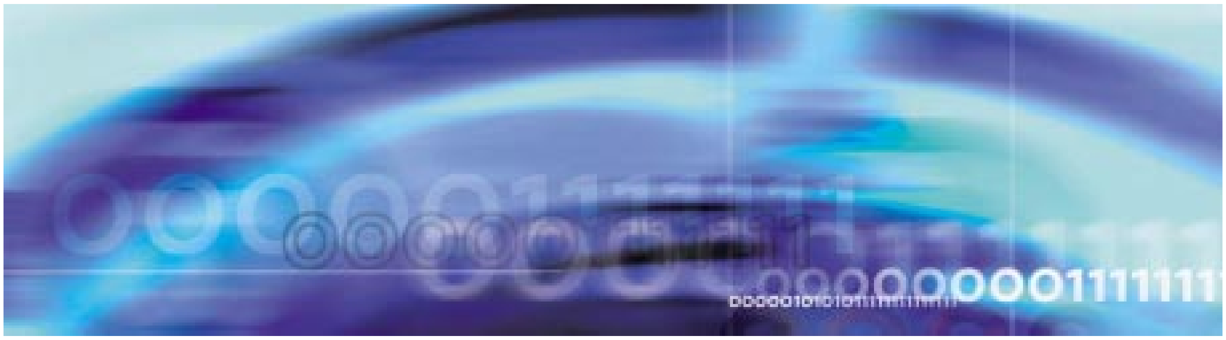

Upgrading the UAS

This document contains the following procedures:

- Upgrades
  - Upgrade from release UAS06 or UAS07 to release UAS08
  - Upgrade from one version of release UAS08 to a later version of release UAS08
  - UAS08 ground up installation
- Downgrades
  - Downgrade from release UAS08 to release UAS07 or UAS06
  - Downgrade from one version of release UAS08 to a previous version of release UAS08

Tools and utilities

This section contains the following information, which will help you prepare for an upgrade or downgrade of the system:

- a description of upgrade prerequisites, such as hardware replacements that must be completed before the upgrade is started
- a description of special considerations, such as where the upgrade is performed, impact of the upgrade on office operation, and how datafiles can be backed up for restoration
- information about the media necessary for performing an upgrade
- a description of the UAS database backup and restoration strategy
- information about upgrading the APS, including where the APS upgrade instructions can be found

UAS Installation prerequisites

Before an upgrade is started, the configuration information outlined in Configuration information on page 9, appropriate for the type of upgrade, should be collected and recorded for quick reference during the upgrade. For additional information about configuration parameter input, see Customer Questionnaire on page 17.

Before installation of the UAS or APS software is performed, the following tasks must be completed:

- installation of the audio management software on the APS node, if the UAS system is connected to its own APS node
- installation of the following third-party hardware necessary for the operation of a specific UAS application
  - Natural MicroSystems CG6000C card(s) - (VoIP) (For a procedure used to install or reconfigure CG6000 cards, see “Adding a CG6000 card to a UAS node” or “Removing a CG6000 card from a UAS” in the document NN10073-911, entitled “UAS Fault Management.”)
  - Natural MicroSystems AG4000C card(s) - (VoATM) (For a procedure used to install or reconfigure AG4000 cards, see “Adding an AG4000 card to a UAS node” or “Removing an AG4000 from a UAS node” in the document NN10073-911, entitled “UAS Fault Management.”)
  - Natural MicroSystems PA200 card - (VoATM-AAL1 and AAL2) (For a procedure used to install a PA200 card, see Replacing a BX4000c (S007) card with a PA200 card on page 30.)

UAS upgrade special considerations

Where an installation or upgrade is performed

All steps in the installation and upgrade procedures are performed at the local console.

> **CAUTION**
>
> No remote access sessions (telnet, ftp) should be in progress on a unit that is being installed, upgraded, or downgraded.

Upgrade interdependencies

None.

Office impact

The following general impact on an office can be expected during a UAS software upgrade:

- A UAS unit must be out of service when it is being upgraded. When the unit is out of service, other UAS units in the cluster continue to process calls.
- While an APS is out of service, audio provisioning cannot be performed; the UAS units in the cluster can, however, continue to process calls.
- During software installation, audio distribution to the UAS unit being upgraded is disabled.
- Multiple UAS units can also be upgraded in parallel as long as the requisite number of units required to handle call processing during the upgrade procedure remain in service.
- When, through the Universal Audio Server Manager, the administrative state of the UAS is set to “lock graceful” in preparation for the upgrade, all active calls in the UAS unit being upgraded complete before the unit goes out of service.

Software removal

Before an upgraded, or previous, version of the UAS software can be installed, it is necessary to remove the existing UAS software. If a software upgrade or downgrade is attempted when the existing software has not been removed, an error message is issued and the UAS installation program (“setup.exe”) exits.

The procedures used to remove UAS software include steps that save the UAS system configuration parameters before the system configuration files are removed. Thus, during a subsequent re-installation, the configuration parameters can be restored.

Hardware precautions

CAUTION
Catastrophic Hardware Failures - Please Read
If, during the Universal Audio Server installation, a catastrophic hardware failure is experienced on the node, it is necessary to terminate the installation at that point and execute a ground up installation. A catastrophic hardware failure is characterized by, but not limited to, loss of power to the node, surprise extraction of a system controller card, or surprise extraction of the hard disk drive. In the event that a catastrophic hardware failure occurs, contact your Nortel Networks service representative for assistance.

Disk Drive 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. If a disk becomes faulty during a system upgrade and requires replacement, the procedure, “Replacing a UAS disk drive,” located in the document, NN10047-461, entitled “UAS Fault Management” should be consulted for instructions.

UAS Installation media

Installation is performed from the Universal Audio Server UAS08.0 Installation CD. This CD contains one folder, named “WINNT.”

WINNT folder

The WINNT folder contains the callp application software to be installed on the cPCI. Specifically, the folder contains the Setup.exe installation file and its associated files. In addition, the folder contains the sub-folders, “Extras,” “IML,” and “NMS.”

The “NMS” folder contains the self-extracting/self-installing files used for the installation of the Natural MicroSystems Software applications.

The “ATM” folder contains the self-extracting/self-installing file used for the installation of the Natural MicroSystems software application.

The “Extras” folder contains files for the Microsoft tool, “Visual File Information,” which retrieves and generates file information. This tool can be used to uncover differences between two seemingly identical machines. Although the tool is not used during installation, it is available for administrative use.

UAS system configuration backup/restore strategy

All configuration data supporting the operation of the UAS is stored in configuration files. The configuration files include:

- uas.conf - containing configuration parameters that support the function of the UAS, including CG6000C card settings, Call Agent definition, APS hostname definition, network element settings, and conferencing service state definition
- ugw.conf - containing trunk configuration information for PRI Solutions
- snmpd.cnf - containing parameters that support the SNMP function, including management station address, SNMP user names, community names, and trap version
- hosts - containing parameters that support the function of the APS, including APS hostname and IP address
- atmhard.con - containing ATM bearer interface settings that link a local port ATM address to a particular ATM interface port
- atmconn.con - containing ATM bearer connections settings that provide the UAS with a remote gateway's name and ATM address
- mainsa.conf - containing Main Subagent program settings specifying the kinds of error and log messages to be sent to the management station
- atmSvcProfile.con - containing data on Switched Virtual Channel (SVC) traffic parameters associated with AAL2 SVCs
- atmhardloop.con - containing information associated with the loopback of SVCs

Automatic configuration file back-up

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network associated with the UAS node you are updating, the configuration files for that UAS node, and all UAS nodes in the network, can be backed up to the APS node. This capability is set up by entering the APS node IP address in the "Backup Storage IP" field of the Local Configuration Interface GUI screen, in the Procedure, UAS07 application software installation on page 126106106. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server. This capability is established through step 19 of the UAS07 application software installation procedure. The remote server IP address must then be entered in the "backup Storage IP" field of the Local Configuration Interface GUI screen using the Procedure, "Modifying configuration parameters through the Local Configuration Interface

GUI" in the document NN10095-511, entitled, "UAS Configuration Management."

The backed-up files can be restored should a catastrophic system event, such as a hard disk drive failure, create the need for a re-installation. The files are restored by manually transferring the files from the APS node or remote UNIX server to the UAS node after the UAS software (and NGS software, if necessary) has been re-installed. The backed-up files are located in the directory, /opt/uas/uas_conf_backup.

The files that are backed up include:

- C:\UAS\etc\UAS.conf (all configurations)
- C:\UAS\etc\ugw.conf (for a PRI gateway only)
- C:\UAS\etc\atmconn.con (ATM only)
- C:\UAS\etc\mainsa.conf (all configurations)
- C:\UAS\etc\atmhard.con (ATM only)
- C:\etc\srconf\agt\snmpd.cnf (all configurations)
- C:\Winnt\system32\drivers\etc\hosts (all configurations)
- C:\UAS\etc\atmSvcProfile.con (ATM only)
- C:\UAS\etc\atmhardloop.con (ATM only)

APS installation

Starting with release APS07, the APS server is configured on a server that also hosts the CS 2000 Management Components (CS2M), "Succession Element and Sub-Network Manager (SESM)," "CS 2000 GWC Mgr," "UAS Mgr," and "Network Patch Manager (NPM)." For the procedure used to upgrade the APS software when the APS resides on this CS2M server, see the CS 2000 Management Tools document NN10062-461, entitled, "Upgrading the CS 2000 Management Tools."

> ***Note:*** Release APS08 can only be installed on an APS that is configured on the CS2M server (described in the paragraph above). For a procedure used to combine an APS at release level APS06 or APS07 with the CS2M server, see the CS 2000 Management Tools document NN10062-461, entitled, "Upgrading the CS 2000 Management Tools."

APS Patching

Patches to the APS software are delivered in the form of patch packages, which replace one or more application files. The procedure, APS08 maintenance release process on page 157 contains the instructions for applying a patch or “maintenance release.” For assistance in performing a maintenance release, contact your Nortel Networks service representative.

Upgrade procedures

The following tables list the procedures you use to perform upgrades or downgrades.

> ***Note:*** The procedures in this document are presented in a hierarchical format: top-level procedures consisting of steps that describe the tasks to perform reference sub-procedures that enable you to actually perform the tasks. It is important, therefore, that you use and follow the top-level procedures listed in the following tables. The Bookmarks panel, which displays on the left side of this document, lists the content of the document. Although it can be used for quick access to the procedures in this document, it doesn't show which upgrade or downgrade tasks to perform or the order in which to perform the tasks.

UAS08 upgrade procedures

Procedure and page
UAS06 or UAS07 to UAS08 software upgrade procedure on page 22 UAS08 to UAS08 Upgrade on page 72 UAS08 ground up installation on page 75

UAS08 downgrade procedures

Procedure and page
UAS08 to UAS07 or UAS06 software downgrade on page 93 UAS08 to UAS08 downgrade on page 155

Procedure for performing an APS maintenance release

Procedure and page
APS08 maintenance release process on page 157

Configuration information

Before an upgrade is started, the configuration information outlined in the tables below should be collected and recorded for quick reference during the upgrade. For additional information about configuration parameter input, see, Customer Questionnaire on page 17.

The following table contains the configuration parameters that must be datafilled for an ATM-AAL1 fabric UAS node.

Configuration information for an ATM-AAL1 fabric UAS

Parameter	Entry for this node
General	
ATM companding mode	
optical carrier mode	
NTP server IP	
backup storage IP	
ATM Ctone support	
Call Agent	
Primary Call Agent name	
Primary Call Agent IP address	
Primary Call Agent port	
UAS call control port	
Log Levels	
system log level	
UAS log level	
application log level	
security log level	

The following table contains the configuration parameters that must be datafilled for an ATM-AAL2 fabric UAS node.

Configuration information for an ATM-AAL2 fabric UAS (Sheet 1 of 2)

Parameter	Entry for this node
General	
ATM companding mode	
optical carrier mode	
Gateway control protocol	
IVR support	
NTP server IP	
primary DBserver host	
primary DBserver IP	
backup storage IP	
audio synch on restart	
ATM BCT support	
ATM Ctone support	
Call Agent	
Primary Call Agent name	
Primary Call Agent IP address	
Primary Call Agent port	
UAS call control port	
legacy announcements	
primary language	
secondary language	
Log Levels	
system log level	

Configuration information for an ATM-AAL2 fabric UAS (Sheet 2 of 2)

Parameter	Entry for this node
UAS log level	
application log level	
security log level	

The following table contains the configuration parameters that must be datafilled for AG4000 cards provisioned in an ATM-AAL2 fabric UAS node that supports trunk testing.

Configuration information for ATM-AAL2 fabric AG4000 cards

Parameter	**Entry for this node**
test trunk support	
test trunk config size	
Sage box 1 IP	
Sage box 2 IP	

The following table contains the configuration parameters that must be datafilled for an IP fabric UAS node.

Configuration information for an IP fabric UAS (Sheet 1 of 2)

Parameter	Entry for this node
General	
Gateway control protocol	
IVR support	
conferencing state	
conference spanning	
conference expansion ports	
NTP server IP	
primary DBserver host	
primary DBserver IP	
backup storage IP	
audio synch on restart	
tone set	
Bearer	
RTP base port	
transmit gain	
receive gain	
default TOS	
RFC2833 DTMF	
RFC2833 DTMF squelch	
G729B	
supported codec	
Call Agent	

Configuration information for an IP fabric UAS (Sheet 2 of 2)

Parameter	Entry for this node
Primary Call Agent name	
Primary Call Agent IP address	
Primary Call Agent port	
UAS call control port	
legacy announcements	
primary language	
secondary language	
Log Levels	
system log level	
UAS log level	
application log level	
security log level	

The following table contains the configuration parameters that must be datafilled for each CG6000C card provisioned in an IP fabric UAS node.

Configuration information for IP fabric CG6000C cards

Parameter	Entry for this node
IP address	
router IP address	
netmask	
BCT support	
test trunk support	
test trunk config size	
Sage box 1 IP	
Sage box 2 IP	

The following table contains the SNMP management configuration parameters that must be datafilled for ATM and IP fabric UAS nodes.

Configuration information for SNMP management in an ATM or IP fabric UAS

Parameter	Entry for this node
v2c read-write community	
v2c read only community	
v3 read/write user	
v3 read-only user	
trap version	
trap destination	
trap port	

Customer Questionnaire

The following outline provides a guideline for gathering information in order to properly engineer a Universal Audio Server (UAS) application server or Audio Provisioning Server (APS).

The Universal Audio Server (UAS) consists of two different types of nodes: the application server and an Audio Provisioning Server (APS). The function of the APS is to host the web server used for provisioning audio across nodes that require audio, such as the application server, as well as hosting the audio database for the application server that defines the correlation between audio identifier and audio segment. The function of the application server is to host the call processing application that is driven by a call server application somewhere in the network for performing actions such as IVR and conferencing service. The application server can be configured on the network in one of two “bearer type” technologies: Internet Protocol (IP) or Asynchronous Transfer Mode (ATM). The information you collect, based on the questions listed below, will vary according to the bearer type to be configured.

1. Each host must have a valid computer or host name associated with it. This host name must be unique across the domain in which the host is contained.

    1.1. What is the hostname for the node?

2. An application server node is part of a set of computers on a network that has been assigned a group or domain name. A domain name on the Internet could resemble something like “ourcompany.com”.

    2.1. What is the domain name for this application server node?

3. For an application server host, one or more Domain Name System (DNS) servers will exist that the application server host will search for the name assigned to the node. Multiple servers can be defined and will be searched in the order listed.

    3.1. What is the IP address for the DNS server(s) hosting this application server node?

4. A domain suffix is a name such as “mycompany.com” that helps identify the host on the Internet. The host name for the node combines with the domain suffix to create the Internet address for the node. A

DNS server takes into account the domain suffix(es) that a host can appear in when it is searching for a host name in its database.

4.1. What is the domain suffix(es) to be searched by the DNS server for this host?

5. The UAS can serve as a PRI trunk gateway or as a traditional UAS (IVR and conferencing server).

5.2. What is the gateway type (Gateway or UAS)?

6. In an IP-configured system, a fixed number of IP addresses are required for either an application server or APS node in order to communicate over the LAN network.

6.1. If the node is an application server, the number of IP addresses is dependent upon the amount of traffic (busy hour call attempts (BHCA)) to be handled by the node.

6.1.1. What is the targeted BHCA traffic level for this node?

6.1.2. Based upon spreadsheet calculations, how many bearer VoIP interfaces are required to support this traffic volume?

6.1.3. The quantity of IP addresses that are required for configuring this node is 1 (for the host interface) + (number of bearer VoIP interfaces)

Note 1: The UAS host interface contains two NIC interfaces that are operated in a redundant fashion managed by software on the UAS in an active/standby arrangement. In the event that the active interface detects a network problem, the UAS host automatically switches traffic processing to the standby interface. If the network problem is resolved, the UAS host will not automatically switch back to using that interface as the active interface unless a network problem is detected on the interface currently in use.

Note 2: Each VoIP interface card (CG6000C) contains two bearer NIC interfaces that are operated in Ethernet redundancy mode, which means that they operate in an active/standby or primary/secondary arrangement. In this configuration, the topmost interface on the VoIP card is designated the “primary,” and is commonly used to send and receive bearer Ethernet traffic, primarily RTP/RTCP streams. In the event that the primary interface detects a network problem, the VoIP card automatically switches traffic processing to the secondary interface. Once the network is re-established on the primary interface, the VoIP card automatically switches traffic back to the primary.

6.1.3.1. What is the IP address and network (subnet) mask associated with the application server host NIC interface?

6.1.3.2. What is the IP address and network (subnet) mask associated with each bearer NIC interface?

6.2. If this node is an APS, then it requires one IP address.

6.2.1. What is the IP address and network (subnet) mask associated with the APS?

7. In an IP-configured system, an application server or APS node requires, for each NIC interface (or IP bearer card (CG6000C)), the IP address of the default gateway that is used to forward packets to other networks or subnets. This address is required for nodes on inter-networks. If this IP address is not provided, the IP functionality will be limited to the local subnet unless a route is specified through the TCP/IP route command.

7.1. What is the IP address of the default gateway to which the host NIC adapter on the application server will be connected?

7.2. What is the IP address(es) of the default gateway to which each bearer NIC adapter on the application server will be connected?

7.3. What is the IP address of the default gateway to which the APS NIC adapter will be connected?

7.4. For an application server, Bearer Channel Tandeming (BCT) can be either enabled or disabled on each IP bearer interface card (CG6000C). What is the BCT status for each IP bearer interface card?

8. For the RTP/RTCP stream, a base number of ports can be supported.

8.1. What is the base number of ports to be supported by the RTP/RTCP stream? (The value must be an even number in the range, 1024 through 63094; the default is 30000).

9. In both IP and ATM-configured systems, the functionality provided by the application server is controlled by a Call Server ("gatekeeper") application somewhere in the network.

9.1. What is the IP address associated with the node that is the Call Server application? (In a CS 2000 node, this is the IP address of the active gateway controller.)

9.2. What is the port number that this Call Server application has bound against in order to provide this control function? (The default port number is 2944).

10. In both IP and ATM-configured systems, the application server communicates with the Audio Provisioning Server (APS).

 10.1. What is the host name and IP address of the APS?

11. Will a CS 2000 Call Server that is providing service in a multi-lingual environment control this application server? If so, the following languages can be supported by the application server: Basque, Belgian Dutch, Cantonese, Catalan, Czech, English, French, Galician, German, Greek, Hebrew, Italian, Japanese, Korean, Malay, Mandarin, Netherlands Dutch, Portuguese, Spanish, Tagalog, Thai, Turkish, Vietnamese.

 11.1. From the list of supported languages, what is the primary supported language for this node?

 11.2. From the list of supported languages, what is the secondary supported language for this node?

12. Conferencing services are supported by IP-configured systems.

 12.1. Will the application server provide support for conferencing services?

13. The APS and the application server for both IP and ATM-configured systems are managed from an element management system (EMS) through the SNMP protocol. The application server supports the SNMP protocols, SNMPv1, SNMPv2, SNMPv2c, and SNMPv3. The APS supports the SNMP protocols, SNMPv1, SNMPv2, and SNMPv2c. The EMS supported by the application server and APS for the Succession CS 2000 program is the CS 2000 Management Tool, Universal Audio Server Manager. All SNMP traps are sent by network elements, including the application server and APS, to the server that hosts the CS 2000 Management Tools. This node will generate SNMP traps to the management station.

 13.1. What is the destination IP address for the SNMP management station? This is the IP address to which SNMP traps should be sent.

 13.2. What is the UDP port number associated with the SNMP management workstation to which the SNMP traps are to be sent? For a CS 2000-based Succession system, this is “162”.

 13.3. Which SNMP version does the EMS for this node support? For a CS 2000-based Succession system, this should be set to “SNMPv3”.

 13.4. The SNMPv2 community names are defined to allow the SNMP-based management station to access or modify information on this node.

13.4.1. What is the community name associated with read access? (For a CS 2000-based Succession system, this should be set to “public”)

13.4.2. What is the community name associated with read/write access? (For a CS 2000-based Succession system, this should be set to “admin”.)

13.5. If the SNMP-based management station is configured SNMPv3, user names are defined, as well, for read access and read/write access by the management station.

13.5.1. What is the user name associated with read access? (For a CS 2000-based Succession system, this should be set to “v3user”)

13.5.2. What is the user name associated with read/write access? (For a CS 2000-based Succession system, this should be set to “v3admin”)

UAS06 or UAS07 to UAS08 (SN06) software upgrade procedure

This procedure enables you to perform an upgrade from release UAS06 or UAS07 to release UAS08. Steps 1 through 15 of this procedure must be performed for each domain that you are upgrading.

> ***Note:*** The UAS is normally deployed on the network in pairs of systems, with two separate systems per chassis. The left-hand side of the chassis is designated as domain A. The right-hand side of the chassis is designated as domain B. If you are upgrading two domains on a chassis from release UAS06 to release UAS08, you must perform the upgrade on domain B first.

CAUTION

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

UAS06 or UAS07 to UAS08 software upgrade procedure

At your console

1 Using the APS Administration GUI procedure “Disabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” disable audio provisioning for this UAS unit.

2 Using the Universal Audio Server Manager, look in the States window of the Network Element Status panel at the Usage category to determine whether the UAS is active and is processing calls. If the UAS is idle, proceed to step 3 of this procedure. If the UAS is active, determine whether any conferences are in progress by pulling down the Component menu in the System Identification window of the Network Element Status panel and selecting “conferencing service.” From the “conferences in progress” value in the component-specific panel of the Performance tab screen, determine whether to proceed to step 3 of this procedure: if conferences are in progress, wait until they complete; if conferences are not in progress, proceed with this procedure.

3 Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit being upgraded to “graceful lock.”

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

4 Uninstall (remove) the release UAS06 or UAS07 software by performing the procedure, UAS06/UAS07 application software removal on page 26. Removing the software creates the proper archive files for the following steps.

5 Archive the UAS06 and/or UAS07 configuration files by performing the following steps:

> ***Note:*** This step is performed to ensure that you have the latest version of the configuration files backed up in the event that you need to perform a downgrade back to an earlier release later on.

a Open a command line interface at the UAS:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

b If you wish to archive UAS06 configuration files, enter the following commands:

mkdir D:\UAS06restore

xcopy C:\Winnt\Temp\*.archive D:\UAS06restore /Y

Messages showing the files being copied display.

Go to step d

c If you wish to archive UAS07 configuration files, enter the following commands:

mkdir D:\UAS07restore

xcopy C:\Winnt\Temp\*.archive D:\UAS07restore /Y

Messages showing the files being copied display.

d Close the command line interface.

6 If you are upgrading from release UAS06 and if the fabric type of your system is ATM-AAL2, remove the BX4000c (S007) card and replace it with a PA200 card by performing the procedure, Replacing a BX4000c (S007) card with a PA200 card on page 30.

> ***Note:*** Before replacing the BX4000c (S007) card with a PA200 card, you must have completed replacing the CPV5350 processor card with a CPV5370 processor card. For

assistance, contact your Nortel Networks service representative.

7 Upgrade the Global Server (GS) base platform software by performing the procedure, Upgrading Global Server base platform software on page 33.

8 If you are upgrading from UAS06 to UAS08, perform the procedure, Configuring NetMeeting on a Win2K AS on page 35. NetMeeting can be used for accessing the UAS from a remote location in the event that any additional configuration or troubleshooting is required after the installation.

9 Install the UAS08 software by performing the procedure, UAS08 application software installation on page 37.

10 If the CG6000 card configuration is to be changed, perform the procedure, “Adding a CG6000 card to a UAS node,” or the procedure, “Removing a CG6000 card from a UAS” in the NTP NN10073-911, entitled “UAS Fault Management.”

11 Enable audio distribution at the APS for this UAS unit by performing the procedure “Enabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management.”

12 Perform the procedure “Provisioning a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” to force immediate provisioning of any files created before the start of the upgrade.

13 Update any remaining UAS units by performing this procedure for each unit.

14 Using the procedure “Viewing UAS performance measurements,” in the document, NN10139-711, entitled “UAS Performance Management,” verify that the UAS unit is enabled and is processing calls. In the procedure view, specifically, the performance measurements for the “Conferencing Service” and “IVR Service” components.

15 Reactivate audio provisioning capability for system users by performing the procedure “Editing user profiles,” in the document, NN10095-511, entitled “UAS Configuration Management,” changing the user status of all system users to “activated.”

16 If you wish to limit access to the “regedit.exe” and “regedt32.exe” utilities, perform the procedure, Limiting access to the “regedit.exe” and “regedt32.exe” utilities on page 62.

17 If you wish to limit access to the shared network folders, perform the procedure, Limiting access to shared network folders on page 64.

18 If you wish to limit access to the “hh.exe”, “winhelp.exe”, or “winhlp32.exe” utilities, perform the procedure, Limiting access to the “hh.exe”, “winhelp.exe”, and “winhlp32.exe” utilities on page 65.

19 If you wish to configure IP Security on the UAS, perform the procedure, Configuring IPSec and IKE on page 67.

20 You have completed this procedure.

UAS06 or UAS07 application software removal

This procedure enables you to remove existing UAS06 or UAS07 application software.

> ***Note:*** During this procedure, existing UAS configuration parameters are automatically saved before the configuration files containing these parameters are removed. Thus, these configuration parameters can then be restored during the installation process.

CAUTION

No remote access sessions (telnet, ftp) should be in progress on a unit from which application software is being removed.

UAS06/UAS07 application software removal

At your console

1 Select the fabric type of your system, either IP or ATM.

If	Do
the UAS bearer fabric type is IP	step 5
the UAS bearer fabric type is ATM	step 2

2 Select the appropriate ATM bearer fabric type and UAS release.

If	Do
the UAS bearer fabric type is ATM-AAL1 and the release is UAS06	step 3
the UAS bearer fabric type is ATM-AAL1 and the release is UAS07	step 3
the UAS bearer fabric type is ATM-AAL2 and the release is UAS06	step 4
the UAS bearer fabric type is ATM-AAL2 and the release is UAS07	step 3

3 For AAL1 UAS06 or UAS07 systems or AAL2 UAS07 systems, perform the following steps:

a Right-click My Computer and select “Properties.”

b In the System Properties window, click the Hardware tab and then select “Device Manager.”

c In the Device Manager window, click the plus (+) sign located at the left of “TDM/ATM bridge 2”.

d Right-click PA200 base board WDM and then select “Properties”.

e In the PA200 Base Board WDM Properties window that displays, select the Driver tab.

f In the Driver tab screen that displays, click Uninstall.

g In the Confirm Device Removal window that displays, click OK.

h In the “Systems Settings Change” pop-up window that displays, the system asks whether to restart the computer. Select “NO”.

i In the “Systems Settings Change” pop-up window that displays, the system indicates that the hardware settings have been changed and asks whether to restart the computer. Select “NO”.

j Close the Device Manager window (click X, located in the upper right-hand corner of the window).

k Close the System Properties window (click OK).

l Go to step 5.

4 For AAL2 UAS06 systems, perform the following steps:

a Remove the bindings by performing the following steps:

i Right-click My Computer and select “Properties.”

ii In the System Properties window, click the Hardware tab and then select “Device Manager.”

iii In the Device Manager window, double-click Network Adapters. Right-click ArTeMux s00x Adapter - Win2K and then select “Uninstall.”

iv In the Confirm Device Removal window, verify that the device being removed is “ArTeMux s00x Adapter - Win2K” and then click OK.

The Device Manager window will refresh and the ArTeMux adapter will then be absent from the window.

v Close the Device Manager window (click X, located in the upper right-hand corner of the window).

vi Close the System Properties window (click OK).

b Verify that the fourth Local Area Connection has been removed by performing the following steps:

i Right-click My Network Places and select “Properties.”

In the Network and Dial-up Connections window, the fourth Local Area Connection should now be absent.

ii Close the Network and Dial-up Connections window (click X, located in the upper right-hand corner of the window).

5 Perform the following steps:

a select **Start -> Settings -> Control Panel**

b In the Control Panel window, double-click Add/Remove Programs.

c Determine whether you are removing patches in addition to the UAS software.

If	Do
you are removing patches in addition to the UAS software	step d
you are only removing the UAS software	step h

d In the Add/Remove Program Properties window, scroll down the list of software programs and select “Universal Audio Server patch to be removed”.

e Click Add/Remove.

f In all succeeding confirmation and status screens, click OK (or any equivalent positive response displayed).

g Perform steps d through f until all patches that display are removed.

Note: If you are prompted for a re-boot, respond “NO”.

h In the Add/Remove Program Properties window, scroll down the list of software programs and select “Universal Audio Server”.

i Click Change/Remove.

The “Welcome Modify, Repair, or Remove the Program” window of the InstallShield Wizard for UAS displays.

j Click Next.

> ***Note:*** The Remove button is the only functional option in this window and is selected by default.

The Confirm File Deletion screen displays and asks whether you wish to remove completely the selected application and all of its components.

6 Click OK.

The following InstallShield message windows display:

- *Stopping pmgrdaemon service*
- *Stopping SNMP services*
- *Removing SNMP subagents*
- *Stopping time service NTP Client*
- *Please wait while InstallShield removes and restores files*

An InstallShield Wizard screen displays, indicating that maintenance is complete.

> ***Note:*** If at any time a pop-up window displays that prompts for the removal of “read-only” files, select YES.

7 Ensure that the “Yes, I want to restart my computer now” option on the screen has been selected, and then click Finish.

The system performs a restart.

> ***Note:*** If the system reboots when the UAS software is not yet installed and when telephony cards (CG6000, AG4000, S007, PA200) are installed in the chassis, the “Found New Hardware Wizard” window will display. Press the Escape key to dismiss each instance of the display of this window.

8 You have completed this procedure.

Replacing a BX4000c (S007) card with a PA200 card

This procedure enables you to upgrade from a BX4000c (S007) card to a PA200 card in ATM-AAL2 systems. Before you start performing this procedure, ensure that you have a complete PA200 card set, that is, a PA200 card and an R200 rear transition module.

Replacing a BX4000c (S007) card with a PA200 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.

DANGER
Laser radiation exposure
The exposed ends of fiber optic cables can emit harmful laser radiation. Do not look at the ends of fiber optic cables unless protector caps are in place. Disconnect all laser sources when personnel are working with fiber-optic cables.

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.

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

1 Stop any applications that may be running.

- **a** Access the “Services” window as follows:

  select **Start -> Programs -> Administrative Tools -> Services**

- **b** Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

2 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.

3 Locate the BX4000c card. If the UAS node is located on the left side of the shelf, the card will be in slot 5; if the node is located on the right side of the shelf, the card will be in slot 12. Remove the BX4000c card by performing the following steps:

- **a** Disconnect the OC3c interface cable from the BX4000c card. After the cable has been removed, cap the connectors on the card and on the fiber cable.
- **b** Remove the BX4000c card. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed.)

  Note: There is no rear transition module for this card.

- **c** Install a filler plate over the slot from which the BX4000c card was removed.

4 Install the PA200 card set by performing the following steps:

- **a** Remove the filler plate either from slot 6 or from slot 11 on the back of the chassis, depending on where you will install the R200 rear transition module of the PA200 card set, and then remove the corresponding filler plate from slot 6 or 11 on the front of the chassis, where you will install the PA200 card.
- **b** Insert the new R200 rear transition module in the back of the chassis. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

- **c** Insert the new PA200 card in the front of the chassis. Lock the lock latches on the card and tighten the screws that secure the card in the shelf.
- **d** Remove the protective caps from the connectors on the new R200 rear transition module and from the connectors on the fiber cable. Connect the OC3c interface cable to the module.

5 With an appropriate device, press the guarded reset switch located on the front panel of the CPV5370 Processor card that is associated with the domain in which the PA200 card is being installed. The CPV5370 card is located in slot 7 for the left domain and in slot 9 for the right domain.

6 You have completed this procedure.

Upgrading Global Server base platform software

This procedure enables you to remove existing Global Server base platform software and upgrade to release Global Server 3.3.

Upgrading Global Server base platform software

At your console

1 Insert the CD-ROM, “Global Server Platform Software, GS v3.3” into the CD-ROM drive of the domain (A or B) of the application server on which you are installing operating system software.

2 Select **Start -> Programs -> Accessories -> Command Prompt**

3 Upgrade from the previous version of the platform software by entering the following command at the command prompt:

```
<cdrom>:\upgrade <cdrom>:\
```

where *<cdrom>* is the letter of the CD-ROM drive on the application server. For example: **E:\upgrade E:\**

> ***Note 1:*** Software upgrade will take several minutes to complete; if a security lock screen appears before the upgrade completes, log back in.
>
> ***Note 2:*** A message will appear in the MS-DOS window that indicates when the upgrade has completed.

4 The upgrade of the platform reverts the Global Server Program Manager service password to its default value. It may be necessary at this point to synchronize passwords in order for the service to start properly.

If	Do
you have the default system password, “superuser”	step 8
you have changed the password	step 5

5 Perform the following steps to synchronize the Global Server Program Manager service, PMGR, with the system password:

a select **Start -> Run**

b Enter the following:

```
Services.msc
```

The Services window displays.

6 In the Services window, right-click pmgrDaemon and select Properties.

The PMGRdaemon Properties (Local Computer) window displays.

7 In the PMGRdaemon Properties (Local Computer) window, select the Log On tab.

a Select “This account.”

b In the “account name” field, verify the entry or enter:

`.\Administrator`

c In the “password” and “confirm password” fields, enter the new password.

d Click OK.

The Microsoft Management Console dialog box displays.

8 Remove the CD-ROM from the CD-ROM drive.

9 You have completed this procedure.

Configuring NetMeeting on a Win2K AS

This procedure enables you to configure NetMeeting software on a single Win2K application server. This procedure is required only when you are upgrading from UAS06.

> ***Note:*** In order to prevent possible access problems, you should install NetMeeting on your desktop only when logged in as "administrator".

Configuring NetMeeting on a Win2K AS

At your console

1 Perform the following steps:

- **a** select **Start -> Programs -> Accessories -> Communications -> NetMeeting**

  The NetMeeting Setup Wizard window displays.

- **b** Click Next.

- **c** In the subsequent NetMeeting Setup Wizard window, enter the requested information about your system and then click Next.

- **d** In the subsequent NetMeeting Setup Wizard window, deselect the "Log into a directory server when NetMeeting starts" check box and then click Next.

- **e** In the subsequent NetMeeting Setup Wizard window, select the "Local Area Network" check box for the speed of your network connection and then click Next.

- **f** In the subsequent NetMeeting Setup Wizard window, deselect all check boxes for the desktop shortcuts and then click Next.

- **g** In the final NetMeeting Setup Wizard window, ignore the Sound Card hardware warning message and click Finish.

  The NetMeeting application starts.

2 In the NetMeeting application main window, perform the following steps:

- **a** select **Tools -> Remote Desktop Sharing**

- **b** In the Remote Desktop Sharing Settings window that displays, click the "WIZARD ..." box.

  The Remote Desktop Sharing Wizard window displays.

c Click Next.

d In the subsequent Remote Desktop Sharing Wizard window, click Next.

e In the subsequent Remote Desktop Sharing window, select the “No, I will do this later” and then click Next.

f In the final Remote Desktop Sharing Wizard window, click Finish.

g In the Remote Desktop Sharing Settings window, click OK.

3 In the NetMeeting application main window, select **Call -> Automatically Accept Calls**

4 In the NetMeeting application main window, select **Call -> Exit and Activate Remote Desktop Sharing**

5 You have completed this procedure.

UAS08 application software installation

This procedure enables you to install the UAS08 application software.

UAS08 application software installation

At your console

1 Close all applications.

2 Insert the UAS08 installation CD into the CD-ROM drive.

3 Launch the InstallShield Wizard for Universal Audio Server program by performing the following steps:

a select **Start -> Run**

b In the Run window, click Browse.

c In the Browse window, navigate to the file, *<cd-rom>*: \winnt\setup.exe, select the file, and click Open.

Note: *<cd-rom>* is the “drive letter” assigned to the CD-ROM device.

d Click OK.

The Welcome window for the InstallShield Wizard for Universal Audio Server displays.

4 In the Welcome window for the InstallShield, click Next.

The Choose Node Type screen displays.

5 Select the appropriate gateway type, Gateway or Universal Audio Server (audio server).

If	Do
you chose Gateway (in support of an IMS release)	step 6
you chose Universal Audio Server	step 8

6 Click Next.

7 In the screen that displays, select “PRI” and then click Next.

a Go to step 12.

8 Select the bearer fabric type of your system, either IP or ATM.

If	Do
you chose IP	step 12
you chose ATM	step 9

9 In the InstallShield Wizard Complete screen, click Finish.

Note 1: In some cases, an application error will display immediately after the information message, “Stopping Program Manager.” This is a known platform problem that is patched by the UAS installation. If an error dialog appears with an “AM.EXE Application error” pop-up indicating a problem with an instruction at a referenced memory location, dismiss the error dialog by clicking the “OK” button.

Note 2: Up to 60 seconds may pass before the InstallShield Wizard Complete screen first appears.

Note 3: If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

10 Perform the following steps.

a Perform the following steps to install the PCI drivers:

i Right-click My computer, and then select “Properties.”

ii In the pop-up window that displays, select the Hardware tab and click Device Manager (located in the middle of the window).

iii In the Device Manager window that displays, right-click PCI Memory Controller (located under “TDM/ATM bridge 2” on the window) and select “Properties.”

Note: For ground-up installations and for UAS06 AAL2 upgrades, PCI Memory Controller will appear under “Other devices” on the window.

iv In the PCI Memory Controller Properties window that displays, select the Driver tab and then click the Update Driver button.

v In the Upgrade Device Driver Wizard window that displays, click Next.

- **vi** In the Install Hardware Device Drivers subscreen (of the Upgrade Device Driver Wizard window), the radio button, “Search for a suitable driver for my device” is selected by default. Click Next.
- **vii** In the Locate Driver Files subscreen (of the Upgrade Device Driver Wizard window), deselect “Floppy disk driver” and “CD-ROM driver”, then select “Specify a location” box, and, finally, click Next.
- **viii** In the Upgrade Device Driver Wizard pop-up window (subtitled, “Insert the manufacturer’s installation disk into the drive selected and then click OK”), type (or browse for) “c:\NMS_pa200\Pa200\system” and then click OK.
- **ix** In the Driver Files Search Results window, click Next.
- **x** In the Completing the Upgrade Device Driver Wizard subscreen (of the Upgrade Device Driver Wizard window), click Finish.
- **xi** In the PA200 Base Board WDM Properties window, click Close.
- **xii** Close the Device Manager window (click X, located in the upper right-hand corner of the window).
- **xiii** Close the System Properties window (click OK).

b Re-boot the system by performing the following steps:

- **i** select **Start -> Shutdown**
- **ii** select “restart the computer” in the Shutdown Windows screen.

c After the system re-boots, log back into the system as “administrator” (user name), and enter either “superuser” as the password or the password supplied by your network administrator.

d Open a command line interface at the UAS:

- **i** select **Start -> Run**
- **ii** type **cmd** in the window that displays
- **iii** press Enter
- **iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications
- **v** press Enter

e Launch the Local Configuration Interface GUI by performing the following steps:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **lci** on the command line

> ***Note:*** The first letter in the lci command is an "l", as in "local."

v press Enter

The main Local Configuration Interface GUI screen displays.

vi select the "node" folder in the Network Element Tree pane.

The Bearer Type ATM Local Configuration Interface GUI screen displays. Three tabs display in the "Details of selected tree node" window. Each tab selects a separate screen used for data filling.

vii You may see a pop-up window explaining that the configuration is not consistent with ATM. The system will ask you whether you want to update. Click OK.

viii You may see a pop-up message window that indicates the configuration data has been updated. Click OK.

f Examine the Adaptation Layer heading on the screen and ensure that the appropriate screen for the ATM bearer fabric type of your system displays.

> ***Note:*** If you are performing a ground-up installation, the Adaptation Layer heading on the screen will be blank. If you are, instead, upgrading an existing ATM system, the Adaptation Layer heading will contain the appropriate ATM bearer fabric type for your system.

If	Do
the appropriate screen for the bearer fabric type displays	step h
the appropriate screen for the bearer fabric type does not display	step g

g Pull down the Adaptation Layer menu and select the appropriate bearer fabric type. The following rules dictate the system reaction to your selection:

- When you select a bearer fabric type for the first time during a ground-up installation, the pop-up message

"Setting the default ATM mode ..." displays; click OK in the message pop-up.

- When you select ATM-AAL1, the system checks to ensure that IVR is disabled and BCT is enabled, as required, for the ATM-AAL1 system. If the system detects that IVR is enabled or BCT is disabled, it will react in the following manner:
  - — A pop-up window explaining that the configuration is not consistent with ATM displays. The system will ask you whether you want to update; click OK in the message pop-up.
  - — Another pop-up message window that indicates the configuration has been updated will then display; click OK in the message pop-up.

The Bearer Type ATM Local Configuration Interface GUI screen that you selected displays.

Note: In each of the screens that display when you manipulate the ATM fabric version of the LCI GUI in the following steps, fields containing default data that cannot be changed appear in the color grey. In addition, when data is entered in an incorrect format in some of the fields that can be changed, the field label changes to a red color. When the data is then corrected in the field, the field label changes back to black. None of the screen changes can be validated and saved until all fields in all of the screens associated with the bearer fabric contain correct information.

h Determine whether the fabric type of your system is ATM-AAL1 or ATM-AAL2.

If	Do
your UAS bearer fabric type is ATM-AAL1	step i
your UAS bearer fabric type is ATM-AAL2	step m

i In the General tab screen, verify and/or enter information for the following fields:

- **Atm Companding Mode**

  This is the companding mode, either A-Law or Mu-Law.

- **Optical Carrier Mode**

  This field allows selection of the appropriate optical carrier standard for your ATM card, either SONET (a North American standard for optical carriers) or SDH (a European standard for optical carriers). The default for AAL1 systems is SONET.

- **NTP Server IP**

  This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.

  > ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

- **ATM CTone Support**

  This field, which must be datafilled when ATM BCT Support is ENABLED (ATM BCT Support is always ENABLED for an AAL1 system), determines how the audio endpoints for the ATM AG4000 card are defined. The possible responses are: ENABLED or DISABLED. If an AG4000 card is not provisioned in the system, this field should be set to DISABLED.

j Select the “Call Agent” tab.

The Call Agent tab screen displays in the “Details of selected tree node” window.

k In the Call Agent tab screen, verify and/or enter information for the following fields:

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2944).

- **UAS Call Control Port**

  This is the port associated with receiving the call control message stream (default is 2944).

l Go to step 13.

m Ensure that the General tab screen is selected.

n In the General tab screen, verify and/or enter information for the following fields:

- **Atm Companding Mode**

  This is the companding mode, either A-Law or Mu-Law.

- **Optical Carrier Mode**

  This field allows selection of the appropriate optical carrier standard for your ATM card, either SONET (a North American standard for optical carriers) or SDH (a European standard for optical carriers). The default for AAL2 systems (including wireless systems) is SDH; if a

North American AAL2 system is being configured, this field must be changed to SONET.

- **Gateway Control Protocol**

  This is the control protocol for the UAS, either H.248 or MGCP.

- **IVR Support**

  This indicates whether IVR support is enabled on this system.

- **NTP Server IP**

  This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.

  > ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

- **Primary DBServer Host**

  This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, when IVR Support is enabled, an entry must still be made in this field.

- **Primary DBServer IP**

  This is the IP address of the APS that is hosting the database server used by this UAS node.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

- **Audio Synch on Restart**

  For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled,

hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.

- **ATM BCT Support**

  This indicates whether Bearer Channel Tandeming is supported on this system

- **ATM CTone Support**

  This field, which must be datafilled when ATM BCT Support is ENABLED, determines how the audio endpoints for the ATM AG4000 card are defined. The possible responses are: ENABLED or DISABLED. If an AG4000 dedicated to CTone is not provisioned, this field should be set to DISABLED.

o Select the “Call Agent” tab.

The Call Agent tab screen displays in the “Details of selected tree node” window.

p In the Call Agent tab screen, verify and/or enter information for the following fields:

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2944).

- **UAS Call Control Port**

  This is the port associated with receiving the call control message stream.

- **Legacy Announcements**

  This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.

  > ***Note:*** If Legacy Announcements is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Announcements is

Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **Primary Languag**e

  This is the primary language associated with the node.

  > ***Note:*** A Primary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  This is the secondary language associated with the node.

  > ***Note:*** A Secondary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Secondary Language field will also be Disabled.

11 Double click the “Cards Folder”, which is located in the Nodes folder in the Network element Tree pane.

A list of the cards that are installed in the system displays below the “Cards Folder”.

a Review the card list. In the list, click the bullet associated with a card for which information is to be examined or changed.

A card detail window displays in the “Details of selected tree node” screen.

If	Do
card information is to be changed	step b
card information is not to be changed	step 13

b Enter information in the following fields in the dedicated card details window:

- Test Trunk Support; select either Enabled or Disabled
- Test Trunk Config Size; select the appropriate size (small - 50k trunks; medium - 100k trunks; large - 200k trunks), when Test Trunk Support is Enabled. This determines the number of channels available for tests.

- Sage Box 1 IP (address); enter when Test Trunk Support is Enabled. One Sage test box is use for small and medium test trunk configurations.
- Sage Box 2 IP (address); enter if a second Sage test box is required, when Test Trunk Support is Enabled. Two Sage test boxes are used for large configurations.

c Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step d
you do not want to save the information	step g

d Click Validate.

e Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI card detail screen) and select “Save”. Click OK when the confirmation screen displays.

f Go to step 13.

g Click Cancel.

h Either return to step a and select another card, or go to step 13.

12 In the InstallShield Wizard Complete screen, which displays after a slight delay, select “Yes, I want to restart my computer now.” Click Finish.

Note 1: The system re-boot (restart) is required in order for the installation program to complete registry updates.

Note 2: If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

a After the system re-boots, log back into the system as “administrator” (user name), and enter either “superuser” as the password or the password supplied by your network administrator.

b Open a command line interface at the UAS:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

v press Enter

c Launch the Local Configuration Interface GUI by performing the following steps:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **lci** on the command line

> ***Note:*** The first letter in the lci command is an “l”, as in “local.”

v press Enter

The main Local Configuration Interface GUI screen displays.

> ***Note:*** In each of the screens that display when you manipulate the IP fabric version of the LCI GUI in the following steps, fields containing default data that cannot be changed appear in the color grey. In addition, when data is entered in an incorrect format in some of the fields that can be changed, the field label changes to a red color. When the data is then corrected in the field, the field label changes back to black. None of the screen changes can be validated and saved until all fields in all of the screens associated with the bearer fabric contain correct information.

vi select the “node” folder in the Network Element Tree pane.

The Bearer Type IP Local Configuration Interface GUI screen displays. Four tabs display in the “Details of selected tree node” window. Each tab selects a separate screen used for data filling.

d In the General tab screen, verify and/or enter information for the following fields:

- **Gateway Control Protocol**

  This is the control protocol for the UAS, either H.248 or MGCP. Ensure that the Gateway Control Protocol is set to H.248.

- **IVR Support**

  This field determines whether IVR support is enabled in this system.

- **Conferencing State:**

  This field determines whether Conferencing is enabled in this node.

  > ***Note:*** If Conferencing State is Disabled, then the Conference Spanning field is also Disabled.

- **Conference Spanning**

  This field determines whether Conference Spanning is supported by the node. Conference Spanning allows conferences with up to 128 participants.

  > ***Note:*** If “Conferencing State” is Disabled, then the Conference Spanning field is also Disabled.

- **Conference Expansion Ports**

  This field indicates the number of reserved conference ports that can be used to grow existing conferences, but that cannot be used in reservations for new conferences. This prevents existing conferences from running out of resources. Once a port from this buffer is used, it is restored to the pool of resources after any member of the conference in the pool drops out of the conference.

  W*hen you increase this number, fewer ports are available for general use. For example, if you reserve four ports, a 32-port pool will have only 28 ports available for new conferences. If you decrease this number, fewer ports are* *available to grow existing conferences when the pool is full.*

- **NTP Server IP**

  This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.

  > ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

- **Primary DBServer Host**

  This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, accept the default settings.

- **Primary DBServer IP**

  This is the IP address of the APS that is hosting the database server used by this UAS node.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

- **Audio Synch on Restart**

  For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled, hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.

- **Tone set**

  This is the default tone set provided for the country that you select from the pull-down menu associated with this field.

e Select the “Bearer” tab.

The Bearer tab screen displays in the “Details of selected tree node” window.

f In the Bearer tab screen, verify and/or enter information for the following fields:

- **Rtp Base Port**

  This is the first port number used for real-time protocol streams on VoIP cards.

  > ***Note:*** This must be an even number. In addition, commas must not be entered in the number.

- **Annc Circuits per Card**

  This is the number of circuits available for announcements on each bearer card in the system. This number is taken from the engineering data for the system. If IVR is enabled, this number should be greater than zero. The allowable values are one through the value of Max. Annc Circuits per Card.

- **Conference Circuits per Card**

  This is the number of circuits available for conferencing on each bearer card in the system. This number is taken from the engineering data for the system. If conferencing is enabled, this number should be greater than zero. The allowable values are one through the value of Max. Conf. Circuits per Card.

- **Max. Annc Circuits per Card**

  This is the maximum value for Annc Circuits per Card, for the network element. This number can vary depending on the software release of the network element and also depending on whether the network element is configured for IP or for ATM. The element manager uses this value to perform error checking on the user's input for Annc Circuits per Card.

- **Max. Conf. Circuits per Card**

  This is the maximum value for Conference Circuits per Card for the network element. This number can vary depending on the software release of the network element. The element manager uses this value to perform error checking on the user's input for Conference Circuits per Card.

- **Transmit Gain**

  This is the strength of a signal going out from the vocoder of an rtp endpoint as compared with the strength of a *signal going into the vocoder. Transmit Gain does not apply to conferencing service.*

- **Receive Gain**

  This is the strength of a signal coming into an rtp endpoint from the decoder as compared with the strength of a signal coming into the decoder.

- **Default TOS**

  This field determines the Type of Service bit usage for this UAS, 0-255. The default is 0, which indicates “normal” delay, throughput, and reliability, with “routine” precedence.

- **RFC2833 DTMF**

  This field indicates how the UAS will determine whether RFC2833 is enabled for each RTP connection. RFC2833 defines a method for passing DTMF digits “out-of-band” in special RTP packets, in order to provide more reliable

DTMF recognition than is possible with low-bandwidth codecs. The possible selections include:

- — *AlwaysOff (RFC2833 support is always disabled, regardless of call control)*
- — *Negotiated (RFC2833 support is enabled per call control messaging, that is, SDP and/or LCO negotiation)*

Note: The setting should be AlwaysOff when announcements or conferencing are supported.

- **RFC2833 DTMF Squelch**

  Not applicable

- **G729B**

  This field indicates G.729B audio codec support.

- **Clock Sync Mode**

  Not applicable

- **Primary Clock Source**

  Not applicable

- **Secondary Clock Source**

  Not applicable

- **Clock Source Carrier Type**

  Not applicable

- **Supported Codec**

  These check boxes determine which codecs, G711, G723, G726, G729, and T.38 are supported. The following guidelines should be followed when you are selecting the codecs:

  - — *T.38 is selectable only when at least one CG6000 card with BCT capability is installed in the system.*
  - — *In an all-BCT system, all voice codecs should be disabled.*
  - — *In a non-BCT system, up to a maximum of four voice codecs can be selected; the T.38 codec cannot be selected.*
  - — *In a mixed system (BCT + IVR, BCT + Conf, BCT + IVR + Conf), up to a maximum of four of the codecs*

can be selected; one of the four codecs selected must be a voice codec.

— *In a non-BCT system supporting only conferencing service, G.729 must not be selected.*

— *It is recommended that you select G.711 for systems supporting conferencing service, to avoid any possible deterioration of voice quality.*

g Select the “Call Agent” tab.

The Call Agent tab screen displays in the “Details of selected tree node” window.

h In the Call Agent tab screen, verify and/or enter information for the following fields:

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2944).

- **UAS Call Control Port**

  This is the port associated with receiving the call control message stream (default is 2944).

- **Legacy Announcements**

  This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.

  Note: If Legacy Announcements is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Announcements is Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **Primary Languag**e

  This is the primary language associated with the node.

  Note: A Primary Language is required only if the Legacy Announcements field is Enabled. If Legacy

Announcements is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  This is the secondary language associated with the node.

  Note: A Secondary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Secondary Language field will also be Disabled.

13 Select the “Log Levels” tab.

The Log Levels tab screen displays in the “Details of selected tree node” window.

14 In the Log Levels tab screen, verify and/or enter information for the following fields:

- **System Log Level**

  System logs are information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.

- **UAS Log Level**

  Audio Server logs include information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.

- **Application Log Level**

  Application logs include information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.

- **Security Log Level**

  Logs are either audit-succeed or audit-fail. This field specifies that the Main Subagent is to send either all security *logs, only audit-fail logs, or no logs for that source to the element management station.*

15 Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step 16
you do not want to save the information	step 19

16 Click Validate.

17 Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK in the confirmation screen and then click OK in the acknowledgement screen.

18 Go to step 20.

19 Click Cancel.

The entries in the screen fields revert to the default values.

20 Determine whether SNMP management configuration parameters need to be changed.

If	Do
SNMP management configuration parameters need to be changed	step 21
SNMP management configuration parameters do not need to be changed	step 22

21 Click the “Reconfigure SNMP” button, located at the bottom of the Local Configuration Interface GUI screen.

An SNMP re-configuration warning pop-up window displays. When you click OK in response to the message in the pop-up window, the Local Configuration Interface GUI SNMP window displays, showing default values delivered with the UAS system.

a Enter information for the following fields in the screen:

- **v2c read/write community**

  This is the SNMPv2c community name for read/write access through the SNMP-based management station.

- **v2c read only community**

  This is the SNMPv2c community name for read-only access through the SNMP-based management station.

- **v3 read/write use**r

  This is the SNMPv3 community name for read/write access through the SNMP-based management station.

- **v3 read only user**

  This is the SNMPv3 community name for read-only access through the SNMP-based management station.

- **trap version**

  This is the SNMP version of the SNMP traps sent by the UAS.

- **trap destination**

  This is the destination IP address associated with the remote SNMP management station. This is the address to which SNMP traps are sent.

- **trap port**

  This is the UDP port associated with the remote SNMP management station.

b Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step c
you do not want to save the information	step f

c Click OK.

d Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK in the confirmation screen and then click OK in the acknowledgement screen.

e Go to step 22.

f Click Cancel.

The entries in the screen fields revert to the default values.

22 Determine whether the bearer fabric of the UAS you are installing is ATM or IP.

If	Do
the bearer fabric type is IP	step 24
the bearer fabric type is ATM	step 23

23 Close the Local Configuration Interface GUI screens by pulling down the menu under File and selecting "Exit".

a Go to step 26.

24 In the Network element Tree pane, select the "Cards" folder, which is located in the Nodes folder.

The "Details of selected tree node" card screen displays.

a Review the card list. The Card Type field will be set automatically to "CG6000C" if a card is present. The Card Type field will be set to "none" and the information detail field labels will be colored grey, if no card is present. Note the current configuration.

If	Do
card information is not to be changed	step j
card information is to be changed,	step b

b Double click the "Cards" folder, located in the Network element Tree pane and, from the list of cards that displays below the "Cards Folder", click the bullet associated with a card to be changed.

A card detail window displays in the "Details of selected tree node" screen.

c Enter information in the following fields in the dedicated card details window:

- IP address associated with each CG6000C card
- default router associated with each CG6000C card
- network mask associated with each CG6000C card
- Bearer Channel Tandeming (BCT) support capability for each CG6000C card, either Enabled or Disabled.
- Test Trunk Support; select either Enabled or Disabled
- Test Trunk Config Size; select the appropriate size (small - 50k trunks; medium - 100k trunks; large - 200k trunks), when Test Trunk Support is Enabled. This determines the number of channels available for tests.

- Sage Box 1 IP (address); enter when Test Trunk Support is Enabled. One Sage test box is use for small and medium test trunk configurations.
- Sage Box 2 IP (address); enter if a second Sage test box is required, when Test Trunk Support is Enabled. Two Sage test boxes are used for large configurations.

d Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step e
you do not want to save the information	step h

e Click Validate.

f Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

g Go to step i.

h Click Cancel.

i Either return to step a and enter information for another card, or go to step j.

j Close the Local Configuration Interface GUI screens by pulling down the menu under File and selecting “Exit”.

25 If you are installing a PRI gateway, and if you are performing an upgrade, you should already have a valid “ugw.conf” file; go to step 26. If you are installing a PRI gateway, and if you are performing a ground-up installation, ftp a new ugw.conf file to c:\uas\etc. Contact UAS Product Design if you need a new ugw.conf file, then go to step 26.

26 This optional step validates configuration files and updates other configuration files. Any problems encountered will cause error messages to display in the command window. Note that this same action is performed upon the next application start-up.

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d Enter the following command in the window that displays:

```
configmgr -update -v
```

e press Enter

27 This optional step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server. For additional information about this capability, see the "UAS system configuration backup/restore strategy" in the "Tools and Utilities" section of this document. The following steps are performed on a remote Unix system.

a Open a telnet session with the remote UNIX server and log in as the Root user. Then enter:

```
cd /;mkdir /opt;chmod 777 opt

cd /opt;

mkdir uas;chmod 777 uas

cd uas;

mkdir uas_conf_backup;chmod 777
uas_conf_backup

cd /

cd /opt/uas/uas_conf_backup
```

b Configure NFS to share the "/opt/uas" file system and start the NFS server:

```
echo "share -F nfs /opt/uas" >>
/etc/dfs/dfstab
```

> ***Note:*** The commands from this point forward are specific for a Sun Solaris system.

```
/etc/init.d/nfs.server start
```

c Create a user login called "Administrator" that does not require a password:

```
/usr/sbin/useradd -d
/export/home/Administrator -g 1 -s /bin/ksh
-m -u 1002 Administrator 2> /dev/null

passwd -d Administrator 2> /dev/null
```

d At your local console, enter the IP address of the remote server in the "Backup Storage IP" field of the Local Configuration Interface GUI screen, using the procedure, "Modifying configuration parameters through the Local Configuration Interface GUI" of the UAS07 document, NN10095-511, entitled "UAS Configuration Management."

28 Start the application by performing the following steps:

- **a** select **Start -> Run**
- **b** enter **net start pmgrdaemon** in the window that displays
- **c** press Enter

29 If you installed the software from a CD, remove the installation CD from the CD-ROM drive.

30 Inspect the UAS installation log file (UASinstLog.txt) for indications of any errors that may have occurred during the application software installation. The file is located in the c:\winnt\temp directory. If you find errors, contact your next level of support or your Nortel Networks service representative for assistance.

31 For ATM bearer fabric systems, this step ensures that the ATM cards have been upgraded with the latest firmware.

- **a** select **Start -> Run**
- **b** type **cmd** in the window that displays
- **c** press Enter
- **d** Enter the following command in the window that displays:

```
atmfirmware -upgrade
```

- **e** press Enter
- **f** select **Start -> Shutdown**
- **g** select “restart the computer” in the Shutdown Windows screen.

32 Contact your Nortel Networks service representative to determine whether any patches need to be applied to the newly-installed UAS08 software.

33 To adjust the system time to your time zone, perform the following steps:

- **a** select **Start -> Settings -> Control Panel -> Date/Time Window**
- **b** select the Time Zone tab, adjust the time in the window that displays, and then click OK

34 You have completed this procedure.

Limiting access to the “regedit.exe” and “regedt32.exe” utilities

The utilities, “regedit.exe” and “regedt32.exe” cannot be removed from the system. Therefore, the following optional procedure enables you to restrict access to the utilities. After you have completed this procedure, any attempt to the access either of the utilities will result in the pop-up message display, “Access to the specified device, path, or file is denied.”

Limiting access to the “regedit.exe” and “regedt32.exe” utilities

At the system console (Windows desktop interface)

1 Access Windows Explorer by performing the following steps:

```
select Start -> Programs -> Accessories ->
Windows Explorer
```

2 Select and open “My Computer”.

3 Select and open “GS_SYSTEM”. (This is the “C:” drive.)

4 Select “WINNT”, and then right-click Search.

5 Perform Steps 5 through 10 for each utility. In the Search Results pop-up that displays, enter either **regedit.exe** or **regedt32.exe**.

6 Click Search Now.

7 In the results panel that displays, right-click the “regedit.exe” file and select “Properties”.

8 In the Properties pop-up that displays, select the “Security” tab.

9 For each user listed in the resulting display:

a Click on the user.

b Ensure that “Allow inheritable permissions from parent to propagate to this object” has not been selected.

Note: When you de-select this option, a security pop-up window displays. In the pop-up window, select “copy”.

c In the Permissions box, for every permission that is marked “Allow”, select the equivalent “Deny” and then click the Apply button.

Note: This may not reset the “Allow” setting.

10 After you have completed updating the permissions for all users, click OK. If a Security pop-up displays the message, “Caution! Deny takes priority over Allow entries, which can cause unintended effects due to group memberships. Do you want to continue?”, click Yes.

11 After you have performed steps 5 through 10 for each of the two utilities, you have completed this procedure.

Limiting access to shared network folders

This procedure enables you to disable sharing of any network folder. The affected shared folders include “C:” (which is also known as “GS_SYSTEM”), “D:” (which is also known as “New Volume”), and “C: \WINNT”.

Limiting access to shared network folders

At the system console (Windows desktop interface)

1 Access Windows Explorer by performing the following steps:

```
select Start -> Programs -> Accessories ->
Windows Explorer
```

2 Select and open “My Computer”.

3 Perform steps 3 and 4 for each of the folders in the resulting display. Right-click the folder and select “Sharing”.

> ***Note:*** “C: \WINNT” is contained on the C: folder/drive.

4 In the resulting Properties pop-up, ensure that “Do not share this folder” has been selected, and then click OK.

5 After you have performed steps 3 and 4 for each of the shared folders, you have completed this procedure.

Limiting access to the “hh.exe”, “winhelp.exe”, and “winhlp32.exe” utilities

The utilities, “hh.exe”, “winhelp.exe”, and “winhlp32.exe” cannot be removed from the system. Therefore, the following procedure enables you to restrict access to the utilities. After you have completed this procedure, any attempt to the access any of these utilities will result in the pop-up message display, “Access to the specified device, path, or file is denied.”

Note: The three utilities are located in C: \WINNT.

Limiting access to the “hh.exe”, “winhelp.exe”, and “winhlp32.exe” utilities

At the system console (Windows desktop interface)

1 Access Windows Explorer by performing the following steps:

```
select Start -> Programs -> Accessories ->
Windows Explorer
```

2 Select and open “My Computer”.

3 Select and open “GS_SYSTEM”. (This is the “C:” drive.)

4 Select “WINNT”, and then right-click Search.

5 Perform Steps 5 through 10 for each utility. In the Search Results pop-up that displays, enter either **hh.exe**, **winhelp.exe**, or **winhlp32.exe**.

6 Click Search Now.

7 In the results panel that displays, right-click the “hh.exe”, “winhelp.exe” or “winhlp32.exe” file and select “Properties”.

8 In the Properties pop-up that displays, select the “Security” tab.

9 For each user listed in the resulting display:

a Click on the user.

b Ensure that “Allow inheritable permissions from parent to propagate to this object” has not been selected.

c In the Permissions box, for every permission that is marked, “Allow”, select the equivalent, “Deny”.

Note: This may not reset the “Allow” setting.

10 After you have completed updating the permissions for all users, click OK. If a Security pop-up displays the message, “Caution! Deny takes priority over Allow entries, which can cause unintended effects due to group memberships. Do you want to continue?”, click Yes.

11 After you have performed steps 5 through 10 for each of the three utilities, you have completed this procedure.

Configuring IPSec and IKE

The following procedure provides the steps required to configure IPSec and IKE. Additional information and instructions for configuring IPSec and IKE can be found at the Microsoft web site: http://www.microsoft.com/windows2000/en/server/help/ipsec_sec_pol_create.htm

Note: This procedure should be performed during non-peak hours to prevent loss of network communication.

> **CAUTION**
> **Possible communication disruption**
> Failure to match UAS IPSec configuration values with those of the Gateway Controller may result in loss of communication capabilities between the Gateway Controller and the UAS.

Configuring IPSec and IKE

At your Windows desktop interface:

1 select **`Start -> Run`**

2 Enter the following command:

`secpol.msc`

3 In the file tree of the Local Security Settings window that displays, select “IP Security Policies on Local Machine.”

4 In the pull-down menu under Action (located in the tool bar at the top of the window), select “Create IP Security Policy.”

5 In the next window that displays, click Next.

6 In the IP Security Policy Wizard “IP Security Policy Name” window that displays, enter a policy name and description, and then click Next.

Note: Entering a policy name and description is optional.

7 In the next window that displays, ensure that the “Activate the default response rule” option is deselected, and then click Next.

8 In the next window that displays, ensure that the “Edit properties” option is selected, and then click Finish.

9 In the “Security rules for communicating with other computers” window that displays, click Add.

10 In the next window that displays, click Next.

11 In the Security Rule Wizard “Tunnel Endpoint” window that displays, ensure that the “This rule does not specify a tunnel” option is selected, and then click Next.

12 In the Security Rule Wizard “Network Type” window that displays, ensure that the “All network connections” option is selected, and then click Next.

13 In the IP Security Policy Wizard “Authentication Method” window that displays, select the “Use this string to protect the key exchange (preshared key)” option, and then enter the preshared key in the accompanying box. Click Next.

Note: The preshared key entered must match exactly the preshared key on the Gateway Controller.

14 In the Security Rule Wizard “IP Filter List” window that displays, click Add.

15 In the IP Filter List window that displays, select a name and description for the IP filter list. Click Add to enter the source, destination, and protocol information for your IP filter. Click Next in the next window that displays.

16 In the Filter Wizard “IP Traffic Source” window that displays, select a source address from the pull-down menu, and then click Next.

Note: Ensure that you set the Source address to “My IP Address.”

17 In the Filter Wizard “IP Traffic Destination” window that displays, select “A specific IP address” from the pulldown menu for the “Destination address” field. In the “IP Address” field, enter the IP address of the Gateway Controller, and then click Next.

18 In the Filter Wizard “IP Protocol Type” window that displays, select a protocol type from the pull-down menu for the “Select a protocol type” field. Click Next, and in the next window that displays, click Finish. Click Close in the next window that displays.

Note: It is recommended that you set the protocol type to “Any.”

19 In the Security Rule Wizard “IP Filter List” window, click the circle located next to the newly-created filter, and then click Next.

20 In the Filter Action window, click Add. Click Next in the next window that displays.

21 In the Filter Action "Filter Action Name" window that displays, select a name and description for the filter action. Click Next.

> ***Note:*** A sample entry is: "ESP: MD5 / 300s SA lifetime," which means that ESP is being used with MD5 authentication and a security association lifetime of 300 seconds. The security values that you enter, however, must be compatible with those being used on the Gateway Controller.

22 In the Filter Action "Filter Action General Options" window that displays, set your policy behavior from the following options:

- The "Permit" (bypass) option allows all IP traffic from the Gateway Controller to pass through the IPSec filter.
- The "Block" option prevents all IP traffic from the Gateway Controller from passing through the IPSec filter.
- The "Negotiate Security" option allows the UAS and the Gateway Controller to negotiate security settings. If negotiation fails, all traffic to and from the Gateway Controller is prevented.

If	Perform
you set your policy behavior to "Permit"	click Next**,** and then click Finish in the next window that displays. Go to step 29
you set your policy behavior to "Block"	click Next**,** and then click Finish in the next window that displays. Go to step 29
you set your policy behavior to "Negotiate Security"	click Next and then go to step 23

23 In the Filter Action Wizard "Communicating with computers that do not support IPSec" window that displays, ensure that you set the security option to "Do not communicate with computers that do not support IPSec" and then click Next.

24 In the Security Method Wizard "IP Traffic Security" window that displays, select the "Custom" option and then click Settings.

25 In the Custom Security Method Settings window that displays, select the "Data integrity and encryption (ESP)" option. Make the appropriate selections in the pull down window for the "Integrity algorithm" field and in the pull-down window for the "Encryption algorithm" field. In the "Session key settings" panel, select "Generate a new key every" and enter the value of the Gateway Controller IPSec SA lifetime. Click OK.

26 In the IP Traffic Security window that displays, click Next.

27 In the Filter Action Wizard window that displays, ensure that "Edit properties" option is selected and then click Finish.

28 In the New Filter Action Properties window that displays, deselect "Accept unsecured communication, but always respond using IPSec option." The "Session key Perfect Forward Secrecy" option must be selected. Click Apply and then OK in the next screen that displays.

29 In the Security Rule Wizard "Filter Action" window that displays, click the circle next to the new filter action that you have created and then click Next. Click Finish in the next window that displays.

30 In the *<security policy>* Properties window that displays, select the "General" tab and then click Advanced.

31 In the Key Exchange Settings window that displays, enable "Master key Perfect Forward Secrecy." Then enter a key negotiation time value that is compatible with the Gateway Controller's internet key exchange (IKE) SA lifetime, in the "Protect identities with these security methods" field. Click Methods.

> ***Note:*** If you don't know the minute values that are compatible, use the same value used with the Gateway Controller. Ensure that you enter the value in minutes equivalent to the Gateway Controller's value, which is expressed in seconds.

32 In the Key Exchange Security Methods window that displays, you can alter the security method preference order or the encryption and authentication settings used, for the internet key exchange (IKE).

> ***Note:*** Since the "Master key Perfect Forward Secrecy" option was enabled in step 31, the Gateway Controller must have both the IKE and IPSec Diffie-Hellman groups that match the

Diffie-Hellman group set in the IKE Security Algorithms window.

If	Perform
IKE settings for the Gateway Controller are known	move the matching preference to the top of the list in the Key Exchange Security Methods window. Click OK in the Key Exchange Security Methods window. Click OK in the Key Exchange Settings window.
you do not find a matching preference	click Add**.** In the IKE Security Algorithms window that displays, select the necessary IKE from the pull-down menus, click OK, and then move this preference to the top of the list in the Key Exchange Security Methods window. Click OK in the Key Exchange Security Methods window. Click OK in the Key Exchange Settings window.

33 Click Close in the next window that displays.

34 To activate the newly-created IP Security policy, select the policy name from the list under the “Name” column in the Local Security Settings window and select “Assign” from the pull-down “Action” menu located in the tool bar.

Note 1: An IP Security policy can be un-assigned by selecting a policy from the list and selecting Unassign from the pull-down “Action” menu.

Note 2: The security policies for the Gateway Controller and for the UAS must be assigned, or unassigned, at the same time, in order to prevent communication disruption.

35 You have completed this procedure.

UAS08 to UAS08 upgrade

The following procedure enables you to perform a release UAS08 to UAS08 upgrade.

CAUTION

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

UAS08 to UAS08 Upgrade

At your console

1 Using the APS Administration GUI procedure “Disabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” disable audio provisioning for this UAS unit.

2 Using the Universal Audio Server Manager, look in the States window of the Network Element Status panel at the Usage category to determine whether the UAS is active and is processing calls. If the UAS is idle, proceed to step 3 of this procedure. If the UAS is active, determine whether any conferences are in progress by pulling down the Component menu in the System Identification window of the Network Element Status panel and selecting “conferencing service.” From the “conferences in progress” value in the component-specific panel of the Performance tab screen, determine whether to proceed to step 3 of this procedure: if conferences are in progress, wait until they complete; if conferences are not in progress, proceed with this procedure.

3 Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit being upgraded to “lock graceful.”

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

4 Uninstall (remove) the release UAS08 software by performing the procedure, UAS08 application software removal on page 96.

> ***Note:*** You must remove any patches applied to the software, in addition to the software.

5 Install the UAS08 software by performing the procedure, UAS08 application software installation on page 37.

6 Determine whether audio distribution is to be enabled on the node you are upgrading.

If	Do
you are upgrading an ATM-AAL1, SIP conference-only, or PRI node	step 9
you are not upgrading an ATM-AAL1, SIP conference-only, or PRI node	step 7

7 Enable audio distribution at the APS for this UAS unit by performing the procedure "Enabling provisioning of a UAS node," in the document, NN10095-511, entitled "UAS Configuration Management."

8 Perform the procedure entitled "Provisioning a UAS node," in the document, NN10095-511, entitled, "UAS Configuration Management," to force immediate provisioning of any files created before the start of the upgrade.

9 Using the procedure "Changing the Admin state," in the document, NN10073-911, entitled "UAS Fault Management," set the administrative state for this UAS unit to "unlocked."

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

10 Using the procedure "Viewing UAS performance measurements," in the document, NN10139-711, entitled "UAS Performance Management," verify that the UAS unit is enabled and is processing calls. In the procedure view, specifically, the performance measurements for the "Conferencing Service" and "IVR Service" components.

11 Update any remaining UAS units by performing this procedure for each unit.

12 Reactivate audio provisioning capability for system users by performing the procedure "Editing user profiles," in the document, NN10095-511, entitled "UAS Configuration Management," changing the user status of all system users to "activated."

13 You have completed this procedure.

UAS08 ground up installation

This section provides the steps required to perform a ground-up installation of release UAS08 software. This procedure is performed only on a UAS operating in an SN06 Solution.

The UAS is normally deployed on the network in pairs of systems, with two separate systems per chassis. The left-hand side of the chassis is designated as domain A and is always installed first. The right-hand side of the chassis is designated as domain B. Normally, steps 1 through 9 of this procedure must be performed for each domain that you are installing.

> ***Note:*** In some situations, where more than two systems are being deployed on a network, the right-hand side of the chassis will not require a UAS installation. In these situations, perform this procedure for the domain A installation and then perform the procedure for the domain B installation.

The following general impact on an office can be expected during a UAS software ground-up installation:

- All UAS units are out of service after the GWC has been upgraded. The UAS units can process calls, however, after they have been installed with the new software.
- A UAS unit is out of service during installation. While the unit is out of service, other UAS units in the cluster that have been installed and are enabled can process calls.

CAUTION

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

UAS08 ground up installation

At your console

1 Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit being upgraded to “lock graceful.”

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

2 Install the Nortel Networks Global Server Software in the unit by performing the procedure, Installing Nortel Networks Global Server 3.3 base software on the UAS on page 80.

3 If you are performing a ground up installation in response to a catastrophic hardware failure on a node that contains a D:\ drive with archived UAS configuration files, restore these files prior to installing the UAS software by performing the following steps:

> ***Note:*** Under certain circumstances, the ground up installation CD may reformat both the C drive and the D drive on your system. In that event, the following file restore steps will not work. It is then necessary to run the Local Configuration Interface (LCI) GUI after the application installation in order to configure the UAS system.

a Open a command line interface at the UAS:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

b In the command window, enter:

```
xcopy D:\UAS0Xrestore\*.archive
C:\Winnt\Temp
```

where *X* is the release level of UAS software configurations you wish to restore. For example, to restore UAS06 configurations, you would enter “UAS06restore”.

Messages showing the files being copied display.

c Close the command line interface.

4 Install the UAS08 software by performing the procedure, UAS08 application software installation on page 37.

5 Determine whether audio distribution is to be enabled on the node you are upgrading.

If	Do
you are upgrading an ATM-AAL1, SIP conference-only, or PRI node	step 8

If	Do
you are not upgrading an ATM-AAL1, SIP conference-only, or PRI node	step 6

6 Enable audio distribution at the APS for this UAS unit by performing the procedure “Enabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management.”

> ***Note:*** If you are adding this UAS to an existing APS system, ensure that the UAS has been added to the APS, and that a provision set has been associated with the node, through the procedure “Creating a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management.”

7 Perform the procedure “Provisioning a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” to force immediate provisioning of any files created before the start of the upgrade.

8 Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit to “unlocked.”

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

9 Using the procedure “Viewing UAS performance measurements,” in the document, NN10139-711, entitled “UAS Performance Management,” verify that the UAS unit is enabled and is processing calls. In the procedure view, specifically, the performance measurements for the “Conferencing Service” and “IVR Service” components.

10 Update any remaining UAS units by performing this procedure for each unit.

11 Reactivate audio provisioning capability for system users by performing the procedure “Editing user profiles,” in the document, NN10095-511, entitled “UAS Configuration Management,” changing the user status of all system users to “activated.”

12 If you wish to limit access to the “regedit.exe” and “regedt32.exe” utilities, perform the procedure, Limiting access to the “regedit.exe” and “regedt32.exe” utilities on page 62.

13 If you wish to limit access to the shared network folders, perform the procedure, Limiting access to shared network folders on page 64.

14 If you wish to limit access to the “hh.exe”, “winhelp.exe”, or “winhlp32.exe” utilities, perform the procedure, Limiting access to the “hh.exe”, “winhelp.exe”, and “winhlp32.exe” utilities on page 65.

15 If you wish to configure IP Security on the UAS, perform the procedure, Configuring IPSec and IKE on page 67.

16 To adjust the system time to your time zone, perform the following steps:

- **a** select **Start -> Settings -> Control Panel -> Date/Time Window**
- **b** select the Time Zone tab, adjust the time in the window that displays, and then click OK

17 You have completed this procedure.

Nortel Networks Global Server 3.3 installation

The following procedure enables you to install the Nortel Networks Global Server 3.3 software on the UAS.

In UAS nodes equipped with the CPV5350SCSI configuration, the SCSI controller does not reside on the same board as the host processor. In UAS nodes equipped with the CPV5370 SCSI configuration, the SCSI controller resides on the same board as the host processor. Although the procedure below appears to only address installation of the Nortel Networks Global Server 3.3 software on a chassis equipped with the CPV5370 SCSI configuration, it is still applicable if your system is equipped with a CPV5350 SCSI configuration.

The following table lists the procedures performed during the Global Server 3.3 installation on the SAM16-based UAS application server, showing the method used for the installation, the CD-ROM, if any, used during the installation, and the approximate amount of time required for performing the procedure.

Global Server 3.3 Installation Procedures

Procedure	Script, application, interface used during installation	CD-ROM	Minimum duration (minutes)
Installing operating system software on a Win2K	boot from CD-ROM	Win2K: Win2K OS and System Software for CPV5350, GS v3.3 or Win2K: Win2K OS and System Software for CPV5370, GS v3.3	30
Installing HAE software on a Win2K AS	none	none	15
Installing platform software on a Win2K AS	none	none	15

This procedure provides the required order in which the Global Server installation procedures are performed for a ground-up installation.

CAUTION

You must perform the steps in the Win2K application server software installation procedures exactly as instructed. Errors cannot be undone during the installation. If a procedure or step is skipped, if incorrect information is entered, or if there is any change in the hardware configuration, all data may be lost and the entire Win2K application server software installation process must be performed again.

Installing Nortel Networks Global Server 3.3 base software on the UAS

At your console:

1 Perform the procedure, Installing OS and system software on a Win2K AS on page 81

2 Perform the procedure, Installing HAE software on a Win2K AS on page 85

3 Perform the procedure, Configuring Global Server base platform software on a Win2K AS on page 89

4 If you want to change the system password, perform the procedure, Setting the system password on page 91

5 You have completed this procedure.

Installing OS and system software on a Win2K AS

This procedure enables you to install Win2K OS and system software on a single Win2K application server host processor.

Before you start performing this procedure, it is important that you have satisfied the following requirements:

- the UAS SAM16 application server hardware has been properly configured. Refer to NTP 203-7009-201, *Hardware Installation Guide* for information about configuring SAM16 hardware.
- the CD-ROM entitled “Win2K: Win2K OS and System Software for CPV 5350, GS v3.3” or “Win2K: Win2K OS and System Software for CPV 5370, GS v3.3” is available
- you have identified the type SCSI adapter(s) PMC configured in your system

Installing OS and system software on a Win2K AS

At your console:

1 Prepare the SAM16 for the Win2K installation by turning the machine on.

> ***Note:*** This step needs to be performed only during a ground-up installation.

2 Restart the system by performing the following steps:

- **a** select **Start -> Shutdown**
- **b** Select “restart” in the Shutdown Windows screen.

  > ***Note:*** This step is applicable only if you are upgrading the system.

3 During the boot process, break into the BIOS menu using function key (F2) and change the BIOS settings for the processor card your system is equipped with.

> ***Note:*** Ensure that a CD is not present in the CD-ROM drive while you are checking the BIOS settings.

If your system is configured with	**Refer to**
CPV5350 card	“BIOS Settings for CPV5350 SCSI” in the document, NN10073-911, entitled “UAS Fault Management” in your UAS document suite
CPV5370 card	“BIOS Settings for CPV5370 SCSI” in the document, NN10073-911, entitled “UAS Fault Management “ in your UAS document suite

4 Insert the bootable CD-ROM, “Win2K: Win2K OS and System Software for CPV5350, GS v3.3” or “Win2K: Win2K OS and System Software for CPV5370, GS v3.3” into the CD-ROM drive of the domain (A or B) of the application server on which you are installing operating system software.

5 Exit the BIOS settings menu, saving changes by using the function key (F10).

6 Select “Yes” in the Setup Confirmation window that displays.

The system responds by automatically restarting and displaying the MS-DOS 6.2 Startup Menu.

> ***Note:*** If the MS-DOS 6.2 Startup Menu does not display, contact your next level of support.

7 At this point, the installation CD can continue unattended. Part or all of the hard drive will need to be reformatted, depending on the previous configuration. The system may reboot one or more times and continue automatically through the MS-DOS menu and, eventually, into the Ghost installation applications that install the Global Server OS and System Software.

> ***Note:*** If the hard drive has been used previously in a system that could not be shut down cleanly, as described in step 2, error messages may display. These messages should be ignored. Perform the following steps in response to the

messages, <u>but do not QUIT or restart the system until the Ghost installation has completed</u>.

- Select “OK” if the message, “NTFS ERROR: NTFS log file has not been flushed(fl=1). Restart NT then try again,” displays.
- Use the Tab and Enter keys to select “Continue” in the resulting pop-up window that displays, “NTFS Problem Detected: Ghost has detected problems with an NTFS partition. Recommend that you quit ghost and correct the problem by rebooting NT and running chkdsk. May also choose to continue normally, or perform a sector by sector copy of partition. QUIT; CONTINUE; SECTOR COPY.”

The installation will continue and install successfully.

8 The installation will take about 30 minutes, during which various status and progress messages will be issued to the console. At the end of the installation, the message, “Loading of system partition complete ...” will display. Remove the CD from the CD-ROM drive and then press the **Ctrl** - **Alt** - **Delete** key combination.

Note: The initial reboot of the Windows operating system will take slightly longer than usual; do not be concerned. After the system reboots, several status windows display as the installation proceeds. The installation will complete in approximately 5 minutes. Wait until all installation activity completes before making any keystrokes or mouse activity. Then, dismiss any new hardware wizard-related windows that display by clicking the “Cancel” button. DO NOT reboot the system at any point in this procedure. Dismiss any reboot pop-up windows by selecting “No”.

9 You have completed this procedure.

Installing HAE software on a Win2K AS

This procedure enables you to install HAE software on a single Win2K application server.

Before you start performing this procedure, it is important that the following information is available to you for the application server that is being installed:

- hostname
- IP address
- subnet mask
- default gateway address
- domain name (optional)
- Domain Name Server (DNS) IP addresses search order (optional)
- Domain Suffix addresses search order (optional)

Installing HAE software on a Win2K AS

At your console:

1 Double-click the green network card icon located in the right-hand corner of the task bar.

The system displays the Intel (R) ProSet II window.

2 In the left pane of the Intel (R) ProSet II window, right-click on the top network adapter.

3 Select **Add to Team -> Create New Team** from the drop-down menu.

The Teaming Wizard window displays.

4 Ensure that “Adapter Fault Tolerance” mode is selected, and then click Next.

5 Select both adapters, then click Next.

6 Observe the team configuration and click Finish.

The Intel (R) ProSet II window displays.

7 In the Intel (R) ProSet II window, right-click the first adapter, then click Preferred Primary.

8 In the Intel (R) ProSet II window, right-click the second adapter, then click Preferred Secondary.

9 Click OK.

10 On the host processor desktop, right-click the "My Network Places" icon and select Properties from the drop-down menu.

The Network and Dial-up Connections window displays.

11 In the Network and Dial-up Connections window, right-click Local Area Connection 3 and select Properties from the drop-down menu.

The Local Area Connection 3 Properties window displays.

12 In the Local Area Connection 3 Properties window, scroll to Internet Protocol and double-click Internet Protocol (TCP/IP).

The Internet Protocol TCP/IP Properties window displays.

13 In the Internet Protocol TCP/IP Properties window, select "Use the following IP addresses" and fill in all fields with the addresses previously obtained from the system administrator, including:

- IP address
- subnet mask
- default gateway address
- Domain Name Server (DNS) IP addresses search order (optional)
- Domain Suffix addresses search order (optional)

Note: You may need to click Advanced to set some optional settings.

a Click OK.

14 In the Local Area Connection 3 Properties window, click OK.

15 You may see the prompt, "This connection has empty primary WINS address - do you want to continue?" If this prompt displays, click Yes.

16 Close the Network and Dial-up Connection window.

17 Right-click the "My Computer" icon, and then select Properties from the drop-down menu.

The System Properties box displays.

18 Select the Network Identification tab, and then click Properties.

The Identification Changes window displays.

19 Enter the hostname of the host processor in the Computer Name field, then click More.

Note: Ensure that "Caps lock" on your PC is not "on."

The DNS Suffix and NetBIOS Computer Name window displays.

20 In the DNS Suffix and NetBIOS Computer Name window, enter the Primary DNS suffix and click OK.

The Identification Changes window displays.

21 In the Identification Changes window, click OK.

The Network Identification information dialog window displays.

22 In the Network Identification information dialog window, click OK.

23 In the System Properties box, click OK.

24 Click NO in the System Settings Change pop-up to reboot the computer with the new name and IP address.

25 You have completed this procedure.

Configuring Global Server base platform software on a Win2K AS

At your console:

1 Determine whether you are installing platform software on the “B” domain (right side) or on the “A” domain (left side).

If	Start with
you are configuring platform software on the B domain	step a
you are configuring platform software on the A domain	step b

a Using the Notepad tool, edit file “EventSrv.cfg” to contain EMS sub-system datafill by performing the following steps:

i `select` **`Start -> Run`**

ii Enter the following on a single line:

```
 Notepad
c:\GlobalServer\config\EventSrv.cfg
```

iii Change the data value for the EMSServerName key by entering the following:

```
EMSServerName mate_sc
```

> ***Note:*** Enter only a tab (using the tab key) between “EMSServerName” and “mate_sc.”

iv Save the file and close the Notepad window.

v Go to step b.

b Using the Notepad tool, edit the host file and add the IP address and host name (if any) associated with the peer and local domains by performing the following steps:

i `select` **`Start -> Run`**

ii Enter the following on a single line:

```
 Notepad
c:\winnt\system32\drivers\etc\hosts
```

iii Add the following two lines in the format shown:

```
<IP address> <hostname> mate_sc
```

where <IP address> is the IP address of the peer domain (opposite of your domain) and <hostname> is the hostname of the peer domain

```
<IP address> <hostname> local_sc
```

where <IP address> is the IP address of your local domain and <hostname> is the hostname of your local domain

iv Save the file and close the Notepad window.

2 Re-boot the system by performing the following steps:

a select **Start -> Shutdown**

b Select “restart” in the Shutdown Windows screen.

Note 1: If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

Note 2: If the system reboots when the UAS software is not yet installed and when telephony cards (CG6000, AG4000, PA200) are installed in the chassis, the “Found New Hardware Wizard” window will display. Press the Escape key to dismiss each instance of the display of this window.

3 You have completed this procedure.

Setting the system password

This optional procedure enables you to change the system password to ensure system security.

Setting the system password

At your console:

1 Select **Start -> Programs -> Administrative Tools -> Computer Management**

2 In the left pane of the Computer Management screen that displays, expand “Local Users and Groups.”

3 Select Users.

4 In the right pane of the “Users” screen, right-click Administrator.

5 Select “Set Password.”

6 In the Set Password window that displays, enter the new password and confirm your entry, and then click OK.

7 In the Local Users and Groups box that displays, click OK.

8 Close the Computer Management screen.

9 Perform the following steps to set the system password:

a `select` **`Start -> Run`**

b Enter the following:

```
Services.msc
```

The Services window displays.

10 In the Services window, right-click pmgrDaemon and select Properties.

The PMGRdaemon Properties (Local Computer) window displays.

11 In the PMGRdaemon Properties (Local Computer) window, select the Log On tab.

a Select “This account.”

b In the “account name” field, verify the entry or enter:

```
.\Administrator
```

c In the “password” and “confirm password” fields, enter the new password.

d Click OK.

The Microsoft Management Console dialog box displays.

12 To effect the change to the system password that you have made, log off by performing the following step:

`select` **`Start`** **->** **`Shutdown -> Log off`**

13 Log back in.

14 You have completed this procedure.

UAS08 to UAS07 or UAS06 software downgrade procedure

This procedure provides the steps required for downgrading (removing) the release UAS08 software and restoring the release UAS07 or UAS06 software.

> ***Note:*** The UAS is normally deployed on the network in pairs of systems, with two separate systems per chassis. The left-hand side of the chassis is designated as domain A. The right-hand side of the chassis is designated as domain B. If you are downgrading two domains on a chassis from release UAS08 to release UAS06, you must perform the downgrade on domain A first.

CAUTION

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

UAS08 to UAS07 or UAS06 software downgrade

At your console

1 Using the procedure "Changing the Admin state," in the document, NN10073-911, entitled "UAS Fault Management," set the administrative state for this UAS unit being downgraded to "lock graceful."

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

2 Using the APS Administration GUI procedure "Disabling provisioning of a UAS node," in the document, NN10095-511, entitled "UAS Configuration Management," disable audio provisioning for this UAS unit.

Audio distribution should be disabled for this UAS unit.

3 Remove the UAS08 software in the unit by performing the procedure, UAS08 application software removal on page 96.

> ***Note:*** Any configuration changes made while the UAS08 software was being installed will not be retained in the downgrade to UAS07. Instead, the UAS07 software will be installed with the configuration settings in effect at the time of the UAS07 installation.

4 If you are downgrading to release UAS07 or UAS06, downgrade the Global Server (GS) base platform software by performing the procedure, Downgrading Global Server base platform software on page 99.

5 If you are downgrading to release UAS06 and if the fabric type of your system is ATM-AAL2, remove the PA200 card and replace it with a BX4000c (S007) card by performing the procedure, Replacing a PA200 card with a BX4000c (S007) card on page 101.

6 If you are downgrading to release UAS06, perform the procedure, Disabling web browsers on page 104.

7 Restore the UAS06 or UAS07 configuration files, by performing the following steps:

a Open a command line interface at the UAS:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

b If you are downgrading to release UAS06, enter the following commands:

xcopy D:\UAS06restore\*.archive C:\Winnt\Temp /Y

Messages showing the files being copied display.

c If you are downgrading to release UAS07, enter the following commands:

xcopy D:\UAS07restore\*.archive C:\Winnt\Temp /Y

Messages showing the files being copied display.

d Close the command line interface.

8 If you are downgrading to release UAS06, install the UAS06 software, by performing the procedure, UAS06 application software installation on page 106.

9 If you are downgrading to release UAS07, install the UAS07 software by performing the procedure, UAS07 application software installation on page 126.

10 Enable audio distribution at the APS for this UAS unit by performing the following steps:

a Enable audio distribution at the APS for this UAS unit by performing the procedure “Enabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management.”

b Perform the procedure “Provisioning a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” to force immediate provisioning of any files created before the start of the downgrade.

11 Using the procedure “Viewing UAS performance measurements,” in the document, NN10139-711, entitled “UAS Performance Management,” verify that the UAS unit is enabled and is processing calls. In the procedure view, specifically, the performance measurements for the “Conferencing Service” and “IVR Service” components.

12 Update any remaining UAS units by performing this procedure for each unit.

13 You have completed this procedure.

UAS08 application software removal

This procedure enables you to remove existing UAS08 application software.

> ***Note:*** During this procedure, existing UAS configuration parameters are automatically saved before the configuration files containing these parameters are removed. Thus, these configuration parameters can then be restored during the installation process.

CAUTION

No remote access sessions (telnet, ftp) should be in progress on a unit from which application software is being removed.

UAS08 application software removal

At your console

1 Select the fabric type of your system, either IP or ATM.

If	Do
the UAS bearer fabric type is IP	step 3
the UAS bearer fabric type is ATM	step 2

2 Perform the following steps:

a Right-click My Computer and select “Properties.”

b In the System Properties window, click the Hardware tab and then select “Device Manager.”

c In the Device Manager window, click the plus (+) sign located at the left of “TDM/ATM bridge 2”.

d Right-click PA200 base board WDM and then select “Properties”.

e In the PA200 Base Board WDM Properties window that displays, select the Driver tab.

f In the Driver tab screen that displays, click Uninstall.

g In the Confirm Device Removal window that displays, click OK.

h In the “Systems Settings Change” pop-up window that displays, the system asks whether to restart the computer. Select “NO”.

i In the “Systems Settings Change” pop-up window that displays, the system indicates that the hardware settings have been changed and asks whether to restart the computer. Select “NO”.

j Close the Device Manager window (click X, located in the upper right-hand corner of the window).

k Close the System Properties window (click OK).

l Go to step 3.

3 Perform the following steps:

a select **Start -> Settings -> Control Panel**

b In the Control Panel window, double-click Add/Remove Programs.

c Determine whether you are removing patches in addition to the UAS software.

If	Do
you are removing patches in addition to the UAS software	step d
you are only removing the UAS software	step h

d In the Add/Remove Program Properties window, scroll down the list of software programs and select “Universal Audio Server patch to be removed”.

e Click Add/Remove.

f In all succeeding confirmation and status screens, click OK (or any equivalent positive response displayed).

g Perform steps d through f until all patches that display are removed.

Note: If you are prompted for a re-boot, respond “NO”.

h In the Add/Remove Program Properties window, scroll down the list of software programs and select Universal Audio Server.

i Click Change/Remove.

The “Welcome Modify, Repair, or Remove the Program” window of the InstallShield Wizard for UAS displays.

j Click Next.

> ***Note:*** The Remove button is the only functional option in this window and is selected by default.

The Confirm File Deletion screen displays and asks whether you wish to remove completely the selected application and all of its components.

4 Click OK.

The following InstallShield message windows display:

- *Stopping pmgrdaemon service*
- *Stopping SNMP services*
- *Removing SNMP subagents*
- *Stopping time service NTP Client*
- *Please wait while InstallShield removes and restores files*

In the Java WebStart uninstall confirmation message window that displays, click Next; then click OK in response to the “uninstall completed successfully” window that displays.

An InstallShield WIzard screen displays, indicating that maintenance is complete.

5 Ensure that the “Yes, I want to restart my computer now” option on the screen has been selected, and then click Finish.

The system performs a restart.

> ***Note:*** If the system reboots when the UAS software is not yet installed and when telephony cards (CG6000, AG4000, S007, PA200) are installed in the chassis, the “Found New Hardware Wizard” window will display. Press the Escape key to dismiss each instance of the display of this window.

6 You have completed this procedure.

Downgrading Global Server base platform software

This procedure enables you to remove existing Global Server base platform software and downgrade to release Global Server 3.2.

Downgrading Global Server base platform software

At your console

1 Insert the CD-ROM, “Global Server Platform Software, GS v3.3” into the CD-ROM drive of the domain (A or B) of the application server on which you are installing operating system software.

2 Select **Start -> Programs -> Accessories -> Command Prompt**

3 Determine whether you are downgrading to a UAS06 release or to a UAS07 release.

If	Start with
you are downgrading to a UAS06 release	step a
you are downgrading to a UAS07 release	step b

a Downgrade the software by entering the following command at the MS-DOS command prompt:

```
<cdrom>:\downgrade UAS06 <cdrom>:\
```

where *<cdrom>* is the letter of the CD-ROM drive on the application server. For example: **E:\downgrade UAS06 E:\**

Note 1: The software downgrade will take several minutes to complete.

Note 2: The black “cmd” window will be obscured during the installation of the Netscape third party software by a full-sized File Explorer Window. This will make it difficult to determine when the command processing has completed. It is more convenient to minimize this window during the installation and to dismiss it after the processing completes.

b Downgrade the software by entering the following command at the MS-DOS command prompt:

```
<cdrom>:\downgrade UAS07 <cdrom>:\
```

where *<cdrom>* is the letter of the CD-ROM drive on the application server. For example: **E:\downgrade UAS07 E:\**

> ***Note:*** The software downgrade will take several minutes to complete.

4 The downgrade of the platform reverts the Global Server Program Manager service password to its default value. It may be necessary at this point to synchronize passwords in order for the service to start properly.

If	Do
you have the default system password, “superuser”	step 8
you have changed the password	step 5

5 Perform the following steps to synchronize the Global Server Program Manager service, PMGR, with the system password:

a `select` **`Start -> Run`**

b Enter the following:

```
Services.msc
```

The Services window displays.

6 In the Services window, right-click pmgrDaemon and select Properties.

The PMGRdaemon Properties (Local Computer) window displays.

7 In the PMGRdaemon Properties (Local Computer) window, select the Log On tab.

a Select “This account.”

b In the “account name” field, verify the entry or enter:

```
.\Administrator
```

c In the “password” and “confirm password” fields, enter the new password.

d Click OK.

The Microsoft Management Console dialog box displays.

8 Remove the CD-ROM from the CD-ROM drive.

9 You have completed this procedure.

Replacing a PA200 card with a BX4000c (S007) card

This procedure enables you to downgrade from a PA200 card to a BX4000c (S007) card in ATM-AAL2 systems.

Replacing a PA200 card with a BX4000c (S007) 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.

DANGER
Laser radiation exposure
The exposed ends of fiber optic cables can emit harmful laser radiation. Do not look at the ends of fiber optic cables unless protector caps are in place. Disconnect all laser sources when personnel are working with fiber-optic cables.

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.

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

1 Stop any applications that may be running.

a Access the “Services” window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click **PMGRdaemon service** and select Stop. Wait for notification that the applications have stopped.

2 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.

3 Remove the PA200 card set by performing the following steps:

a Locate the R200 rear transition module at the rear of the chassis. The card will either be in slot 6 or in slot 11.

b Disconnect the OC3c interface cable from the rear R200 module. After the cable has been removed, cap the connectors on the module and on the fiber cable.

c Locate the PA200 card in the front of the chassis. The card will either be in slot 6 or in slot 11, according to the location of the R200 rear transition module.

d Remove both front and rear modules, in that order. (The screws that secure the modules in the slots must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

e Install filler plates to cover the slots from which the R200 rear transition module and PA200 card were removed.

4 Install the BX4000c card by performing the following steps:

a Remove the filler plate from the slot into which the BX4000c card will be installed. This will be slot 5 if the node is located in the left side of the shelf, or in slot 12 if the node is located on the right side of the shelf.

b Insert the BX4000c card in the front chassis slot. Lock the lock latches, and tighten the screws that secure the card in the shelf.

Note: There is no rear module for the BX4000c card.

c Remove the protective caps from the connectors on the BX4000c card and on the fiber cable. Connect the OC3c interface cable to the BX4000c card.

5 With an appropriate device, press the guarded reset switch located on the front panel of the CPV5370 Processor card that is associated with the domain in which the BX4000c card is being installed. The CPV5370 card is located in slot 7 for the left domain and in slot 9 for the right domain.

6 You have completed this procedure.

Disabling web browsers (UAS06)

This procedure enables you to disable the Windows Explorer and Netscape Navigator web browsers in order to enhance system operation. The procedure must be performed separately for each browser.

> ***Note:*** The steps presented in this procedure assume that you are operating using a right-hand mouse.

Disabling web browsers

At the system console (Windows desktop interface)

1 Using Windows Explorer (select **Start -> Programs -> Accessories -> Windows Explorer**).

2 In the Tools menu, select “Folder Options.”

3 Select the View tab and ensure that “Hide files extension for known file types” is not checked, and then click OK.

4 Locate either the “c:\Program Files\Internet Explorer\Iexplore.exe” file to disable Internet Explorer, or the “c:\Program Files\Netscape Communicator\Program\netscape.exe” file to disable Netscape Communicator.

5 After you have located the file, click on the file to select it and then right-click. In the pop-up window that displays, scroll the cursor down to “Properties” and then left-click “Properties”.

6 In the Properties pop-up window that displays, select the Security tab.

7 In the Permissions box in the Security panel, deny access for the groups, Administrators, Power Users, and Users by selecting each group, one at a time, and then selecting “Deny for Full Control”. After the selection has been made for all groups, click Apply.

8 When the Security change acknowledgment pop-up window displays, click Yes.

9 Click OK to close the Properties window.

10 Remove the desktop shortcuts to the web browser by performing the following steps:

- **a** Exit all applications to the Windows desktop.
- **b** On the Windows desktop, right-click on the shortcut for the browser (Internet Explorer or Netscape Communicator).

c In the pop-up window that displays, click Delete.

d In the deletion confirmation window that displays, click Yes.

11 If you have performed this procedure for both browsers, go on to step 12. If you have not performed this procedure for both browsers, perform steps 1 through 10 for the other browser.

12 You have completed this procedure.

UAS06 application software installation

This procedure enables you to install the UAS06 application software.

UAS06 application software installation

At your console

1 Close all applications.

2 Insert the UAS06 installation CD into the CD-ROM drive.

3 Launch the InstallShield Wizard for Universal Audio Server program by performing the following steps:

a select **Start -> Run**

b In the Run window, click Browse.

c In the Browse window, navigate to the file, *<cd-rom>*:\winnt\setup.exe, and click Open.

> ***Note:*** *<cd-rom>* is the “drive letter” assigned to the CD-ROM device.

The Welcome window for the InstallShield Wizard for Universal Audio Server displays.

d Click OK.

4 In the Welcome window for the InstallShield, click Next.

The Choose Node Type screen displays.

5 Select the appropriate gateway type, Gateway or Universal Audio Server (audio server).

If	Do
you chose Gateway	step 6
you chose Universal Audio Server	step 7

6 In the screen that displays, select “PRI” and then click Next.

a Go to step 11.

7 Select the bearer fabric type of your system, either IP or ATM.

If	Do
you chose IP	step 11
you chose ATM	step 8

8 Select the appropriate ATM bearer fabric type.

If	Do
the UAS bearer fabric type is ATM-AAL1	step 9
the UAS bearer fabric type is ATM-AAL2	step 10

9 In the InstallShield Wizard Complete screen, click Finish.

Note 1: Up to 60 seconds may pass before the InstallShield Wizard Complete screen first appears.

Note 2: If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

a Perform the following steps to install the PCI drivers:

i Right-click My computer, and then select “Properties.”

ii In the pop-up window that displays, select the Hardware tab and click Device Manager (located in the middle of the window).

iii In the Device Manager window that displays, right-click PCI Memory Controller (located under “Other devices” on the window) and select “Properties.”

iv In the PCI Memory Controller Properties window that displays, select the Driver tab and then click the Update Driver button.

v In the Upgrade Device Driver Wizard window that displays, click Next.

vi In the Install Hardware Device Drivers subscreen (of the Upgrade Device Driver Wizard window), the radio button, “Search for a suitable driver for my device” is selected by default. Click Next.

- **vii** In Locate Driver Files subscreen (of the Upgrade Device Driver Wizard window), deselect "Floppy disk driver" and "CD-ROM driver", then select "Specify a location" box, and, finally, click Next.
- **viii** In the Upgrade Device Driver Wizard pop-up window, type (or browse for) "c:\NMS_PA200\Pa200\system" in the "Copy manufacturer's files from" box, and then click OK.
- **ix** In the Driver Files Search Results subscreen (of the Upgrade Device Driver Wizard window), click Next.
- **x** In the Completing the Upgrade Device Driver Wizard subscreen (of the Upgrade Device Driver Wizard window), click Finish.
- **xi** In the PA200 Base Board WDM Properties window, click Close.
- **xii** Close the Device Manager window (click X, located in the upper right-hand corner of the window).
- **xiii** Close the System Properties window (click OK).

b Re-boot the system by performing the following steps:

- **i** select **Start -> Shutdown**
- **ii** select "restart the computer" in the Shutdown Windows screen.

c After the system re-boots, log back into the system as "administrator" (user name), and enter "superuser" as the password.

d Open a command line interface at the UAS:

- **i** select **Start -> Run**
- **ii** type **cmd** in the window that displays
- **iii** press Enter
- **iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications
- **v** press Enter
- **vi** If you are performing an upgrade and you do not want to change configuration file content, go to step 17, otherwise continue with the next step.

e Launch the Local Configuration Interface GUI by performing the following steps:

- **i** select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **lci** on the command line

Note: The first letter in the lci command is an “l”, as in “local.”

v press Enter

The Bearer Type ATM/AAL1 Local Configuration Interface GUI screen displays.

f Enter information for the following fields in the screen:

Note 1: Fields containing default data that cannot be changed appear in the color grey.

Note 2: When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2427).

- **Atm Companding Mode**

  This is the companding mode, either A-Law or Mu-Law.

- **Primary DBServer Host**

  This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the *system does not support its own APS, accept the default settings.*

- **Primary DBServer IP**

  This is the IP address of the APS that is hosting the database server used by this UAS node.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

g Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step h
you do not want to save the information	step k

h Click Apply.

i Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

j Go to step 12.

k Click Cancel.

The entries in the screen fields revert to the default values.

l Either return to step f and enter new information in the screen or go to step 12.

10 In the InstallShield Wizard Complete screen, click Finish.

Note 1: Up to 30 seconds may pass before the InstallShield Wizard Complete screen first appears.

Note 2: If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

a Perform the following steps to install the ArTeMux S007 drivers, protocol, and bindings:

i Right-click My computer, and then select “Properties.”

ii In the pop-up window that displays, select the Hardware tab and click Device Manager (located in the middle of the window).

iii In the Device Manager window that displays, right-click ATM Network Controller (located under “Other devices” on the window) and select “Properties.”

iv In the ATM Network Controller Properties pop-up window that displays, click the Reinstall Driver button, located at the bottom of the window.

v In the Upgrade Device Driver Wizard window that displays, click Next.

vi In the Install Hardware Device Drivers window that displays, select the radio button that asks to “Display a list of the known drivers for this device ...”, and then click Next.

vii In the Hardware Type window that displays, select “Network Adapters” and then click Next.

viii In the Select Network Adapter window that displays, click the Have Disk button, located below the list of network adapters in the window.

ix In the Install From Disk window that displays, you may either:

click the Browse button and then select **“**Open**”**

or

enter **c: \ArTeMux\Driver\s00x_W2K** to the left of the Browse button

x In the Install From Disk window that displays, click OK after the directory name appears correctly in the line next to the Browse button.

xi In the Select Network Adapter window that displays, choose (highlight) “ArTeMux s00x Adapter - Win2K” and then click Next.

xii In the Update Driver Warning pop-up window that displays, click Yes.

xiii In the Start Device Driver Installation window that displays, click Next.

A window that shows the progress of the installation displays for about 60 seconds.

xiv In the Update Device Driver Wizard window that displays, “Completing the Upgrade Device Driver Wizard” and lists the ArTeMux s00x Adapter - Win2K, click Finish.

xv In response to the query about restarting the computer that appears in the System Settings Change window, enter “No.”

xvi The Device Manager lists the network adapters, including the s00x adapter. Exit from the window by pressing the “X” located in the upper right corner of the window.

xvii In the System Properties window, click OK.

xviii Right-click the “My Network Places” icon, and select “Properties.”

xix When the four local area connections display, right-click the last (fourth) one, and select “Properties.”

xx Choose “Install” in the Local Area Connection 4 Properties window.

xxi In the Select Network Component Type window that displays, choose “Protocol” and click the Add ... button.

xxii In the Select Network Protocol window that displays, click the Have Disk ... button.

xxiii In the Install From Disk window that displays, you may either:

click the Browse button and then select **“**Open**”**

or

enter **c: \ArTeMux\Protocol\W2K** to the left of the Browse button

xxiv In the Install From Disk window that displays, click OK after the directory name appears correctly in the “Copy manufacturer’s files from:” field, located next to the Browse button.

xxv In the Select Network Protocol window that displays, choose (highlight) “ArTeMux Protocol Driver” and then click OK.

A file transfer progress window displays briefly.

xxviIn the Local Area Connection 4 Properties window, deselect (remove the check marks from) all protocols except the ArTeMux Protocol Driver, and then click Close.

xxviiRight-click the “My Network Places” icon, and select “Properties.”

xxviiiWhen the four local area connections display, right-click Local Area Connection 3, and select “Properties.” If checked, deselect the ArTeMux Protocol Driver from the components list. Click OK.

xxixFollowing the procedure outlined in steps xxvii and xxviii, ensure that for both the Local Area Connection 2 and Local Area Connection the ArTeMux Protocol Driver is <u>not</u> selected.

b Re-boot the system by performing the following steps:

i select **Start -> Shutdown**

ii select “restart the computer” in the Shutdown Windows screen.

c After the system re-boots, log back into the system as “administrator” (user name), and enter “superuser” as the password.

d Open a command line interface at the UAS:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

v press Enter

vi If you are performing an <u>upgrade</u> and you <u>do not</u> want to change configuration file content, go to step 17, otherwise continue with the next step.

e Launch the Local Configuration Interface GUI by performing the following steps:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **lci** on the command line

> ***Note:*** The first letter in the lci command is an “l”, as in “local.”

v press Enter

The Bearer Type ATM/AAL2 Local Configuration Interface GUI screen displays.

f Enter information for the following fields in the screen:

Note 1: Fields containing default data that cannot be changed appear in the color grey.

Note 2: When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2427).

- **Legacy Call Server**

  This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.

  > ***Note:*** If Legacy Call Server is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Call Server is Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **Audio Synch on Restart**

  For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled,

hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.

- **Atm Companding Mode**

  This is the companding mode, either A-Law or Mu-Law.

- **Primary Languag**e

  This is the primary language associated with the node.

  Note: A Primary Language is required only if the Legacy Call Server field is Enabled. If Legacy Call Server is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  This is the secondary language associated with the node.

  Note: A Secondary Language is required only if the Legacy Call Server field is Enabled. If Legacy Call Server is Disabled, then the Secondary Language field will also be Disabled.

- **Primary DBServer Host**

  This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, accept the default settings.

- **Primary DBServer IP**

  This is the IP address of the APS that is hosting the database server used by this UAS node.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

- **Gateway Control Protocol**

  This is the control protocol for the UAS, either H.248 or MGCP.

g Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step h

If	Do
you do not want to save the information	step k

h Click Apply.

i Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

j Go to step 12.

k Click Cancel.

The entries in the screen fields revert to the default values.

l Either return to step f and enter new information in the screen or go to step 12.

11 In the InstallShield Wizard Complete screen, which displays after a slight delay, select “Yes, I want to restart my computer now.” Click Finish.

Note 1: The system re-boot (restart) is required in order for the installation program to complete registry updates.

Note 2: If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

a After the system re-boots, log back into the system as “administrator” (user name), and enter “superuser” as the password.

b Open a command line interface at the UAS:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

v press Enter

vi If you are performing an upgrade and you do not want to change configuration file content, go to step 17, otherwise continue with the next step.

c Launch the Local Configuration Interface GUI by performing the following step:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **lci** on the command line

> ***Note:*** The first letter in the lci command is an “l”, as in “local.”

v press Enter

The Bearer Type IP Local Configuration Interface GUI screen displays.

d Enter information for the following fields in the screen:

> ***Note:*** When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes

can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2427).

- **Rtp Base Port**

  This is the number of base ports for the RTP stream, within the range 1024 through 63094.

  > ***Note:*** This must be an even number. In addition, commas must not be entered in the number.

- **Legacy Call Server**

  This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.

  > ***Note:*** If Legacy Call Server is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Call Server is Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **IVR Support**

  This field determines whether IVR support is enabled in this system.

- **Audio Synch on Restart**

  For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled,

hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.

- **Primary Languag**e

  This is the primary language associated with the node.

  > ***Note:*** A Primary Language is required only if the Legacy Call Server field is Enabled. If Legacy Call Server is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  This is the secondary language associated with the node.

  > ***Note:*** A Secondary Language is required only if the Legacy Call Server field is Enabled. If Legacy Call Server is Disabled, then the Secondary Language field will also be Disabled.

- **Conferencing State:**

  This field determines whether Conferencing is enabled in this node.

  > ***Note:*** If Conferencing State is Disabled, then the Conference Spanning field is also Disabled.

- **Conference Spanning**

  This field determines whether Conference Spanning is supported by the node.

  > ***Note:*** If “Conferencing State” is Disabled, then the Conference Spanning field is also Disabled.

- **Primary DBServer Host**

  This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the *system does not support its own APS, accept the default settings.*

- **Primary DBServer IP**

  This is the IP address of the APS that is hosting the database server used by this UAS node.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

- **Gateway Control Protocol**

  This is the control protocol for the UAS, either H.248 or MGCP.

  > ***Note:*** This field can be datafilled only for systems with bearer type IP and bearer type ATM-AAL2.

- **Force G711**

  This field indicates G.711 audio codec support.

  > ***Note:*** If Force G711 is Enabled, then the G729B field is Disabled.

- **G729B**

  This field indicates G.729B audio codec support.

e Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step f
you do not want to save the information	step i

f Click Apply.

g Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

h Go to step 12.

i Click Cancel.

The entries in the screen fields revert to the default values.

j Either return to step d and enter new information in the screen or go to step 12.

12 Determine whether SNMP management configuration parameters need to be changed.

If	Do
SNMP management configuration parameters need to be changed	step 13
SNMP management configuration parameters do not need to be changed	step 14

13 Click the “Reconfigure SNMP” button, located at the bottom of the Local Configuration Interface GUI screen.

The Local Configuration Interface GUI SNMP screen displays, showing default values delivered with the UAS06 system.

a Enter information for the following fields in the screen:

- **v2c read/write community**

  This is the SNMPv2c community name for read/write access through the SNMP-based management station.

- **v2c read only community**

  This is the SNMPv2c community name for read-only access through the SNMP-based management station.

- **v3 read/write use**r

  This is the SNMPv3 community name for read/write access through the SNMP-based management station.

- **v3 read only user**

  This is the SNMPv3 community name for read-only access through the SNMP-based management station.

- **trap version**

  This is the SNMP version of the SNMP traps sent by the UAS.

- **trap destination**

  This is the destination IP address associated with the remote SNMP management station. This is the destination IP address associated with the remote SNMP management station. This is the address to which SNMP traps are sent.

- **trap port**

  This is the UDP port associated with the remote SNMP management station.

b Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step c
you do not want to save the information	step f

c Click OK.

d Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

e Go to step 14.

f Click Cancel.

The entries in the screen fields revert to the default values.

g Either return to step 13 and enter new information in the screen fields or go to step 14.

14 Determine whether the bearer fabric of the UAS you are installing is ATM or IP.

If	Do
the bearer fabric type is IP	step 16
the bearer fabric type is ATM	step 15

15 Close the Local Configuration Interface GUI screens by selecting **File -> Exit**

a Go to step 17.

16 In the Topology pane of the Local Configuration Interface GUI screen, select the “Nodes” folder and then select the “Cards” folder, which is located in the Nodes folder.

The Local Configuration Interface GUI cards screen displays.

a Review the card list. The Card Type field will be set automatically to “CG6000C” if a card is present. The Card Type field will be set to “none” and the information detail field labels will be colored grey, if no card is present. Note the current configuration.

If	Do
If card information is not to be changed	step i
If card information is to be changed,	step b

b Double click the “Cards” folder, located in the Topology pane and, from the list of cards that displays below the Cards folder, click the bullet associated with a card to be changed. Enter information in the following fields in the dedicated card details screen that displays:

- IP address associated with each CG6000C card
- default router associated with each CG6000C card
- network mask associated with each CG6000C card
- Bearer Channel Tandeming (BCT) support capability for each CG6000C card, either Enabled or Disabled.

c For each card, determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step d
you do not want to save the information	step g

d Click Apply.

e Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI card detail screen) and select “Save”. Click OK when the confirmation screen displays.

f When you have finished updating the cards, go to step i.

g Click Cancel.

h Either return to step b and enter information for another card, or go to step i.

i Close the Local Configuration Interface GUI screens by selecting **File -> Exit**

17 If you are installing a PRI gateway, and if you are performing an upgrade, you should already have a valid “ugw.conf” file; go to step 18. If you are installing a PRI gateway, and if you are performing a ground-up installation, ftp a new ugw.conf file to c:\uas\etc. Contact UAS Product Design if you need a new ugw.conf file, then go to step 18.

> ***Note:*** This step is to be performed only if you are installing a PRI gateway. If you are not installing a PRI gateway, go to step 18.

18 This optional step validates configuration files and updates other configuration files. Any problems encountered will cause error messages to display in the command window. Note that this same action is performed upon the next application start-up.

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d Enter the following command in the window that displays:

```
ConfigMgr -install -v
```

e press Enter

19 This optional step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server. For additional information about this capability, see Automatic configuration file back-up on page 5. The following steps are performed on a remote Unix system.

a In a Unix shell, as Root user, enter:

```
cd /;mkdir /opt;chmod 777 opt

cd /opt;

mkdir uas;chmod 777 uas

cd uas;

mkdir uas_conf_backup;chmod 777
uas_conf_backup

cd /

cd /opt/uas/uas_conf_backup
```

b Configure NFS to share the “/opt/uas” filesystem and start the NFS server:

```
echo “share -F nfs /opt/uas” >>
/etc/dfs/dfstab
```

> ***Note:*** The commands from this point forward are specific for a Sun Solaris system.

```
/etc/init.d/nfs.server start
```

c Create a user login called “Administrator” that does not require a password:

```
/usr/sbin/useradd -d
/export/home/Administrator -g 1 -s /bin/ksh
-m -u 1002 Administrator 2> /dev/null
```

```
passwd -d Administrator 2> /dev/null
```

20 Start the application by performing the following steps:

a select **Start -> Run**

b enter **net start pmgrdaemon** in the window that displays

c press Enter

21 Inspect the UAS installation log file (UASinstLog.txt) for indications of any errors that may have occurred during the application software installation. The file is located in the c:\winnt\temp directory. If you find errors, contact your next level of support or your Nortel Networks service representative for assistance.

22 Refer to any existing UAS06 patch documentation and reapply any patches that had been previously applied to the UAS06 software now.

23 You have completed this procedure.

UAS07 application software installation

This procedure enables you to install the UAS07 application software.

UAS07 application software installation

At your console

1 Close all applications.

2 Insert the UAS07 installation CD into the CD-ROM drive.

3 Launch the InstallShield Wizard for Universal Audio Server program by performing the following steps:

a select **Start -> Run**

b In the Run window, click Browse.

c In the Browse window, navigate to the file, *<cd-rom>*:\winnt\setup.exe, select the file, and click Open.

> ***Note:*** *<cd-rom>* is the “drive letter” assigned to the CD-ROM device.

d Click OK.

The Welcome window for the InstallShield Wizard for Universal Audio Server displays.

4 In the Welcome window for the InstallShield, click Next.

The Choose Node Type screen displays.

5 Select the appropriate gateway type, Gateway or Universal Audio Server (audio server).

If	Do
you chose Gateway (in support of release IMS 1.0 or IMS 1.1)	step 6
you chose Universal Audio Server	step 8

6 Click Next.

7 In the screen that displays, select “PRI” and then click Next.

a Go to step 11.

8 Select the bearer fabric type of your system, either IP or ATM.

If	Do
you chose IP	step 11
you chose ATM	step 9

9 In the InstallShield Wizard Complete screen, click Finish.

Note 1: Up to 60 seconds may pass before the InstallShield Wizard Complete screen first appears.

Note 2: If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

10 Perform the following steps.

a Perform the following steps to install the PCI drivers:

i Right-click My computer, and then select “Properties.”

ii In the pop-up window that displays, select the Hardware tab and click Device Manager (located in the middle of the window).

iii In the Device Manager window that displays, right-click PCI Memory Controller (located under “TDM/ATM bridge 2” on the window) and select “Properties.”

Note: For ground-up installations, PCI Memory Controller will appear under “Other devices” on the window.

iv In the PCI Memory Controller Properties window that displays, select the Driver tab and then click the Update Driver button.

v In the Upgrade Device Driver Wizard window that displays, click Next.

vi In the Install Hardware Device Drivers subscreen (of the Upgrade Device Driver Wizard window), the radio button, “Search for a suitable driver for my device” is selected by default. Click Next.

vii In Locate Driver Files subscreen (of the Upgrade Device Driver Wizard window), deselect “Floppy disk driver” and

“CD-ROM driver”, then select “Specify a location” box, and, finally, click Next.

viii In the Upgrade Device Driver Wizard pop-up window, type (or browse for) “c:\NMS_PA200\Pa200\system” in the “Copy manufacturer’s files from” box, and then click OK.

ix In the Driver Files Search Results subscreen (of the Upgrade Device Driver Wizard window), click Next.

x In the Completing the Upgrade Device Driver Wizard subscreen (of the Upgrade Device Driver Wizard window), click Finish.

xi In the PA200 Base Board WDM Properties window, click Close.

xii Close the Device Manager window (click X, located in the upper right-hand corner of the window).

xiii Close the System Properties window (click OK).

b Re-boot the system by performing the following steps:

i select **Start -> Shutdown**

ii select “restart the computer” in the Shutdown Windows screen.

c After the system re-boots, log back into the system as “administrator” (user name), and enter either “superuser” as the password or the password supplied by your network administrator.

d Open a command line interface at the UAS:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

v press Enter

e Launch the Local Configuration Interface GUI by performing the following steps:

i select **Start -> Run**

ii type **cmd** in the window that displays

iii press Enter

iv type **lci** on the command line

Note: The first letter in the lci command is an "l", as in "local."

v press Enter

The main Local Configuration Interface GUI screen displays.

vi select the "nodes" folder in the Network Element Tree pane.

An ATM Local Configuration Interface GUI screen displays.

f Examine the Adaptation Layer heading on the screen and ensure that the appropriate screen for the ATM bearer fabric type of your system displays.

If	Do
the appropriate screen for the bearer fabric type displays	step h
the appropriate screen for the bearer fabric type does not display	step g

g Pull down the Adaptation Layer menu and select the appropriate bearer fabric type.

An ATM Local Configuration Interface GUI screen for your fabric type displays.

If	Do
your UAS bearer fabric type is ATM-AAL1	step i
your UAS bearer fabric type is ATM-AAL2	step k

h Determine whether the fabric type of your system is ATM-AAL1 or ATM-AAL2.

If	Do
your UAS bearer fabric type is ATM-AAL1	step i
your UAS bearer fabric type is ATM-AAL2	step k

i Verify and/or enter information for the following fields in the screen:

Note 1: Fields containing default data that cannot be changed appear in the color grey.

Note 2: When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2944).

- **UAS Call Control Port**

  This is the port associated with receiving the call control message stream (default is 2944).

- **Atm Companding Mode**

  This is the companding mode, either A-Law or Mu-Law.

- **Optical Carrier Mode**

  This field allows selection of the appropriate optical carrier standard for your ATM card, either SONET (a North American standard for optical carriers) or SDH (a European standard for optical carriers). The default for AAL1 systems is SONET.

- **IVR Support**

  This indicates whether IVR support is enabled on this system.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

- **ATM CTone Support**

This field, which must be datafilled when ATM BCT Support is ENABLED (ATM BCT Support is always ENABLED for an AAL1 system), determines how the audio endpoints for the ATM card are defined. The possible responses are: ENABLED or DISABLED.

- **NTP Server IP**

  This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.

  > ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

j Go to step l.

k Verify and/or enter information for the following fields in the screen:

> ***Note 1:*** Fields containing default data that cannot be changed appear in the color grey.
>
> ***Note 2:*** When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes

can be applied and saved until all entry errors in the screen are corrected.

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2944).

- **UAS Call Control Port**

  This is the port associated with receiving the call control message stream.

- **Gateway Control Protocol**

  This is the control protocol for the UAS, either H.248 or MGCP.

- **Atm Companding Mode**

  This is the companding mode, either A-Law or Mu-Law.

- **Optical Carrier Mode**

  This field allows selection of the appropriate optical carrier standard for your ATM card, either SONET (a North American standard for optical carriers) or SDH (a European standard for optical carriers). The default for AAL2 systems (including wireless systems) is SDH. If a North American AAL2 system is being configured, this field must be set to SONET.

- **Legacy Announcements**

  This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.

  > ***Note:*** If Legacy Announcements is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Announcements field is

Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **IVR Support**

  This field determines whether IVR support is enabled in this system.

- **Primary Languag**e

  This is the primary language associated with the node.

  Note: A Primary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  This is the secondary language associated with the node.

  Note: A Secondary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Secondary Language field will also be Disabled.

- **Audio Synch on Restart**

  For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled, hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.

- **Primary DBServer Host**

  This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, accept the default settings.

- **Primary DBServer IP**

  This is the IP address of the APS that is hosting the database server used by this UAS node.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

- **ATM BCT Support**

This indicates whether Bearer Channel Tandeming is supported on this system

- **ATM CTone Support**

  This field, which must be datafilled when ATM BCT Support is ENABLED, determines how the audio endpoints for the ATM card are defined. The possible responses are: ENABLED or DISABLED.

- **NTP Server IP**

  This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.

  > ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

l Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step m
you do not want to save the information	step p

m Click Apply.

n Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

o Go to step 12.

p Click Cancel.

The entries in the screen fields revert to the default values.

q Either return to step i (for the ATM-AAL1 fabric type) or step k (for the ATM-AAL2 fabric type) and enter new information in the screen, or go to step 12.

11 In the InstallShield Wizard Complete screen, which displays after a slight delay, select “Yes, I want to restart my computer now.” Click Finish.

> ***Note 1:*** The system re-boot (restart) is required in order for the installation program to complete registry updates.

Note 2: If a Service Control Manager pop-up window displays with the message, “At least one service or driver failed during system startup,” dismiss the message. The following description is available in the Microsoft SFU release notes:

Erroneous Event Viewer Message:

The Service Control Manager may display an event in the Event Viewer with the following message:

The NfsRdr service failed to start due to the following error: the system cannot find the file specified.

If this message appears, check to see if the nfsrdr service has started. If it has started, you can ignore the above event. If it has not started, use net start nfsrdr to start the nfsrdr service.

a After the system re-boots, log back into the system as “administrator” (user name), and enter either “superuser” as the password or the password supplied by your network administrator.

b Open a command line interface at the UAS:

- **i** select **Start -> Run**
- **ii** type **cmd** in the window that displays
- **iii** press Enter
- **iv** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications
- **v** press Enter

c Launch the Local Configuration Interface GUI by performing the following steps:

- **i** select **Start -> Run**
- **ii** type **cmd** in the window that displays
- **iii** press Enter
- **iv** type **lci** on the command line

  Note: The first letter in the lci command is an “l”, as in “local.”

- **v** press Enter

  The main Local Configuration Interface GUI screen displays.

- **vi** select the “nodes” folder in the Network Element Tree pane.

The Bearer Type IP Local Configuration Interface GUI screen displays.

d Verify and/or enter information for the following fields in the screen:

Note 1: When data is entered in an incorrect format in certain of these fields, the field label changes to a red color. When the data is then corrected in field, the field label changes back to black. None of the screen changes can be applied and saved until all entry errors in the screen are corrected.

Note 2: Ensure that the Gateway Control Protocol is set to H.248 and ensure that the UAS Call Control Port and

Primary Call Agent Port are set to the appropriate value (the UAS default is 2944).

- **Primary Call Agent Name**

  This is the computer name associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent IP Address**

  This is the IP address associated with the remote node that is hosting the Primary Call Agent application.

- **Primary Call Agent Port**

  This is the port of the Call Agent application (default is 2944).

- **UAS Call Control Port**

  This is the port associated with receiving the call control message stream (default is 2944).

- **Gateway Control Protocol**

  This is the control protocol for the UAS, either H.248 or MGCP.

  > ***Note:*** This field can be datafilled only for systems with bearer type IP and bearer type ATM-AAL2.

- **Rtp Base Port**

  This is the number of base ports for the RTP stream, within the range 1024 through 63094.

  > ***Note:*** This must be an even number. In addition, commas must not be entered in the number.

- **Legacy Announcements**

  This indicates that the UAS is used in a CS2K network, in a multilingual environment. The pull-down menu allows you to select either Enabled or Disabled.

  > ***Note:*** If Legacy Announcements is Enabled, then both a Primary Language and Secondary Language must also be entered. If the Legacy Announcements field is

Disabled, then both the Primary Language and the Secondary Language fields are Disabled.

- **IVR Support**

  This field determines whether IVR support is enabled in this system.

- **Primary Languag**e

  This is the primary language associated with the node.

  Note: A Primary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Primary Language field will also be Disabled.

- **Secondary Language**

  This is the secondary language associated with the node.

  Note: A Secondary Language is required only if the Legacy Announcements field is Enabled. If Legacy Announcements is Disabled, then the Secondary Language field will also be Disabled.

- **Conferencing State:**

  This field determines whether Conferencing is enabled in this node.

  Note: If Conferencing State is Disabled, then the Conference Spanning field is also Disabled.

- **Conference Spanning**

  This field determines whether Conference Spanning is supported by the node. Conference Spanning allows conferences with up to 64 participants.

  Note: If “Conferencing State” is Disabled, then the Conference Spanning field is also Disabled.

- **Audio Synch on Restart**

  For audio server applications of the UAS, this entry determines whether you want audio distribution refresh upon node startup, in addition to the regularly-scheduled,

hourly audio distribution. The pull-down menu allows you to select either Enabled or Disabled.

- **Primary DBServer Host**

  This is the hostname associated with the APS that is hosting the database server used by this UAS node. If the system does not support its own APS, accept the default settings.

- **Primary DBServer IP**

  This is the IP address of the APS that is hosting the database server used by this UAS node.

- **Backup Storage IP**

  This is the IP address of the database that will contain backup copies of the UAS configuration files. Datafilling this field is optional.

- **G729B**

  This field indicates G.729B audio codec support.

- **Default TOS**

  This field determines the Type of Service bit usage for this UAS. 0-255.

- **RFC2833 DTMF**

  This field indicates how the UAS will determine whether RFC2833 is enabled for each RTP connection. RFC2833 defines a method for passing DTMF digits "out-of-band" in special RTP packets, in order to provide more reliable DTMF recognition than is possible with low-bandwidth codecs. The possible selections include:

  — *AlwaysOff (RFC2833 support is always disabled, regardless of call control)*

  — *Negotiated (RFC2833 support is enabled per call control messaging, that is, SDP and/or LCO negotiation)*

- **RFC2833 DTMF Squelch**

  Not applicable

- **Tone set**

  This is the default tone set provided for the country that you select from the pull-down menu associated with this field.

- **NTP Server IP**

This is the IP address of the Network Time Protocol server on your network. The NTP server is used for synchronizing logs and alarms on the UAS.

> ***Note:*** The Windows time service queries the NTP server for time synchronization once every 24 hours. Therefore, a system time correction will occur only after the next time synchronization.

- **Supported Codec**

  These check boxes determine which codecs, G711, G723, G726, G729, and T.38 are supported. The following guidelines should be followed when you are selecting the codecs:

  — *T.38 is selectable only when at least one CG6000 card with BCT capability is installed in the system.*

  — *In an all-BCT system, all voice codecs should be disabled.*

  — *In a non-BCT system, up to a maximum of four voice codecs can be selected; the T.38 codec cannot be selected.*

  — *In a mixed system (BCT + IVR, BCT + Conf, BCT + IVR + Conf), up to a maximum of four of the codecs can be selected; one of the four codecs selected must be a voice codec.*

  — *It is recommended that you select G.711 for systems supporting conferencing service, to avoid any possible deterioration of voice quality.*

e Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step f
you do not want to save the information	step i

f Click Apply.

g Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

h Go to step 12.

i Click Cancel.

The entries in the screen fields revert to the default values.

j Either return to step d and enter new information in the screen or go to step 12.

12 Determine whether SNMP management configuration parameters need to be changed.

If	Do
SNMP management configuration parameters need to be changed	step 13
SNMP management configuration parameters do not need to be changed	step 14

13 Click the “Reconfigure SNMP” button, located at the bottom of the Local Configuration Interface GUI screen.

The Local Configuration Interface GUI SNMP screen displays, showing default values delivered with the UAS07 system.

a Enter information for the following fields in the screen:

- **v2c read/write community**

  This is the SNMPv2c community name for read/write access through the SNMP-based management station.

- **v2c read only community**

  This is the SNMPv2c community name for read-only access through the SNMP-based management station.

- **v3 read/write use**r

  This is the SNMPv3 community name for read/write access through the SNMP-based management station.

- **v3 read only user**

  This is the SNMPv3 community name for read-only access through the SNMP-based management station.

- **trap version**

  This is the SNMP version of the SNMP traps sent by the UAS.

- **trap destination**

This is the destination IP address associated with the remote SNMP management station. This is the address to which SNMP traps are sent.

- **trap port**

  This is the UDP port associated with the remote SNMP management station.

b Determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step c
you do not want to save the information	step f

c Click OK.

d Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save”. Click OK when the confirmation screen displays.

e Go to step 14.

f Click Cancel.

The entries in the screen fields revert to the default values.

g Either return to step a and enter new information in the screen fields or go to step 14.

14 Determine whether the bearer fabric of the UAS you are installing is ATM or IP.

If	Do
the bearer fabric type is IP	step 16
the bearer fabric type is ATM	step 15

15 Close the Local Configuration Interface GUI screens by selecting **File -> Exit**

a Go to step 17.

16 In the Topology pane of the Local Configuration Interface GUI screen, select the “Nodes” folder and then select the “Cards” folder, which is located in the Nodes folder.

The Local Configuration Interface GUI cards screen displays.

a Review the card list. The Card Type field will be set automatically to “CG6000C” if a card is present. The Card

Type field will be set to “none” and the information detail field labels will be colored grey, if no card is present. Note the current configuration.

If	Do
If card information is not to be changed	step i
If card information is to be changed,	step b

b Double click the “Cards” folder, located in the Topology pane and, from the list of cards that displays below the Cards folder, click the bullet associated with a card to be changed. Enter information in the following fields in the dedicated card details screen that displays:

- IP address associated with each CG6000C card
- default router associated with each CG6000C card
- network mask associated with each CG6000C card
- Bearer Channel Tandeming (BCT) support capability for each CG6000C card, either Enabled or Disabled.

c For each card, determine whether you want to save the information that you have entered.

If	Do
you want to save the information	step d
you do not want to save the information	step g

d Click Apply.

e Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI card detail screen) and select “Save”. Click OK when the confirmation screen displays.

f Go to step h.

g Click Cancel.

h Either return to step a and enter information for another card, or go to step i.

i Close the Local Configuration Interface GUI screens by selecting **File -> Exit**

17 If you are installing a PRI gateway, and if you are performing an upgrade, you should already have a valid “ugw.conf” file; go to step 18. If you are installing a PRI gateway, and if you are performing a ground-up installation, ftp a new ugw.conf file to c:\uas\etc. Contact UAS Product Design if you need a new ugw.conf file, then go to step 18.

18 This optional step validates configuration files and updates other configuration files. Any problems encountered will cause error messages to display in the command window. Note that this same action is performed upon the next application start-up.

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d Enter the following command in the window that displays:

```
configmgr -update -v
```

e press Enter

19 This optional step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server. For additional information about this capability, see UAS system configuration backup/restore strategy on page 5. The following steps are performed on a remote Unix system.

a In a Unix shell, as Root user, enter:

```
cd /;mkdir /opt;chmod 777 opt

cd /opt;

mkdir uas;chmod 777 uas

cd uas;

mkdir uas_conf_backup;chmod 777
uas_conf_backup

cd /

cd /opt/uas/uas_conf_backup
```

b Configure NFS to share the “/opt/uas” file system and start the NFS server:

```
echo “share -F nfs /opt/uas” >>
/etc/dfs/dfstab
```

> ***Note:*** The commands from this point forward are specific for a Sun Solaris system.

```
/etc/init.d/nfs.server start
```

c Create a user login called “Administrator” that does not require a password:

```
/usr/sbin/useradd -d
/export/home/Administrator -g 1 -s /bin/ksh
-m -u 1002 Administrator 2> /dev/null
```

```
passwd -d Administrator 2> /dev/null
```

20 Start the application by performing the following steps:

a select **Start -> Run**

b enter **net start pmgrdaemon** in the window that displays

c press Enter

21 Inspect the UAS installation log file (UASinstLog.txt) for indications of any errors that may have occurred during the application software installation. The file is located in the c:\winnt\temp directory. If you find errors, contact your next level of support or your Nortel Networks service representative for assistance.

22 Refer to any existing UAS07 patch documentation and reapply any patches that had been previously applied to the UAS07 software now.

23 You have completed this procedure.

The following procedure is performed in response to the display of the message, “ConfigMgr failed. See C:\WINNT\Temp\restoreLog.txt file for details” in a pop-up window, when the UAS07 software is being installed.

Handling a “ConfigMgr failed” error

At the system console (Windows desktop interface)

1 Using the Notepad tool, view file “restoreLog.txt” file by performing the following steps:

a select **`Start -> Run`**

b Enter the following on a single line:

```
Notepad c:\WINNT\Temp\restoreLog.txt
```

c Look in the file display for a message similar to the following: “Warning: number of cards in old config file (2) is not the same as the number of cards in the system (0).”

If	Do
you see such a message	step d
you don’t see this kind of message	step e

d Close the Notepad window and then go to step 2.

e Log the message and report the problem to your Nortel Networks service representative. Click Finish in the InstallShield Wizard Complete screen and abandon the UAS06 software installation until the problem can be corrected.

2 Open a command line interface at the UAS:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

e press Enter

3 Perform the procedure, Checking the status of AG4000 and CG6000 device drivers on page 152.

If	Do
entries for cards are missing from the list of NMS Telecomm Devices, indicating a possible problem with the Hot Swap Controller card	step 4
there are entries for all cards in the list of NMS Telecomm Devices, but problems are indicated with one or more devices	step 14

4 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.

5 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 Using a Phillips head screwdriver, loosen the screws that secure the card in the slot, and then unlock the lock latches.

Note: There is no rear transition module for this card.

b Slide the card out in the slot approximately one inch and then reseat the card in the slot. Lock the lock latches and then, using a Phillips head screwdriver, tighten the screws that secure the card in the slot. The node will reboot automatically upon insertion of the new card.

6 After the system finishes rebooting, open a command line interface at the UAS:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications

e press Enter

7 Perform the procedure, Checking the status of AG4000 and CG6000 device drivers on page 152.

If	Do
entries for cards are missing from the list of NMS Telecomm Devices, indicating a possible problem with the Hot Swap Controller card	step 8
there are entries for all cards in the list of NMS Telecomm Devices, but problems are indicated with one or more devices	step 14
the problem seems to have been corrected	step 17

8 Stop any applications that may be running.

a Access the “Services” window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

9 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.

10 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. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed.)

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.) The node will reboot automatically upon insertion of the new card.

11 After the system finishes rebooting, open a command line interface at the UAS:

- **a** select **Start -> Run**
- **b** type **cmd** in the window that displays
- **c** press Enter
- **d** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications
- **e** press Enter

12 Perform the procedure, Checking the status of AG4000 and CG6000 device drivers on page 152.

If	Do
entries for cards are missing from the list of NMS Telecomm Devices, indicating a possible problem with the Hot Swap Controller card	step 13
there are entries for all cards in the list of NMS Telecomm Devices, but problems are indicated with one or more devices	step 14
the problem seems to have been corrected	step 17

13 Contact your Nortel Networks service representative and abandon the installation until the problem is corrected.

14 Perform the procedure, Reinstalling an AG4000 or CG6000 device driver on page 153.

15 After the system finishes rebooting, open a command line interface at the UAS:

- **a** select **Start -> Run**
- **b** type **cmd** in the window that displays
- **c** press Enter
- **d** type **net stop pmgrdaemon** in the window that displays, to stop global server and UAS applications
- **e** press Enter

16 Perform the procedure, Checking the status of AG4000 and CG6000 device drivers on page 152.

If	Do
entries for cards are missing from the list of NMS Telecomm Devices, indicating a possible problem with the Hot Swap Controller card	Contact your Nortel Networks service representative and abandon the installation until the problem has been corrected.
there are entries for all cards in the list of NMS Telecomm Devices, but problems are indicated with one or more devices	Contact your Nortel Networks service representative and abandon the installation until the problem has been corrected.
the problem seems to have been corrected	step 18

17 Re-boot the system by performing the following steps:

a select **Start -> Shutdown**

b Select “restart” in the Shutdown Windows screen.

18 Stop any applications that may be running:

a Access the “Services” window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

19 Open a command line interface at the UAS:

a select **Start -> Run**

b type **cmd** in the window that displays

c press Enter

d type **configmgr -restore -v** in the window that displays

e press Enter

If	Do
the configmgr tool reports a “successful” completion status, and does not display a warning message	step 20
the configmgr tool does not report a “successful” completion message	Contact your Nortel Networks service representative and abandon the installation until the problem has been corrected.

20 You have completed this procedure. Return to the step in the procedure that you were performing when you were referred to this procedure.

Checking the status of AG4000 and CG6000 device drivers

This procedure enables you to determine the status of the AG4000 or CG6000 device drivers.

Checking the status of the AG4000 or CG6000 device drivers

At the system console (Windows desktop interface)

1 Right-click “My Computer” and then select “Properties”.

2 In the System Properties pop-up window that displays, select the Hardware tab.

3 Click the “Device Manager” button.

The Device Manager window opens.

4 Expand the “NMS Telecomm Devices” entry. In the expanded entry, you should see one NMS cPCI CG6000 entry for each CG6000 card provisioned in the system, and one NMS cPCI AG4000 entry for each AG4000 card provisioned in the system.

5 Examine the status of each card in the list, one at a time, by double-clicking the icon for a card.

An NMS cPCI <AG4000 or CG6000> Properties window displays.

If the device is operating normally, you will see in the Device Status panel the message, “This device is working properly.”

6 You have completed this procedure.

Reinstalling an AG4000 or CG6000 device driver

This procedure enables you to reinstall AG4000 or CG6000 device drivers.

Reinstalling an AG4000 or CG6000 device driver

At the system console (Windows desktop interface)

1 Right-click “My Computer” and then select “Properties”.

2 In the System Properties pop-up window that displays, select the Hardware tab.

3 Click the “Device Manager” button.

The Device Manager window opens.

4 Expand the “NMS Telecomm Devices” entry. In the expanded entry, you will see one NMS cPCI CG6000 entry for each CG6000 card provisioned in the system, and one NMS cPCI AG4000 entry for each AG4000 card provisioned in the system.

5 Double-click the icon associated with the card driver to be reinstalled.

An NMS cPCI <AG4000 or CG6000> Properties window displays.

6 Click the Driver tab and then click the “Update Driver” button.

7 In the Welcome screen that displays, click Next.

8 In the Install Hardware Device Drivers screen that displays, select “Search for a suitable driver for my device (recommended).”

9 In the Locate Driver Files screen that displays, click Next.

10 In the popup window that displays, click OK to select the default folder name, “C:\NMS\CG\Sys” for CG6000 cards, and “C:\NMS\AG\Sys” for AG4000 cards.

11 In the Driver Files Search Results window that displays, select “Install one of the other drivers” and then click Next.

12 In the Driver Files Found window that displays, the NMS cPCI CG6000 entry or the NMS cPCI AG4000 entry will already be selected. Click Next.

13 When the Completing the Upgrade Device Driver Wizard window displays, indicating that the driver has been installed, click Finish.

14 Either perform steps 5 through 13 for another driver, or proceed to step 15.

15 Re-boot the system by performing the following steps:

a select **Start -> Shutdown**

b Select “restart” in the Shutdown Windows screen.

16 You have completed this procedure.

UAS08 to UAS08 downgrade

This procedure enables you to perform a downgrade from release UAS08 to UAS08.

CAUTION

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

UAS08 to UAS08 downgrade

At your console

1 Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit being upgraded to “lock graceful”

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

2 Using the APS Administration GUI procedure “Disabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” disable audio provisioning for this UAS unit.

Audio distribution should be disabled for this UAS unit.

3 Remove the UAS08 software in the unit by performing the procedure, UAS08 application software removal on page 96.

4 Install the UAS08 software, by performing the procedure, UAS08 application software installation on page 37.

5 Enable audio distribution at the APS for this UAS unit by performing the following steps:

a Enable audio distribution at the APS for this UAS unit by performing the procedure “Enabling provisioning of a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management.”

b Perform the procedure “Provisioning a UAS node,” in the document, NN10095-511, entitled “UAS Configuration Management,” to force immediate provisioning of any files created before the start of the downgrade.

6 Using the procedure “Changing the Admin state,” in the document, NN10073-911, entitled “UAS Fault Management,” set the administrative state for this UAS unit to “unlocked.”

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

7 Using the procedure “Viewing UAS performance measurements,” in the document, NN10139-711, entitled “UAS Performance Management,” verify that the UAS unit is enabled and is processing calls. In the procedure view, specifically, the performance measurements for the “Conferencing Service” and “IVR Service” components.

8 Update any remaining UAS units by performing this procedure for each unit.

9 You have completed this procedure.

APS08 maintenance release process

After the APS08 software load is installed, “maintenance” releases are used to apply software fixes (corrections) for the load. A maintenance release consists of one or more SUN packages that replace one or more application files with newer versions and correct the software problem.

A maintenance release is delivered to a customer site on a CD. An APS08 software maintenance release CD contains the following two SUN packages:

- NTaps08.*xx-y.z*.pkg
- NORTips08.*xx.yy*.pkg

The following procedure provides you with the steps necessary to apply a patch to the APS08 software through the maintenance release process.

APS08 maintenance release process

At the system console (Windows desktop interface)

1 Log on as the “root” user.

2 If you wish to view information about the current APS load, enter the following command:

```
more /opt/uas/aps/conf/APSBuildStamp.txt
```

Information about the current load, including the date and time of installation, displays.

3 If you wish to view information about the SUN packages currently loaded on the APS, enter the following command:

```
pkginfo | grep aps
```

Information about the SUN packages installed on the APS displays.

4 Determine whether you are backing up the database and application files. In this procedure, the APS database and application files are left intact. Backing up the database is only a recommended precautionary measure.

If	Do
you are backing up the database and application files	step 5

If	Do
you are not backing up the database and application files	step 16

5 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) DAT tape into the 4mm DAT drive on the server, and then rewind the tape by entering the following command:

```
mt -f /dev/rmt/0 rewind
```

6 Initiate a backup of the database to the tape by entering the following command (on one command line):

```
ips_export_db.sh -t /dev/rmt/0
```

The system displays a log of activity as the database backup proceeds.

7 After the backup has completed, review the “export log” for any errors that may have occurred, by entering the following commands:

```
cd /APS_spool/ips_export
```

```
ls -l -t
```

The system displays a listing of files in the “ips_export” directory.

```
more export.log.x
```

where “*export.log.x*” is the name of the most recent log file. To determine the most recent log file, look at the time stamps associated with the listing that results from the “ls -l -t” command.

The system displays the log messages in the “export.log.x” file.

8 Rewind the backup tape by performing the following command:

```
mt -f /dev/rmt/0 rewind
```

9 List the contents of the tape by entering the following command:

```
tar -tvf /dev/rmt/0 | more
```

The system displays a listing of the tape contents. You should review this listing to ensure that all of the files were backed up.

10 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen), to prevent the data on the tape from being accidentally over-written. The tape should be stored for use later.

11 Insert another write-enabled (white or grey tab is moved to the right where it can be seen) DAT tape into the 4mm DAT drive on the server, and then rewind the tape by entering the following command:

```
mt -f /dev/rmt/0 rewind
```

12 Enter the following commands to back up the APS file systems:

```
cd /
```

```
tar -cvf /dev/rmt/0c /PROV_data /audio_files
/user_audio_files (this command is entered on
one command line)
```

> ***Note:*** When entering the command, you must ensure that a space is placed between the files, "/PROV_data" and "/audio_files", between "/audio_files" and "/user_audio_files", and between "/user_audio_files" and "/etc/inet/hosts/.rhosts"

13 Rewind the backup tape by performing the following command:

```
mt -f /dev/rmt/0c rewind
```

14 List the contents of the tape by entering the following command:

```
tar -tvf /dev/rmt/0c | more
```

The system displays a listing of the tape contents. You should review this listing to ensure that all of the files were backed up.

15 Eject the backup tape, label it, and move the write-enable tab to the "read-only" position (white or grey tab is moved to the left where it cannot be seen), to prevent the data on the tape from being accidentally over-written. The tape should be stored for use later.

16 Insert the APS08 software maintenance release CD into the CD-ROM drive.

17 Enter the following command to ensure that the CD has been properly mounted:

```
df
```

In the list that displays, you should see the entry "/cdrom/*<xxx>*/", where *<xxx>* is the CD volume label name.

18 List the contents of the maintenance CD by entering the following command:

```
ls -l /cdrom/<xxx>/*
```

where "/cdrom/*<xxx>*/" is the CD volume label name that you listed in step 17.

19 Copy the contents of the CD to the APS root disk by entering the following command:

```
cp /cdrom/<xxx>/* /
```

20 Look for a text file labeled "README" on the CD (check the CD contents listing that you created in step 18) or for instructions on paper supplied with the CD.

If	Do
instructions were supplied either on the CD or on paper	read and follow the instructions, and then go to step 26
instructions were not supplied	step 21

21 Apply the SUN packages containing the APS08 maintenance software patch by entering the following commands:

```
pkgadd -d NTaps08.xx-y.z.pkg
```

where *NTaps08.xx-y.z.pkg* is one of the package labels listed on the CD (check the CD contents listing that you created in step 18)

```
pkgadd -d NORTips08.xx.yy.pkg
```

where *NORTips08.xx.yy.pkg* is one of the package labels listed on the CD (check the CD contents listing that you created in step 18)

22 If you wish to list the packages that you have installed, enter the following command:

```
pkginfo | grep aps
```

23 Run the APS installer script, to reapply any changed DB triggers or database scripts on the load, by entering the following commands:

```
cd /
./start.sh 2>&1 | tee /startinstall.log
```

24 Verify the new APS load build number in the listing generated by entering the following command:

```
more /opt/uas/aps/conf/APSBuildStamp.txt
```

25 If necessary, configure the APS SNMP agent by performing the procedure "Configuring the SNMP agent" located in the document, NN10095-511, entitled "UAS Configuration Management."

26 You have completed this procedure. You should be able to log in to the APS GUI within approximately five minutes.