

NN10034-111

Succession Multimedia Communications Portfolio

# MCP SIP Audio Server

## Basics

Standard MCP 1.1 FP1 (02.02) April 2003

---





# Overview

---

## How this chapter is organized

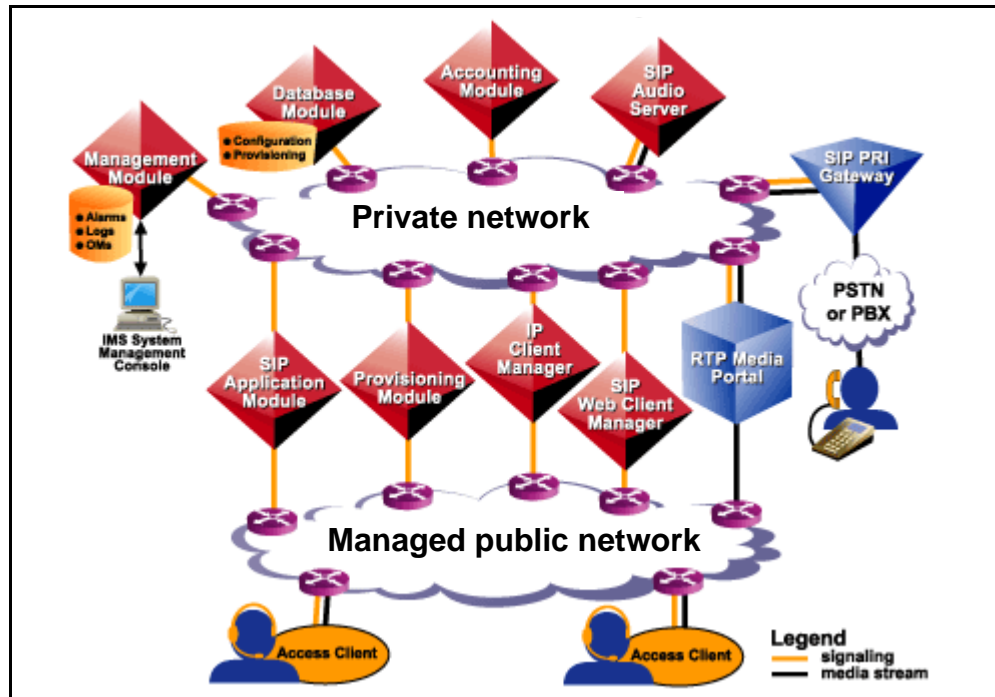
This chapter is organized as follows:

- “Overview” on page 3
- “Hardware” on page 5
- “Software” on page 11
- “Supported services” on page 12
- “OAM&P strategy” on page 15

## Overview

The SIP Audio Server is an optional SIP-enabled platform providing unique resources for audio conferencing within the Media Communications Portfolio (MCP). Figure 1, “Network connectivity,” shows how the SIP Audio Server fits into the MCP network. The following sections provide more details about the SIP Audio Server.

Figure 1 Network connectivity



The SIP Audio Server provides the conference call resources that bridge all the separate legs of an audio conference together in one connection. Conferencing service support is dependent upon the number of conference ports available on the hardware being used and upon the ability of the endpoint hardware to bridge onto the voice bus. The SIP Audio Server can provide conferencing for three or more parties. Any SIP-enabled client, such as the i2004 Internet telephones, the SIP Multimedia Web Client, or the SIP Multimedia PC Soft Client, can originate a conference. Any PSTN phone can be a part of that conference. Conferences up to 32 ports (talk/listen) can be established.

Because of the way the media cards perform audio-mixing, as the packet time increases, the number of available end points for each card also increases. For example, if all the clients are using 30-millisecond packet time, then you get the full 120. If all the clients are using 10 milliseconds, then it is about 90. Conferencing is based upon the Natural MicroSystems CG6000C card. Each CG6000C card can provide from 92 to 120 ports of conferencing capability by using six separate conference resources that each accommodate up to 32 conferees in a single conference. The actual conference capacity of the

system is also determined by the number of CG6000C cards provisioned and the amount of system play and monitor port usage.

**Note:** All of the resources required for a particular conference must be hosted by the same card and the same pool. A pool is a group of conference end points from which all the conference resources are allocated for any conference session. A conference session cannot span pools.

### Codec negotiation

The SIP Audio Server performs codec negotiation between various Voice over IP codecs. Codec is a compression scheme for audio and video data. End-user benefits of codec negotiation include bandwidth preservation and increased voice quality.

Codec negotiation is performed during call setup as outlined in RFC3261 SIP: Session Initiation Protocol. Call setup occurs during a normal call, mid-call codec changes, call transfer, conference, and call retrieve; basically, any time an Invite is sent. The SIP Audio Server supports the codecs listed in Table 1, "Supported codecs." The Packetization column lists the transmission rates in milliseconds supported by that codec.

**Table 1 Supported codecs**

Codecs	Packetization
G.729a, PCMU (G.711 mu-law), PCMA (G.711 a-law)	10,20,30,40,50,60
G.726-32	10,20,30,40,50,60
G.723	30,60

### Hardware

The SIP Audio Server runs on a Motorola CPX8216T, which is a compact PCI 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 CPX8216T chassis is configured as two independent processing systems or 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

Audio Server or SIP PRI Gateway. Hardware for the SIP Audio Server consists of the following:

- Intel processor board including 1 GB memory and a SCSI IO daughter board (CPV5370 host card)
- HSC (Hot Swap Controller and Bridge) module
- SCSI CD-ROM drive
- SCSI hard drive
- floppy drive
- Natural MicroSystems (NMS) CG6000C (input/output) cards provide VoIP conference resources (four ports on each card)
- available AC or DC power options

**Note:** The NMS cards are physically keyed (with red and blue keys) to only fit the backplane of the CPX8216T chassis. They are not compatible with other CPX8216 models.

The following is a list of additional, non-Motorola hardware required:

- mouse
- keyboard
- monitor
- KVM switch

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.

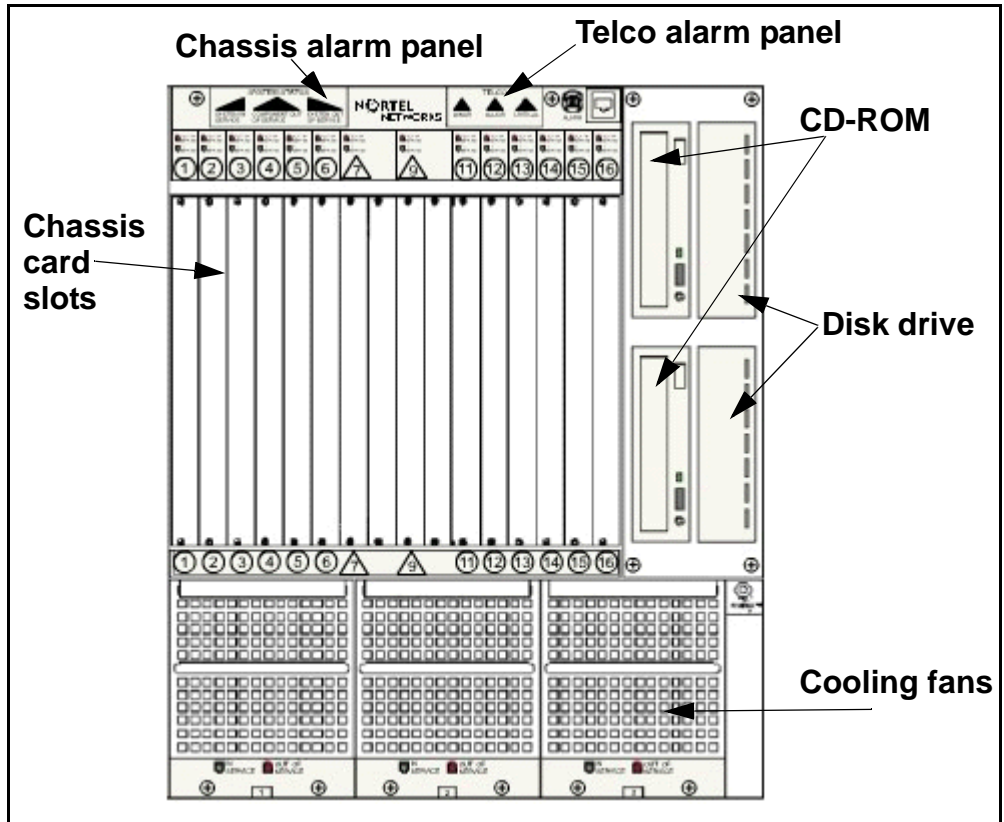


#### CAUTION

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

As a result, the CPX8216T, when configured for the SIP Audio Server, uses its separate processors and I/O domains as a dual-host system. Each half of the CPX8216T chassis can be an independent SIP Audio Server (or SIP PRI Gateway).

Figure 2 Chassis diagram (CPX8216T)



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 things 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

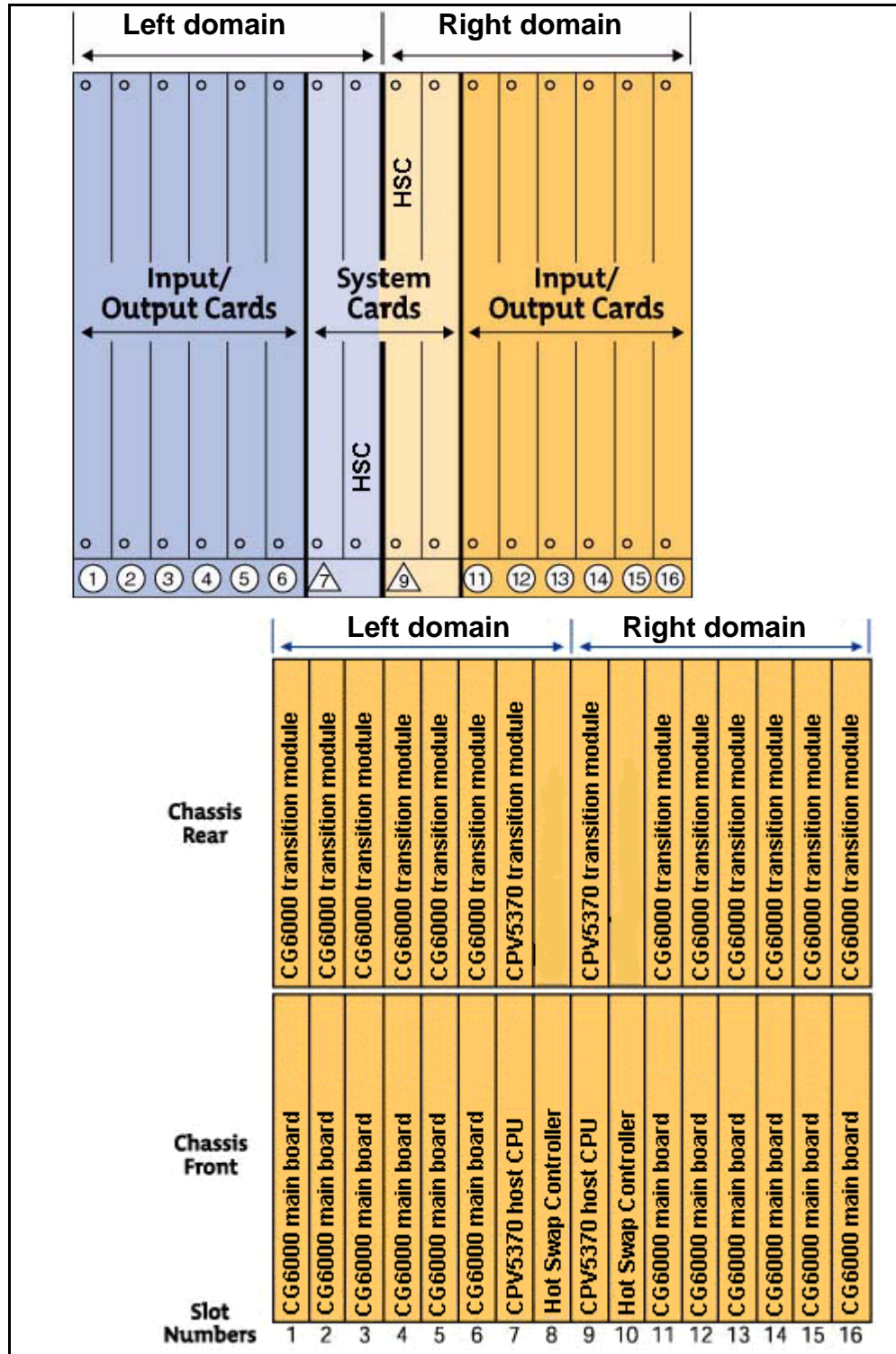
The CG6000C Input/Output (I/O) card is carrier-grade and, based on how it is configured, provides connectivity to the private network

through Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) media streaming capability.

Figure 3, “CPX8216T cards,” shows a front view of the card slots. Notice that the slots are numbered from left to right.



Figure 3 CPX8216T cards



The **Telco alarm panel** located at the top of the CPX8216T 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 (CPX8216T),” on page 7), 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 2.

**Table 2 Telco Alarm Indicators**

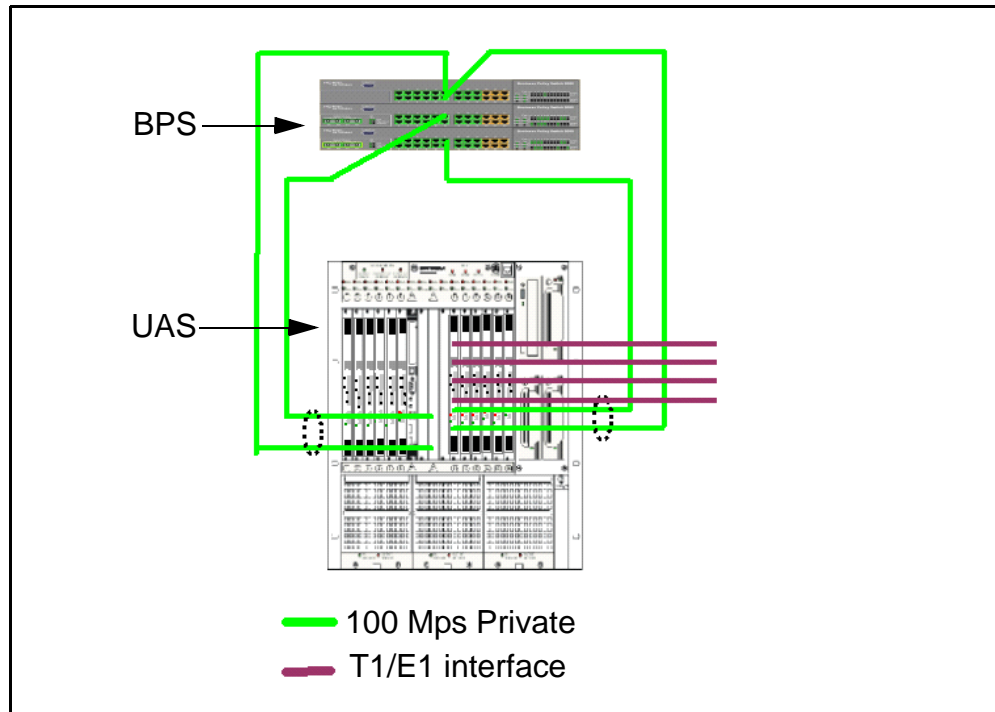
LED	Color
No alarm	Lights are off
Minor	Yellow
Major	Red
Critical	Red

The SIP Audio Server 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 ensures that the system alarms can activate the appropriate Telco alarm LEDs on the CX8216T chassis alarm panel.

The SIP Audio Server 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 CPX8216T chassis provisioned in the cabinet.

### Hardware redundancy

A SIP Audio Server sits on one 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 resources 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 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 continue to operate normally. To ensure that the engineered service capacity is not 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 73 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. 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 Global Server is the base software layer and is loaded onto the disk drive of the SIP Audio Server chassis domain to be used by the Host Central Processing Unit (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

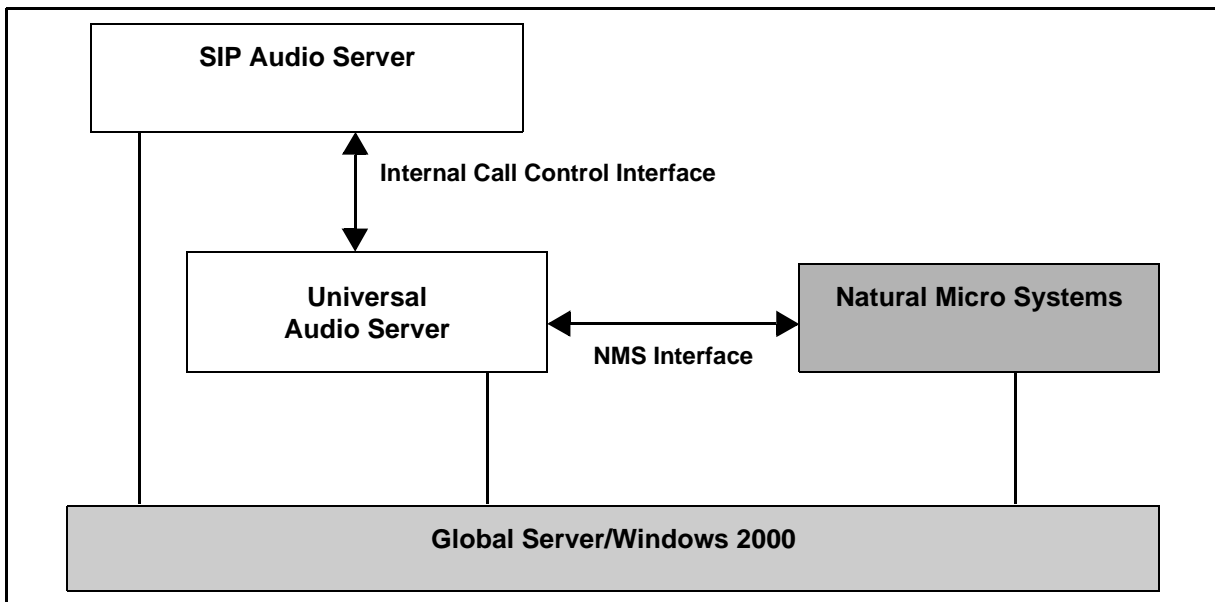
Systems (NMS) software. NMS software is preloaded on each card by the manufacturer.

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 Audio Server software is downloaded onto each Host CPU card after installation of the UAS base software and provides conference server functionality.

See Figure 5, "Software configuration," for a diagrammatic view of the software configuration.

**Figure 5 Software configuration**



## Supported services

The SIP Audio Server configuration provides ad hoc, multiple-leg, audio conference call capabilities and services that include:

- conference call support for up to 32 ports for each conference call
- The SIP Audio Server uses tokens to uniquely identify a conference session. When the originator sends an INVITE to the SIP Audio Server, the server provides a token. The originator client must inform other interested parties about that token using either BYE-ALSO or REFER. In response to that, the other interested parties add that token either in the REQUESTED-BY header or in

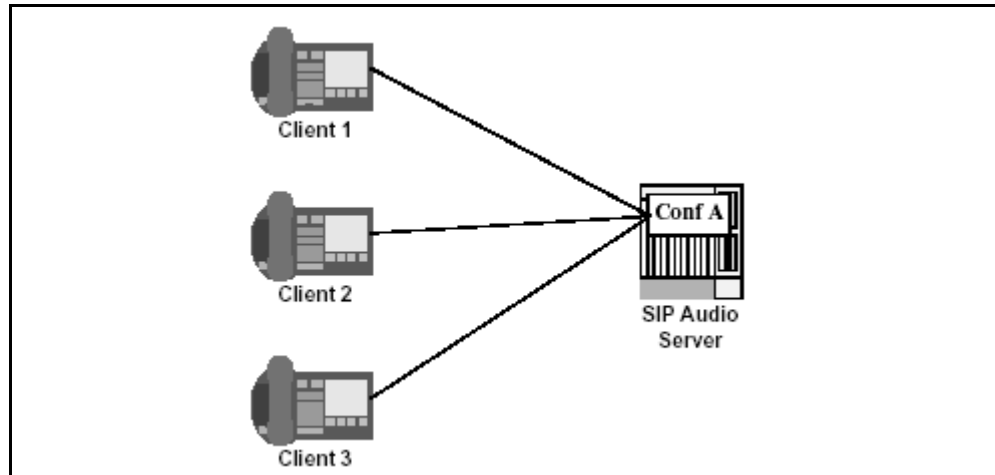
the REQUEST-URI of the INVITE. The SIP Audio Server looks at both places for the token. Once the server gets the token, it knows which conference this client wants to join.

When the SIP Audio Server receives the INVITE to initiate a conference session, it looks at the information in the INVITE message to know how many parties are going to join that conference and whether or not it has enough resources to handle it. If not, the SIP Audio Server rejects it with a 404 “Unavailable resources” message. If the information about how many parties want to join is missing, then the server uses the **Default Num of Ports** property, provisioned at the Media Gateway Controller tab, to allocate that conference.

During a conference call on the SIP Audio Server, any client may add additional clients onto the conference call. Although the addition of a client to a conference call appears to be seamless to the end-users, the SIP Audio Server must actually set up two conferences in order to achieve this.

As an example, Figure 6, “Illustration of a single audio conference,” shows Client 1, Client 2, and Client 3 connected within a conference (Conf A) at the SIP Audio Server.

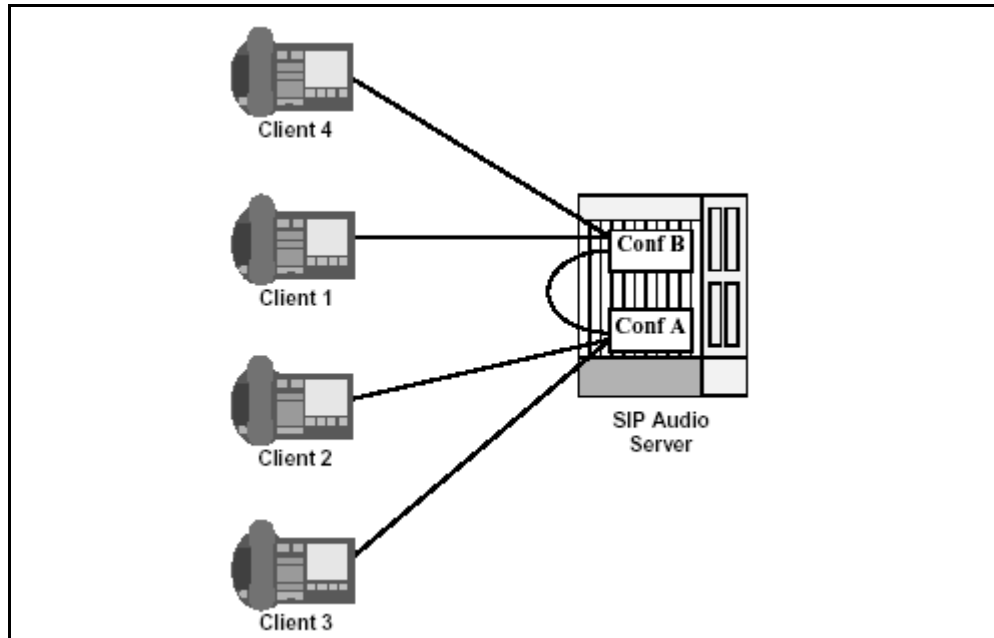
**Figure 6 Illustration of a single audio conference**



If Client 1 decides to conference in a new party, Client 4, then the SIP Audio Server sets up a new conference (Conf B) between Client 1 and Client 4. The SIP Audio Server then conferences Conf B into Conf A, where each of these conferences is considered a user of

each other, as shown in Figure 7, “Illustration of two daisy-chained audio conferences.”

**Figure 7 Illustration of two daisy-chained audio conferences**



Because of this complexity, Nortel Networks recommends that you limit the addition of conferences to two to avoid degradation in voice quality.

Once the conference call is up between all the parties, any party (including the conference originators) may leave the conference call without affecting the other parties within the conference. For example, if Client 1 leaves the conference call in the above scenario, Clients 2-3 remain on the conference call with no disruption.

- SIP BYE-ALSO/REFER messaging
- call transfers (a user in a conference call can transfer the call to another party)
- independent codec negotiation for each conference call leg (port)
- Hold/Retrieve: Once the client puts the call on hold, the SIP Audio Server stops sending media to that client until the call is retrieved.
- nodal authentication

If nodal authentication is turned off (left unchecked) in the **Authentication** tab (see “Completing the Authentication tab” on page 51 in the Configuration chapter), then the SIP Audio Server will accept requests from any other node in the network. If nodal

authentication is turned on (checked) in the **Authentication** tab, then the SIP Audio Server accepts messages from only those IP addresses that are listed as *trustedNodes*. If the message is not from a trusted node then it is rejected and the server sends a *305 Use Proxy* message containing one of the IP addresses from the *trustedNodes* list. Each time, the server uses the next trusted IP address in the list, in order.

- round-robin resource allocation

The SIP Audio Server uses a method called *round robin* for selecting media resources for conference calls. When the SIP Audio Server receives an Invite for a conference call, it will *round robin*, or rotate, through the media cards and conference pools installed on its chassis to determine which resources to use for the conference. The server rotates through the cards until a card is found with enough free conference ports to support the requested call.

The server searches for free resources beginning with the media cards and conference pool used by the last assigned conference call. From this card, the server rotates in numerical order through all the cards on the chassis until it finds a free resource. Even if there is still an active conference using a particular card, the SIP Audio Server begins its search for free resources with the last resource assigned to a conference call. This call may or may not be the conference call currently active. If there is just one card available, the SIP Audio Server only looks for resources on this card.

The following scenario will serve as an example of the round-robin resource allocation technique: A SIP Audio Server has four cards available on its chassis, and there is currently a conference call active on card 2. However, the last assigned conference call used card 3. The SIP Audio Server will begin to round robin on card 4 to find a free resource for the next conference call request.

- 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 Audio Server. For additional information, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents.







# Upgrades

## How this chapter is organized

This chapter is organized as follows:

- “Overview” on page 17
- “Software update procedure” on page 17
- “Update failures” on page 23
- “OAM&P strategy” on page 23

## Overview

This section describes the update strategies for the SIP Audio Server. 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.

## Software update procedure

Administrators can perform a SIP Audio Server maintenance load update from the System Management Console using the following procedures.

### ATTENTION

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



### CAUTION

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

**CAUTION**

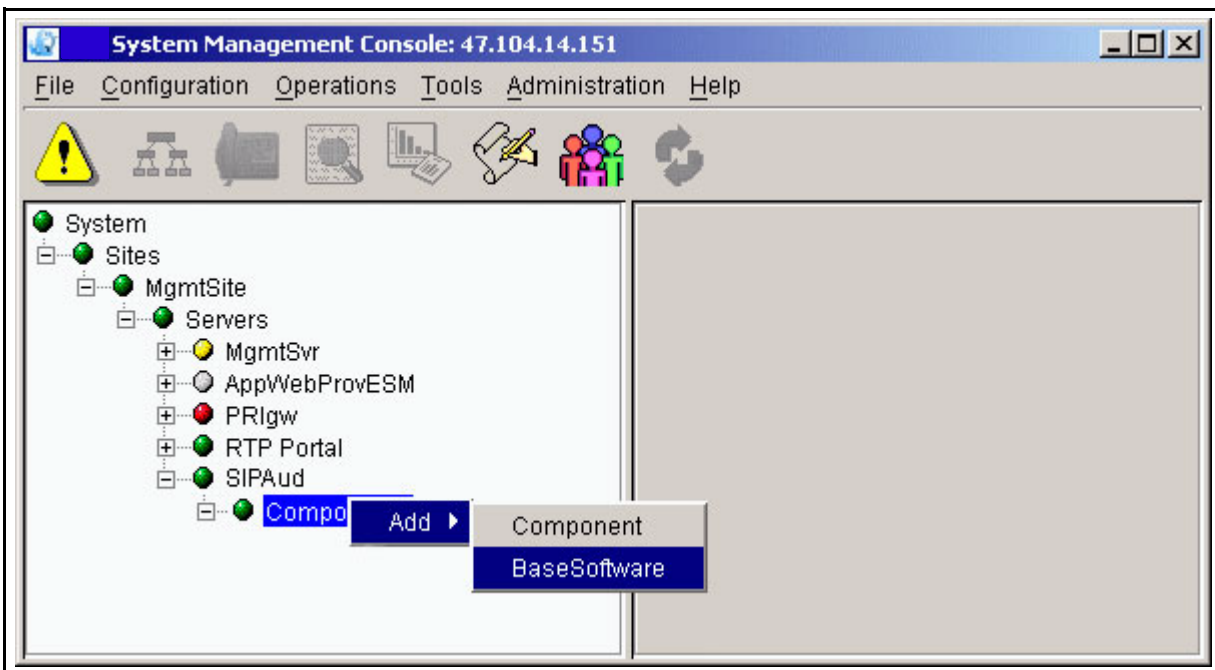
Under no circumstances should the locking key on the system hard drive be turned while the system is operational. Turning this key while the system is operational can result in false error condition reporting by the system.

**Procedure 1 Updating the UAS base software*****at your workstation***

- 1 Updating the UAS base software means applying the UAS maintenance release patches to the already deployed UAS base software. To do this, you need to deploy that particular UAS maintenance release using this procedure.

Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP Audio Server bullet, as shown in Figure 8, “Adding Base Software.”

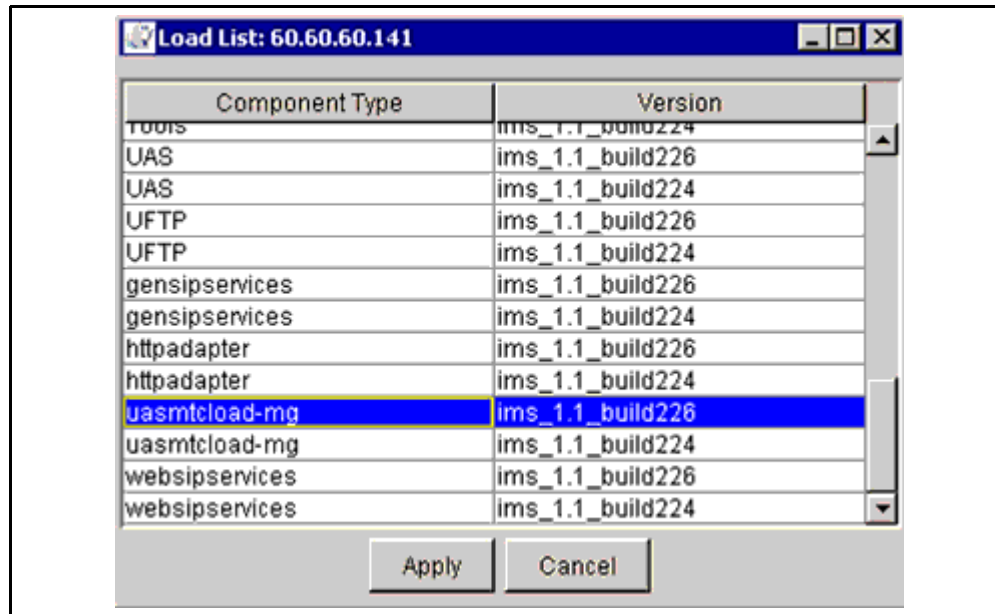
**Note:** The name of the SIP Audio Server is the name assigned to it during deployment, **SIPAud** in this example.

**Figure 8 Adding Base Software**

- 2 Right click on **Components**.

- 3 Select **Add->BaseSoftware**.
- 4 Select the UAS maintenance software load as shown in Figure 9, "Selecting the UAS maintenance software load."

**Figure 9 Selecting the UAS maintenance software load**



- 5 Click the **Apply** button. The UAS maintenance software is downloaded to the target SIP Audio Server node.
- 6 After the software load deployment is complete, log into the system.
- 7 Connect to the node that you are updating.
- 8 Install the new software load by double-clicking **D: \IMS\uasload-xx\WINNT\Setup.exe** where xx is the UAS maintenance release. For example, if the UAS maintenance release is **mg**, then you would double-click **D: \IMS\uasload-mg\WINNT\Setup.exe**.
- 9 An installation Wizard appears. Follow the steps in the Wizard.
- 10 If prompted to reboot, do so.

## Procedure 2 Performing the SIP Audio Server software update

### ATTENTION

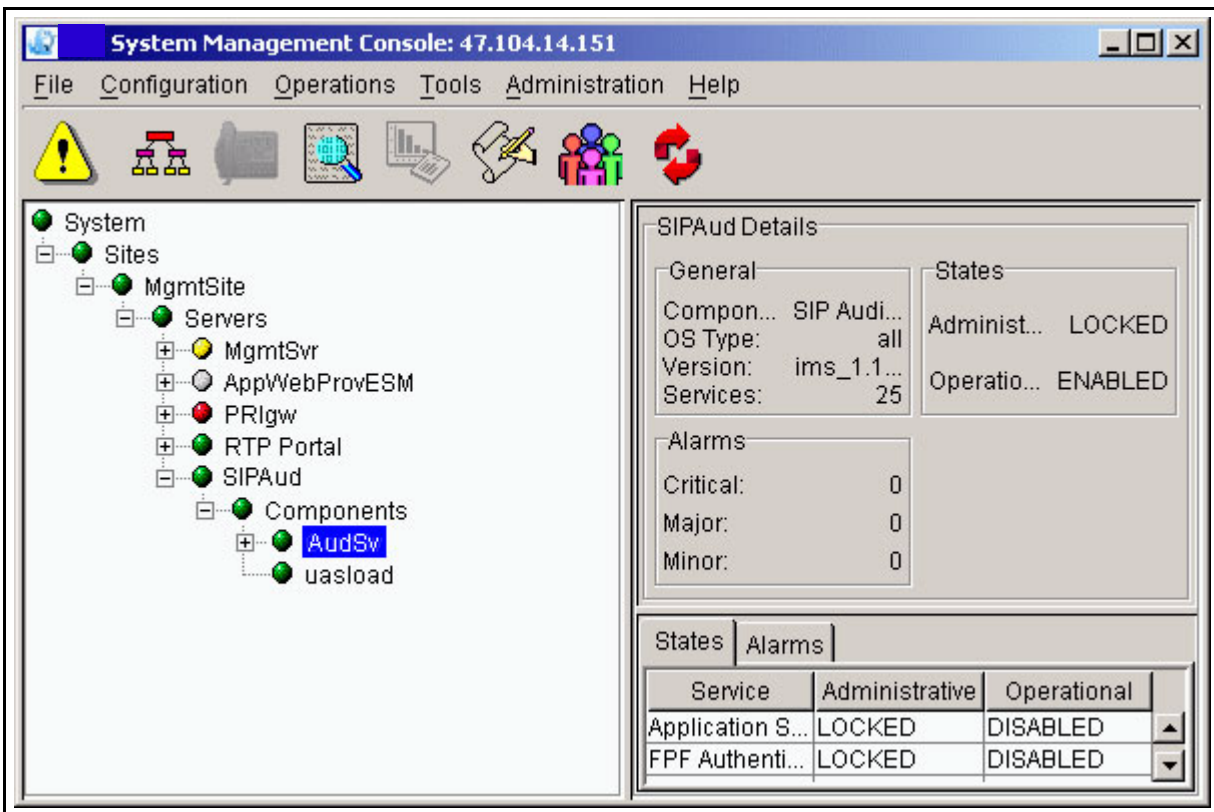
The server will be unavailable during the update. Existing calls will lose voice path and no new calls will be established.

### at the System Management Console

- 1 A software 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.

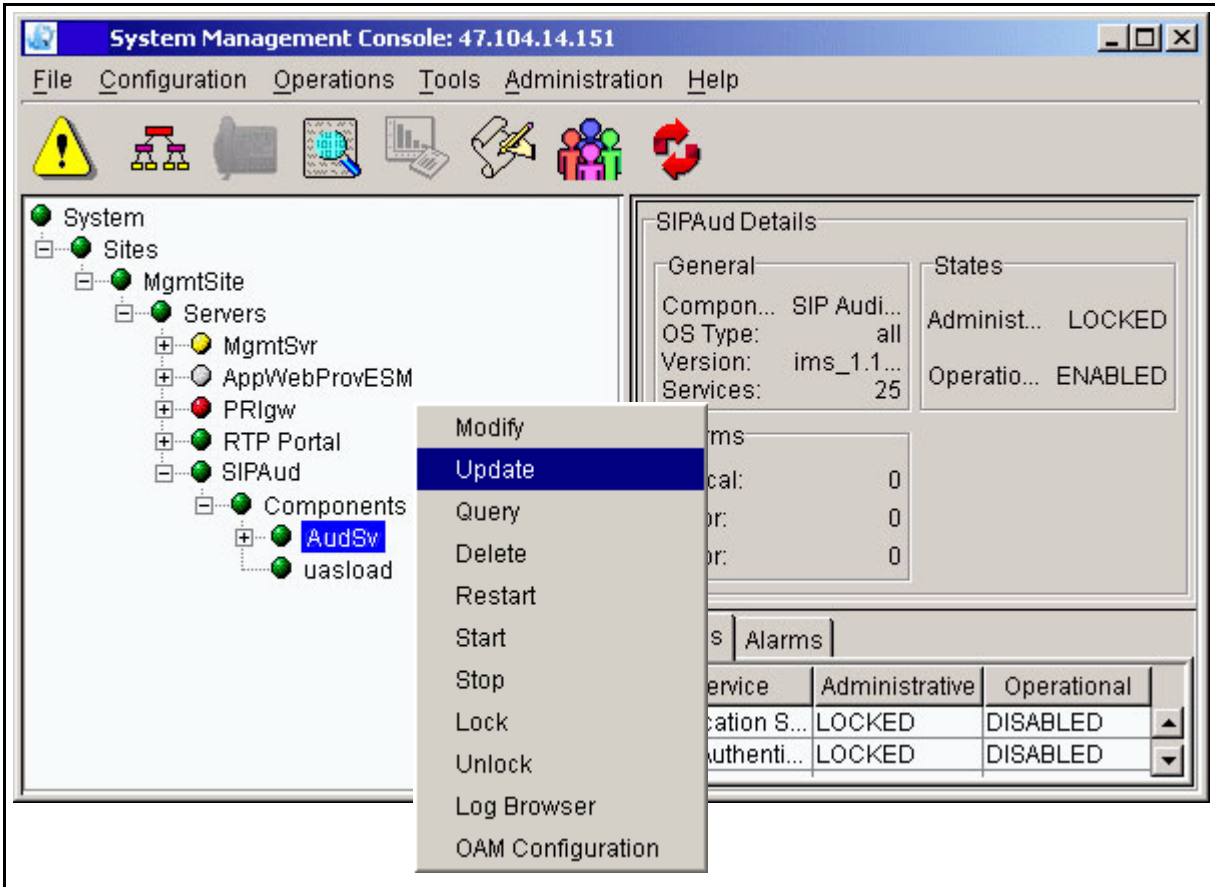
Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP Audio Server component bullet (**SIPAud** in the example), as shown in Figure 11, “Updating the SIP Audio Server from the menu tree.”

Figure 10 Updating the SIP Audio Server from the menu tree



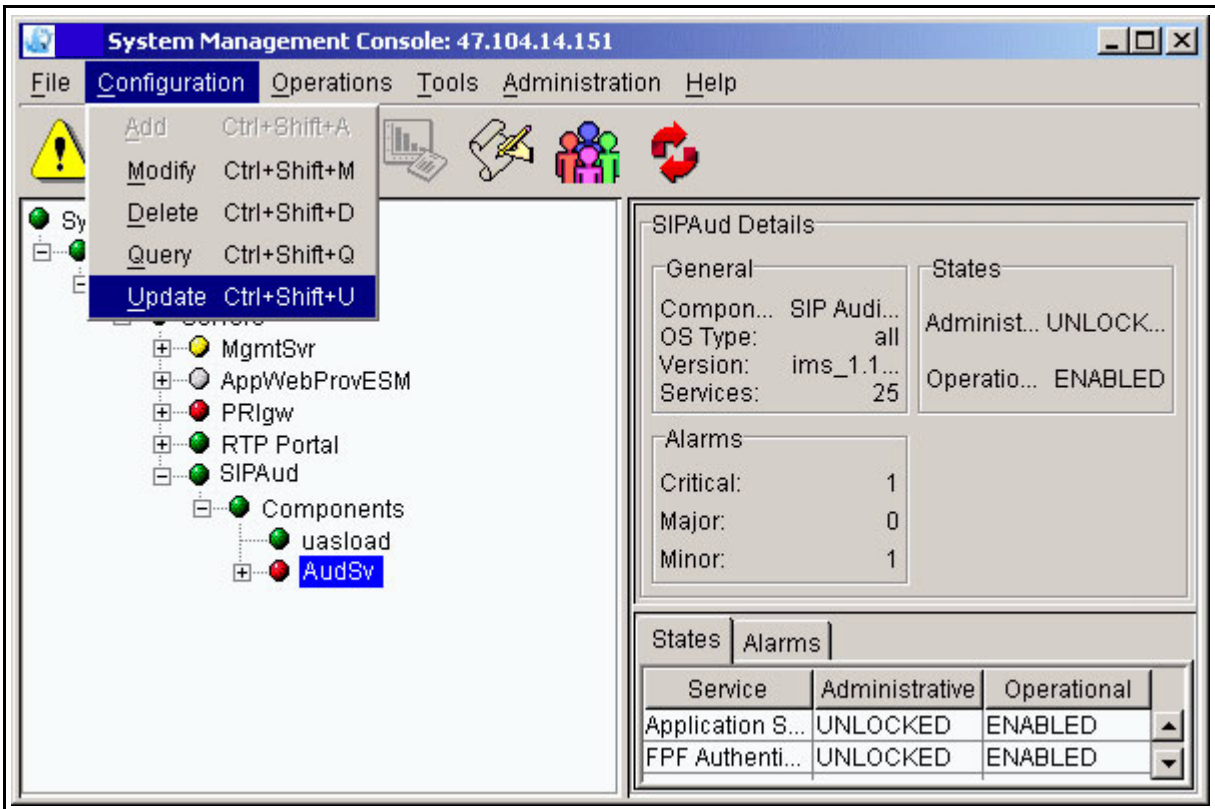
- 2 Right-click on the named component (**AudSv** in the example).
- 3 Select the **Update** option from the popup menu.

Figure 11 Updating the SIP Audio Server from the menu tree



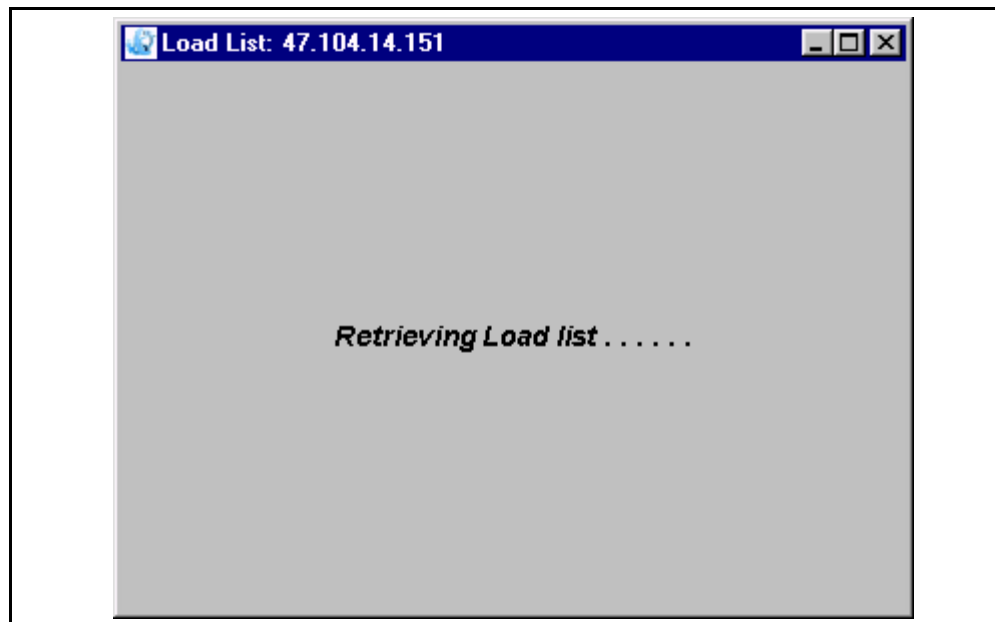
You can also launch the update from the pull-down Configuration menu, as shown in Figure 12, “Updating the SIP Audio Server from the pull-down menu.”

**Figure 12 Updating the SIP Audio Server from the pull-down menu**



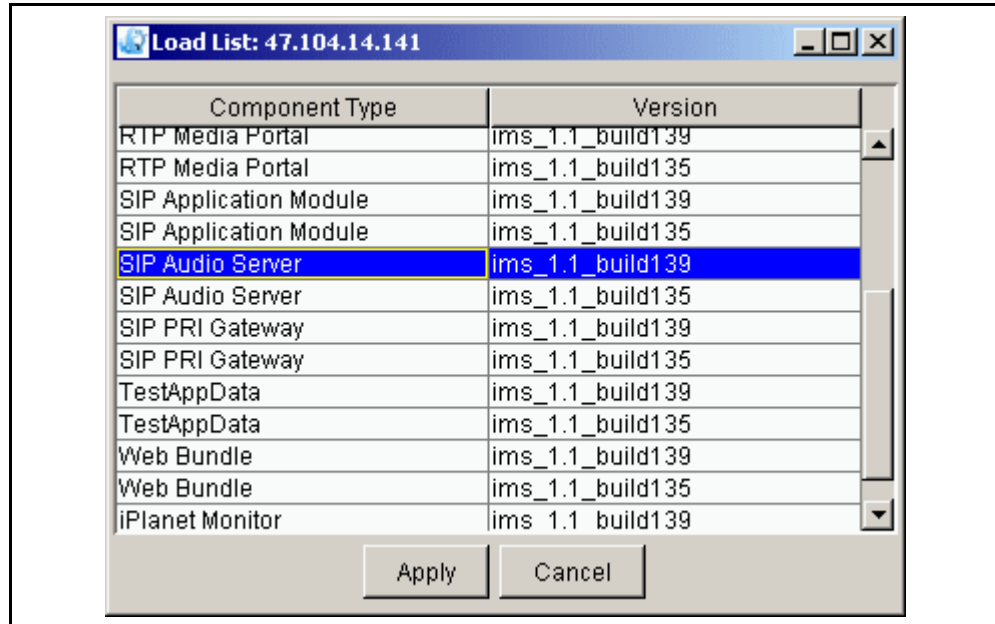
4 Select the **Update** command. The following window appears.

**Figure 13 The update window, retrieving the load list**



- 5 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 to which you want to update.

**Figure 14 Load list for updating**



- 6 Click on the **Apply** button.  
The console that appears displays the differences between the configuration data of the old version and the configuration data of the updated version by highlighting the tab(s). In the tabs shown on the configuration window, modify any configuration values required.
- 7 *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 Audio Server. For additional information, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents.







## Fault management

### How this chapter is organized

The procedures in this section are organized as follows:

- “Term definitions” on page 26
- “Clearing alarms” on page 26
  - “Clearing the ACS101 alarm” on page 26
  - “Clearing the UAS190 alarm” on page 27
  - “Clearing the UAS790 alarm” on page 27
  - “Clearing the UAS791 alarm” on page 27
  - “Clearing the UAS912 alarm” on page 28
  - “Clearing the UAS913 alarm” on page 28
  - “Clearing the UAS923 alarm (Ethernet connection failure on NMS CG6000 cards)” on page 28
  - “Clearing the UAS936 alarm (CG6000 card not present)” on page 29
  - “Clearing the UAS939 (CG6000 card failure) alarm” on page 30
- “Interpreting software errors” on page 30
- “Repairing hardware failures” on page 33
  - “Clearing the Motorola 5370 Ethernet connection failure” on page 33
  - “Replacing a CPV5370 Processor card” on page 33
  - “Replacing a Hot Swap Controller card” on page 36
  - “Replacing a CG6000 card through a hot swap” on page 38

See the *MCP System Management Console Basics* document for more information about logs and alarms that pertain to the SIP Audio Server.

## Term definitions

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

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

## Clearing alarms

The following section details how to clear certain alarms that affect the hardware or software.

### Procedure 1 Clearing the ACS101 alarm

#### *at the System Management Console*

- 1 The UAS Unreachable alarm (ACS101) indicates “Resource Discovery and Initialization Complete. No media resources are available at this time. Calls using this SIP Audio Server cannot be made at this time.”

This alarm should be automatically cleared within 15 minutes. If it is not cleared,

  - a Check for configuration errors in `C:\uas\etc\uas.conf` and `C:\uas\etc\ugw.conf` files
  - b Restart the application. If that fails, contact your next level of support.

## Procedure 2 Clearing the UAS190 alarm

### *at the System Management Console*

- 1 The UAS\_SNMP\_Agent\_Unreachable alarm (UAS190) indicates that the SNMP agent has stopped responding. Synchronization with the active alarm table of the UAS is failing. Performance measurements cannot be retrieved from the UAS.  
Check the CPU utilization and available system memory.
- 2 Wait for several minutes. If the alarm has not cleared at that time, contact your next level of support.

## Procedure 3 Clearing the UAS790 alarm

### *at the System Management Console*

- 1 The probable cause of the UAS\_Trapping\_Monitor\_Inactive alarm is an error encountered when the UAS Trapping Monitor was being initialized. This condition will prevent synchronizing with the active alarm table of the UAS. Call processing is not affected by this error.  
Check for the configuration error in the Trap Destination IP address in the `uasagent.xml` file.
- 2 After making this correction, restart the application. If the alarm has not cleared, contact your next level of support.

## Procedure 4 Clearing the UAS791 alarm

### *at the System Management Console*

- 1 The probable cause of the UAS\_Trapping\_Monitor\_Inactive alarm is an error encountered during initialization. This condition prevents retrieval of performance measurements from the UAS. Call processing is not affected by this error.  
Check for the configuration error either in the Trap Destination IP address or in the declaration of the number of cards configured, in the `uasagent.xml` file.
- 2 After making this correction, restart the application. If the alarm has not cleared, contact your next level of support.

### Procedure 5 Clearing the UAS912 alarm

#### *at the System Management Console*

- 1 The SNTP Set Failed warning alarm appears as a warning message: "Error encountered in synchronizing the clock with NTP server."  
  
Perform a **Query** on the SIP Audio Server's Media Gateway tab using the System Management Console and check the NTP Server IP address.
- 2 Correct the IP address if necessary. To do so,
  - a Select the **Modify** button.
  - b Type in the correct IP address.
  - c Select the **Apply** button.
  - d Wait 10 minutes.
- 3 If the alarm is not cleared within 10 minutes, contact your next level of support.

### Procedure 6 Clearing the UAS913 alarm

#### *at the System Management Console*

- 1 The SNTP Validation Failed warning alarm appears as a warning message: "Error encountered in synchronizing the clock with NTP server."  
  
Perform a **Query** on the SIP Audio Server's Media Gateway tab using the System Management Console and check the NTP Server IP address.
- 2 Correct the IP address if necessary. To do so,
  - a Select the **Modify** button.
  - b Type in the correct IP address.
  - c Select the **Apply** button.
  - d Wait 10 minutes.
- 3 If the alarm is not cleared within 10 minutes, contact your next level of support.

### Procedure 7 Clearing the UAS923 alarm (Ethernet connection

**failure on NMS CG6000 cards)*****At the frame***

- 1 The NMS CG6000 cards contain two Ethernet ports configured in a fault-tolerant topology. A failure of an Ethernet port is determined by not detecting any voltage on the port.
  - a When one Ethernet cable connection on a CG6000 card fails, all traffic starts to use the second port. A UAS923 alarm with severity = MINOR is raised to indicate the problem.

To clear the alarm, restore the connection. The port is automatically recovered.
  - b When both Ethernet cables on a CG6000 card fail, the voice path on all the call legs for the existing conference calls using that card is lost. The conference calls are dropped only when the conferees hang up. The card is no longer used for subsequent conference calls. If there are other cards available in the system then all subsequent conference calls are established using the resources available on those cards. A UAS923 alarm with severity = CRITICAL is raised to indicate the problem.

To clear the alarm, restore one or both of the connections. Once you plug the cable back in, all the resources on that card are available for allocating subsequent conferences.

**Procedure 8 Clearing the UAS936 alarm (CG6000 card not present)*****At the frame***

- 1 A card failure results when the card is removed from the system. The voice path on all of the call legs for the existing conference calls using that card is lost. The conference calls are dropped only when the conferees hang up. The card is no longer used for subsequent conference calls. If there are other cards available in the system, then all subsequent conference calls are established using the resources available on those cards. A

UAS936 alarm with severity = MAJOR is raised to indicate the problem.

To clear the alarm,

- a Lock the card.
- b Remove and reseal the card. See “Replacing a CG6000 card through a hot swap” on page 38 for specific instructions.
- c Unlock the card.
- d Restart the SIP Audio Server.
- e If the problem continues, replace the card. (See “Replacing a CG6000 card through a hot swap” on page 38 for specific instructions.)
- f If the problem still continues, contact your next level of support.

### **Procedure 9 Clearing the UAS939 (CG6000 card failure) alarm**

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

- 1 A card failure results when the card stops responding. The voice path on all of the call legs for the existing conference calls using that card is lost. The conference calls are dropped only when the conferees hang up. The card is no longer used for subsequent conference calls. If there are other cards available in the system, then all subsequent conference calls are established using the resources available on those cards. 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 38 for specific instructions.
- c Unlock the card.
- d Restart the SIP Audio Server.
- e If the problem continues, contact your next level of support.

## **Interpreting software errors**

Table 3, “Interpreting software errors,” details the possible software errors a user may encounter at the client interface. The user reports the error to the administrator for action.

**Table 3 Interpreting software errors (Sheet 1 of 2)**

Errors	Symptoms/causes	Actions
<i>Unknown Conference</i>	The SIP Audio Server failed to locate a specified conference. This error occurs if the client contacts the SIP Audio Server with an invalid conference token (such as a token that was never allocated by the SIP Audio Server).	If this happens each time, contact your next level of support.
<i>Conference Resource Full</i>	<p>The conference session is full, and no more users are allowed. A client would receive this error in the following scenario: An originator of a call plans a 4-party conference call. Five or more users try to join that conference session. Any users past the fourth will get this error.</p> <p>The conference Invite was missing the number of parties (rtpmap) field and therefore a 3-party conference was allocated because the SIP Audio Server uses the <b>Default Number of Ports</b> property in the Media Gateway Controller tab, which is set to 3 by default, to allocate the conference.</p>	Increase the value for the <b>Default Number of Ports</b> . For more information about this property, see “Configuring the Media Gateway Controller tab” on page 50. If clients continue to show this error, contact your next level of support.

**Table 3 Interpreting software errors (Sheet 2 of 2)**

Errors	Symptoms/causes	Actions
<p><i>Unavailable Resources</i></p>	<p>1) There are not enough conference ports available to allocate this conference session. For example, if you are trying a 5-party conference but only three ports are available in any of the pools in any of the cards, then users will see this error.</p>	<p>Add media cards if this error occurs frequently.</p>
	<p>2) One or more media cards may have become corrupted, making it unavailable as a valid conference resource.</p>	<p>Check for alarms using the Alarm browser on the System Management Console. If there are any alarms then take the corrective action shown on the Alarm browser to clear that alarm. For more information, see the <i>MCP System Management Console Basics</i>.</p>
	<p>3) Users may get this error within 6 to 8 minutes of the SIP Audio Server restart/update (maintenance). Card initialization takes several minutes before the cards come into an in-service state.</p>	<p>Check for alarms at the Media Gateway Controller bullet using the Alarm browser on the System Management Console. If there are any alarms, then take the corrective action shown on the Alarm browser to clear that alarm. For more information, see the <i>MCP System Management Console Basics</i>.</p>
<p><i>Method Not Allowed</i></p>	<p>The SIP Audio Server received a message that it does not support. A client would receive this error if it sent an instant message to the SIP Audio Server.</p>	<p>Contact your next level of support.</p>



## Repairing hardware failures

Use the following procedures to recover from hardware failures.

### Procedure 10 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. 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 ISDN call attempts fail since communication to the SIP Application Module is lost. All existing calls remain active.

Replace the host card (see the procedure “Replacing a CPV5370 Processor card” on page 33).

### Procedure 11 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 wrist strap 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.

**Figure 15 Loose spiral gasket**



***At the System Management Console***

- 1 Navigate to the Maintenance window as shown in “Accessing the Maintenance window” on page 78.
- 2 Click the **Change** button, located in the States pane.  
A Change Administrative State window appears.
- 3 If you want to forcefully lock the server, select the **Lock Force** radio button.  
  
If you want to gracefully lock the server, select the **Lock Graceful** radio button.  
  
If you want to unlock the server, select the **Unlock** radio button.
- 4 Click **OK**. Ensure that the new Administrative State is locked.

- 5 Shut down the system:  
select **Start -> Shut Down**
  - a 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.
- 6 Locate the CPV5370 card. If the SIP Audio Server 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 module in the slot with a Phillips head screwdriver, and unlock the lock latches before removing 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 will reboot upon insertion of 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 module in the slot with a Phillips head screwdriver, and unlock the lock latches before removing 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 will reboot upon insertion of 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 module in the slot with a Phillips head screwdriver, and unlock the lock latches before removing 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.
- 7 Click the **Change** button, located in the States pane.  
A Change Administrative State window appears.
- 8 Click **OK**.
- 9 Ensure that the New Administrative State is **Unlocked**.
- 10 You have completed this procedure.

### Procedure 12 Replacing 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 wrist strap 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 15, "Loose spiral gasket," on page 34.

***At the System Management Console***

- 1 Navigate to the Maintenance window as shown in "Accessing the Maintenance window" on page 78.
- 2 Click the **Change** button, located in the States pane.  
A Change Administrative State window appears.
- 3 If you want to forcefully lock the server, select the **Lock Force** radio button.  
  
If you want to gracefully lock the server, select the **Lock Graceful** radio button.  
  
If you want to unlock the server, select the **Unlock** radio button.
- 4 Click **OK**. Ensure that the New Administrative State is locked.

***At the System Management Console (Windows desktop interface) connected to the domain containing the card being replaced:***

- 5 Shut down the system by selecting  
**Start -> Shut Down**
- 6 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.
- 7 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 card in the slot with a Phillips head

screwdriver, and unlock the lock latches before removing the cards.).

**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.)
- 8** Restart the system.

***At the System Management Console:***

- 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 CG6000 card through a hot swap**

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

**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 15, "Loose spiral gasket," on page 34.

**At the SIP Audio Server machine**

- 1 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	steps b through m
you are replacing only a rear module	steps e through m
you are replacing both a front module and a rear module	steps 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 2.
- 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 2.
- 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.
- 2** Using the procedure “Locking or unlocking an interface card (CG6000)” on page 85, unlock the CG6000 card that was just replaced.
  - 3** You have completed this procedure.





# Configuration management

The SIP Audio Server is deployed and configured using the MCP System Management Console. For more information, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics*. This chapter describes the configurable parameters affecting operation of the SIP Audio Server and the procedures for configuration required at the service provider premises.

Configuration management for the SIP Audio Server involves modifying system parameters in response to changes in the system configuration. Changes to system parameters are made through the System Management Console.

## How this chapter is organized

This chapter is organized as follows:

- “Configuration procedures” on page 43
- “Configuring the SIP Audio Server tabs” on page 49
- “Changing SIP Audio Server configuration” on page 66

## Configuration procedures



### CAUTION

Before making any changes to the base configuration, consult your next level of support.

This section contains the following procedures:

- “Adding the UAS base software” on page 44
- “Adding the SIP Audio Server software” on page 45
- “Configuring the SIP Audio Server tabs” on page 49

Before adding the SIP Audio Server component, make sure that the **uasload** base software has been installed. For information on adding the server hardware, see the *MCP System Management Console Basics* document.

## Adding the UAS base software

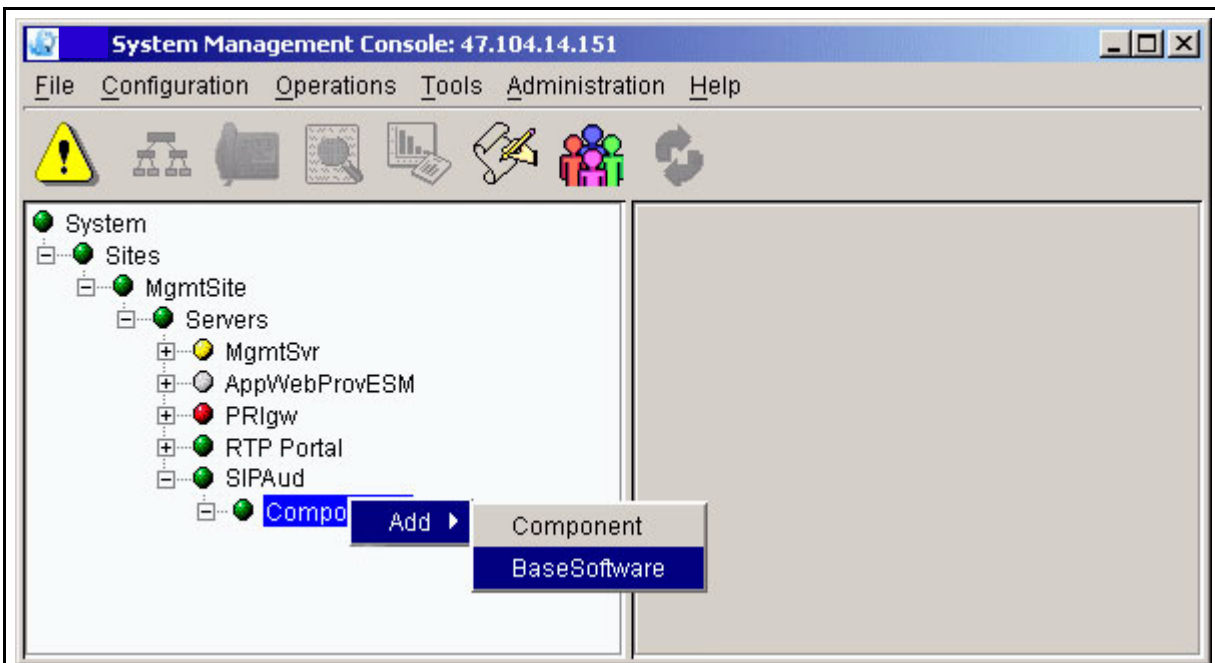
### at your workstation

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP Audio Server bullet, as shown in Figure 16, “Adding Base Software.”

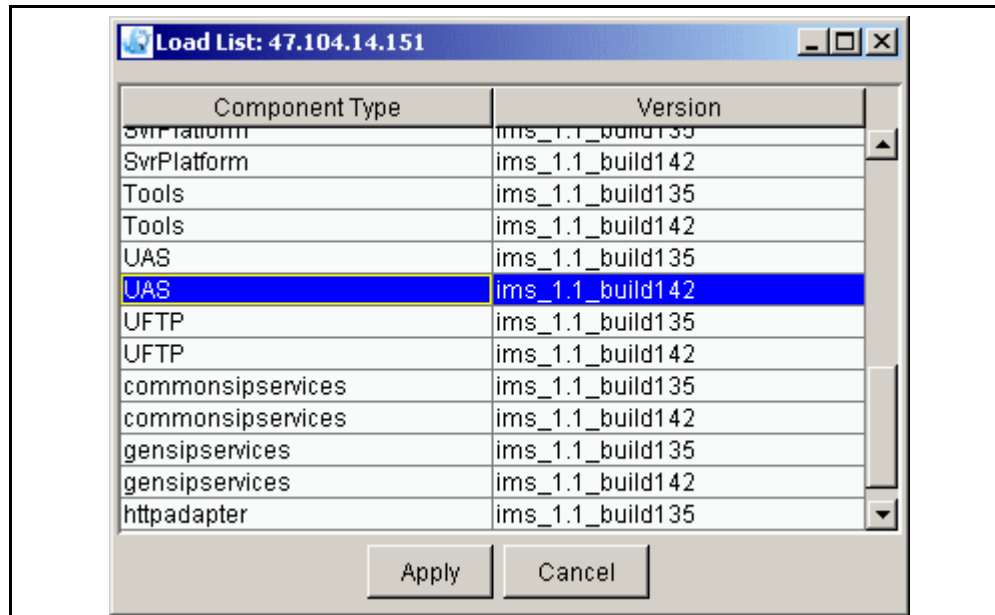
**Note:** The name of the SIP Audio Server is the name assigned to it during deployment, **SIPAud** in this example.

- 2 Right click on **Components**.
- 3 Select **Add->BaseSoftware**.

Figure 16 Adding Base Software



- 4 Select the UAS load as shown in Figure 17, “Selecting the UAS software load.”

**Figure 17 Selecting the UAS software load**

- 5 Click the **Apply** button. The UAS software is downloaded to the target SIP Audio Server node.
- 6 After the download is complete, connect to the node that you are updating, and then install the new software load by double-clicking  
**D: \IMS\uasload\WINNT\Setup.exe.**
- 7 An installation Wizard appears. Follow the steps in the Wizard.
- 8 If prompted to reboot, do so.

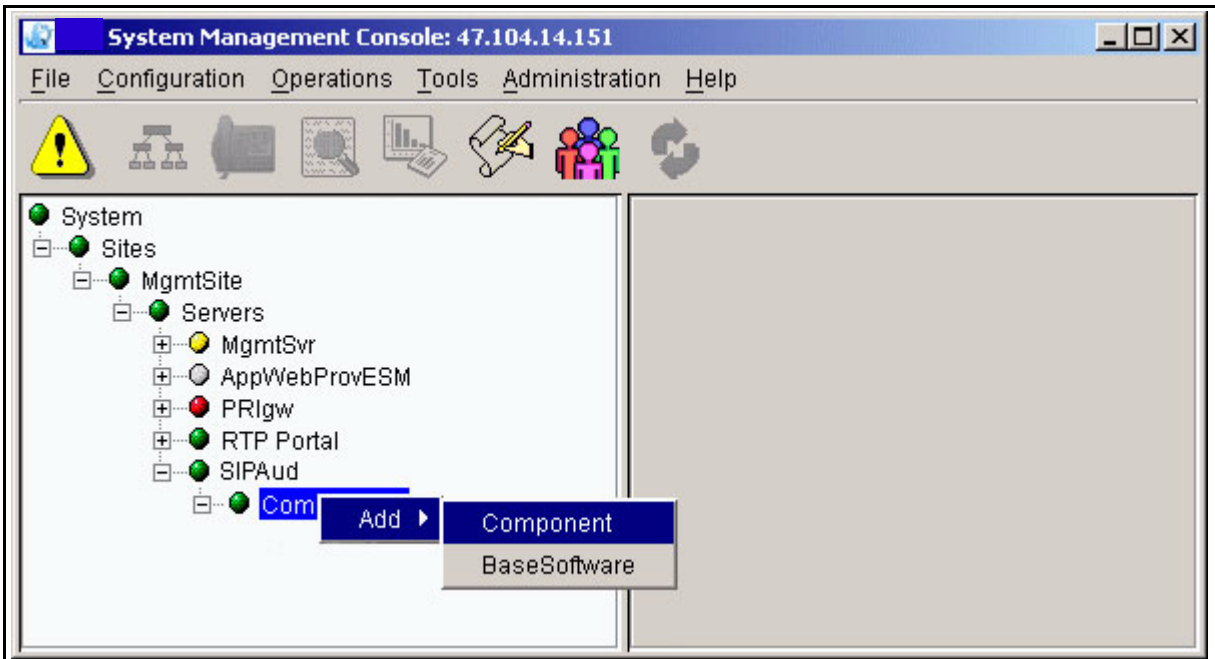
### Adding the SIP Audio Server software

Use the following procedure to add the SIP Audio Server component. The example shown assumes that the server on which the SIP Audio Server will be deployed has already been configured. For example, Figure 18, "Adding the component," shows the SIP Audio Server being deployed onto the previously configured server **SIPAud**. For the procedure for adding a server, refer to the *MCP System Management Console Basics*.

#### at the System Management Console

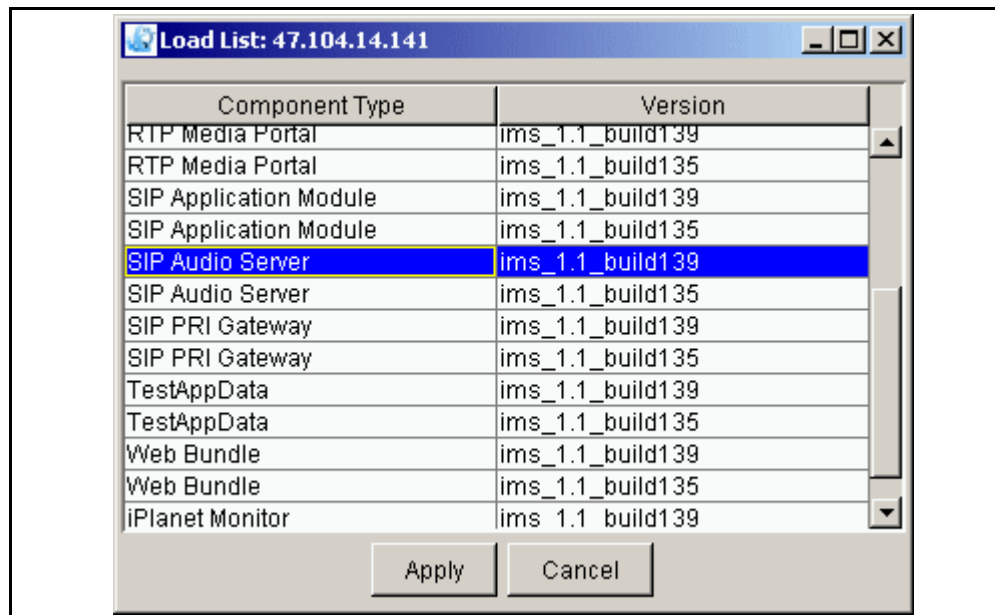
- 1 To add the SIP Audio Server, right-click on **Components** under the server **SIPAud** and select **Add->Component** as shown in Figure 18, "Adding the component."

Figure 18 Adding the component



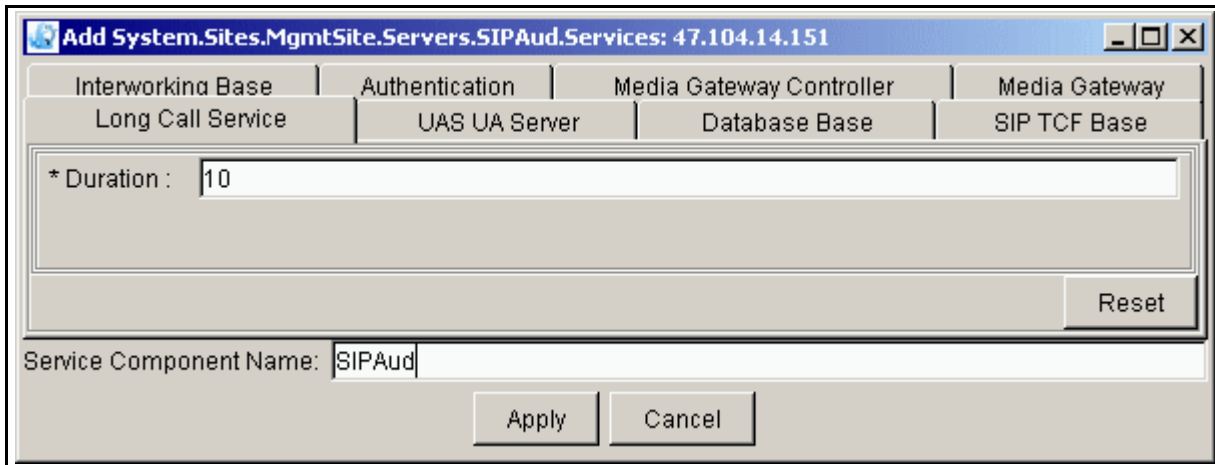
- 2 The window shown in Figure 19, "Selecting the SIP Audio Server load," appears. There may or may not be multiple software loads for you to choose from. Select the SIP Audio Server load you want and click on the **Apply** button.

Figure 19 Selecting the SIP Audio Server 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 **SIPAud** entered in the Service Component Name field.

**Figure 20 Example GUI with Service Component Name added**



4

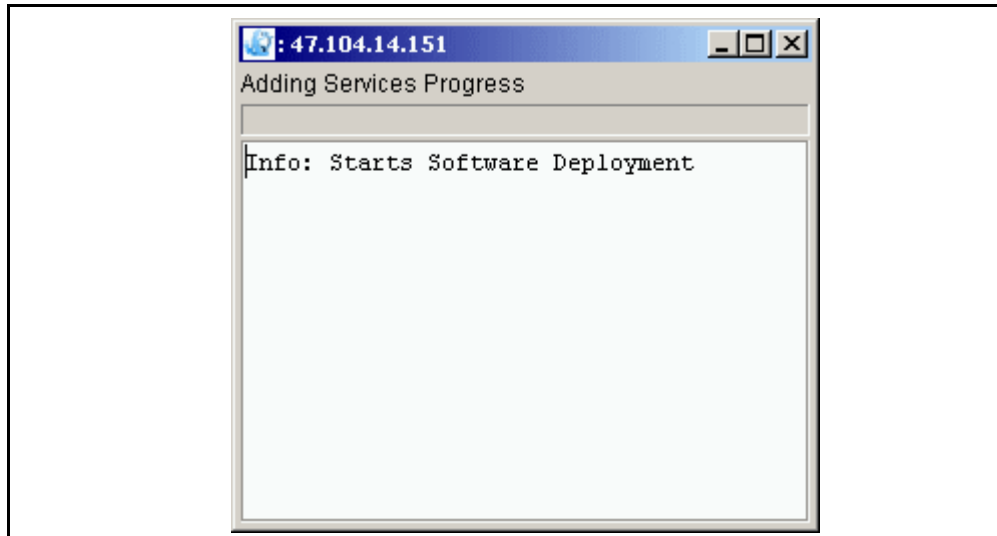
#### **ATTENTION**

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

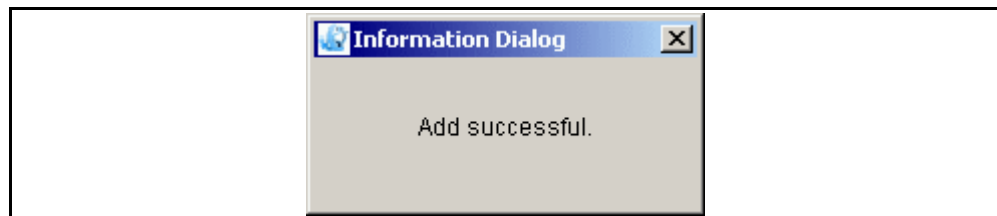
Note that there are eight different tabs representing the configurable services that the SIP Audio Server requires. The following section in this chapter describes each tab in detail and provide guidance on how to configure the tabs. Many of the fields already contain default values, and administrators 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 on the **Apply** button, the System Management software begins the deployment of the SIP Audio Server software. The Adding Services Progress dialog box appears as shown in Figure 21, "Adding Services Progress dialog box."

**Figure 21 Adding Services Progress dialog box**

If the deployment is successful, an "Add successful" box appears, as shown in Figure 22, "The Add successful dialog box."

**Figure 22 The Add successful dialog box**

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 Audio Server 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 *MCP System Management Console Basics* document.



### Configuring the SIP Audio Server tabs

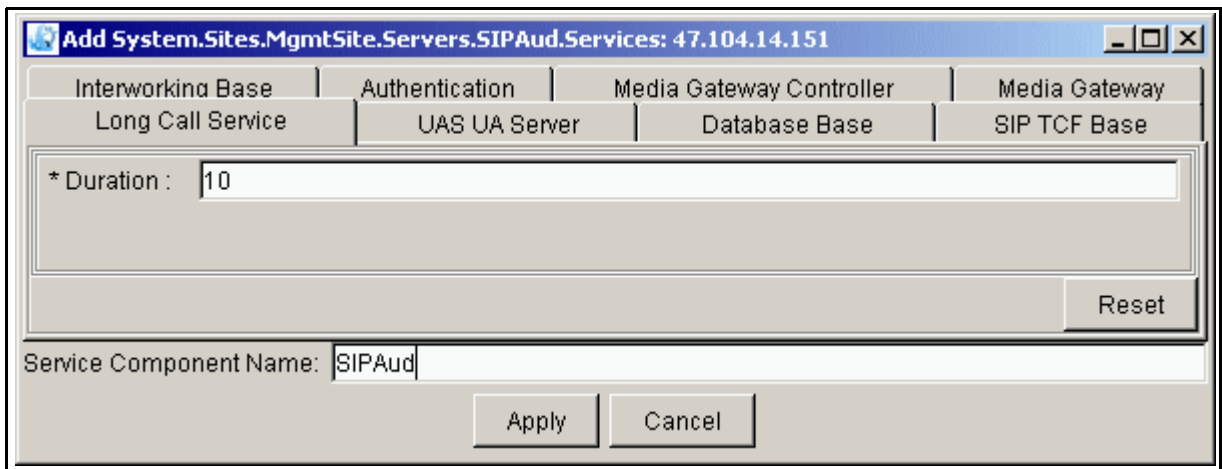
**ATTENTION**  
 DO NOT click on **Apply** until you have FINISHED filling in the fields that you need.

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

#### Completing the Long Call Service tab

Click on the Long Call Service tab and fill in the field as appropriate. This service detects abandoned calls and releases the resources used by such calls.

**Figure 23 The Long Call Service tab**



**Table 4 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.

### Configuring the Media Gateway Controller tab

Click on the Media Gateway tab and fill in the fields as appropriate. This service controls and communicates with the UAS software using an internal protocol. All the configuration that is used during allocation/deallocation of conference sessions is provided here.

**Figure 24 The Media Gateway Controller tab**

**Table 5 Media Gateway Controller tab field descriptions (Sheet 1 of 2)**

Field	Value	Description
Conference Svr. IP Addr	Type=IP address Range=1-15 characters Default=0.0.0.0	This field contains the private IP address of the host CPU of the SIP Audio Server.
Conference Svr. Domain	Type=string Range=1-64 characters Default=domain.com	This field contains the SIP Audio Server 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;audio server IP address&gt;</b> .
Supported Media Types	Type=string Range=audio Default=audio	This is a read-only field.

**Table 5 Media Gateway Controller tab field descriptions (Sheet 2 of 2)**

Field	Value	Description
Default Num of Ports	Type=integer Range=1-32 characters Default=3	This field contains the number of conference ports that are allocated if the SDP does not contain this value in the rtpmap header. Nortel Networks recommends a value of 3 to prevent a waste of resources.
Max Ports Supported	Type=integer Range=1-32 characters Default=32	This field contains the maximum number of conferees in a single conference supported by the SIP Audio Server.

**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 Audio Server processes the request (or message) if it is from an unauthorized (non-trusted) node.

**Figure 25 The Authentication tab fields**
**Table 6 Authentication tab field descriptions (Sheet 1 of 2)**

Field	Value	Description
Methods to Authorize	Type=string Default=blank	This field is not used for the SIP Audio Server.
Realm	Type=string Range=0-256 characters	This field is not used for the SIP Audio Server.
Private Key	Type=string Range=0-256 characters Default=MCP	This field is not used for the SIP Audio Server.
Nonce Interval	Type=integer Range=10000-600000 milliseconds Default=600000	This field is not used for the SIP Audio Server

**Table 6 Authentication tab field descriptions (Sheet 2 of 2)**

Field	Value	Description
Authorized SIP Nodes	Type=IP address Range=0-2000 characters	This field contains a + -delimited list of all the SIP Application Module node IP addresses that send an INVITE to the SIP Audio Server. Use the private IP addresses. This is the list of valid proxies from which the SIP Audio Server 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 this list.
Nodal Auth.	Type=checkbox Default=unchecked	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 Audio Server is one of several components that use the SIP TCF Base. Click on the SIP TCF Base 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.

Figure 26 The SIP TCF Base tabs

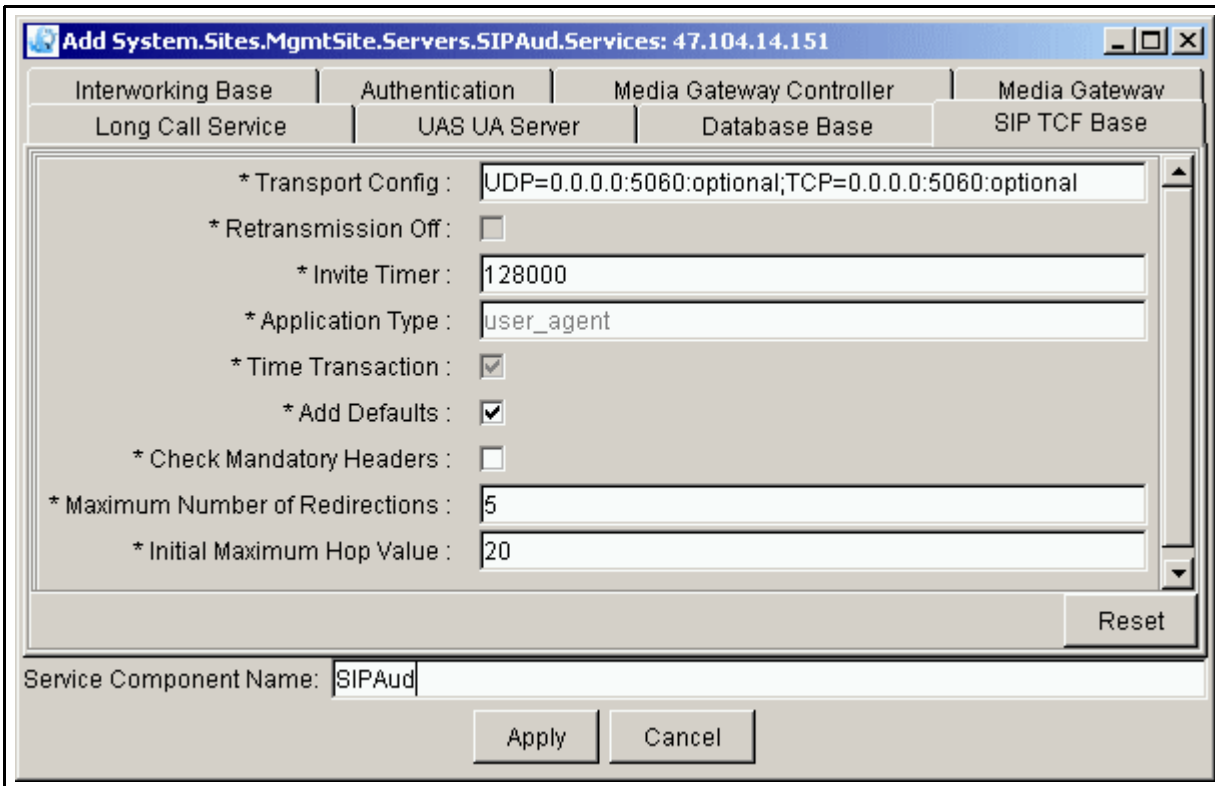


Table 7 SIP TCF Base tab field descriptions (Sheet 1 of 2)

Field	Value	Description
Transport Config	Type=string Default=UDP=0.0.0.0:5060:optional;TCP=0.0.0.0:5060:optional	This field opens the interfaces for the SIP connections and tells which network interfaces and port on which to listen for SIP messages. Transports can appear more than once. Replace 0.0.0.0 with the private IP Address of the SIP Audio Server.
Retransmission Off	Type=checkbox Default=unchecked (false)	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 7 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 is a read-only field.
Time Transaction	Type=checkbox Default=checked (true)	This is a read-only field.
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 Default=5	This is the maximum number of redirections allowed before the SIP Audio Server drops the request.
Initial Maximum Hop Value	Type=integer Range=5-50 Default=20	This is the maximum number of hops allowed before the SIP Audio Server drops the request.

**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 27 The Media Gateway tab, General subfield, left side**

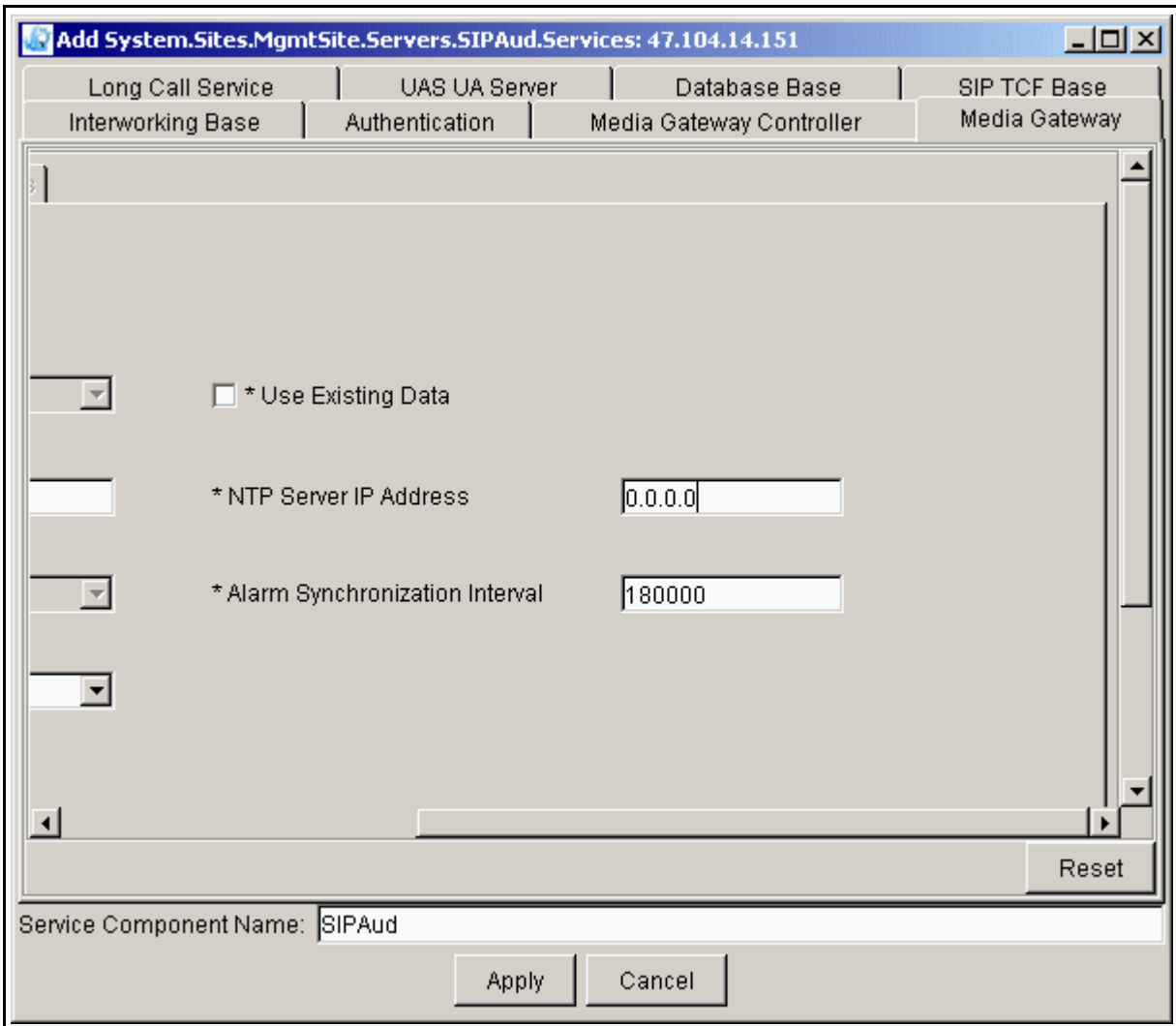
The screenshot shows a configuration window titled "Add System.Sites.MgmtSite.Servers.SIPAud.Services: 47.104.14.151". The window has a tabbed interface with the following tabs: Long Call Service, UAS UA Server, Database Base, SIP TCF Base, Interworking Base, Authentication, Media Gateway Controller, and Media Gateway. The "Media Gateway" tab is active, and within it, the "General" subfield is selected. The "General" subfield contains the following fields and controls:

- \* Host Card Type: A dropdown menu with the value "5370".
- \* RTP Base Port: A text input field with the value "30000".
- \* Toneset: A dropdown menu with the value "France".
- \* Slot Number: A dropdown menu with a list of values: "9", "7", and "9". The value "9" is currently selected.
- \* Use Existing Data: A checkbox that is currently unchecked.
- \* NTP Server IP Address: A text input field.
- \* Alarm Synchronization Interval: A text input field.

At the bottom right of the "General" subfield, there is a "Reset" button. Below the "General" subfield, there is a "Service Component Name" field with the value "SIPAud". At the bottom of the window, there are "Apply" and "Cancel" buttons.



**Figure 28 The Media Gateway tab, General subfield, right side**



**Table 8 Media Gateway tab, General subfield descriptions (Sheet 1 of 2)**

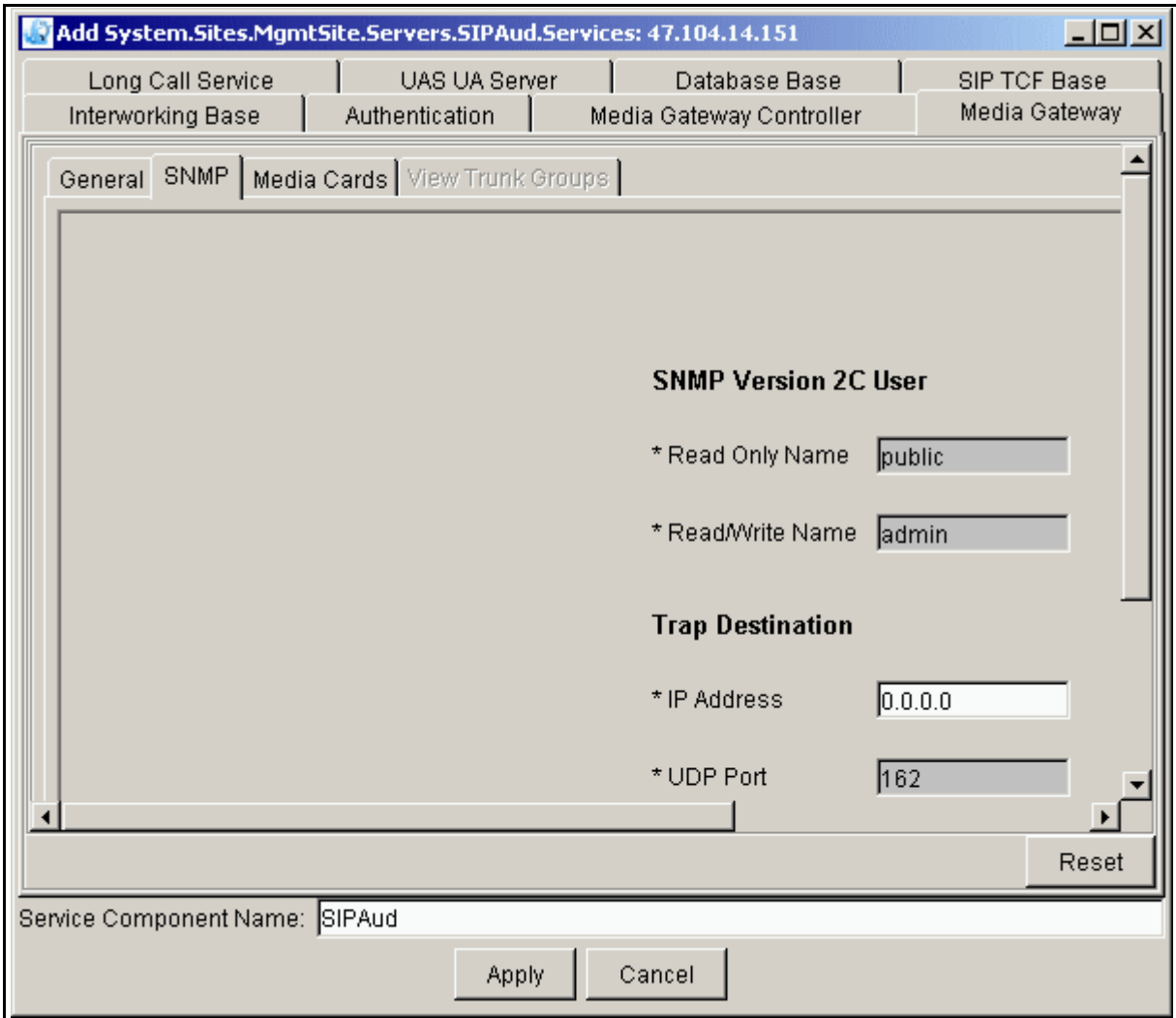
Field	Value	Description
Host Card Type	Type=dropdown menu Range=5370 Default= 5370	This read-only field contains the host card type.
RTP Base Port	Type=string Range=1024-63094 characters Default=30000	This field contains the base number of ports for the RTP stream. Nortel Networks recommends that you use the default.

**Table 8 Media Gateway tab, General subfield descriptions (Sheet 2 of 2)**

Field	Value	Description
Toneset	Type=string	This field is not used for the SIP Audio Server.
Slot Number	Type=integer Range=7, 9 Default=9	Physical slot on which the CPV5370 host card is installed. Slot number 7 is for the left half of the chassis, and 9 is for the right half.
Use Existing Data	Type=checkbox Default=unchecked	If checked, the software uses the existing configuration data on the SIP Audio Server. If unchecked, the existing data is not used. Nortel Networks recommends that this be checked when you do an update so that you can reuse the UAS configuration data that was already deployed.
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=30000-600000 milliseconds Default=180000	Time interval in milliseconds after which alarms from the UAS will be retrieved. The software queries the UAS active alarm summary table for alarms raised by the UAS software and Global Server. If this is 60000, the software queries after every minute.

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

**Figure 29 The Media Gateway, SNMP sub-tab**



**Table 9 Media Gateway, SNMP sub-tab field descriptions**

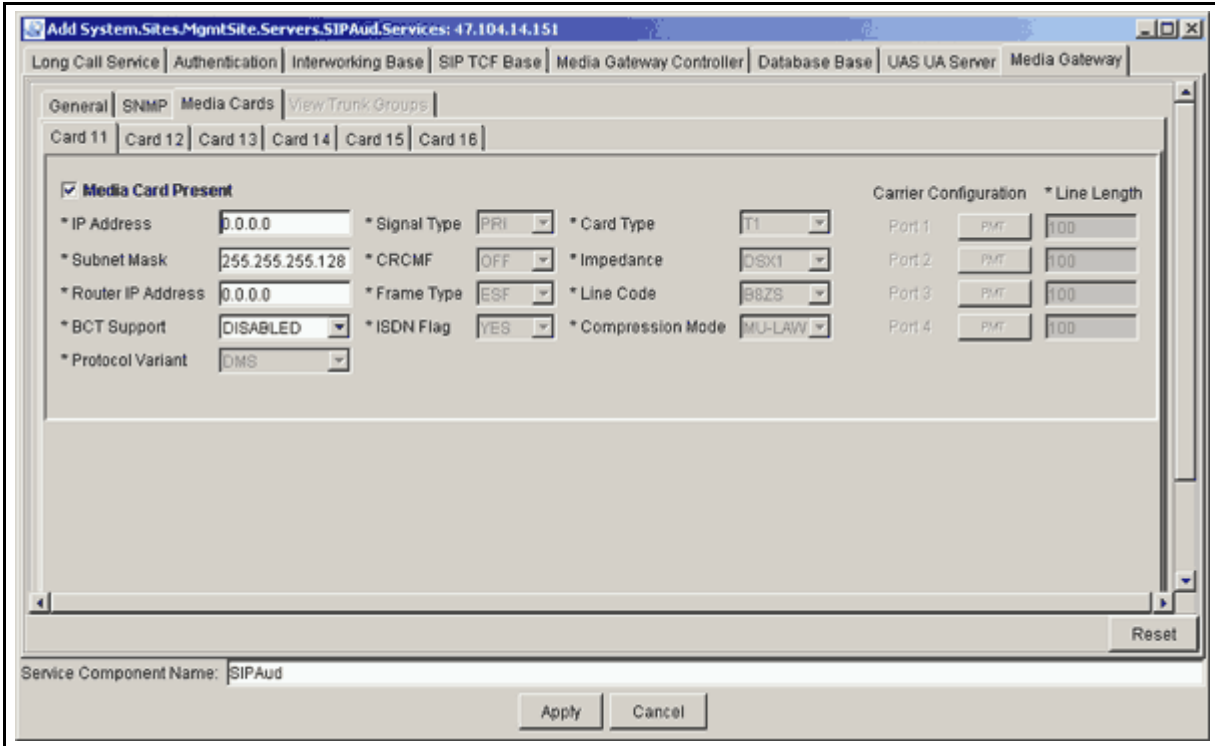
Field	Value	Description
Read Only Name	Type=string Default=public	This is a read-only field.
Read/Write Name	Type=string Default=admin	This is a read-only field.

**Table 9 Media Gateway, SNMP sub-tab field descriptions**

Field	Value	Description
IP Address	Type=IP address Range=1-15 characters Default=0.0.0.0	This field contains the private IP address of the SIP Audio Server to which the software sends all the SNMP traps containing alarms and logs
UDP Port	Type=integer Default=162	This read-only field indicates that SNMP traps will be sent to Port 162.

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

**Figure 30** The Media Gateway, Media Cards sub-tab, left side



**Table 10** Media Gateway, Media Cards sub-tab field descriptions (Sheet 1 of 2)

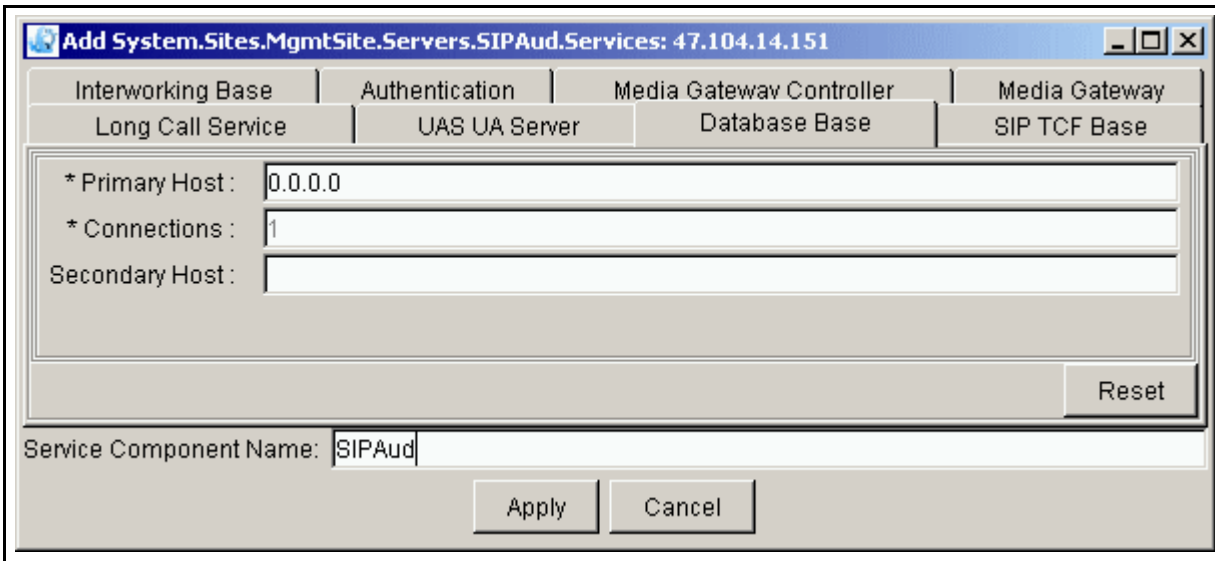
Field	Value	Description
Media Card Present	Type=checkbox Default=unchecked	Check this box only if a media card is installed in any of these slots (Card 11, 12, and so on, in the example shown in Figure 30).
IP Address	Type=IP address Range=7-15 characters Default=0.0.0.0	This field contains the IP address of this particular media card.
Subnet Mask	Type=IP address Range=7-15 characters Default=255.255.255.128	This field contains the subnet mask associated with the card.
Router IP Address	Type=IP address Default=0.0.0.0	This field contains the router associated with the card.

**Table 10 Media Gateway, Media Cards sub-tab field descriptions (Sheet 2 of 2)**

Field	Value	Description
BCT Support	Type=pulldown menu Range=DISABLED, ENABLED Default=DISABLED	This read-only field indicates whether bearer channel tandeming is enabled on the card.
Protocol Variant	Type=pulldown menu Default=DMS	This field is not used for the SIP Audio Server.
Signal Type	Type=pulldown menu Default=PRI	This field is not used for the SIP Audio Server.
CRCMF	Type=pulldown menu Default=OFF	This field is not used for the SIP Audio Server.
Frame Type	Type=pulldown menu Default=ESF	This field is not used for the SIP Audio Server.
ISDN Flag	Type=pulldown menu Default=YES	This field is not used for the SIP Audio Server.
Card Type	Type=pulldown menu Default=T1	This field is not used for the SIP Audio Server.
Impedance	Type=pulldown menu Default=DSX1	This field is not used for the SIP Audio Server.
Line Code	Type=pulldown menu Default=B8ZS	This field is not used for the SIP Audio Server.
Compression Mode	Type=pulldown menu Default=MU-LAW	This field is not used for the SIP Audio Server.

### Configuring the Database Base tab

General properties for the SIP Audio Server's connection to the database are defined in the Database Base tab. The SIP Audio Server software uses this tab to maintain all the database information pertaining to conference sessions, such as conference tokens, information about clients in each session, and resources used by each session.

**Figure 31 The Database Base tab**

The screenshot shows a configuration window titled "Add System.Sites.MgmtSite.Servers.SIPAud.Services: 47.104.14.151". The window has a tabbed interface with the following tabs: Interworking Base, Authentication, Media Gateway Controller, Media Gateway, Long Call Service, UAS UA Server, Database Base (selected), and SIP TCF Base. The "Database Base" tab is active and contains the following fields:

- \* Primary Host : 0.0.0.0
- \* Connections : 1
- Secondary Host : (empty)

At the bottom right of the tab is a "Reset" button. Below the tabbed area is a "Service Component Name:" field containing "SIPAud". At the very bottom are "Apply" and "Cancel" buttons.

**Note:** See the *MCP Database Module Basics* for more information about the Database Base tab and for field descriptions.

#### **Configuring the UAS UA Server tab**

Click on the UAS UA Server tab and fill in the fields as appropriate. The SIP Audio Server software uses this tab when originating requests (sending an INVITE message) to other clients, for example, when one of the legs transfers to another party.

**Figure 32 Configuring the UAS UA Server tab**

The screenshot shows a configuration window titled "Add System.Sites.MgmtSite.Servers.SIPAud.Services: 47.104.14.151". It has four tabs: "Interworking Base", "Authentication", "Media Gateway Controller", and "Media Gateway". The "Authentication" tab is active, showing the "UAS UA Server" configuration. Below the tabs are four input fields:
 

- \* Conference User Name : conference
- \* Application Server : 0.0.0.0:5060
- \* Default Conference Domain : domain.com
- \* Register TTL : 12

 A "Reset" button is located at the bottom right of the input fields. Below the fields is a "Service Component Name" field containing "SIPAud". At the very bottom are "Apply" and "Cancel" buttons.

**Table 11 UAS UA Server tab field descriptions**

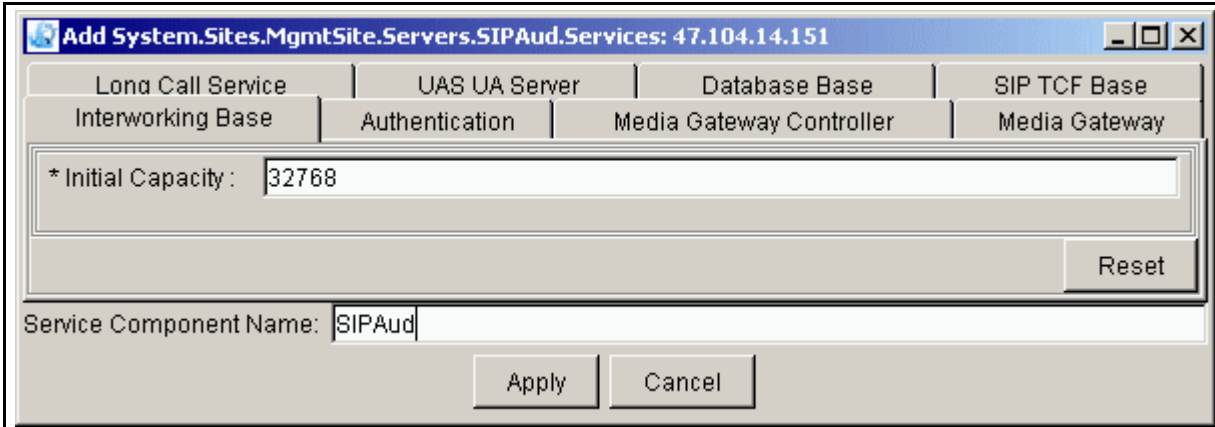
Field	Value	Description
Conference User Name	Type=string Range=1-24 characters Default=conference	Leave the default.
Application Server	Type=IP address Range=12-21 characters Default=0.0.0.0:5060	Private IP address and port of the SIP Application Module. This is used for SIP messaging.
Default Conference Domain	Type=string Range=1-64 characters Default=domain.com	This field is not used.
Register TTL	Type=integer Range=12 Default=12	This is a read-only field.



### Configuring the Interworking Base tab

This tab contains engineering parameters and cannot be changed.

**Figure 33 Interworking Base tab dialog box**



#### Deployment failure

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

## Changing SIP Audio Server configuration

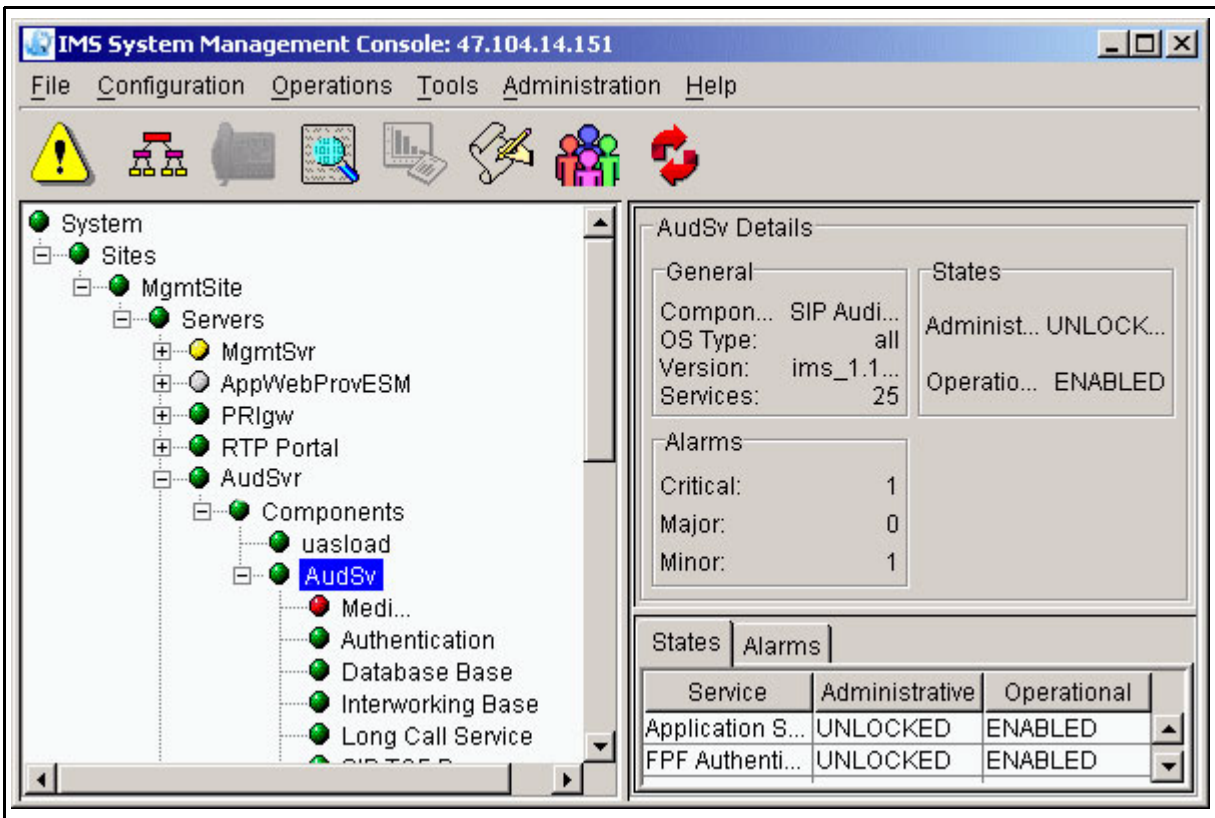
### ATTENTION

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

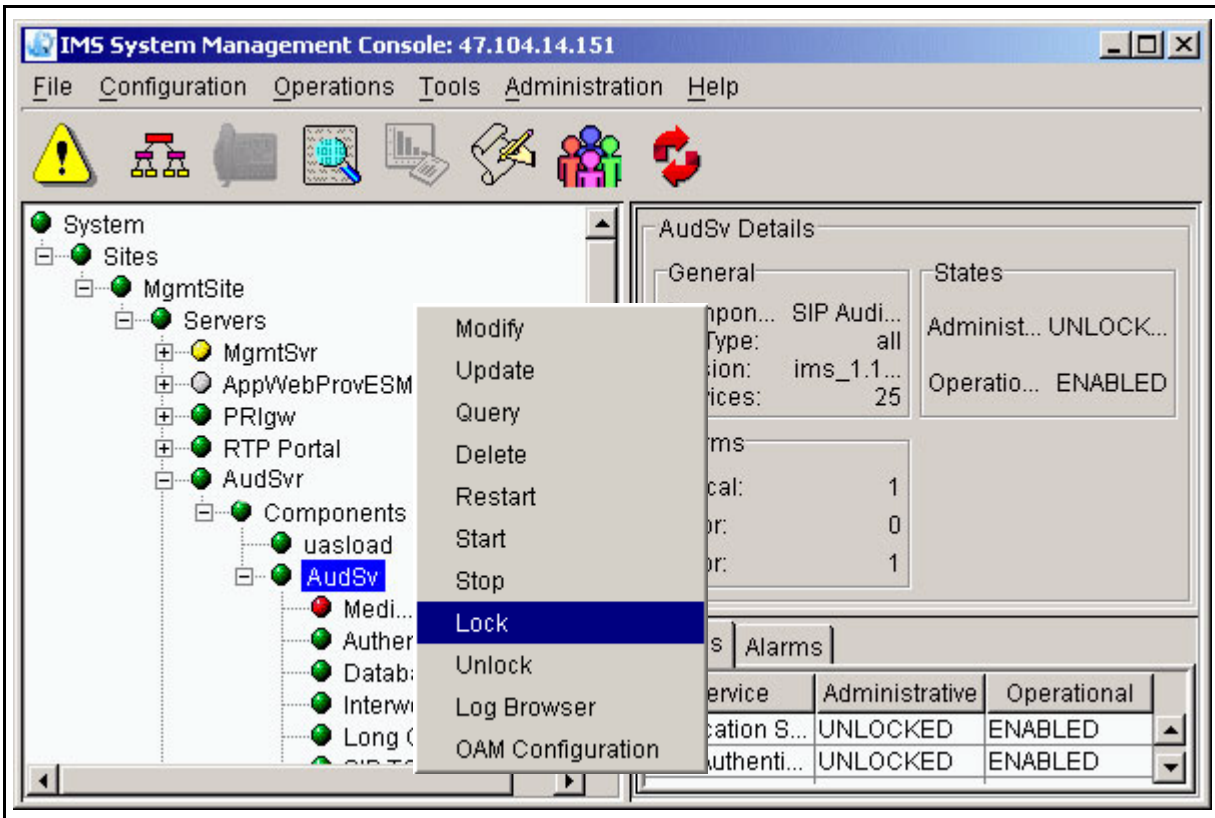
### at the System Management Console

- 1 Navigate through the system hierarchy tree located in the left panel as shown.

Figure 34 Navigation path

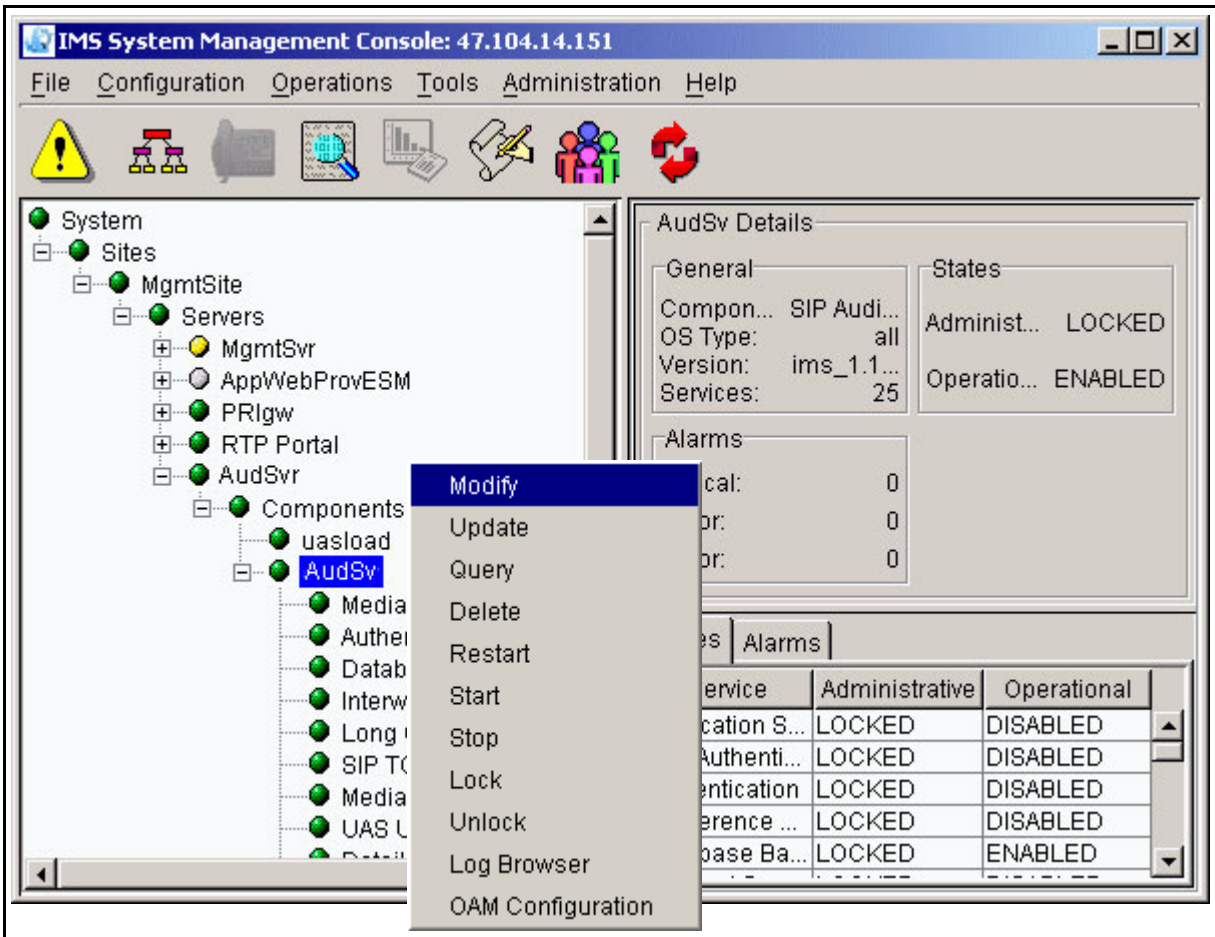


- 2 Right-click on the SIP Audio Server bullet (**AudSv**, in the example).
- 3 Select **Lock** in the pop-up menu that appears.

**Figure 35 Locking the component**

- 4 Right-click on the SIP Audio Server bullet again.
- 5 Select **Modify**, as shown.

Figure 36 Modify menu



The tabs appear.

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

#### ATTENTION

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



## Accounting management

The SIP Audio Server does not do any accounting management. For more information on accounting, please see the *MCP Accounting Module Basics*.





---

## Performance management

---

See the *MCP System Management Console Basics* for more information about performance management on the SIP Audio Server.







# Security and Administration

## How this chapter is organized

This chapter is organized as follows:

- “Security” on page 73
- “Administration” on page 73

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

## Security

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

## Administration

The procedures in this section are organized as follows:

- “Finding help text” on page 74
- “Stopping the SIP Audio Server” on page 74
- “Performing a query” on page 75
- “Restarting a SIP Audio Server” on page 77
- “Accessing the Maintenance window” on page 78
- “Locking and unlocking a SIP Audio Server” on page 83
- “Maintaining the SIP Audio Server node” on page 84
- “Locking or unlocking an interface card (CG6000)” on page 85
- “Performing maintenance on the CG6000 card” on page 86
  - “Adding a CG6000 card” on page 87
  - “Removing a CG6000 card” on page 87
  - “Changing CG6000 card parameters” on page 88

- “Changing the SIP Audio Server administrative state” on page 89
- “Rebooting a peer host card” on page 89
- “Performing maintenance on the Chassis” on page 90
- “Performing maintenance on the SNMP configuration” on page 96

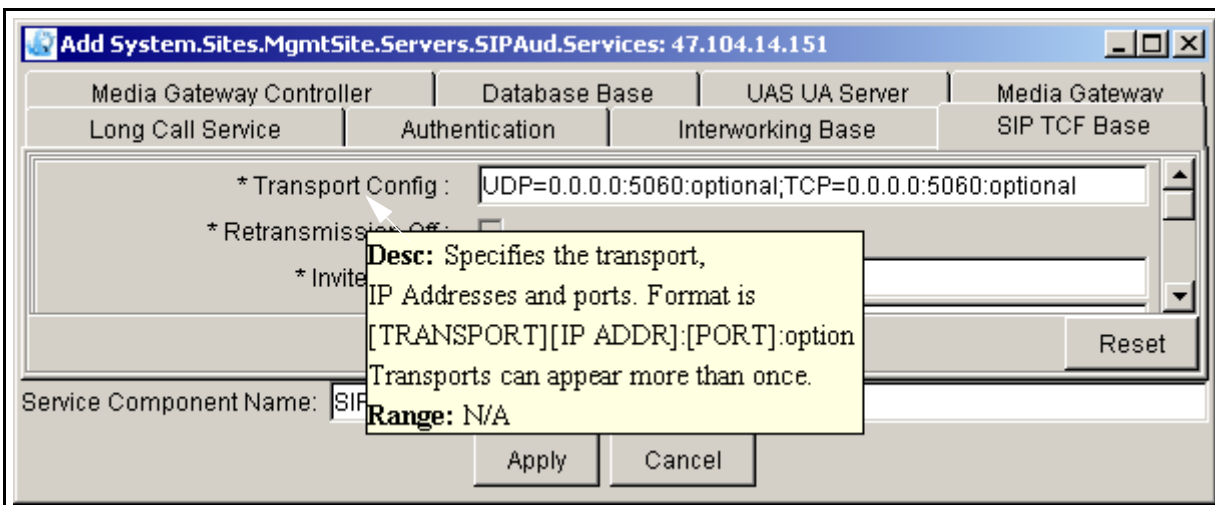
### Procedure 13 Finding help text

#### 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

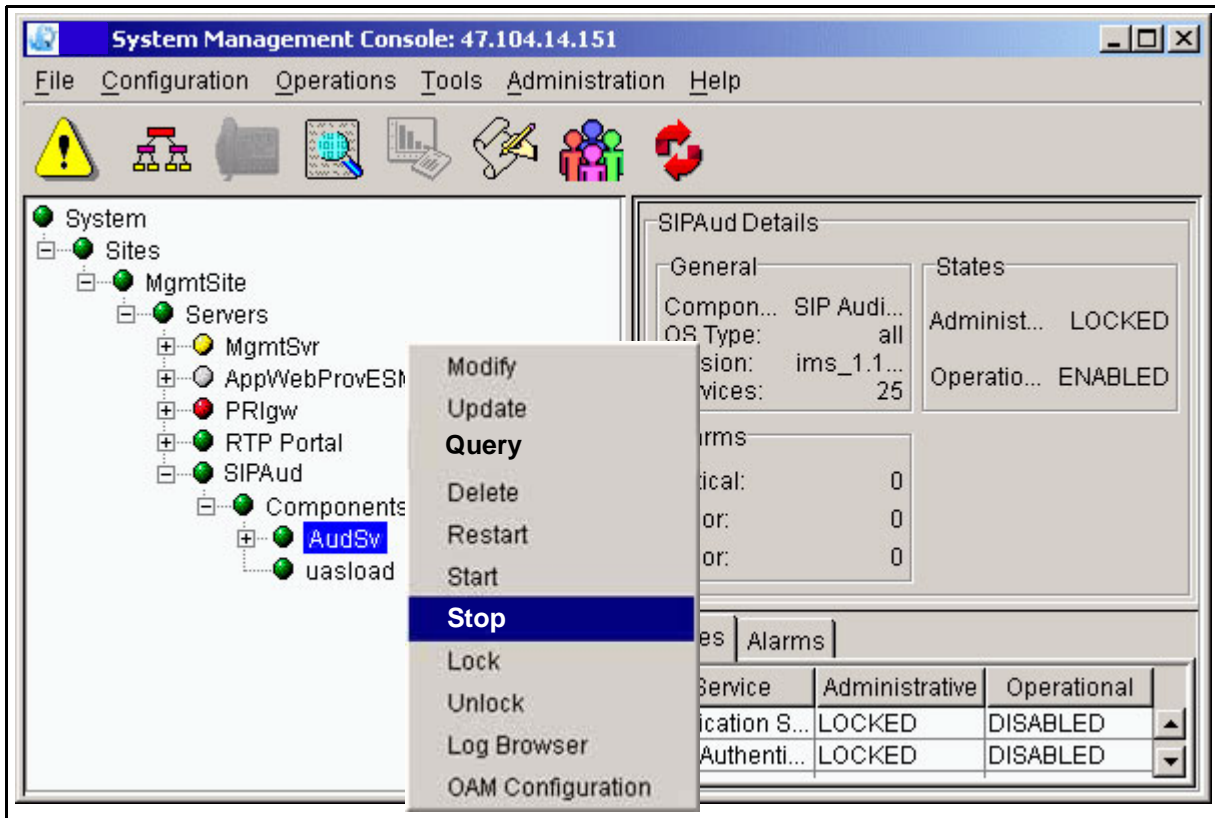


### Stopping the SIP Audio Server

#### At the System Management Console

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, Servers, SIP Audio Server (the name assigned to the SIP Audio Server during deployment, **SIPAud** in the example), and Components bullets, to the SIP Audio Server bullet (the name assigned to the SIP Audio Server load during deployment, **AudSv** in the example). Right-click the SIP Audio Server bullet. Select **Stop** from the pop-up menu. The SIP Audio Server applications stop.

Figure 2 Stopping the SIP Audio Server

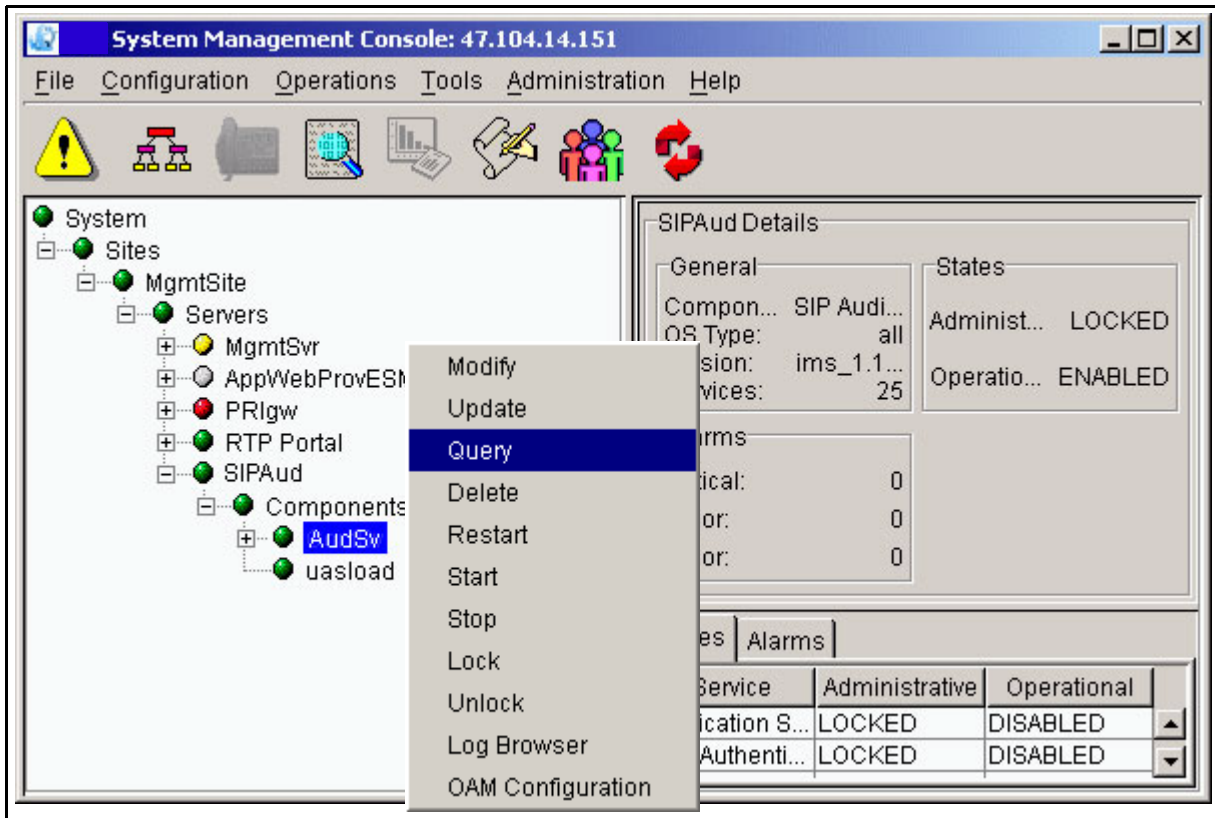


### Performing a query

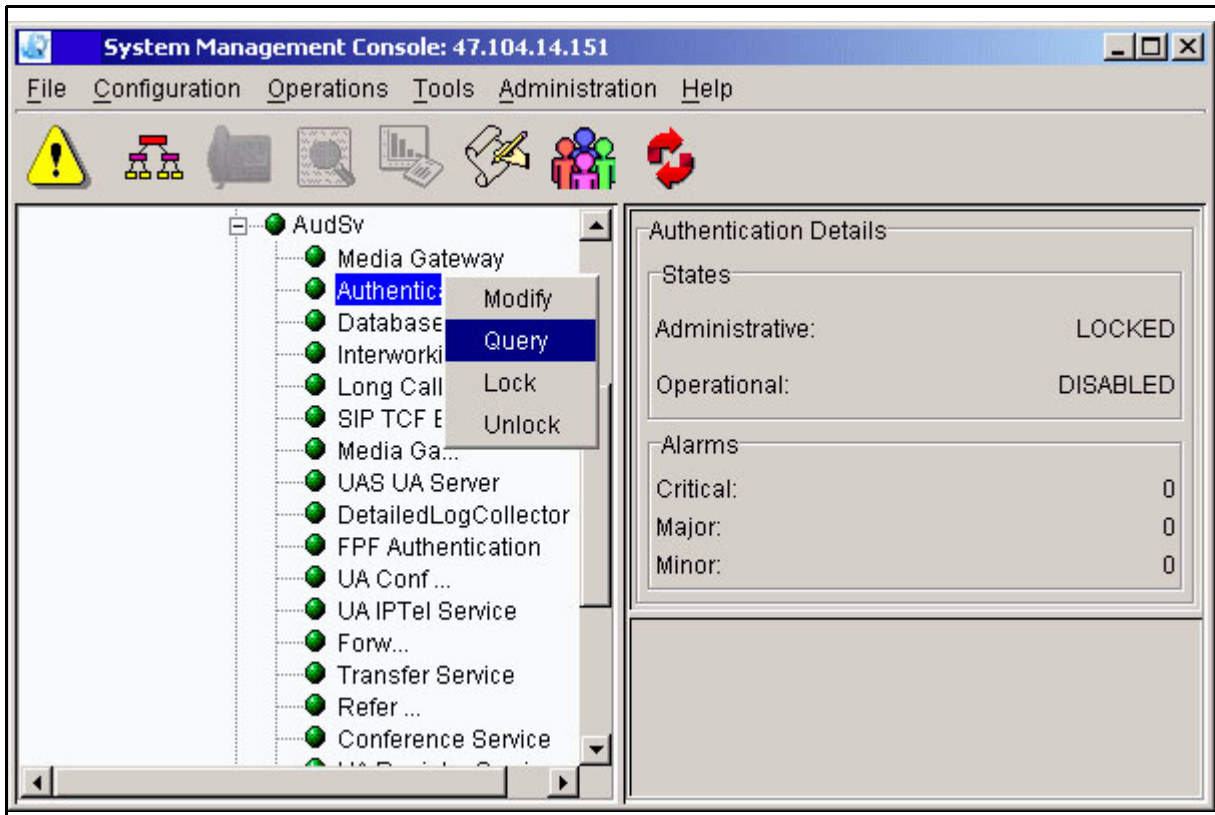
#### *At the System Management Console*

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, Servers, SIP Audio Server (the name assigned to the SIP Audio Server during deployment, **SIPAud** in the example), and Components bullets, to the SIP Audio Server bullet (the name assigned to the SIP Audio Server load during deployment, **AudSv** in the example). Right-click the SIP Audio Server bullet. Select **Query** from the pop-up menu. The tabs will appear.

**Figure 3 Performing a query of the SIP Audio Server component**



As an alternative you can also open the list of services and query the individual tabs. You will be able to see the status of each service in the right-hand panel.

**Figure 4 Performing a query, by tab**

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

### Restarting a SIP Audio Server

#### *At the System Management Console*

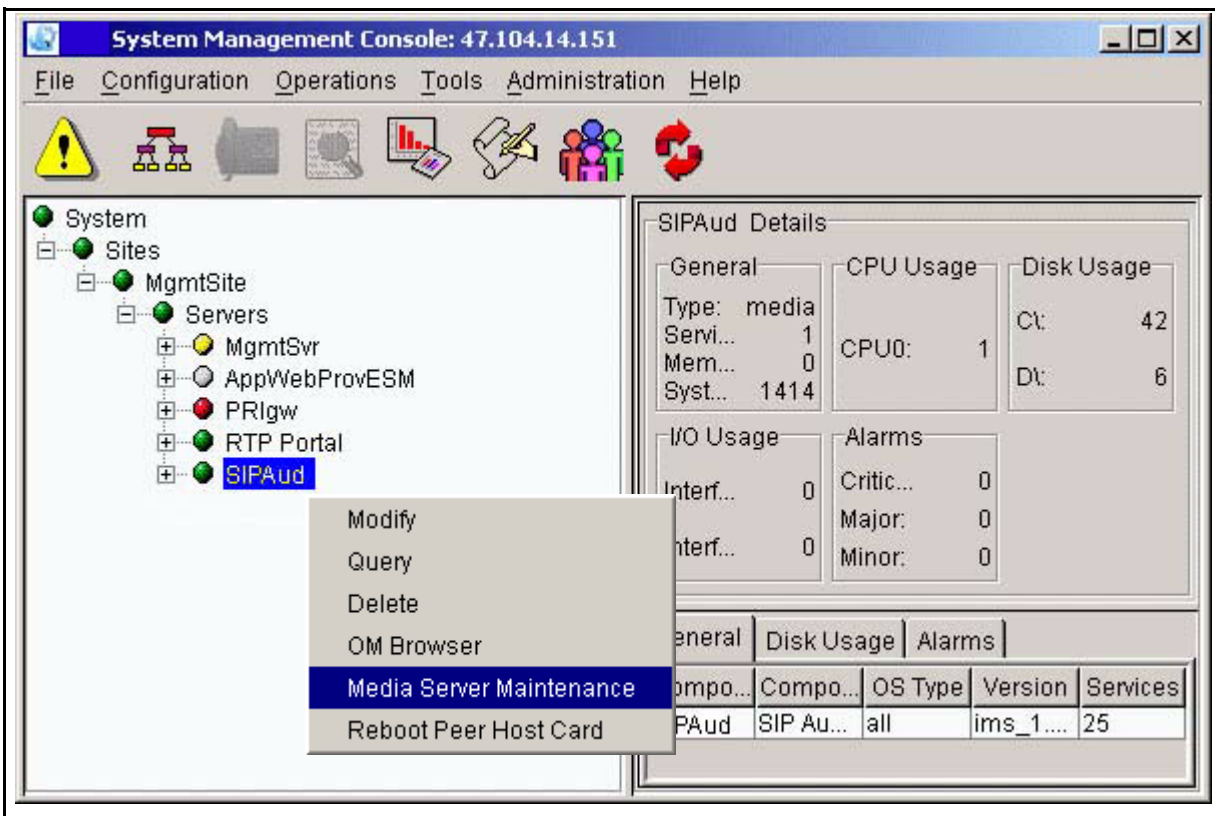
- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP Audio Server bullet (the name assigned to the SIP Audio Server during deployment).
- 2 Right-click on the SIP Audio Server bullet (**SIPAud**, in the example).
- 3 Select **Restart** from the pop-up menu.
- 4 Click **Yes** in the confirmation window that appears.
- 5 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 5, "Finding the Media Server Maintenance GUI." Right-click on the SIP Audio Server bullet (**SIPAud**, in the example). The names that appear in the hierarchy are defined at deployment.

**Figure 5 Finding the Media Server Maintenance GUI**



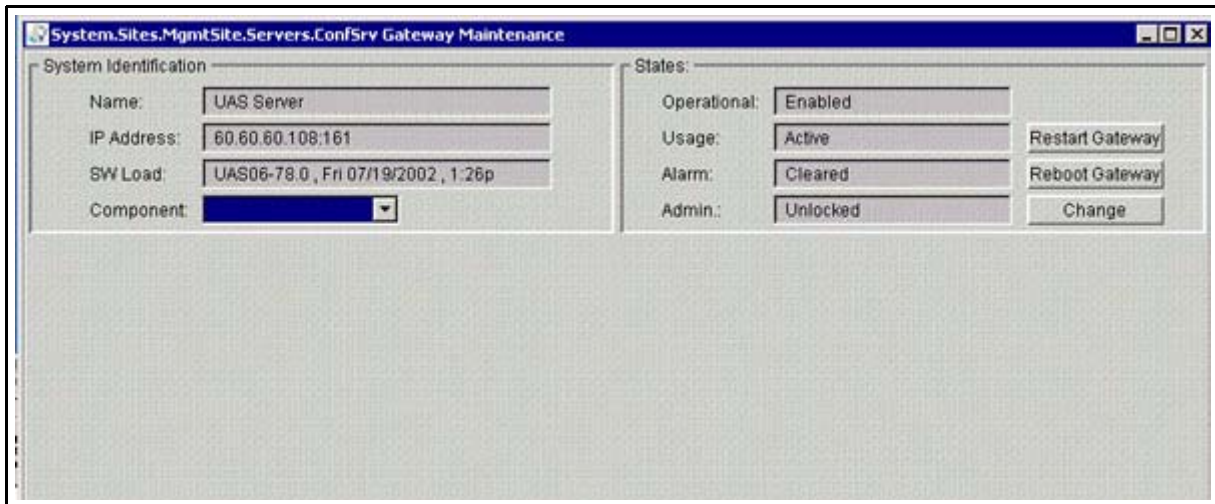
- 2 Select **Media Server Maintenance**.

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

- The *System Identification* panel of the main maintenance window provides basic identification information for the SIP Audio Server, 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 Audio Server, and contains buttons used for

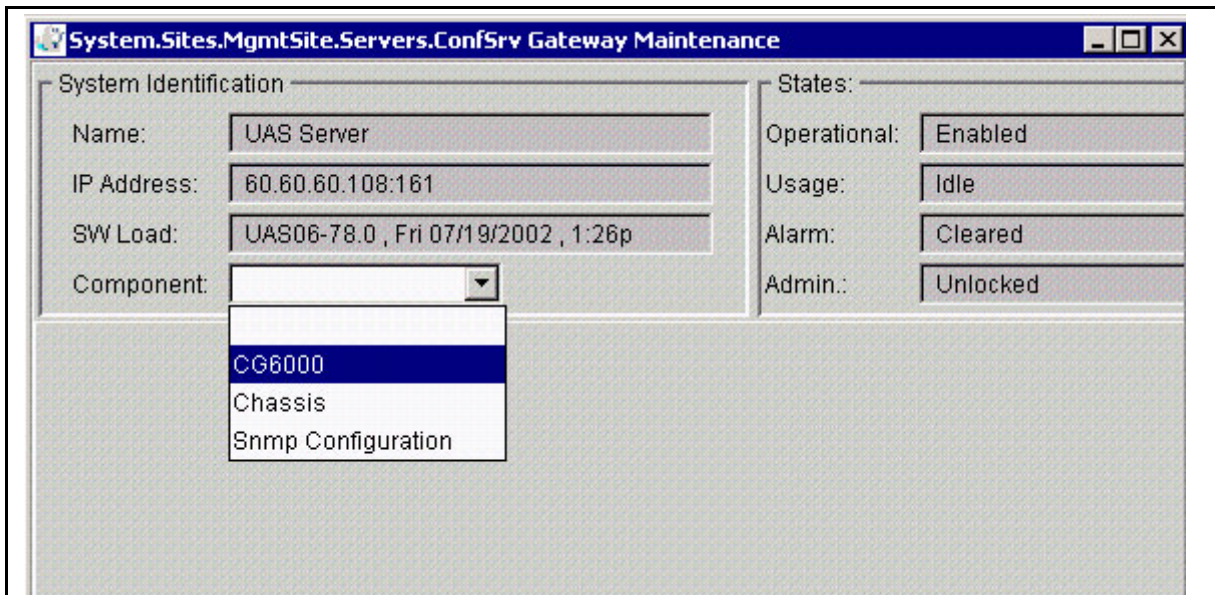
restarting SIP Audio Server processes, for rebooting the unit, or for changing the administrative state of the unit to either locked or unlocked.

**Figure 6 Opening the Maintenance screen**



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

**Figure 7 Selecting from the 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 Audio Server. The screen displayed when you select the **Performance** tab shows performance information for the CG6000c cards.

**Figure 8 Selecting CG6000 from the pulldown menu, General tab**

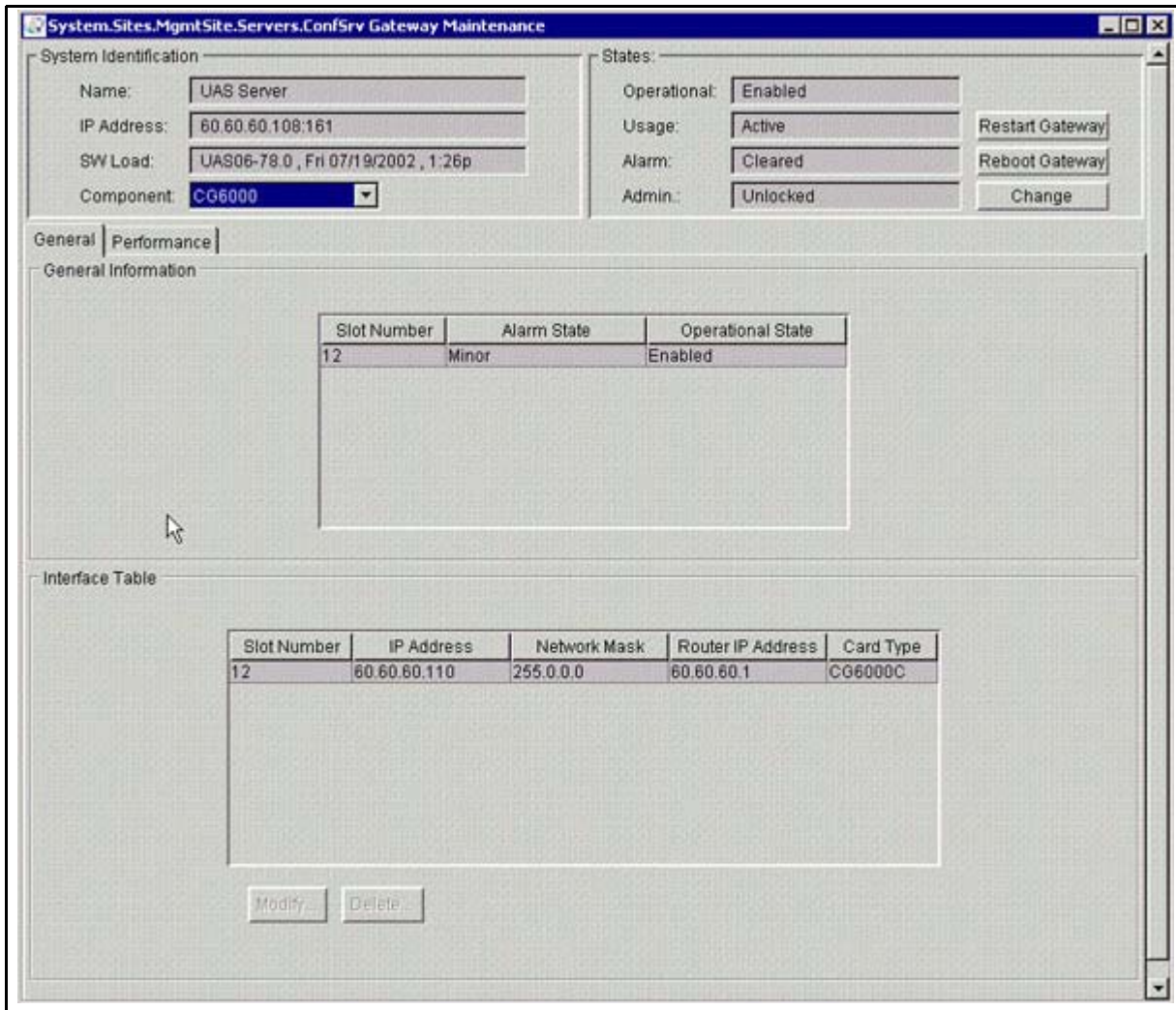
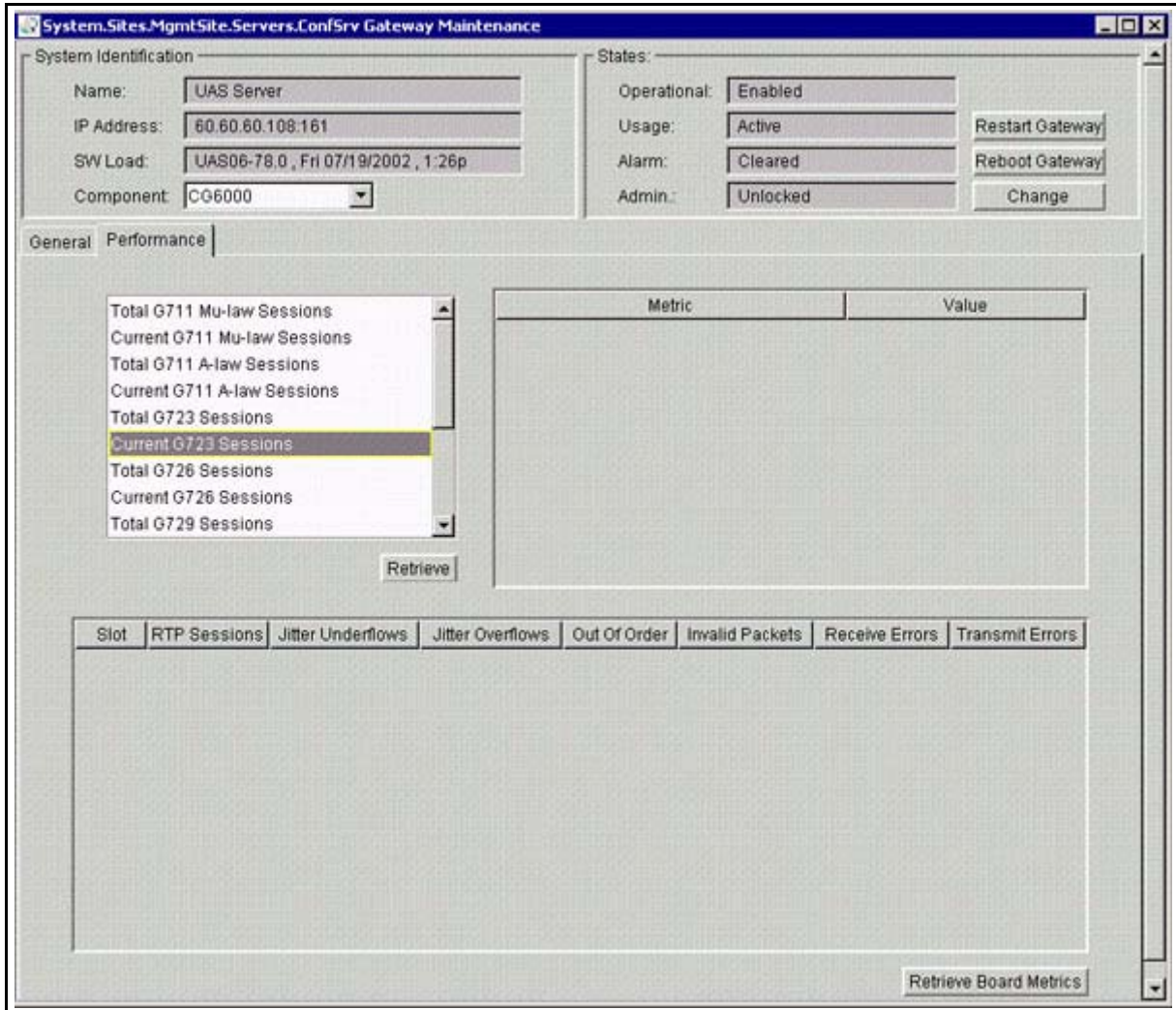


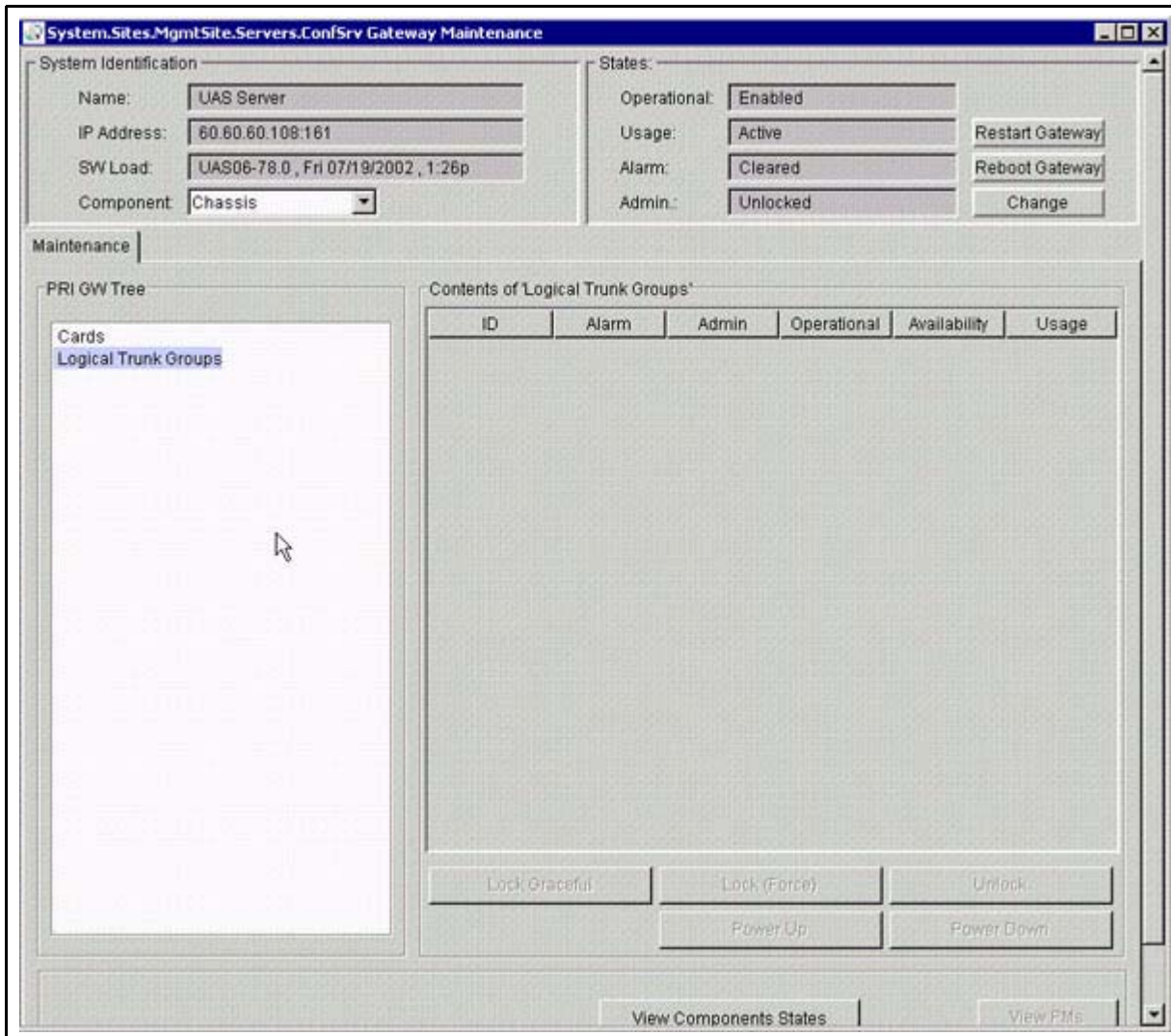


Figure 9 Selecting CG6000 from the pulldown menu, Performance tab



When you select **Chassis** in the **Component** pull-down menu, a Maintenance screen appears, as shown.

Figure 10 Selecting Chassis from the pulldown menu



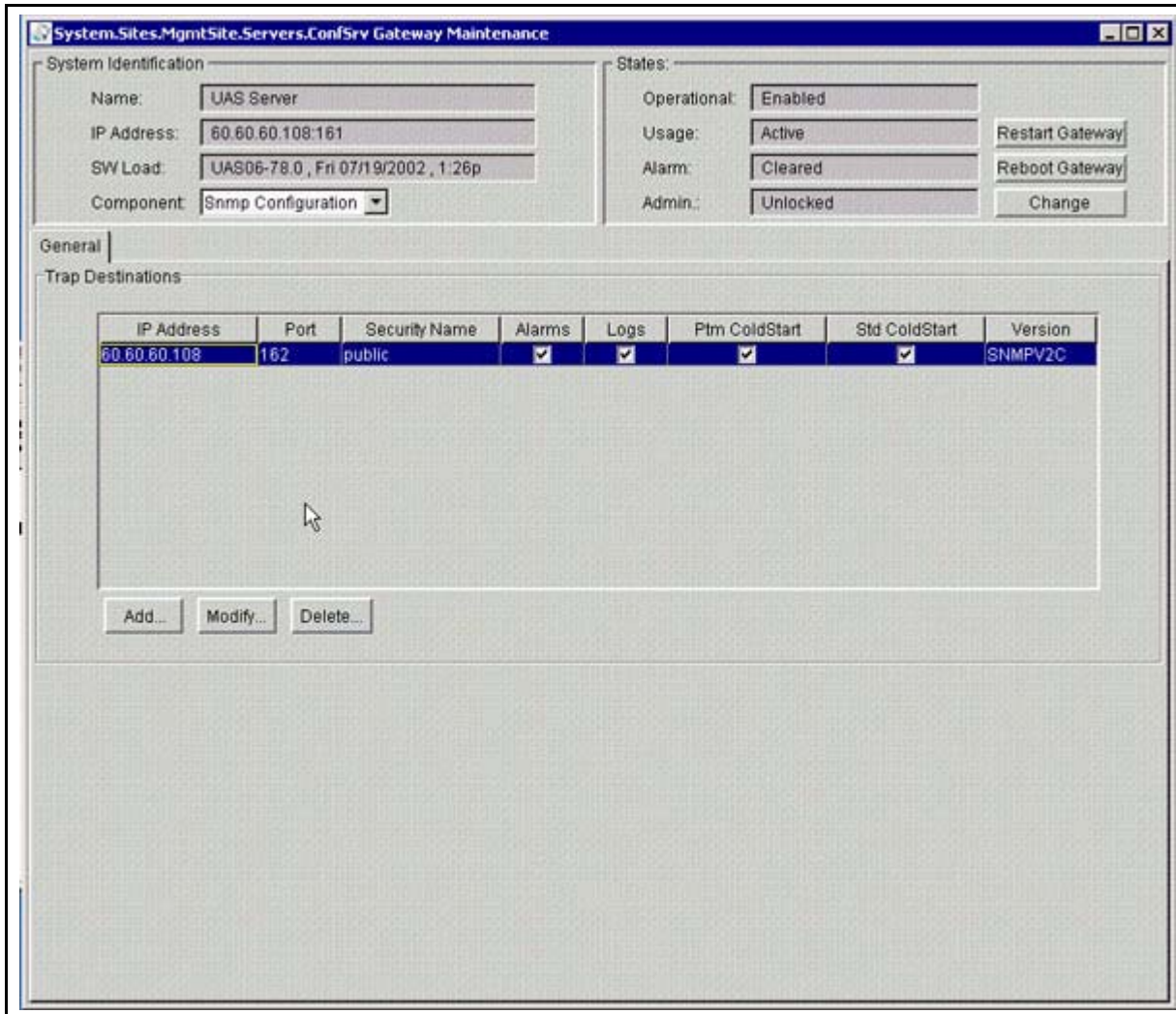
This screen is used for maintenance activities performed on SIP Audio Server CG6000c cards. The following panels appear:

- The PRI GW Tree panel provides you with access to the individual CG6000c cards. The Logical Trunk Groups option is not used for conferencing.
- The Contents panel provides a detailed listing of the cards, 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 Audio Server.

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 Audio Server.

**Figure 11 Selecting Snmp Configuration from the pulldown menu**



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

**Locking and unlocking a SIP Audio Server**

This procedure enables you to place the SIP Audio Server either in unlocked (in service) state or in locked (out of service) state. When a SIP Audio Server is locked, its applications continue to run, but it does

not receive any new requests. This procedure is normally used during SIP Audio Server administrative activities.

### ***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 Audio Server bullet (the name assigned to the SIP Audio Server during deployment).
- 2 Right-click on the SIP Audio Server bullet.
- 3 If you want to lock the server, select **Lock** in the pull-down menu that appears.  
  
If you want to unlock the server, select **Unlock** in the pull-down menu that appears.
- 4 You have completed this procedure.

### **Maintaining the SIP Audio Server node**

The following basic maintenance operations are performed on a SIP Audio Server node either through the System Management Console or through a command line interface:

- **lock force** - administratively locks the SIP Audio Server node immediately, which causes all active calls associated with the node to be dropped immediately
- **lock graceful** - administratively locks the SIP Audio Server node after stable calls using the node have been completed and no more calls are accepted. This option is not available.
- **unlock** - returns the SIP Audio Server node to service if no other conditions exist that prevent it from coming back into service
- **reboot** - reboots the SIP Audio Server hardware
- **restart** - restarts the SIP Audio Server software

Maintenance operations affect the maintenance state associated with the SIP Audio Server 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

### Locking or unlocking an interface card (CG6000)

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.

#### CG6000 interface card maintenance

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.

**Note:** Interface cards cannot be locked gracefully.

- **unlock** - returns the CG6000 card to service if no other conditions exist that prevent it from coming back into service

### Locking or unlocking an interface card

#### At the System Management Console

- 1 Navigate to the Maintenance window as shown in “Accessing the Maintenance window” on page 78.
- 2 In the PRI GW Tree panel, click the **Cards** button.

The Contents panel is populated with entries for the cards configured in the system.

- |           | <b>Do</b>                         |
|-----------|-----------------------------------|
| <b>If</b> | you want to lock or unlock a card |
|           | step 3 through 4                  |
- 3** In the Contents panel, click on the row associated with the card to be locked or unlocked.

The row highlights and, if the card is powered up, the appropriate **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.

### Performing maintenance on the CG6000 card

These procedures enable you either to delete a CG6000 card, to add a new CG6000 card, or to remove a CG6000 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 SAM16 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.

## Procedure 14 Adding a CG6000 card

### *At the System Management Console*

- 1 Navigate through the file system tree located in the left panel, by expanding the Sites, MgmtSite, Servers, SIP Audio Server (the name assigned either the SIP Audio Server during installation, **SIPAud** in the examples), and Components bullets, to the SIP Audio Server (**AudSv** in the examples) load bullet.

**Note:** **AudSv** represents a name that has been assigned to the component software bundle loads. The name may or may not be the actual name of the load that you see.

- 2 Right-click on the **AudSv** load bullet.
- 3 Select **Lock** in the menu that appears.
- 4 Right-click on the **AudSv** load bullet.
- 5 Right-click on the **AudSv** button.
- 6 Select **Modify**.
- 7 Select the **Media Gateway** tab.
- 8 A **Modify** window for Media Cards appears. Bring up the **Media Cards** subtab.
- 9 Click the **Media Card Present** checkbox.  
The media card fields become active, displaying default media card values.
- 10 Change the media card fields in the tab window that appears, as needed.
- 11 Click **Apply**, located at the bottom of the card tab window, to effect the changes you have made.
- 12 Restart the SIP Audio Server hardware.

## Procedure 15 Removing a CG6000 card

### *At the System Management Console*

- 1 Navigate through the file system tree located in the left panel, by expanding the Sites, MgmtSite, Servers, SIP Audio Server (the name assigned either the SIP Audio Server during installation, **SIPAud** in the examples), and Components bullets, to the SIP Audio Server (**AudSv** in the examples) load bullet.

**Note:** **AudSv** represents a name that has been assigned to the component software bundle loads. The name may or may not be the actual name of the load that you see.

- 2 Right-click on the **AudSv** load bullet.
- 3 Select **Lock** in the menu that appears.
- 4 Right-click on the **AudSv** load bullet.
- 5 Right-click on the **AudSv** button.
- 6 Select **Modify**.
- 7 Select the **Media Gateway** tab.
- 8 A **Modify** window for Media Cards appears. Bring up the **Media Cards** subtab.
- 9 Un-click the **Media Card Present** checkbox for the card you are removing.
- 10 Click **Apply**, located at the bottom of the card tab window, to effect the changes you have made.
- 11 Restart the SIP Audio Server hardware.

#### **Procedure 16 Changing CG6000 card parameters**

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

- 1 Navigate through the file system tree located in the left panel, by expanding the Sites, MgmtSite, Servers, SIP Audio Server (the name assigned either the SIP Audio Server during installation, **SIPAud** in the examples), and Components bullets, to the SIP Audio Server (**AudSv** in the examples) load bullet.

**Note:** **AudSv** represents a name that has been assigned to the component software bundle loads. The name may or may not be the actual name of the load that you see.

- 2 Right-click on the **AudSv** load bullet.
- 3 Select **Lock** in the menu that appears.
- 4 Right-click on the **AudSv** load bullet.
- 5 Right-click on the **AudSv** button.
- 6 Select **Modify**.
- 7 Select the **Media Gateway** tab.
- 8 A **Modify** window for Media Cards appears. Bring up the **Media Cards** subtab.
- 9 Click the **Media Card Present** checkbox.

The media card fields become active, displaying default media card values.



- 10 Change the media card fields in the tab window that appears, as needed.
- 11 Click **Apply**, located at the bottom of the card tab window, to effect the changes you have made.
- 12 Select **Unlock** in the menu that appears.
- 13 You have completed this procedure.

### **Changing the SIP Audio Server administrative state**

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

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

- 1 Navigate to the Maintenance window as shown in “Accessing the Maintenance window” on page 78.
- 2 When the Maintenance window appears, click on the **Change** button in the States pane.  
A Change [Network Element] Administrative State window appears.
- 3 If you want to
  - unlock the server, select the **Change** radio button,
  - forcefully lock the server, select the **Lock Force** radio button
  - gracefully lock the server, select the **Lock Graceful** radio button
- 4 Then click the **OK** button.
- 5 You have completed this procedure.

### **Rebooting a peer host card**

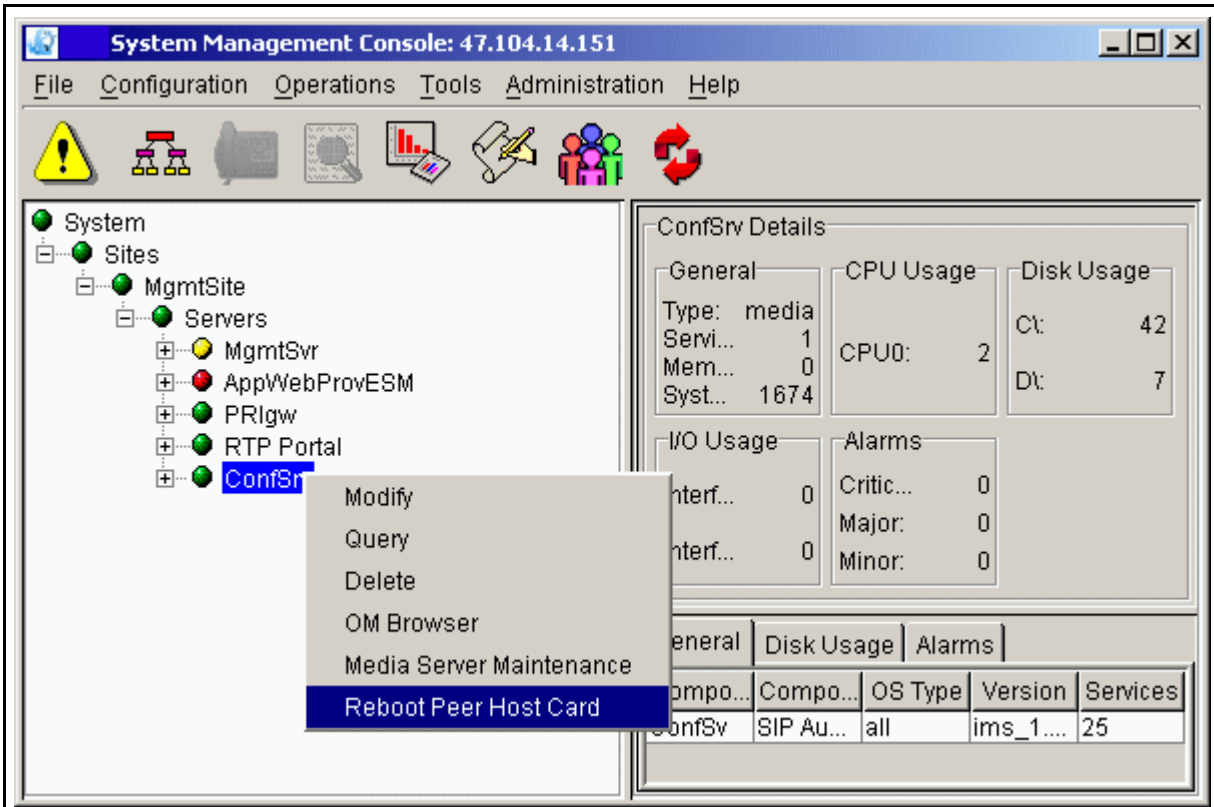
#### ***At the System Management Console***

- 1 Navigate through the system hierarchy tree located in the left panel, by expanding the Sites, MgmtSite, and Servers bullets, to the SIP Audio Server bullet (the name assigned to the SIP Audio Server during deployment).
- 2 Right-click on the SIP Audio Server button (**ConfSrv**, in the example).

- 3 Select **Reboot Peer Host Card** in the menu that appears.

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

**Figure 12 Selecting Reboot Peer Host Card**



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

## 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.

The “PRI GW Tree” panel provides you with access to the individual CG6000c cards.

The “Contents” panel provides a detailed listing of the cards, as well as access to buttons that enable you to perform actions, such as administratively locking or unlocking, on these entities.

- 2 Select an item, then click on the **View Components States** button. 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 shows a separate row of information for each component, including the

- latest alarm state (cleared, critical, major, minor, or warning)
- administrative state (unlocked, locked, or shutting down)
- operational state (enabled or disabled)
- availability
  - 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 13 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_12	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_12	Cleared	Unlocked	Enabled	normal
ChassisEventManager_0	Cleared	Unlocked	Enabled	normal
Conferencing_Service_0	Cleared	Unlocked	Enabled	normal
Cooling_System_0	Cleared	Unlocked	Enabled	normal
EthernetInterface_0	Critical	Unlocked	Enabled	degraded
Fan_1	Cleared	Unlocked	Enabled	normal
Fan_2	Cleared	Unlocked	Enabled	normal
Fan_3	Cleared	Unlocked	Enabled	normal
IVR_Service_0	Cleared	Unlocked	Enabled	normal
LocalResourceManager_0	Cleared	Unlocked	Enabled	normal
Main_Subagent_0	Cleared	Unlocked	Enabled	normal
NodeMtc_0	Cleared	Unlocked	Enabled	normal
Power_Supply_1	Cleared	Unlocked	Enabled	normal
Power_Supply_2	Cleared	Unlocked	Enabled	normal
Power_Supply_3	Cleared	Unlocked	Enabled	normal
ProgramManager_0	Cleared	Unlocked	Enabled	normal
ProgramManager_1	Cleared	Unlocked	Enabled	normal
Resource_Manager_0	Cleared	Unlocked	Enabled	normal
ShelfController_9	Cleared	Unlocked	Enabled	normal

- 3 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 12, “Components information.”

**Table 12 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 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 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).
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.

Table 12 Components information (Sheet 2 of 4)

Field name	Description
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 enabled.
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 12 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 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 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 12 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 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 Audio Server.



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





---

Succession Multimedia Communications Portfolio

## MCP SIP Audio Server

### 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 MCP SIP Audio Server 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, MCP, Nortel, Northern Telecom, and NT, are trademarks of Nortel Networks.

---

Publication number: NN10034-111  
Product release: MCP 1.1 FP1 Standard  
Document release: Standard MCP 1.1 FP1 (02.02)  
Date: April 2003  
Printed in the United States of America.

---

