resources that contains the alias <i>subRich</i> and domain <i>rich.nortel.com</i> .	Trunk Group ID: 2 Alias: subRich Subdomain: rich.nortel.com Domain: nortel.com
INVITE SIP:5551234@ottawa.nortel.com;user=phone;norteldevice=pri;norteltrkgp= subOttawa1	The SIP PRI Gateway selects the first trunk with available resources that contains the alias <i>subOttawa1</i> and domain <i>ottawa.nortel.com</i> .	Trunk Group ID: 7 Alias: subOttawa1 Subdomain: ottawa.nortel.com Domain: nortel.com
INVITE SIP:5551234@ottawa.nortel.com;user=phone;norteldevice=pri;norteltrkgp= subOttawa2	The SIP PRI Gateway selects the first trunk with available resources that contains the alias <i>subOttawa2</i> and domain <i>ottawa.nortel.com</i> .	Trunk Group ID: 9 Alias: subOttawa2 Subdomain: ottawa.nortel.com Domain: nortel.com
<b>URI containing only a domain</b>		
INVITE SIP:5551234@ ottawa.nortel.com;user=phone;norteldevice=pri	The SIP PRI Gateway selects the first trunk with available resources that contains the domain <i>ottawa.nortel.com</i> .	Trunk Group ID: 10 Alias: N/A Subdomain: ottawa.nortel.com Domain: nortel.com

**Table 12 Examples of SIP-to-PRI trunk selection (Sheet 2 of 2)**

URI type	Selection process	Selected trunk group
<b>URI containing only an alias</b>		
INVITE SIP:5551234;user=phone;norteldevice=pri;norteltrkgrp=misc		
Select the trunk group that you added in Table 11, "Sample Trunk Group entries."		

For *PRI-to-SIP* trunk selections, based on the examples in Table 12, "Examples of SIP-to-PRI trunk selection," the SIP PRI Gateway uses the following logic to populate the request URI, which contains the trunk group name and domain. See Table 13, "Examples of PRI-to-SIP trunk selection," for specific datafill examples.

- The SIP PRI Gateway takes the information used to populate the SIP header first from the trunk group entry.
- If there is no data available, then it uses the default domain.

**Table 13 Examples of PRI-to-SIP trunk selection (Sheet 1 of 2)**

URI type	Selection process	Selected trunk group
<b>URI containing both a trunk group name and domain</b>		
INVITE SIP:5551234@nortel.com;user=phone;norteldevice=pri;norteltrkgrp=parent; SIP/2.0 To <a href="mailto:5551234@nortel.com">5551234@nortel.com</a> From 4441234@nortel.com		
	The far-end switch selects the trunk that the call uses.	Trunk Group ID: 1 Alias: parent Domain: nortel.com
INVITE SIP:5551234@rich.nortel.com;user=phone;norteldevice=pri;norteltrkgrp=subRich To <a href="mailto:5551234@nortel.com">5551234@nortel.com</a> From 4441234@nortel.com		
	The far-end switch selects the trunk that the call uses.	Trunk Group ID: 2 Alias: subRich subdomain: rich.nortel.com Domain: nortel.com

**Table 13 Examples of PRI-to-SIP trunk selection (Sheet 2 of 2)**

URI type	Selection process	Selected trunk group
INVITE SIP:5551234@ottawa.nortel.com;user=phone;norteldevice=pri;norteltrkgrp=subOttawa1 To <a href="mailto:5551234@nortel.com">5551234@nortel.com</a> From <a href="mailto:4441234@nortel.com">4441234@nortel.com</a>	The far-end switch selects the trunk that the call uses.	Trunk Group ID: 7 Alias: subOttawa1 Subdomain: ottawa.nortel.com Domain: nortel.com
INVITE SIP:5551234@ottawa.nortel.com;user=phone;norteldevice=pri;norteltrkgrp=subOttawa2 To <a href="mailto:5551234@nortel.com">5551234@nortel.com</a> From <a href="mailto:4441234@nortel.com">4441234@nortel.com</a>	The far-end switch selects the trunk that the call uses.	Trunk Group ID: 9 Alias: subOttawa2 Subdomain: ottawa.nortel.com Domain: nortel.com
<b>URI containing only a domain</b>		
INVITE SIP:5551234@ottawa.nortel.com;user=phone;norteldevice=pri To <a href="mailto:5551234@nortel.com">5551234@nortel.com</a> From 4441234@nortel.com	The far-end switch selects the trunk that the call uses.	Trunk Group ID: 10 Alias: N/A Subdomain: ottawa.nortel.com Domain: nortel.com





## Accounting management

The SIP PRI Gateway does not do any accounting management. Although the SIP PRI Gateway does not supply accounting information directly to the Accounting Module, there are implications for calls that impact the collected data. This information is configurable. For more information on accounting, please see the *Succession MX Accounting Module Basics*.





# Performance management

## OAM&P strategy

The Management Module manages the performance functions for the SIP PRI Gateway. For additional information on the Management Module, refer to the *Succession MX Management Module Basics* and the *Succession MX System Management Console Basics*.







# Security and Administration

## How this chapter is organized

This chapter is organized as follows:

- “Security” on page 93
- “Administration” on page 93
- “OAM&P strategy” on page 135

The security and administration procedures are performed primarily through the System Management Console. For more information, refer to the *Succession MX Management Module Basics* and the *Succession MX System Management Console Basics*.

## Security

The SIP PRI Gateway is on the privately managed LAN and cannot be accessed from the public internet.

## Administration

The procedures in this section are organized as follows:

- “Maintaining the SIP PRI Gateway node” on page 94
- “Finding help text” on page 95
- “Performing a query” on page 96
- “Restarting a SIP PRI Gateway” on page 97
- “Accessing the Maintenance window” on page 98
- “Locking and unlocking a SIP PRI Gateway” on page 101
- “Locking or unlocking an interface card (CG6000), carrier, or channel” on page 101
- “Effect of Locking and Unlocking SIP PRI Gateway entities” on page 104
- “Changing the SIP PRI Gateway administrative state” on page 106

- “Maintaining the SIP PRI Gateway Carrier and Trunk Group” on page 107
- “Maintaining the carrier” on page 107
- “Trunk group maintenance information” on page 108
- “Locking or unlocking a trunk group or a trunk” on page 109
- “Maintaining the Trunk Group Member” on page 110
- “Rebooting a peer host card” on page 111
- “Performing maintenance on the CG6000 card” on page 112
- “Performing maintenance on the Chassis” on page 127
- “Performing maintenance on the SNMP configuration” on page 134

### Maintaining the SIP PRI Gateway node

The following basic maintenance operations are performed on a SIP PRI Gateway node either through the System Management Console:

- **lock force** - administratively locks the SIP PRI Gateway node immediately, which causes all active calls associated with the node to be dropped immediately
- **lock graceful** - administratively locks the SIP PRI Gateway node after stable calls using the node have been completed and no more calls are accepted
- **unlock** - returns the SIP PRI Gateway node to service if no other conditions exist that prevent it from coming back into service
- **reboot** - reboots the SIP PRI Gateway hardware
- **restart** - restarts the SIP PRI Gateway software

Maintenance operations affect the maintenance state associated with the SIP PRI Gateway node. These basic maintenance states include:

- **administrative state** - the state that can be changed through the System Management Console to enable maintenance activity to be performed. These states include:
  - locked - the node has been intentionally made unavailable
  - unlocked - the node has been returned to operational availability
- **operational state** - the state that describes the current operational status of the node. These states include:
  - enabled - the node is capable of handling traffic
  - disabled - the node is out of service

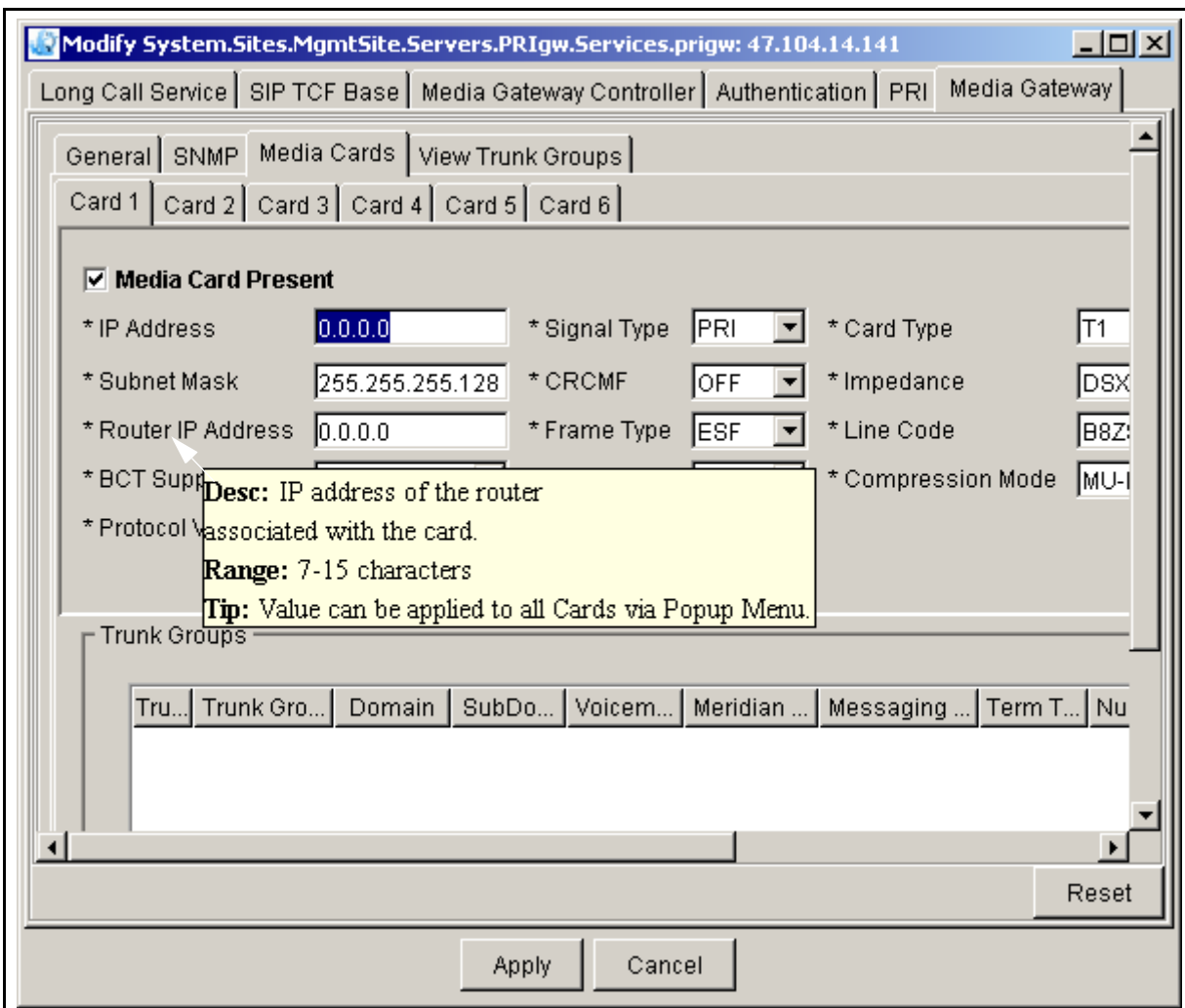
## Finding help text

### at the System Management Console

- 1 Administrators can find help text with descriptions and acceptable ranges by holding the cursor over the field name as shown in Figure 1, "Displaying help text."

**Note:** In all tabs, the fields with asterisks (\*) require an entry. The grayed-out fields are for information only and cannot be changed. Change all occurrences of the IP address "0.0.0.0" to the proper IP address for your situation.

Figure 1 Displaying help text



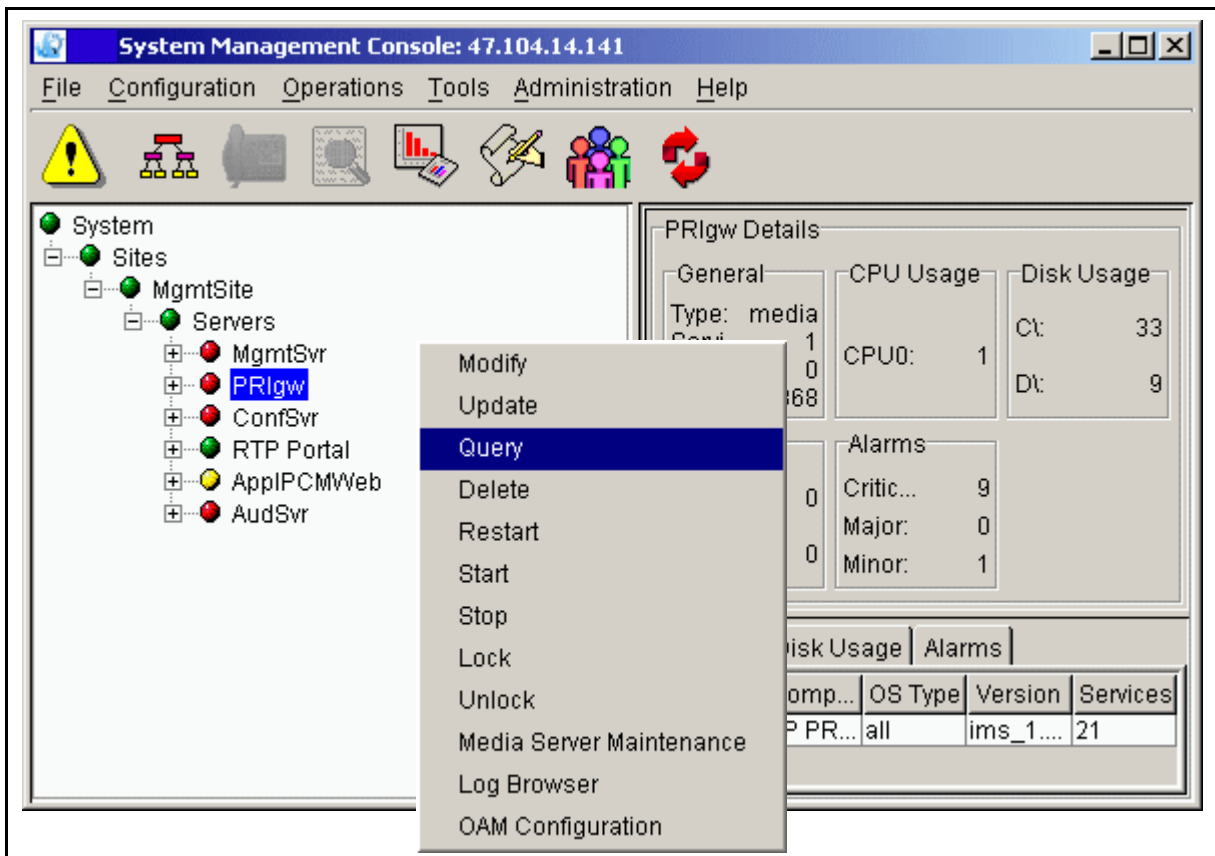
## Performing a query

### At the System Management Console

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, Servers, SIP PRI Gateway (the name assigned to the SIP PRI Gateway during deployment), and Components bullets, to the SIP PRI Gateway bullet (the name assigned to the SIP PRI Gateway load during deployment).

Right-click on the SIP PRI Gateway bullet (**PRlgw** in the example in Figure 2, "Performing a query"). Select **Query** from the pop-up menu. You will be able to see the status of each service in the right-hand panel.

**Figure 2 Performing a query**



- 2 The tabs appear. All of the fields are shown as *read only*.

## Restarting a SIP PRI Gateway

### *At the System Management Console main screen*

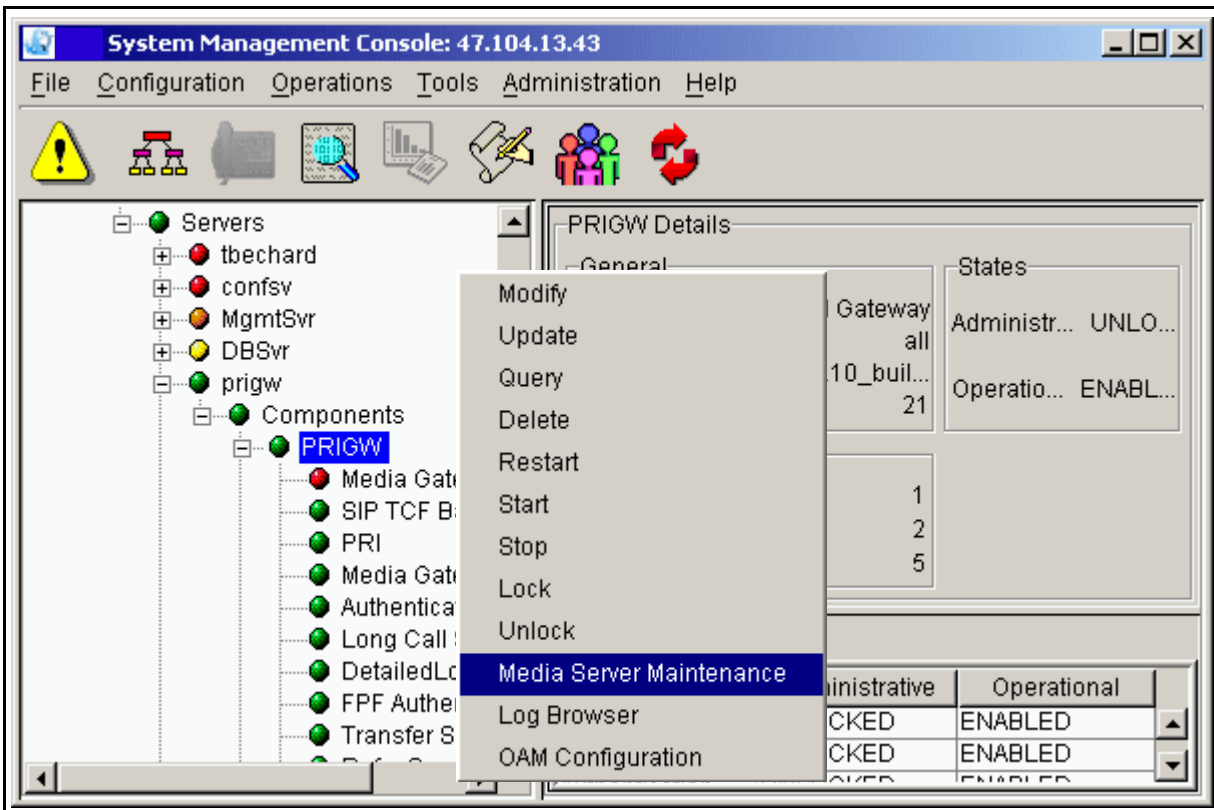
- 1      Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP PRI Gateway bullet (the name assigned to the SIP PRI Gateway during deployment).
- 2      Right-click on the SIP PRI Gateway bullet (**PRlgw** in the example).
- 3      Select **Maintenance** in the menu that appears.
- 4      In the States pane, click the **Restart** button.
- 5      Click **Yes** in the confirmation window that appears.
- 6      You have completed this procedure.

## Accessing the Maintenance window

### At the System Management Console

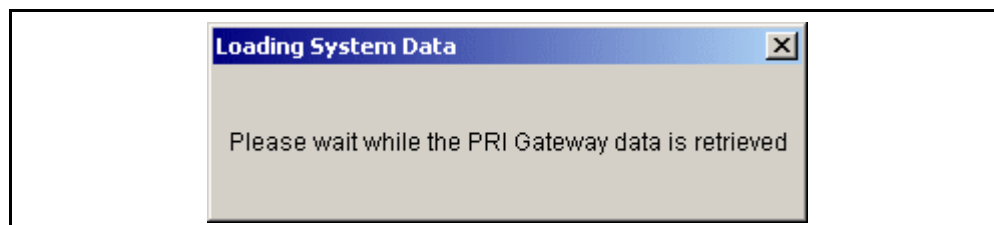
- 1 Navigate through the system hierarchy tree located in the left panel as shown in Figure 3, "Finding the Media Server Maintenance GUI."
- 2 Right-click on the SIP PRI Gateway bullet (**PRIGW** in the example). The names that appear in the hierarchy are defined at deployment.

**Figure 3 Finding the Media Server Maintenance GUI**



- 3 Select **Media Server Maintenance**. The following screen appears.

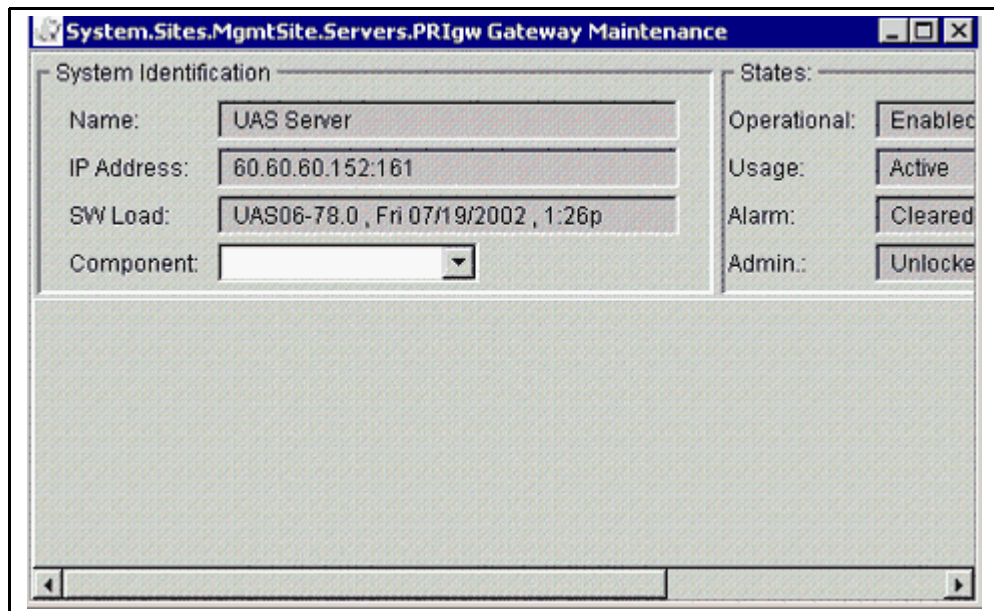
**Figure 4 Data loading dialog box**



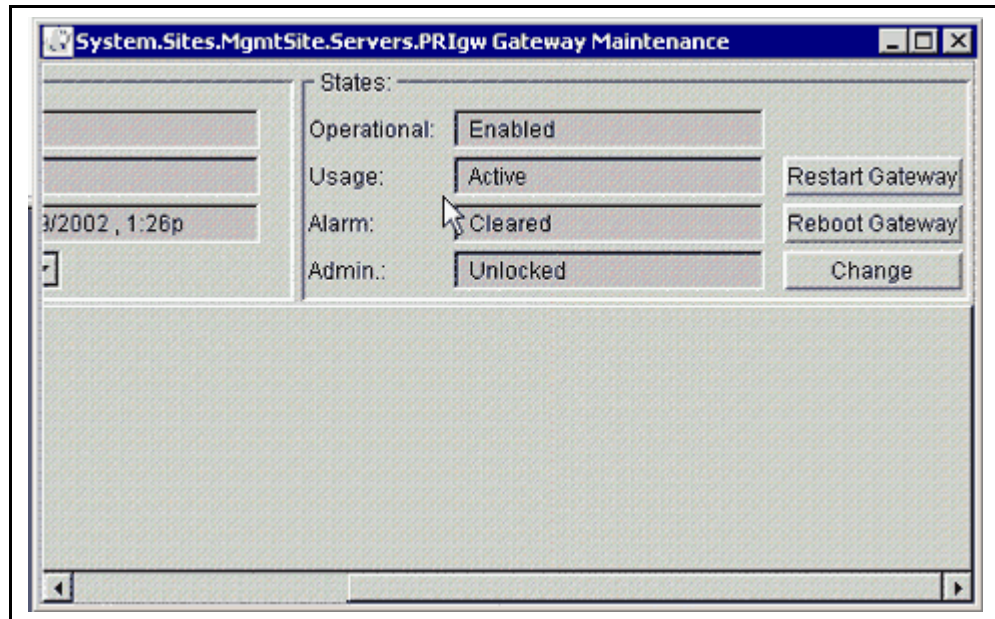
When the data have loaded, the following screen appears (shown here in two parts):

- The *System Identification* pane of the main maintenance window provides basic identification information for the SIP PRI Gateway, and contains a Component pull-down menu that enables you to select screens used for performing maintenance operations.
- The *States* pane provides operational state information about the SIP PRI Gateway, and contains buttons used for restarting SIP PRI Gateway processes, for rebooting the unit, or for changing the administrative state of the unit to either *locked* or *unlocked* states.

**Figure 5 Opening the Maintenance screen, *System Identification* pane**





**Figure 6 Opening the Maintenance screen, *States* pane**

- 4 Select from **CG6000**, **Chassis**, or **Snmp Configuration** in the Component pulldown menu.

When you select **CG6000** in the Component pull-down menu, you will see two panels, labeled *General* and *Performance*. The screen displayed when you select the *General* tab shows basic configuration information about the CG6000c cards provisioned in the SIP PRI Gateway. The screen displayed when you select the *Performance* tab shows performance information for the CG6000c cards.

When you select **Chassis** in the Component pull-down menu, a Maintenance screen appears. This screen is used for maintenance activities performed on SIP PRI Gateway CG6000c cards, carriers, and trunk groups. The following panels appear:

- The *PRI GW Tree* panel provides you with access to the individual CG6000c cards, to the associated carriers, and to the associated trunk groups.
- The *Contents* panel provides a detailed listing of the cards, carriers, and trunk groups, as well as access to buttons that enable you to perform actions, such as administratively locking or unlocking, on these entities.
- The *View Components States* button, located at the bottom of the Maintenance screen, enables you to display the alarm, administrative, operational, and availability status for various components of the SIP PRI Gateway.



When you select **SNMP Configuration** in the Component pull-down menu, a Trap Destinations screen appears. Through this screen you can define multiple SNMP trap destinations for alarms and logs issued from the SIP PRI Gateway.

Procedures in the following sections explain how to perform maintenance in these areas.

### Locking and unlocking a SIP PRI Gateway

This procedure enables you to place the SIP PRI Gateway either in *unlocked* (in service) state or in *locked* (out of service) state. When a SIP PRI Gateway is locked, its applications continue to run, but it does not receive any new requests. This procedure is normally used during SIP PRI Gateway administrative activities.

#### *At the System Management Console main screen*

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP PRI Gateway bullet (the name assigned to the SIP PRI Gateway during deployment).
- 2 Right-click on the SIP PRI Gateway bullet (**PRlgw** in the example).
- 3 If you want to lock the gateway, select **Lock** in the pull-down menu that appears. If you want to unlock the gateway, select **Unlock**.
- 4 You have completed this procedure.

### Locking or unlocking an interface card (CG6000), carrier, or channel

The System Management Console supports base-level (power-up and power-down) I/O card maintenance operations and service-level (lock force and unlock) I/O card maintenance operations. This procedure enables you to perform the service-level I/O card maintenance operations, locking (busy) or unlocking (return to service) an interface card, a carrier, or a carrier channel. Place the carrier in the administrative locked state before performing any provisioning or configuration actions on the carrier.

Perform the following basic maintenance operations on a CG6000c interface card through the System Management Console:

- **lock force** - administratively locks the CG6000 card immediately, causing all active calls associated with the card to be dropped immediately.
- **unlock** - returns the CG6000 card to service if no other conditions exist that prevent it from coming back into service

**At the System Management Console**

- 1 Navigate to the Maintenance window as shown in “Accessing the Maintenance window” on page 98.
  - 2 In the PRI GW Tree panel, click the **Cards** button.  
The Contents panel is populated with entries for the carrier cards configured in the system.
- | If   | Do     |
|--|--------|
| you want to lock or unlock a carrier card      | step 3 |
| you want to lock or unlock a carrier on a card | step 5 |
| you want to lock or unlock a carrier channel   | step 9 |
- 3 In the Contents panel, click on the row associated with the carrier card to be locked or unlocked.  
The row highlights and, if the card is powered up, the appropriate **Lock Graceful**, **Lock (Force)**, and **Unlock** command buttons, located below the Contents panel, become activated.
  - 4 Click the appropriate command button and respond to any warning windows that appear. Then go to step 15.
  - 5 In the PRI GW Tree, double-click the **Cards** button.  
A list of carrier cards configured in the system appears in the PRI GW Tree.
  - 6 In the PRI GW Tree, click the button for the card containing the carrier that you wish to lock or unlock.  
The Contents panel is populated with the carriers that are configured on the card you chose in the PRI GW Tree. The carriers are identified by carrier card port numbers.
  - 7 In the Contents panel, click on the row associated with the carrier to be locked or unlocked.  
The row highlights and the appropriate **Lock Graceful**, **Lock (Force)**, and **Unlock** command buttons, located below the Contents panel, become activated.
  - 8 Click the appropriate command button and respond to any warning windows that appear. Then go to step 15.
  - 9 In the PRI GW Tree, double-click the **Cards** button.  
A list of carrier cards configured in the system appears in the PRI GW Tree.

- 10 In the PRI GW Tree, click the button for the card containing the carrier channel that you wish to lock or unlock.  

The Contents panel is populated with the carriers that are configured on the card you chose in the PRI GW Tree. The carriers are identified by carrier card port numbers.
- 11 In the PRI GW Tree, click the expansion box (containing the plus, “+”, sign) located next to the carrier card containing the carrier channel you want to lock or unlock.  

In the PRI GW Tree, an expanded list of the carriers appears below the carrier card.
- 12 In the PRI GW Tree, click the carrier containing the channel you want to lock or unlock.  

The Contents panel is populated with the carrier channels that are configured on the carrier.
- 13 In the Contents panel, click on the row associated with the carrier channel to be locked or unlocked.  

The row appears highlighted and the appropriate **Lock Graceful**, **Lock (Force)**, and **Unlock** command buttons, located below the Contents panel, become activated.
- 14 Click the appropriate command button and respond to any warning windows that appear.
- 15 You have completed this procedure.

### Effect of Locking and Unlocking SIP PRI Gateway entities

The effect of locking and unlocking operations on the SIP PRI Gateway entities is summarized in Table 1, "Effect of locking and unlocking operations on SIP PRI Gateway entities."

**Table 1 Effect of locking and unlocking operations on SIP PRI Gateway entities (Sheet 1 of 3)**

Entity	Administrative Operation	Effect
Node	lock force	Trunk groups associated with the node are locked and the node is the owner of the lock.
		Member trunks of the trunk groups associated with the node are locked.
		Stable calls on the trunks in the trunk group are dropped immediately.
	lock graceful	Trunk groups associated with the node are locked.
		Member trunks of the trunk groups associated with the node are locked.
	unlock	Stable calls on the trunks in the trunk group are allowed to complete before the trunk groups are locked.
		Trunk groups associated with the node are unlocked. Member trunks of the trunk groups are unlocked depending on existing conditions.
CG6000 Interface card	lock force	Carriers on the card go out of service and are placed in an operationally disabled state.
		Trunks associated with the carriers are placed in operationally disabled, dependent state, although the state of the trunk groups of which the trunks are members is not changed.
		Stable calls on the trunks associated with the card's carriers are dropped immediately.
	unlock	<b>Note:</b> Interface cards <u>cannot</u> be locked gracefully.
		Carriers on the card are placed in the operationally enabled state.

**Table 1 Effect of locking and unlocking operations on SIP PRI Gateway entities (Sheet 2 of 3)**

Entity	Administrative Operation	Effect
Carrier	lock force	Trunks associated with the carrier are locked, although the state of the trunk groups of which the trunks are members is not changed.  Stable calls on the trunks in the trunk group are dropped immediately.  <b>Note:</b> Carriers <u>cannot</u> be locked gracefully.
	unlock	Trunks associated with the carrier are unlocked and are placed in the operationally enabled state.
Trunk group	lock force	Locks the trunk group and its member trunks. The trunks cannot be unlocked independently from the parent trunk group.  Stable calls on the trunks are dropped immediately.
	lock graceful	Locks the trunk group and its member trunks after any stable calls on the trunks have been completed. The trunks are still operationally enabled. The trunks cannot be unlocked independently from the parent trunk group.
	unlock	Unlocks the trunk group, and its member trunks if no conditions exist on the trunks that would otherwise prevent them from returning to service.
Trunk (B-channel)	lock force	Locks the trunk. Any stable call on the trunk is dropped immediately.
	lock graceful	Locks the trunk after any stable call on the trunk has completed.
	unlock	Unlocks the trunk depending on existing conditions.

**Table 1 Effect of locking and unlocking operations on SIP PRI Gateway entities (Sheet 3 of 3)**

Entity	Administrative Operation	Effect
Trunk (D-channel)	lock force	Locks the trunk. All of the associated B-channel trunks are made operationally disabled.  Any stable calls on the associated B-channel trunks are dropped immediately.  <b>Note:</b> D-channels <u>cannot</u> be locked gracefully.
	unlock	Unlocks the D-channel trunk and removes the dependency of the associated B-channel trunks on the condition of the D-channel trunk.

**Changing the SIP PRI Gateway administrative state**

This procedure enables you to toggle between the two administrative states, unlocked (in service) and locked (out of service). When a SIP PRI Gateway is locked, its applications continue to run, but it does not receive any new requests. This procedure is normally used during SIP PRI Gateway maintenance activities.

**At the System Management Console**

- 1 Navigate to the Maintenance window as shown in "Accessing the Maintenance window" on page 98.
- 2 When the Maintenance window appears, click the **Change** button in the States pane.  
A Change [Network Element] Administrative State window appears.
- 3 If you want to forcefully lock the SIP PRI Gateway, select the **Lock Force** radio button.  
  
If you want to gracefully lock the SIP PRI Gateway, select the **Lock Graceful** radio button.  
  
If you want to unlock the SIP PRI Gateway, select **Unlock**.
- 4 Click **OK**.  
You have completed this procedure.

### Maintaining the SIP PRI Gateway Carrier and Trunk Group

Administrators can perform basic maintenance operations on carriers and trunk groups through the System Management Console and include:

- **lock force** - administratively locks the carrier or trunk group immediately without regard for calls that are currently in progress
- **lock graceful** - administratively locks the carrier or trunk group after stable calls have been completed
- **unlock** - returns the carrier or trunk group to service if no other conditions exist that prevent it from coming back into service
- **query state** - provides state information

In addition to the administrative state and operational state information supplied for other SIP PRI Gateway entities, “availability status” is also provided, which gives an additional level of information about a non-operational or performance-degraded carrier or trunk group.

Availability statuses include:

- **none** - no abnormal condition
- **degraded** - degraded level of service (does not apply to trunks)
- **dependent** - the carrier or trunk group is not available due to a parental dependency or facility failure (FAF); for example, a carrier may be unavailable because the interface card on which it is configured is out of service
- **uninstalled** - applies only to trunks, and indicates that the trunk exists but is not a member of a logical trunk group
- **failed** - applies only to trunks, and indicates that call processing detected an error on the trunk or that the remote end is out of service

### Maintaining the carrier

You can perform the following basic operations on a carrier:

- **lock force**
- **unlock**

A carrier can only be forcibly locked (lock force), which causes all active calls on DS0 channels (trunks) associated with the carrier to be dropped immediately. In addition, locking a carrier affects the operational state of all DS0 channels associated with the carrier, putting them into the “disabled” operational state. Unlocking a carrier changes the administrative state of the carrier to *unlocked* and removes the operational state dependency of any associated DS0 channel. The

out-of-service condition is removed and the state of the DS0 channels is determined by existing conditions.

Although carrier administrative state changes can be requested through the System Management Console, operational state and availability status changes are, instead, triggered by alarmable events on the carrier. Table 2, "Carrier administration and operational states," shows the possible administrative and operational states, and applicable availability statuses.

**Table 2 Carrier administration and operational states**

Administrative state	Operational state	Availability status	Description
locked	enabled	none	administratively taken out of service
locked	disabled	dependent	operationally disabled and dependent due to a facility failure or due to a parent entity (card, node) being administratively out-of-service
unlocked	enabled	none	carrier in service
unlocked	enabled	degraded	carrier in service; trouble
unlocked	disabled	dependent	operationally dependent due to a facility failure or due to a parent entity (card, node) being out of service

#### Trunk group maintenance information

You can perform the following basic operations on a trunk group:

- **lock force**
- **lock graceful**
- **unlock**

A trunk group can be either forcibly locked (lock force) or locked gracefully (lock graceful). When a trunk group is forcibly locked, all member trunks of the trunk group are also locked and any active calls on the trunks are dropped immediately. A trunk group is normally locked gracefully when maintenance is to be performed on a member of the trunk group, since it places the trunk in a "shutting-down" state and only locks the trunk when calls on the trunk have been completed. When a



trunk group is unlocked, its member trunks are also unlocked depending on existing conditions.

Although you can request trunk group administrative state changes through the System Management Console, operational state and availability status changes are, instead, triggered by alarmable events or as the result of maintenance actions being performed on supporting entities. For example, locking a node also places all of the trunk groups associated with the node in the locked state; the node is then the owner of the trunk group lock.

### **Locking or unlocking a trunk group or a trunk**

This procedure enables you to perform trunk-related maintenance operations through the System Management Console. These operations include locking or unlocking a trunk group or a trunk before configuration or maintenance activity.

#### ***At the System Management Console***

- 1      Navigate to the Maintenance window as shown in “Accessing the Maintenance window” on page 98.
- 2      In the System Identification pane, select the **Chassis** component in the pull-down Component menu.  
A Chassis Maintenance tab window appears.
- 3      In the PRI GW Tree panel, click the **Logical Trunk Groups** button.  
The Contents panel is populated with entries for the trunk groups configured in the system.
- 4      In the Contents panel, click on the row associated with the trunk group to be locked or unlocked.  
The row highlights and the appropriate **Lock Graceful**, **Lock (Force)**, and **Unlock** command buttons, located below the Contents panel, become activated.
- 5      Click the appropriate command button and respond to any warning windows that appear. Then go to step 10.
- 6      In the PRI GW Tree, double-click the **Logical Trunk Groups** button.  
A list of trunk groups configured in the system appears in the PRI GW Tree.
- 7      In the PRI GW Tree, click the button for the trunk group containing the trunk that you wish to lock or unlock.

The Contents panel is populated with the trunks that are configured in the trunk group you chose in the PRI GW Tree. The trunks are identified by channel (trunk) number, and by the port number and the slot number on which the channel is configured.

- 8 In the Contents panel, click on the row associated with the trunk to be locked or unlocked.

The row is highlighted and the appropriate **Lock Graceful**, **Lock (Force)**, and **Unlock** command buttons, located below the Contents panel, become activated.

- 9 Click the appropriate command button and respond to any warning windows that appear.

- 10 After you have verified that the trunk state has changed, you have completed this procedure.

### Maintaining the Trunk Group Member

The basic operations that can be performed on a trunk group member include:

- **lock force**
- **lock graceful**
- **unlock**

A B-channel trunk group member can be either forcibly locked or locked gracefully. A D-channel trunk group member can only be forcibly locked. When a trunk group member is forcibly locked, any stable call on the trunk group member is dropped immediately and the trunk group member is locked.

**Note:** To determine if a stable call already exists on a channel, note the following: if the usage state on the far-right hand column corresponding to the appropriate channel shows **busy**, this is considered to be an active call. If you select **lock graceful** on this channel, the system waits until this call terminates normally before marking the channel *Out-of-Service*. At the trunk-group level, the usage state shows **Active** if any channels in that trunk group have active calls established.

When a trunk group member is locked gracefully, any stable call on the trunk group member is allowed to complete before the trunk group member is locked. Unlocking a trunk group member brings the trunk group member back into service if no other service-affecting conditions exist.

Trunk group member administrative state changes can be requested through the System Management Console; however, operational state and availability status changes are triggered by alarmable events or by maintenance actions being performed on supporting entities. For example, locking a carrier places all of the DS0 channels (trunk group members) associated with the carrier in the “disabled” operational state. Table 3, “Trunk group member administration and operational states.” shows the possible trunk group member administrative and operational states, and applicable availability statuses.

**Table 3 Trunk group member administration and operational states**

Administrative state	Operational state	Availability status	Description
locked	enabled	none	administratively taken out of service, at the element manager
locked	disabled	dependent	operationally disabled and operationally dependent due to a parent entity (carrier) or a D-channel being out of service.
shutting down	enabled /disabled	any	transition state from unlocked to locked; for graceful locks, allows calls to terminate before the state is changed to locked
unlocked	enabled	none	trunk in service
unlocked	disabled	dependent	operationally dependent due to a parent entity (carrier) being out of service
unlocked /locked	disabled	uninstalled	trunk does not belong to a logical trunk group
unlocked /locked	disabled	failed	call processing reported a failure of a trunk

### Rebooting a peer host card

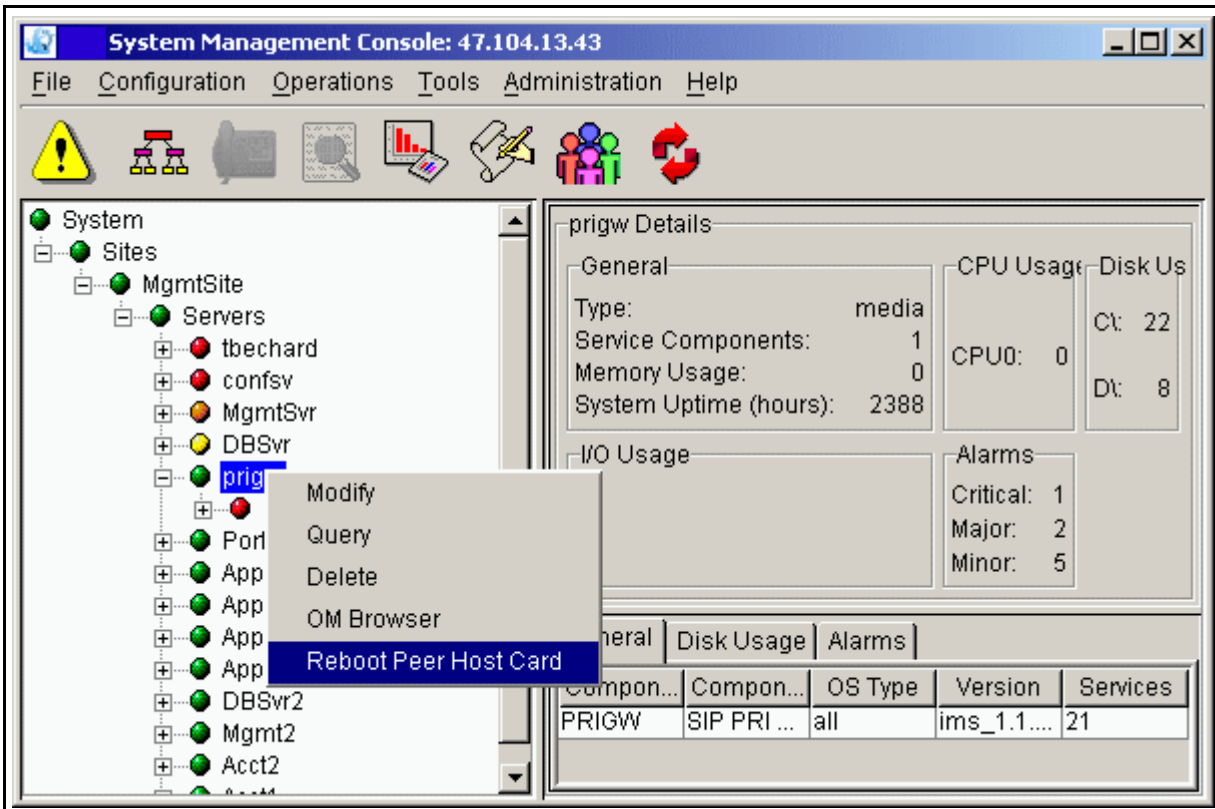
Note that in Domain A, you are selecting the peer host card for Domain B. You are actually rebooting the **other** half of the chassis.

### At the System Management Console

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to

- the SIP PRI Gateway bullet (the name assigned to the SIP PRI Gateway during deployment).
- 2 Right-click on the SIP PRI Gateway bullet (**PRIGW** in the example).
- 3 Select **Reboot Peer Host Card** in the menu that appears.

**Figure 7 Selecting Reboot Peer Host Card**



- 4 Click **Yes** in the confirmation window that appears.
- 5 You have completed this procedure.

### Performing maintenance on the CG6000 card

The procedure enables you to perform the following operations on a SIP PRI Gateway:

- change CG6000 card parameters
- delete a CG6000 card
- change carrier performance measurement thresholds
- change carrier line length
- add a trunk group

Before adding a trunk group associated with a media card, configure all the properties correctly, then click the **Add** button. After you add a trunk group, you cannot modify some of the properties for that media card.

- change trunk group parameters
- delete a trunk group

### Changing SIP PRI Gateway CG6000 parameters

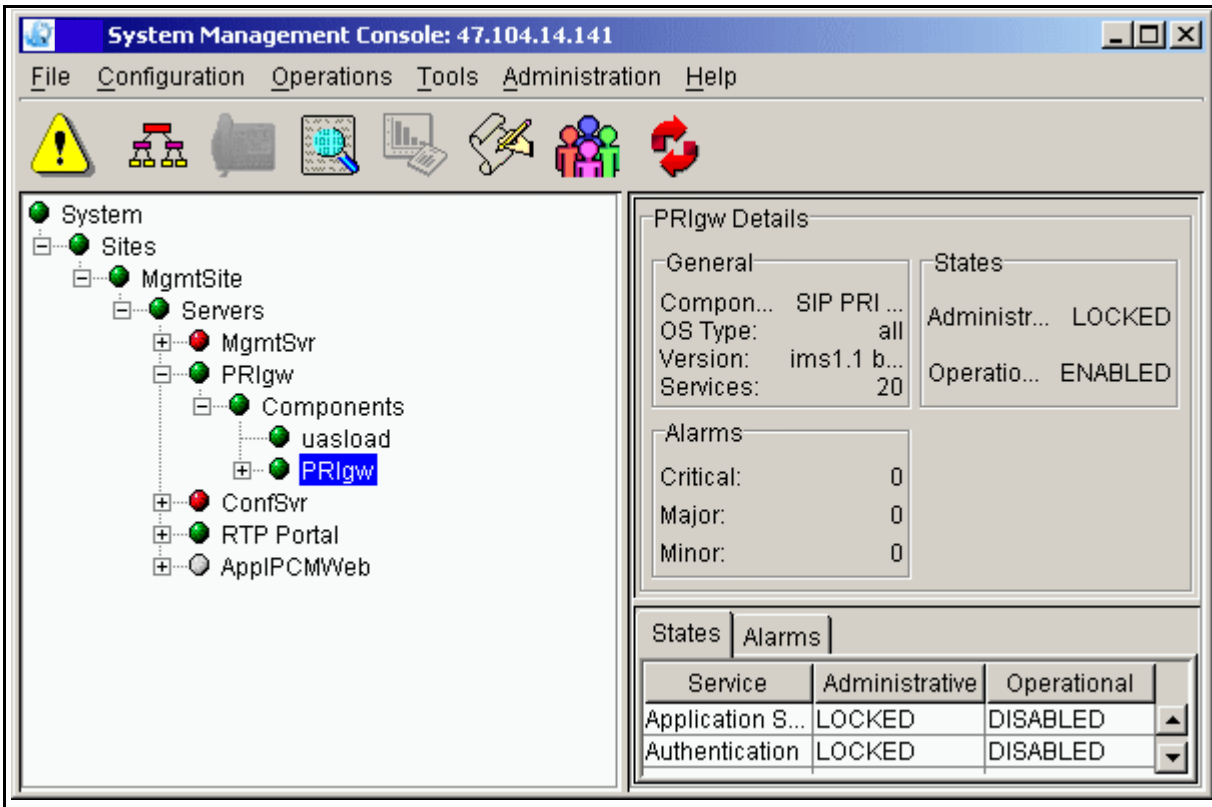


#### CAUTION

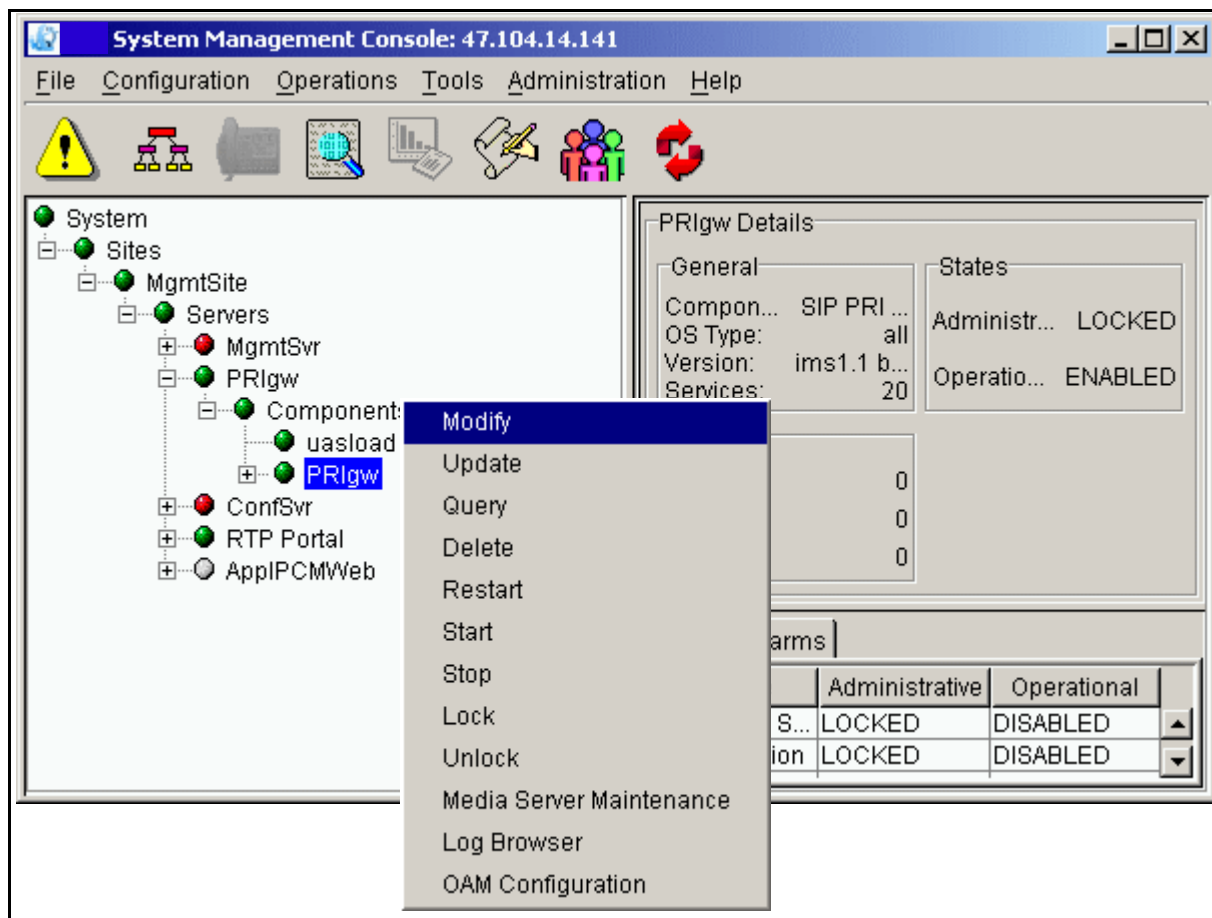
When you press the **Apply** button, the SIP PRI Gateway automatically restarts and all calls drop.

#### *At the System Management Console*

- 1 Navigate through the file system tree located in the left panel, by expanding the Sites, MgmtSite, Servers, SIP PRI Gateway (the name assigned either the SIP PRI Gateway during installation, **PRlgw** in the example), and Components bullets, as shown.

**Figure 8 Selecting Modify in the file menu**

- 2 Right-click on the **PRlgw** load bullet.
- 3 Select **Lock** in the menu that appears.
- 4 Right-click on the **PRlgw** load bullet.
- 5 Select **Modify** in the menu that appears, as shown.

**Figure 9 Selecting Modify in the file menu**

A Modify System Sites window appears. You can modify any of the tabs that appear.

- 6 Click on the **Media Gateway** tab to bring up the four subtabs.

**Figure 10 Modify System Sites dialog box, Media Gateway tab, General sub-tab**

The screenshot shows a web-based configuration interface for a Nortel system. The main window is titled "Modify System.Sites.MgmtSite.Servers.PRlgw.Services.prigw: 47.104.14.141". It features a series of tabs at the top: "Authentication", "Media Gateway Controller", "SIP TCF Base", "PRI", "Long Call Service", and "Media Gateway". The "Media Gateway" tab is selected, and within it, the "General" sub-tab is active. The "General" sub-tab contains several configuration fields: "\* Host Card Type" (a dropdown menu showing "5370"), "\* RTP Base Port" (a text box with "30000"), "\* Toneset" (a dropdown menu showing "United States"), and "\* Slot Number" (a dropdown menu showing "7"). To the right of these fields are two checkboxes: "\* Use Existing Data" (unchecked) and "\* Alarm Synchronization Interval" (unchecked). At the bottom right of the dialog is a "Reset" button. At the bottom center are "Apply" and "Cancel" buttons. The interface has a classic Windows-style look with a scroll bar on the right side of the main content area.



- 7 Click on the **SNMP** sub-tab to make the required changes.

**Figure 11 Modify System Sites dialog box, SNMP sub-tab**

Modify System.Sites.MgmtSite.Servers.PRIgw.Services.priwgw: 47.104.14.141

Long Call Service | SIP TCF Base | Media Gateway Controller | Authentication | PRI | Media Gateway

General | **SNMP** | Media Cards | View Trunk Groups

**SNMP Version 2C User**

\* Read Only Name

\* Read/Write Name

**Trap Destination**

\* IP Address

\* UDP Port

Reset

Apply Cancel

- 8 Click on the **Media Card** sub-tab to make the required changes.

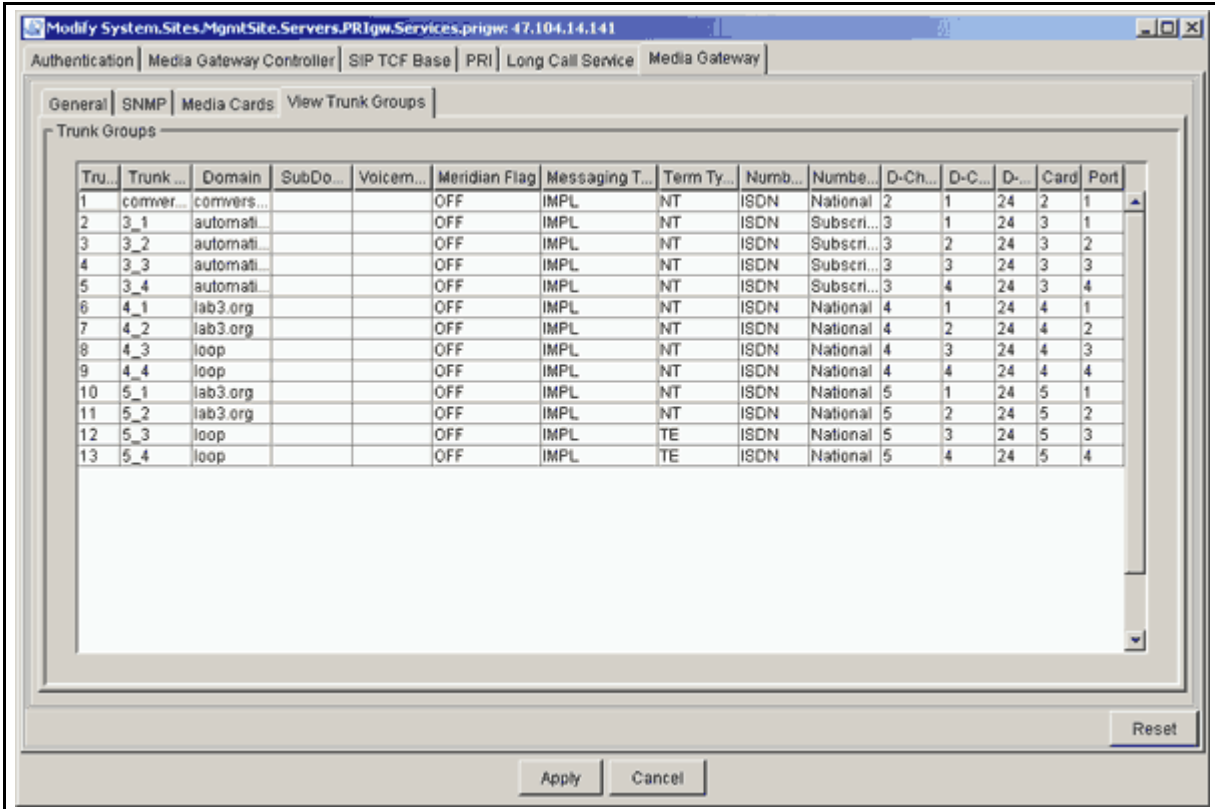
**Figure 12 Modify System Sites dialog box, Media Cards sub-tab**

The screenshot shows the 'Modify System Sites' dialog box with the 'Media Cards' sub-tab selected. The title bar indicates the site is '47.104.14.141'. The 'Media Cards' sub-tab is active, showing configuration for Card 1 through Card 6. The 'Media Card Present' checkbox is checked. The configuration fields include IP Address (60.60.60.154), Subnet Mask (255.255.255.0), Router IP Address (60.60.60.1), BCT Support (DISABLED), Protocol Variant (NI2), Signal Type (PRI), CRCMF (OFF), Frame Type (ESF), ISDN Flag (YES), Card Type (T1), Impedance (DSX1), Line Code (882S), Compression Mode (MU-LAW), and Carrier Configuration (Port 1-4, all set to PMT, Line Length 100). Below the configuration fields is a 'Trunk Groups' table with columns: Tru., Trunk Grou., Domain, SubDo..., Voicerna..., Meridian F..., Messaging T, Term Ty., Numb., Numb..., D-C, D-C..., D-C..., Card, Port. The table contains four rows of data. At the bottom of the dialog are 'Apply', 'Cancel', and 'Reset' buttons.

Tru.	Trunk Grou.	Domain	SubDo...	Voicerna...	Meridian F...	Messaging T	Term Ty.	Numb.	Numb...	D-C	D-C...	D-C...	Card	Port
10	5_1	lab3.org			OFF	IMPL	NT	ISDN	National	5	1	24	5	1
11	5_2	lab3.org			OFF	IMPL	NT	ISDN	National	5	2	24	5	2
12	5_3	loop			OFF	IMPL	TE	ISDN	National	5	3	24	5	3
13	5_4	loop			OFF	IMPL	TE	ISDN	National	5	4	24	5	4

- 9 Click on the **View Trunk Group** tab to ensure the changes have taken effect.

**Figure 13 Modify System Sites dialog box, View Trunk Group sub-tab**



- 10 Click the **Media Card Present** checkbox.  
The media card fields become active, displaying default media card values.

- 11 Change the media card fields in the tab window that appears, as needed.

**Figure 14 Changing the Media Card tabs**

**Media Card Present**

\* IP Address: 60.60.60.154 \* Signal Type: PRI \* Card Type: T1

\* Subnet Mask: 255.255.255.0 \* CRCMF: OFF \* Impedance: DSX1

\* Router IP Address: 60.60.60.1 \* Frame Type: ESF \* Line Code: B8ZS

\* BCT Support: DISABLED \* ISDN Flag: YES \* Compression Mode: MU-LAW

\* Protocol Variant: NI2

**Carrier Configuration \* Line Length**

Port	Configuration	Line Length
Port 1	PMT	100
Port 2	PMT	100
Port 3	PMT	100
Port 4	PMT	100

**Trunk Groups**

Tru...	Trunk Grou...	Domain	SubDo...	Voicema...	Meridian F...	Messaging T...	Term Ty...	Numb...	Numb...	D-C...	D-C...	D-C...	Card	Port
10	5_1	lab3.org			OFF	IMPL	NT	ISDN	National	5	1	24	5	1
11	5_2	lab3.org			OFF	IMPL	NT	ISDN	National	5	2	24	5	2
12	5_3	loop			OFF	IMPL	TE	ISDN	National	5	3	24	5	3
13	5_4	loop			OFF	IMPL	TE	ISDN	National	5	4	24	5	4

Buttons: Add, Modify, Delete, View, Reset, Apply, Cancel

- 12 Go to step 38.
- 13 Determine whether you want to change change card parameters, change carrier configuration, or change trunk group information.

If	Do
you want to change card parameters	step 14
you want to change carrier configuration	step 18
you want to change trunk group information	step 22

- 14 Determine whether you are modifying or adding a card.

If	Do
you are adding a card	step 15

	<b>If</b>	<b>Do</b>
	you are modifying a card	step 16
<b>15</b>	Click the <b>Media Card Present</b> check box. The media card fields become active, displaying default media card values.	
<b>16</b>	Change the media card fields in the tab window that appears, as needed.	
<b>17</b>	Determine whether you want to modify carrier configuration.	
	<b>If</b>	<b>Do</b>
	you want to modify carrier configuration	step 18
	you do not want to modify carrier configuration	step 21
<b>18</b>	If you want to modify carrier performance measurement thresholds, click the <b>PMT</b> button associated with the port on the card that you wish to add information to or to modify; otherwise, go on to step 20.	
<b>19</b>	In the Modify Performance Thresholds for Card screen that appears, add or change the field information, as required and then click <b>Accept</b> .	
<b>20</b>	If you want to modify the carrier line length, enter the line length in the appropriate <b>Line Length</b> field.	
<b>21</b>	Determine whether you want to modify trunk group information.	
	<b>If</b>	<b>Do</b>
	you want to modify trunk group information	step 22
	you do not want to change existing trunk group information	step 38
<b>22</b>	Determine the type of operation you want to perform.	
	<b>If</b>	<b>Do</b>
	you want to add a trunk group to the card	step 23
	you want to change existing trunk group information	step 29
	you want to delete a trunk group from the card	step 34

- 23 Click the **Add** button, located in the Trunk Groups panel.  
The Add Trunk Group window appears.
- 24 Enter the appropriate information in the fields of the Add Trunk Group window.
- 25 Click the **Channel Map** button, located at the bottom of the Add Trunk Group window.  
A Modify Channel Map window appears.
- 26 Click the check boxes associated with the B-channels (trunks) configured in the trunk group. Click **Accept** to effect the changes.
- 27 Click **Accept** to effect the changes you made in the Add Trunk Group window.
- 28 Go to step 38.
- 29 Click on the row containing the trunk group information to be changed.

- 30 Click on the **Modify** button. The Modify Trunk Group window appears.

**Figure 15 Modifying the trunk group**

**Modify Trunk Group**

Trunk Group ID	10
Trunk Group Name	5_1
Domain	lab3.org
SubDomain	
<input type="checkbox"/> Configure Voicemail	none
Meridian Flag	OFF
Messaging Type	IMPL
Term Type	NT
Numbering Plan	ISDN
Numbering Type	National
D-Channel Card ID	5
D-Channel Port	1
D-Channel	24
Card	5
Port	1

Channel Map

Accept Cancel

- 31 Make any desired changes to the fields in the Modify Trunk Group window.
- 32 Click **Accept** to effect the changes you made in the Add Trunk Group window.

- 33 Go to step 38.
- 34 Click on the row containing the trunk group information to be deleted.
- 35 Click **Delete**.
- 36 Click **OK** in the Delete Trunk Group confirmation window that appears.
- 37 Click **Accept** to effect the changes you made in the Add Trunk Group window.
- 38 Click **Apply**, located at the bottom of the card tab window, to effect the changes you have made.
- 39 In the file system tree, right-click on the **prigw** load bullet.
- 40 Select **Unlock** in the menu that appears.
- 41 You have completed this procedure.

### Performing maintenance on the CG6000 card

#### *at the Maintenance GUI*

- 1 To perform maintenance on the CG6000 card, select **CG6000** from the Component pulldown menu as shown in Figure 16, "CG6000 selection, General tab," Figure 17, "CG6000 selection, Performance tab, left side," and Figure 18, "CG6000 selection, Performance tab, right side."

The CG6000 General tab screen appears first. The General Information panel, located at the top of the screen, is populated with a row of status information for each CG6000 card configured in the system, which includes the current alarm state and the current operational state.

The Interface Table panel, located at the bottom of the screen, is populated with a row of information for each CG6000 card configured in the system, which includes the IP address, network mask, and router IP address.

You can choose the Performance tab to view specific metrics.



**Figure 16 CG6000 selection, General tab**

**System.Sites.MgmtSite.Servers.PRIgw Gateway Maintenance**

System Identification

Name: UAS Server

IP Address: 60.60.60.152:161

SW Load: UAS06-78.0, Fri 07/19/2002, 1:26p

Component: CG6000

States:

Operational: Enabled

Usage: Active

Alarm: Cleared

Admin.: Unlocked

General | Performance

General Information

Slot Number	Alarm State	Operational State
2	Minor	Enabled
3	Minor	Enabled
4	Minor	Enabled
5	Minor	Enabled

Interface Table

Slot Number	IP Address	Network Mask	Router IP Address
2	60.60.60.103	255.255.255.0	60.60.60.1

**Figure 17 CG6000 selection, Performance tab, left side**

The screenshot shows a web-based maintenance interface for a PRlgw Gateway. The window title is 'System.Sites.MgmtSite.Servers.PRlgw Gateway Maintenance'. It features a 'System Identification' section with fields for Name (UAS Server), IP Address (60.60.60.152:161), SW Load (UAS06-78.0, Fri 07/19/2002, 1:26p), and Component (CG6000). To the right, a 'States' section shows Operational (Enabled), Usage (Active), Alarm (Cleared), and Admin. (Unlocked). Below these are tabs for 'General' and 'Performance'. The 'Performance' tab is active, displaying a list of metrics on the left: Total G711 Mu-law Sessions, Current G711 Mu-law Sessions, Total G711 A-law Sessions, Current G711 A-law Sessions, Total G723 Sessions, Current G723 Sessions, Total G726 Sessions, Current G726 Sessions, and Total G729 Sessions. A 'Retrieve' button is located below the list. On the right, a table with the header 'Metric' is visible but empty. At the bottom, there are tabs for 'Slot', 'RTP Sessions', 'Jitter Underflows', 'Jitter Overflows', 'Out Of Order', and 'Invalid Packets'.

System Identification	
Name:	UAS Server
IP Address:	60.60.60.152:161
SW Load:	UAS06-78.0, Fri 07/19/2002, 1:26p
Component:	CG6000

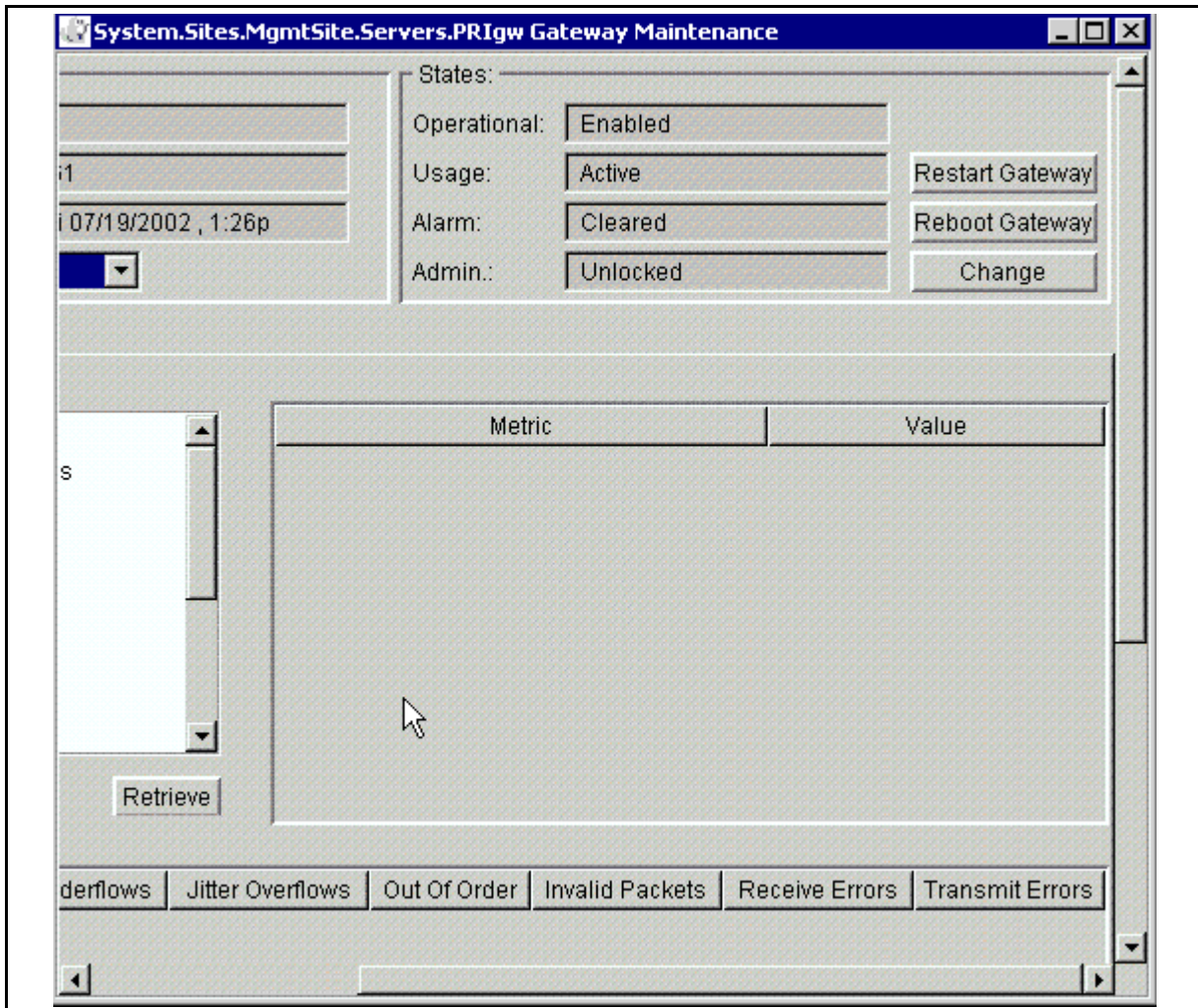
States:	
Operational:	Enabled
Usage:	Active
Alarm:	Cleared
Admin.:	Unlocked

General Performance

Metric
Total G711 Mu-law Sessions
Current G711 Mu-law Sessions
Total G711 A-law Sessions
Current G711 A-law Sessions
Total G723 Sessions
Current G723 Sessions
Total G726 Sessions
Current G726 Sessions
Total G729 Sessions

Retrieve

Slot	RTP Sessions	Jitter Underflows	Jitter Overflows	Out Of Order	Invalid Packets
------	--------------	-------------------	------------------	--------------	-----------------

**Figure 18 CG6000 selection, Performance tab, right side**

### Performing maintenance on the Chassis

#### *at the Maintenance GUI*

- 1 To perform chassis maintenance, select **Chassis** from the Component pulldown menu. The following screen appears. This screen is used for maintenance activities performed on SIP PRI Gateway CG6000c cards, carriers, and trunk groups.

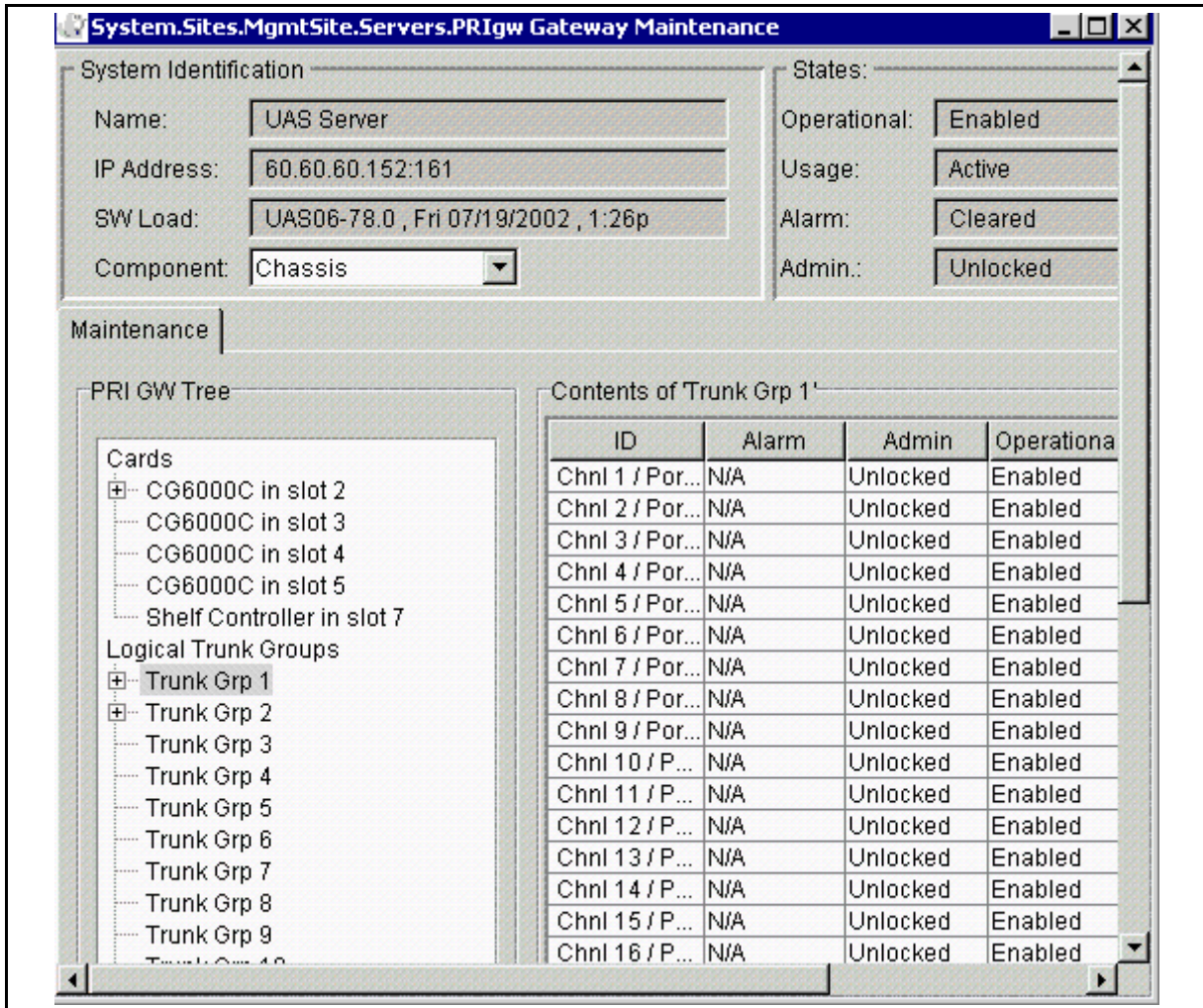
The "PRI GW Tree" panel provides you with access to the individual CG6000c cards, to the associated carriers, and to the associated trunk groups.

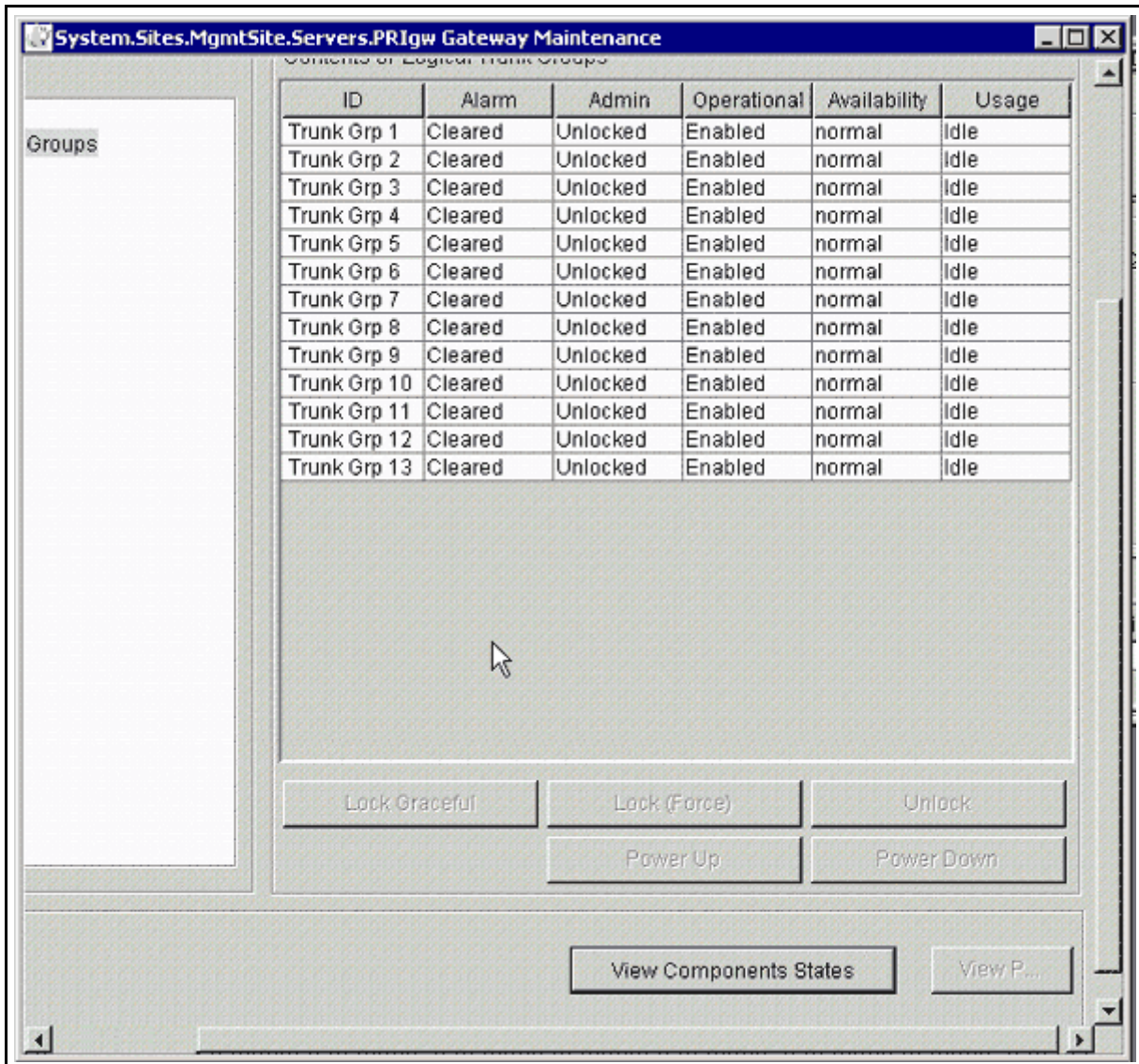
The "Contents" panel provides a detailed listing of the cards, carriers, and trunk groups, as well as access to buttons that



enable you to perform actions, such as administratively locking or unlocking, on these entities.

**Figure 19 Selecting Chassis Maintenance, part 1**



**Figure 20 Selecting Chassis Maintenance, part 2**

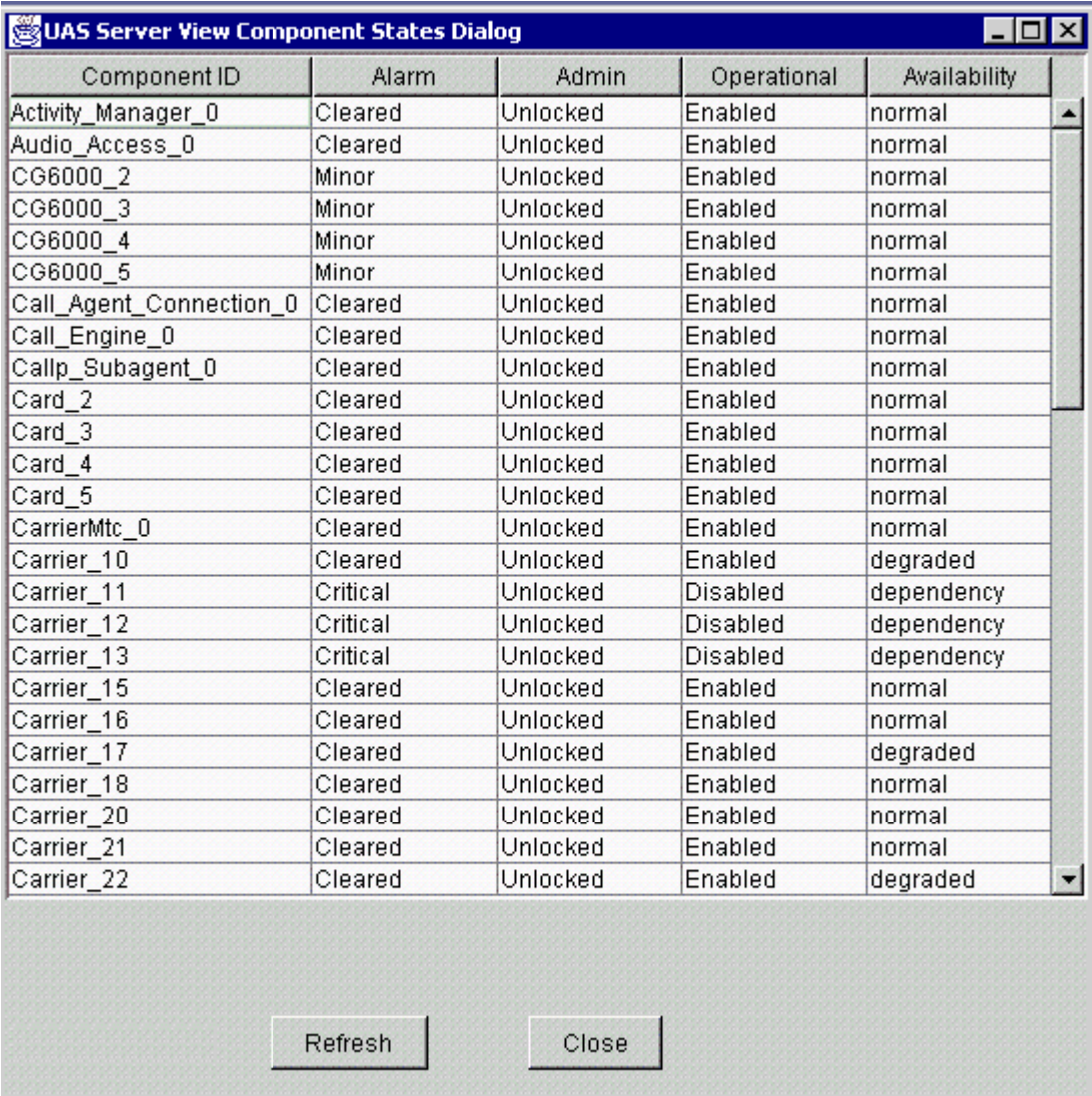
- 2 Select an item, then click on the **View Components States** button. The following figure appears. Since the listing is a real-time snapshot, you may wish to refresh the display by clicking **Refresh**. If you do not wish to refresh the display, click **Close**.

The display includes a separate row of information for each component, which includes

- the latest alarm state (cleared, critical, major, minor, or warning)
- administrative state (unlocked, locked, or shutting down)

- operational state (enabled or disabled)
  - notInstalled or powerOff, for fans
  - notInstalled, powerOff, or normal, for power supplies
  - offline, powerOff, or notInstalled, for card base levels and service levels
  - normal, for all other components

**Figure 21 Viewing the Component States**



Component ID	Alarm	Admin	Operational	Availability
Activity_Manager_0	Cleared	Unlocked	Enabled	normal
Audio_Access_0	Cleared	Unlocked	Enabled	normal
CG6000_2	Minor	Unlocked	Enabled	normal
CG6000_3	Minor	Unlocked	Enabled	normal
CG6000_4	Minor	Unlocked	Enabled	normal
CG6000_5	Minor	Unlocked	Enabled	normal
Call_Agent_Connection_0	Cleared	Unlocked	Enabled	normal
Call_Engine_0	Cleared	Unlocked	Enabled	normal
Callp_Subagent_0	Cleared	Unlocked	Enabled	normal
Card_2	Cleared	Unlocked	Enabled	normal
Card_3	Cleared	Unlocked	Enabled	normal
Card_4	Cleared	Unlocked	Enabled	normal
Card_5	Cleared	Unlocked	Enabled	normal
CarrierMtc_0	Cleared	Unlocked	Enabled	normal
Carrier_10	Cleared	Unlocked	Enabled	degraded
Carrier_11	Critical	Unlocked	Disabled	dependency
Carrier_12	Critical	Unlocked	Disabled	dependency
Carrier_13	Critical	Unlocked	Disabled	dependency
Carrier_15	Cleared	Unlocked	Enabled	normal
Carrier_16	Cleared	Unlocked	Enabled	normal
Carrier_17	Cleared	Unlocked	Enabled	degraded
Carrier_18	Cleared	Unlocked	Enabled	normal
Carrier_20	Cleared	Unlocked	Enabled	normal
Carrier_21	Cleared	Unlocked	Enabled	normal
Carrier_22	Cleared	Unlocked	Enabled	degraded

- 3** At the main screen, select the appropriate item, then click on the button (**Add**, **Modify**, or **Delete**) for the required changes.



Each card component has a set of base-level states that provide information about low-level functionality of the card, as follows:

- The base-level administrative state *unlocked* indicates that the firmware load has been successfully loaded into the card.
- The base-level availability state *offline* indicates that power to the card slot is on but no card is present in the slot.
- The base-level availability state *powerOff* indicates that power to the slot is turned off.
- The base-level availability state *notInstalled* indicates that there is no card installed in the card slot.

Each I/O card, in addition, has a set of *service-level* states, that provide information about high-level functionality of the card, as follows:

- The service-level operational state *enabled* indicates that configuration data has been successfully downloaded into the card and that the card has been started successfully.
- The service-level availability state *offline* indicates that power to the card slot is on but no card is present in the slot.
- The service-level availability state *powerOff* indicates that power to the slot is turned off.
- The service-level availability state *notInstalled* indicates that there is no card installed in the card slot.

The components represented in the rows in the display, and the information about them, include those listed in Table 4, "Components information."

**Table 4 Components information (Sheet 1 of 4)**

Field name	Description
Activity_Manager_0	This row provides state information about the Activity Manager process (AM.exe). This process is part of the Nortel Network Global Server base software upon which the UAS software is built.
Audio_Access_0	This row provides state information about the Audio Access component, which is responsible for accessing audio on the local disk in the node.
CG6000_<slot>	This row provides service-level state information for the CG6000C card, in IP-based UAS nodes. <slot> is the physical slot number in the range 1-6, in domain A (left side) or 11-16, in domain B (right side).

**Table 4 Components information (Sheet 2 of 4)**

Field name	Description
Call_Agent_Connection_0	This row provides state information about the connection to the call agent.
Call_Engine_0	This row provides state information about the Call Engine component.
Callp_Subagent_0	This row provides state information about the SNMP subagent component that runs inside the main call processing application.
Card_<slot>	This row provides base-level state information about an I/O card. <slot> is the physical slot number in the range 1-6, in domain A (left side) or 11-16, in domain B (right side).
CarrierMtc_0	This row provides state information about the carrier maintenance subsystem, which is responsible for maintaining the states of the carriers.
Carrier_<n>	This row provides state information about carriers. <n> represents the index of the carrier in the entPhysicalTable of the Entity MIB (RFC2737).
ChassisEventManager_0	This row provides state information about the Chassis Event Manager process (CEM.exe). This process is part of the Nortel Network Global Server base software upon which the UAS software is built. The Chassis Event Manager is responsible for maintaining and monitoring fans, power supplies, slots, and base-level states of cards.
Conferencing_Service_0	This row provides state information about Conferencing Service in IP-based UAS nodes that have Conferencing Service.
Cooling_System_0	This row provides state information about the cooling system, as determined by temperature sensors located in the chassis. The operational state is always <i>enabled</i> . The alarm status is normally <i>cleared</i> , but changes when a chassis temperature threshold is exceeded.
Fan_<n>	This row provides state information about the cooling fans, 1, 2, or 3. The <i>notInstalled</i> availability state indicates either that there is no fan in the sled or that the fan installed in the sled needs to be reseated.



**Table 4 Components information (Sheet 3 of 4)**

Field name	Description
Hard_Disk_<n>	<p>This row provides state information about the hard disk, where &lt;n&gt; is either 1 or 2. Hard disk 1 is the hard disk for domain A and hard disk 2 is the hard disk for domain B.</p> <p>Currently, states for hard disk 2 can only be monitored by domain A software. Therefore, there will be two hard disk components listed under domain A, Hard_Disk_1 and Hard_Disk_2, but none listed under domain B. If you want to view the hard disk states for domain B, then you must view the components dialog for domain A. Currently, only the alarm status will change. The operational state will always be <i>enabled</i>. Administrative state changes on the hard disk are not supported. The availability status will always be <i>normal</i>.</p>
IVR_Service_0	<p>This row provides state information about the IVR service component.</p> <p>This information also appears on UAS nodes configured only with Conferencing service.</p>
LocalResourceManager_0	<p>This row provides state information about the Local Resource Manager process (LRM.exe). This process is part of the Nortel Networks Global Server base software upon which the UAS software is built. The Local Resource Manager process is responsible for monitoring CPU usage, memory usage, and disk space usage.</p>
Main_Subagent_0	<p>This row provides state information about the Main Subagent application, which is responsible for forwarding logs and alarms to the element manager through SNMP traps.</p>
NodeMtc_0	<p>This row provides state information about the Node Maintenance subsystem, which is responsible for maintaining the states of the network element.</p>
Power_Supply_<n>	<p>This row provides state information about the power supplies, 1, 2, or 3.</p> <p>The <i>notInstalled</i> availability state indicates either that there is no power supply in the sled or that the power supply installed in the sled needs to be reseated. The <i>normal</i> availability state indicates that power is on for that power supply unit in the sled and/or the power supply unit is installed in the sled.</p>

**Table 4 Components information (Sheet 4 of 4)**

Field name	Description
Q931_Event_Handler_0	This row provides state information about the Q931 event handler component in a SIP PRI Gateway.
ProgramManager_0	This row provides state information about the Program Manager process (pmgr.exe). This process is part of the Nortel Networks Global Server base software upon which the UAS software is built. The Program Manager process is responsible for starting, stopping, and monitoring application processes. The Program Manager is a Windows service called <i>pmgrdaemon</i> .
Resource_Manager_0	This row provides state information about the Resource Manager component, which is responsible for maintaining pools of endpoints.
SCSI_Controller_<slot>	This row provides base-level state information about the SCSI Controller card (CPV8540). <slot> is either 8, in domain A (left side) or 10, in domain B (right side). A separate SCSI Controller card is found only in systems configured with the CPV5370 Processor card.
ShelfController_<slot>	This row provides base-level state information about the CPV5370 Processor card (shelf controller card). <slot> is either 7, in domain A (left side) or 9, in domain B (right side).
System_0	This row provides state information about the network element. In the element manager, these states are also displayed in the States panel, located in the right-hand side of the Network Element Status panel (top panel of the element manager main screen).
Trunk_Group_<n>	This row provides state information about trunk groups. <n> is a unique trunk group identifier.

### Performing maintenance on the SNMP configuration

#### *at the Maintenance GUI*

- 1 To perform maintenance on the SNMP configuration, select **Snmp Configuration** from the Component pulldown menu.  
  
When you select SNMP configuration in the **Component** pull-down menu, a Trap Destinations screen appears. Through this screen you can define multiple SNMP trap destinations for alarms and logs issued from the SIP PRI Gateway.

- 2 Make the required changes and select the appropriate button (**Add**, **Modify**, or **Delete**).

**Figure 22 Selecting the SNMP Configuration Maintenance screen**

The screenshot shows a window titled "System.Sites.MgmtSite.Servers.PRIgw Gateway Maintenance". It contains a "System Identification" section with fields for Name, IP Address, SW Load, and Component. The "States" section includes Operational, Usage, Alarm, and Admin. status buttons. Below these is a "General" tab and a "Trap Destinations" table. The table has columns for IP Address, Port, Security Name, Alarms, Logs, and Ptm ColdStart. At the bottom are "Add...", "Modify...", and "Delete..." buttons.

IP Address	Port	Security Name	Alarms	Logs	Ptm ColdStart
60.60.60.152	162	public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## OAM&P strategy

The Management Module performs the security and administrative functions for the SIP PRI Gateway. For additional information on the Management Module, refer to the *Succession MX Management Module Basics* and the *Succession MX System Management Console Basics*.





## Appendix A Mapping tables

### How this Appendix is organized

This Appendix is organized as follows:

- “RPI mappings” on page A-137
  - “Indicator mapping tables” on page A-137
  - “RPI header mapping tables” on page A-138
  - “SIP-to-PRI parameter mapping tables” on page A-145
- “Mapping of cause values” on page A-147

### RPI mappings

The following tables give information about RPI header mappings.

#### Indicator mapping tables

Table 1, “Mapping of Presentation Indicators,” illustrates the mappings between the ISDN presentation indicator and the RPI (Remote Party Identification) restriction indicator.

**Table 1 Mapping of Presentation Indicators**

PRI Presentation Indicator	SIP RPI Indicator
Allowed	off
Restricted	full
Restricted	uri (not used for PRI->SIP)
Restricted	name (not used for PRI->SIP)
Restricted	ipaddr (not used for PRI->SIP)
Allowed	N/A (not set in signal)

Table 2, "Mapping of Screening Indicators," illustrates the mappings between the ISDN screening indicator and the RPI screening indicator.

**Table 2 Mapping of Screening Indicators**

PRI Screening Indicator	SIP RPI Screening Indicator
User provided, not screened	No
User provided, verified and passed	Yes
User provided, verified and failed	No (not used for SIP->PRI)
Network provided	No (not used for SIP->PRI)

### RPI header mapping tables

The SIP PRI Gateway software supports the following RPI headers:

- *calling* to transport the calling party number information for users in SIP-to-PRI-originated calls
- *called* to transport the original called party when the call is redirected. The called header is delivered in the SIP signal to indicate the original called party information after a call has been redirected.
- *redirect* to transport information regarding the last redirection if multiple redirections occur
- *reason* to indicate the reason a call is redirected
- *count* to indicate how many times a call is redirected

The following tables illustrate the mapping of SIP calling, called, and redirect headers and PRI redirection Information Element (IE) and original called party IE. These tables show the mapping of the fields, not the conversion of values between the protocols.

**Table 3 SIP-to-PRI mapping when RPI header calling is received (Sheet 1 of 2)**

SIP header	PRI IE
Rpi-pty-type: calling	Calling Party IE
rpi user	Calling Party Number IE: number digits
rpi-screen: screening level	Calling Party Number IE: screening indicator. If not set, then the default is user provided, not screened



**Table 3 SIP-to-PRI mapping when RPI header calling is received (Sheet 2 of 2)**

SIP header	PRI IE
rpi-privacy: restriction level	Calling Party Number IE: presentation indicator. If not set, then the default is presentation allowed.
Not populated in the redirect RPI	Calling Party Number IE: type of number
Not populated in the redirect RPI	Calling Party Number IE: numbering plan identification
rpi-reason: reason	Not supported in Calling Party IE
rpi-count: count	Not supported in Calling Party IE
rpi-display: name	Display IE: display information
screen-ind	<p>This field carries the screening indicator transparently on PRI-SIP-PRI tandem calls. The field screen-ind=&lt;n&gt;, where &lt;n&gt; is an integer with a value from 0 to 3. This value maps to the following Q.931 screening indicator codepoints:</p> <ul style="list-style-type: none"> <li>• 0=User provided, not screened</li> <li>• 1=User provided, verified and passed</li> <li>• 2=User provided, verified and failed</li> <li>• 3=Network provided</li> </ul>

**Table 4 SIP-to-PRI mapping when RPI Called headers are received (Sheet 1 of 2)**

SIP header	PRI IE
Rpi-pty-type: called	Redirection IE: Populated for all variants except for DMS
rpi user	Redirection Number IE: number digits
rpi-screen: screening level	Redirection Number IE: screening indicator
rpi-privacy: restriction level	Redirection Number IE: presentation indicator
Not populated in the redirect RPI	Redirection Number IE: type of number
Not populated in the redirect RPI	Redirection Number IE: numbering plan identification

**Table 4 SIP-to-PRI mapping when RPI Called headers are received (Sheet 2 of 2)**

SIP header	PRI IE
rpi-reason: reason	Redirection Number IE: reason
rpi-count: count	Not supported in redirection IE
rpi-display: name	Not supported in redirection IE
Rpi-pty-type: called	Original Called Number IE: Populated when the variant is DMS
rpi-user	OCN IE: number digits
rpi-screen: screening level	OCN IE: screening indicator
rpi-privacy: restriction level	OCN IE: presentation indicator
Not populated in the redirect RPI	OCN IE: type of number
Not populated in the redirect RPI	OCN IE: numbering plan identification
Not populated in the redirect RPI	OCN IE: CFNR indicator
rpi- count: count	OCN IE: Redirection counter
rpi-reason: reason	OCN IE: original redirection reason
rpi-display: name	Display IE: Original calling party name (DMS variant only)

**Table 5 SIP-to-PRI mapping when only redirect header is received (Sheet 1 of 2)**

SIP header	PRI IE
Rpi-pty-type: redirect	Redirection IE: Populated for all variants except for DMS
rpi user	Redirection Number IE: number digits
rpi-screen: screening level	Redirection Number IE: screening indicator
rpi-privacy: restriction level	Redirection Number IE: presentation indicator
Not populated in the redirect RPI	Redirection Number IE: type of number
Not populated in the redirect RPI	Redirection Number IE: numbering plan identification



**Table 5 SIP-to-PRI mapping when only redirect header is received (Sheet 2 of 2)**

SIP header	PRI IE
rpi-reason: reason	Redirection Number IE: reason
rpi-count: count	Not supported in redirection IE
rpi-display: name	Not supported in redirection IE
Rpi-pty-type: redirect	Original Called Number IE: Populated when the variant is DMS
rpi-user	OCN IE: number digits
rpi-screen: screening level	OCN IE: screening indicator
rpi-privacy: restriction level	OCN IE: presentation indicator
Not populated in the redirect RPI	OCN IE: type of number
Not populated in the redirect RPI	OCN IE: numbering plan identification
Not populated in the redirect RPI	OCN IE: CFNR indicator
rpi- count: count	OCN IE: Redirection counter
rpi-reason: reason	OCN IE: original redirection reason
rpi-display: name	Display IE: Original calling party name (DMS variant only)

**Table 6 SIP-to-PRI mapping when only called header is received (Sheet 1 of 2)**

SIP header	PRI IE
Rpi-pty-type: called	Redirection IE: Populated for all variants except for DMS
rpi user	Redirection Number IE: number digits
rpi-screen: screening level	Redirection Number IE: screening indicator
rpi-privacy: restriction level	Redirection Number IE: presentation indicator
Not populated in the redirect RPI	Redirection Number IE: type of number
Not populated in the redirect RPI	Redirection Number IE: numbering plan identification

**Table 6 SIP-to-PRI mapping when only called header is received (Sheet 2 of 2)**

SIP header	PRI IE
rpi-reason: reason	Redirection Number IE: reason
rpi-count: count	Not supported in redirection IE
rpi-display: name	Not supported in redirection IE
Rpi-pty-type: called	Original Called Number IE: Populated when the variant is DMS
rpi-user	OCN IE: number digits
rpi-screen: screening level	OCN IE: screening indicator
rpi-privacy: restriction level	OCN IE: presentation indicator
Not populated in the redirect RPI	OCN IE: type of number
Not populated in the redirect RPI	OCN IE: numbering plan identification
Not populated in the redirect RPI	OCN IE: CFNR indicator
rpi- count: count	OCN IE: Redirection counter
rpi-reason: reason	OCN IE: original redirection reason
rpi-display: name	Display IE: Original calling party name (DMS variant only)

**Table 7 PRI-to-SIP mapping when both IEs are received (Sheet 1 of 2)**

SIP header	PRI IE
Rpi-pty-type: redirect	Redirection IE:
rpi user	Redirection Number IE: number digits
rpi-screen: screening level	Redirection Number IE: screening indicator
rpi-privacy: restriction level	Redirection Number IE: presentation indicator
Not populated in the redirect RPI	Redirection Number IE: type of number
Not populated in the redirect RPI	Redirection Number IE: numbering plan identification
rpi-reason: reason	Redirection Number IE: reason

**Table 7 PRI-to-SIP mapping when both IEs are received (Sheet 2 of 2)**

SIP header	PRI IE
rpi-count: count (field is omitted from the header)	Not supported in redirection IE
rpi-display: name (field is omitted from the header)	Not supported in redirection IE
Rpi-pty-type: called	Original Called Number IE: Populated when the variant is DMS
rpi-user	OCN IE: number digits
rpi-screen: screening level	OCN IE: screening indicator
rpi-privacy: restriction level	OCN IE: presentation indicator
Not populated in the redirect RPI	OCN IE: type of number
Not populated in the redirect RPI	OCN IE: numbering plan identification
Not populated in the redirect RPI	OCN IE: CFNR indicator
rpi- count: count	OCN IE: Redirection counter
rpi-reason: reason	OCN IE: original redirection reason
rpi-display: name	Display IE: Original calling party name (DMS variant only)

**Table 8 PRI-to-SIP mapping when only Redirection IE is received (Sheet 1 of 2)**

SIP header	PRI IE
Rpi-pty-type: called	Redirection IE:
rpi user	Redirection Number IE: number digits
rpi-screen: screening level	Redirection Number IE: screening indicator
rpi-privacy: restriction level	Redirection Number IE: presentation indicator
Not populated in the redirect RPI	Redirection Number IE: type of number
Not populated in the redirect RPI	Redirection Number IE: numbering plan identification
rpi-reason: reason	Redirection Number IE: reason

**Table 8 PRI-to-SIP mapping when only Redirection IE is received (Sheet 2 of 2)**

SIP header	PRI IE
rpi-count: count (field is populated with the default of 1)	Not supported in redirection IE
rpi-display: name (field is omitted from the header)	Not supported in redirection IE

**Table 9 PRI-to-SIP mapping when only Original Called Party IE is received**

SIP header	PRI IE
Rpi-pty-type: called	Original Called Number IE: Populated when the variant is DMS
rpi-user	OCN IE: number digits
rpi-screen: screening level	OCN IE: screening indicator
rpi-privacy: restriction level	OCN IE: presentation indicator
Not populated in the redirect RPI	OCN IE: type of number
Not populated in the redirect RPI	OCN IE: numbering plan identification
Not populated in the redirect RPI	OCN IE: CFNR indicator
rpi- count: count	OCN IE: Redirection counter
rpi-reason: reason	OCN IE: original redirection reason
rpi-display: name	Display IE: Original calling party name (DMS variant only)

### SIP-to-PRI parameter mapping tables

The following tables describe the mapping between a PRI SETUP and a SIP INVITE signal.

**Table 10 PRI-to-SIP mapping with Presentation Allowed**

PRI IE	SIP Header
Called Party Number IE: number digits	RequestURI
Called Party Number IE: number digits	To
Calling Party Number IE: number digits	From (user)
Display IE: display information	From (name)
Calling Party Number IE: presentation indicator: Allowed	No RPI calling party header
Not populated in the ISDN signal	rpi-pty-type: redirect
DMS Variant: Original Called Number IE: presentation indicator Other Variants (supporting redirect): redirection IE: presentation indicator	rpi-privacy: restriction level
DMS Variant: Original Called Number IE: screening indicator Other Variants (supporting redirect): redirection IE: screening indicator	rpi-screen: screening Indicator
DMS Variant: Original Called Number IE: number digits Other Variants (supporting redirect): redirection IE: number digits	rpi user
<b>Note:</b> The redirect RPI is only included if the setup signal contains a Redirect IE. Only parameters that map to SIP appear in the table.	

**Table 11 PRI-to-SIP mapping with Presentation Restricted (Sheet 1 of 2)**

PRI IE	SIP Header
Called Party Number IE: number digits	RequestURI
Called Party Number IE: number digits	To
<b>Note:</b> The redirect RPI is only included if the setup signal contains a Redirect IE. Only parameters that map to SIP appear in the table.	

**Table 11 PRI-to-SIP mapping with Presentation Restricted (Sheet 2 of 2)**

PRI IE	SIP Header
Not populated in the setup signal	From (name) populated with "restricted name" property
Not populated in the setup signal	From (user) populated with "restricted user" property
Not populated in ISDN signal	rpi-pty-type: calling
Calling Party Number IE: presentation indicator	rpi-privacy = Full
Calling Party Number IE: screening indicator	rpi-screening: Screening Indicator
Display IE: display information	rpi-display-name
Calling Party Number IE: number digits	rpi user
Not populated in ISDN signal	rpi-pty-type: redirect
DMS Variant: Original Called Number IE: presentation indicator Other Variants (supporting redirect): Redirection IE: presentation indicator	rpi-privacy=restriction level
DMS Variant: Original Called Number IE: screening indicator Other Variants (supporting redirect): Redirection IE: screening indicator	rpi-screening: Screening Indicator
DMS Variant: Original Called Number IE: number digits Other Variants (supporting redirect): Redirection IE: number digits	rpi user
<b>Note:</b> The redirect RPI is only included if the setup signal contains a Redirect IE. Only parameters that map to SIP appear in the table.	

## Mapping of cause values

Table 12, "SIP-to-PRI cause mapping," illustrates the mapping between ISDN cause values and SIP response codes.

**Table 12 SIP-to-PRI cause mapping**

PRI cause value	SIP response code
Unallocated Number	404 Not Found
User Busy	486 Busy Here
Invalid Number Format (Address Incomplete)	400 Bad Request
Call Rejected	603 Decline
Recovery on Timer Expiry	408 Request Timeout
User Busy	480 Temporarily not available (SIP-to-PRI only)
All other cause values	480 Temporarily not available (PRI-to-SIP only)
Normal Call Clearing	All other Response codes (SIP-to-PRI only)







---

Succession Multimedia Xchange

# Succession MX SIP PRI Gateway

## Basics

Copyright © 2003 Nortel Networks,  
All Rights Reserved

**NORTEL NETWORKS CONFIDENTIAL:** The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only. Changes or modifications to the Succession MX SIP PRI Gateway without the express consent of Nortel Networks may void its warranty and void the user's authority to operate the equipment.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

\*Nortel Networks, the Nortel Networks logo, the Globemark, UNISim, Succession MX, Nortel, Northern Telecom, and NT, are trademarks of Nortel Networks.

---

Publication number: NN10255-111  
Product release: Succession MX 1.1 Standard  
Document release: Standard Succession MX 1.1 (02.02)  
Date: July 2003  
Printed in the United States of America.

---

