CS 2000 Management Tools Basics

CS 2000 Management Tools refers to a collection of software packages that contain a set of tools used to manage elements and sub-elements in a Succession network. This set of tools can run on a single server, multiple servers, or be split to run on different servers. Deployment depends on the size of the network being managed, and the customer's operational needs and preferences.

> ***Note:*** The server on which the CS 2000 Management Tools software packages reside is referred to as the CS 2000 Management Tools server in the remainder of the documentation.

For a list of activities that are new for CS 2000 Management Tools in the SN06.2 release, see What's new for the CS 2000 Management Tools.

Software

The CS 2000 Management Tools are delivered in three software packages:

- CS2M (Call Server 2000 Management)
- APS (Audio Provisioning Server)
- SSPFS (Succession Server Platform Foundation)

CS2M

The CS2M (CS 2000 Management Components) software package consists of the following packages:

- the SESM (Succession Element and Sub-Element Manager) software package, which consists of the following applications:
    - CS2000 Management Tools, which includes the following components:
        - CS 2000 GWC Manager
        - Universal Audio Server Manager
        - Audio Provisioning Server Manager application
        - V5.2 Configuration and Maintenance applications (international version only)
        - V5.2 data integrity audit (international version only)
        - Line data integrity audit
        - Trunk data integrity audit
        - CS2K data integrity audit
        - Nodes Configuration
        - Trunks Configuration
        - Carrier Endpoint Configuration
    - Trunk Maintenance Manager (TMM)
    - Line Maintenance Manager (LMM)
    - Batch provisioning tool (BPT)
    - Batch Configuration Monitor
    - Lines Configuration (Servord+)
    - Line Test Manager (LTM)
    - ADSL flowthrough provisioning
    - OSSGate
    - Media Server 2000 Series Configuration Tool

- the NPM (Network Patch Manager) software package, which consists of the patch management application for the CS 2000 Gateway Controller (GWC), Media Gateway 9000 (MG 9000), Media Gateway 9000 Manager (MG 9000 Manager), CS 2000 SAM21 Element Manager (SAM21 EM), Succession Element and Sub-network Manager (SESM), Patching Server Element (PSE), and the NPM itself.
- the SAM21 EM (CS 2000 SAM21 Manager) software package, which consists of the CS 2000 SAM21 Manager application for the SAM21 shelf controller.
- the QCA (QoS Collector application) software package, which consists of the QoS collector application for QoS records sent from the GWC.

APS

The APS (Audio Provisioning Server) software package consists of the APS application, which enables the carrier to provision announcements on the Universal Audio Server (UAS). Refer to the UAS documentation suite for more information.

SSPFS

The Succession Server Platform Foundation Software (SSPFS) package consists of the base operating system and third-party application tools. Service applications provided in the main package are Resource monitor, Service application monitor (servman), and EMS proxy services. Sub-packages such as the PM poller and the OMPUSH application are included as separate packages.

The Service application monitor (servman) is used to register, deregister and query the state of applications on the server where the SSPFS resides. Applications register with servman during package install, and deregister during package removal.

Oracle is the common database for the applications on the CS 2000 Management Tools server.

Hardware

The CS 2000 Management Tools software packages are installed on a Sun Netra t1400 or Sun Netra 240 server from SUN Microsystems.

> ***Note:*** In SN06.2, only new installations will use the Netra 240.

Hardware for client workstations is provided under Client workstation requirements.

User interfaces

Following is a list of the applications available on the CS 2000 Management Tools server and their user interface. For more information, refer to the description of the corresponding application in this document.

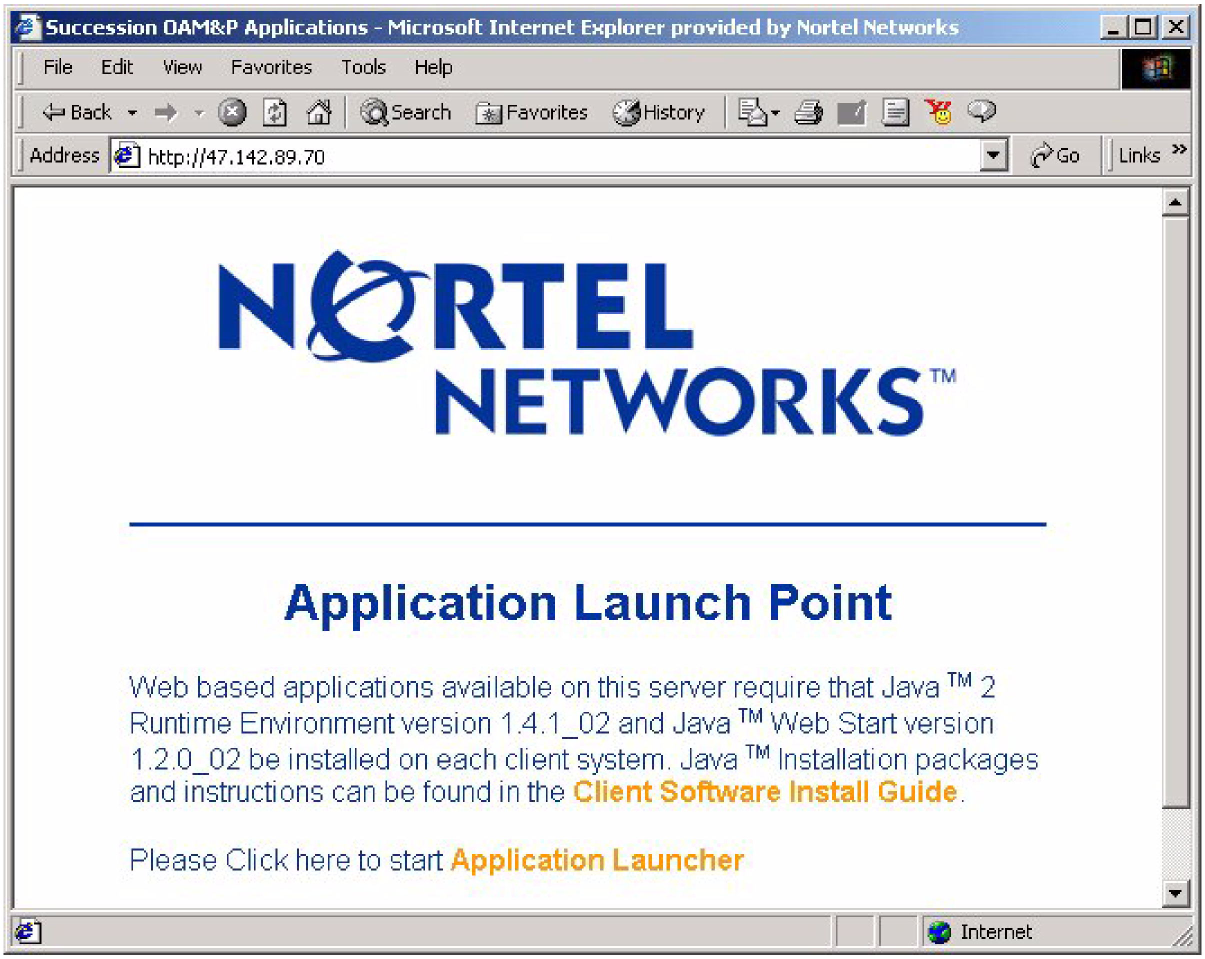
- Batch Provisioning Tool (BPT) - command line user interface (CLUI)
- Batch Configuration Monitor- web browser interface
- Line Maintenance Manager (LMM) - graphical user interface (GUI)
- Trunk Maintenance Manager (TMM) - web browser interface
- Network Patch Manager (NPM) - GUI and CLUI
- CS2000 Management Tools (includes CS 2000 GWC Manager, UAS Manager, APS Manager, V5.2 Configuration and Maintenance, Alarm Manager, and Audit System components) - GUI
- CS 2000 SAM21 Manager - GUI
- PM poller - CLUI
- OMPUSH - CLUI

The user interface for the Batch Configuration Monitor, LMM, TMM, NPM (GUI), CS2000 Management Tools, and CS 2000 SAM21 Manager are accessed through a common launch page.

Common launch page

The launch page is accessible from a Windows or a Sun client workstation using the Internet Explorer or Netscape browser. Entering the IP address or hostname of the CS 2000 Management Tools server in the address field of the browser, launches the Application Launch Point page shown in the illustration that follows.

Application Launch Point page



Succession OAM&P Applications - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47.142.89.70
Go Links
NORTEL NETWORKS
Internet

Application Launch Point

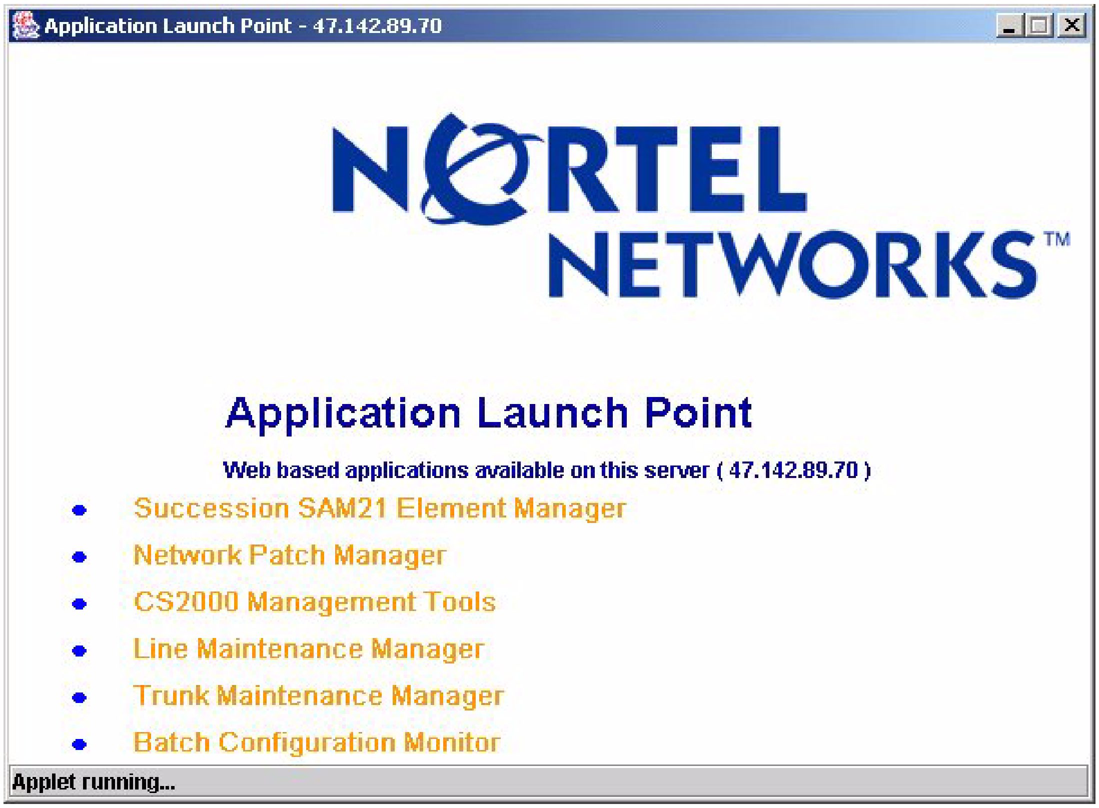
Web based applications available on this server require that Java TM 2 Runtime Environment version 1.4.1_02 and Java TM Web Start version 1.2.0_02 be installed on each client system. Java TM Installation packages and instructions can be found in the Client Software Install Guide.

Please Click here to start Application Launcher

As indicated on the Application Launch Point page, Java TM 2 Runtime Environment (JRE) version 1.4.1_02 and Java TM Web Start (JWS) version 1.2.0_02 must be installed. If an older version of JWS and JRE is installed, an error message will be displayed when you click on the Application Launcher page. The “Client Software Install Guide” link on the Application Launch Point page, provides instructions on how to verify the version, and provides the installation packages and instructions, if required.

Clicking the “Application Launcher” link displays the applications that are installed and configured on the CS 2000 Management Tools server. For example, installing the CS2M software package, provides links to all the applications shown in the illustration that follows, Application Launch Point.

Application Launch Point



Application Launch Point - 47.142.89.70

NORTEL NETWORKS™

Application Launch Point

Web based applications available on this server (47.142.89.70)

- Succession SAM21 Element Manager
- Network Patch Manager
- CS2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- Batch Configuration Monitor

Applet running...

> ***Note:*** You need to configure the Patching Server Element (PSE) to launch the Network Patch Manager. Refer to procedure “Configuring the Patching Server Element” in the CS 2000 Management Tools Configuration Management document, NN10106-511. No manual configuration is necessary to launch the other applications.

To launch client applications, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

The table titled Application to solution mapping, lists the applications that can be launched from the Application Launch Point, and indicates for each application, whether it is supported for a specific Succession Solution.

Application to solution mapping

Application	PT-AAL1 NA	PT-AAL2 Int'l	PT-IP NA	PT-IP Int'l	UA-AAL1 NA	UA-IP NA	UA-IP Int'l	IAC	IA-IP	IAW
Trunk Maintenance Manager	n	n	y	y	n	y	y	y	y	y
CS2000 Management Tools	n	y	y	y	y	y	y	y	y	y
Line Maintenance Manager	n	n	n	n	n	n	n	y	y	y
Batch Configuration Monitor	n	n	n	n	y	y	y	n	n	n
CS2000 SAM21 Manager	n	y	y	y	y	y	y	y	y	y
Succession Audio Provisioning Server Manager	n	y	y	y	n	y	y	y	y	y
n = not supported y = supported										

Client workstation requirements

The operating systems (O/S) supported to run the CS 2000 Management Tools client applications are as follows:

- Windows 2000, NT, and XP
- Solaris 2.7 and later

Note: The functionality of the client applications is the same on a Windows and Solaris O/S, but the appearance of the screens is different.

The supported browsers are as follows:

- Netscape 6.1 and later (Windows and Solaris)
- Internet Explorer 5.5 and later (Windows only)

ATTENTION
For Netscape 7 users on Solaris 2.7 platform, it is necessary that you have the path to the Netscape executable defined in your system $PATH variable. If it is not defined, you will not be able to launch theTrunk Maintenance Manager, or the Batch Configuration Monitor client applications. Contact your system administrator for assistance if required.

ATTENTION
It is important that your memory cache be large enough to keep large search result pages in memory. Therefore, ensure that your cache is set to a minimum of 1024 KB. For Netscape users, you can set your cache under Edit->Preferences->Advanced->Cache. For IE users, you can set your cache under Tools->Internet Options->General->Temporary Internet files->Settings.

Nortel Networks has explicitly tested the following versions:

- Windows: Netscape 6.2.3 and 7.0, Internet Explorer 5.5 SP2, 6.0, and 6.1 SP1
- Solaris: Netscape 6.2.3 and 7.0

Note 1: Nortel Networks recommends the use of Nortel-verified browser and operating system combinations. Use of other versions are supported. Any compatiblity issues will be resolved using standard Nortel support processes.

Note 2: Ensure Solaris clients, using Java^{TM} Web Start (JWS), have font package SUNWi1of installed. This font package ensures correct GUI (graphical user interface) display on Solaris clients. You can view font package requirements for Solaris as follows: http://<host>/client/solaris/font-requirements.html.

Access to some functions of the CS 2000 Management Tools requires the use of SSH-compatible client software for access to secure telnet and ftp services through the SSH standards. SSH clients are supplied bundled with some operating systems, but may need to be obtained separately. Following are some sources for SSH clients:

- PUTTY - freeware
- OpenSSH - freeware
- SSH Inc.- commercial
- Secure CRT- commercial
- WinSCP - freeware

Note: Nortel Networks does not supply or recommend a particular supplier.

Minimum hardware

The minimum hardware for Windows clients is as follows:

- Monitor size: 19 in.
- Resolution: 1280x1024 with 256 colors
- Hard disk space: 10GB (500MB free space for all clients per switch)
- Processor: Pentium III 1.4GHz or higher
- RAM requirements: 1GB
- Network: 10/100Base-T Ethernet network connection

The minimum hardware for Solaris clients is as follows:

- Resolution: 1280x1024 with 256 colors
- Hard disk space: 200MB
- Processor: Ultra 10 400MHz or higher
- RAM requirements: 256MB
- Network: 10B/100Base-T Ethernet network connection

Only PCs with a single network interface card (NIC) can run the Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS 2000 SAM21 Manager client software.

What’s new for the CS 2000 Management Tools

What’s new in SN06.2

The following is a list of activities that are new for CS 2000 Management Tools in the SN06.2 release:

A00001953 - SSPFS/SDM base integration phase I

This activity provides the framework to abstract functionality so that applications that run on the current SSPFS platform and the SDM AIX platform can run on a single SSPFS platform, and includes

- consolidation of common platform capabilities
- product specific installation (prompt for SESM, MG9K, or SDM)
- application monitor - servman
- resource monitor (fan RPM, disk failure, power supply failure, high temperature, NIC failure and file system usage)

A00001954 - Sun N240 introduction for CS2M

This activity introduces the Sun Netra 240 as supported hardware for the Succession Server Platform Foundation Software (SSFPS) and the Operations, Administration, and Maintenance applications that run on the Succession Server Platform Foundation Sofware (SSFPS).

A00001955 - High availability support for N240

This activity introduces the UpSuite High Availability (HA) software included with the Succession Server Platform Foundation software (SSPFS).

A00002152 - Small gateway status query and reachability test from LMM

This activity provides the following enhancements to the Line Maintenance Manager (LMM) graphical user interface (GUI):

- introduces the capability to query gateways in trouble state and configure the date and time of a query from the LMM GUI
- changes the heading in column “Enpoint State” to “Enpoint State/Communication Error” in the LMM GUI
- adds states “on-hook”, “off-hook’, “dial tone”, “ringing”, and “cpb” to the information for posted endpoints following an endpoint audit that the LMM performs

A00002205 - SAM21 Manager authorization

This activity implements authorization to the CS 2000 SAM21 Manager client application on a function basis, which allows the actions of users to be restricted based on the user groups they belong to.

A00002384 - OM push application

This activity introduces the OMPUSH application, which is used to transfer the following OM files to predefined remote servers using FTP or SFTP:

- MG 9000 OM files, which are generated by the MG 9000 OM Collector
- SSPFS, GWC, UAS, and SAM21 SC OM files, which are collected by the SNMP PM Poller.

A00002677 - NPM robustness

This activity provides users with the following capabilities using the Network Patch Manager (NPM):

- priority processing of patching maintenance requests
- simultaneous execution of specified patching maintenance requests
- forwarding of customer logs and alarms to OSS interface
- definition of multiple plans in addition to the existing “SYSTEMPLAN”
- automatic restart of OAM devices when necessary

Note: With this feature, the NPM server application needs to be started manually after an upgrade.

A00002875 - Oracle 9i Enterprise introduction to SSPFS

This activity introduces the Oracle 9i Enterprise Edition with the Succession Server Platform Foundation Software (SSPFS).

A00003004 - AMS OAM, PM Poller, Faults, and Configuration

This feature supports OAM integration changes to replace the SAM16 Universal Audio Server with the Media Server 2000 Series (MS 2000 Series). MS 2000 Series supports VoIP only in this release.

Depending on the package purchased, combinations of the following services are available:

- Conferencing
- IVR (announcement and digit collection)
- Test Trunks
- Lawful Intercept

A00003229 - Enable QCA patching

This activity enables NPM to provide fix patching to QCA. The following restrictions apply to the QCA as a device that can be patched by the NPM:

- QCA devices are not included in the set of OAM devices that can be auto-restarted, nor can a QCA restart be included in any plans scheduled at a designated time. Only manual restart of a QCA device is supported.
- Only one QCA can be started at one time. The multitasking capability of the NPM is not used for QCA.

A warning is dislayed to the user by the NPM CLUI or GUI explaining the implications of restarting QCA. The user will be forced to choose between continuing with the restart or canceling.

A00003589 - Converting authentication interface among MI-2, SAM21 Manger, and MG 9000 Manager applications

This activity changes the way users access the CS 2000 Management Tools client applications.

Succession Server Platform Foundation Software (SSPFS)

Overview

The Succession Server Platform foundation software (SSPFS) is a high-performance, UNIX-based processing platform based on Sun Microsystem's Netra line of NEBS compliant servers.

The SSPFS platform is intended to be used as the platform for OAM&P services in the Succession Network. These services include, but are not limited to the various Element Management systems for the Network Elements.

Process Management

SSPFS platform process management performs the following functions:

- starts applications at boot up
- closes all applications at shutdown
- monitors applications to determine their condition
- restarts applications that fail

Data reliability software

The following features ensure reliable and continuous data storage:

- a journalled file system - confirms the accuracy of the resident file system after accidental shut down and power failure.
- logical volume partitioning - the SSPFS platform supports partitioning of disks into different logical volumes. Each logical volume can be considered an enforced partition of disk resources. Logical volume partitioning protects data and programs from exhaustion of their space by one or more processes.
- disk mirroring - the SSPFS platform stores a copy of all data that is written to logical volume. In the event of a disk failure, the system can read from and write to the remaining disk without interruption.

Third party common software

The SSPFS third party software is contained in SSPFS through the use of Sun packages. This provides a consistent way of delivering all of the Solaris software, third party software and Nortel applications. By using the same software packaging scheme, installing applications is consistent for all OAM&P products that make use of the SSPFS platform.

The following table lists the third party software that is included with the SSPFS:

> ***Note:*** This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at http://OSS.software.ibm.com/icu4j/.

Software included with SSPFS

Vendor	Software
Sun Microsystems	• Solaris 8 Software OS • JDK/JRE • JAXP • Java JSSE • Java Web Start Client
AdventNet	• SNMP API
Apache	• Apache Web Server • Xerces Java Parser • Xalan
IBM	• DCE Client
Exolab group	• OpenORB notification • OpenORB Naming Service
GNU	• Java FTP Client
Jakarta	• Tomcat • ORO • Log4J

Software included with SSPFS

Vendor	Software
Open Source	• OpenSSH • OpenSSL • Java FTP client
ProFTPD	• proftpd
SourceForge.net	• Expat
Oracle	• Oracle client • Oracle server
--	• bootpd
Continuous Computing Corporation	• UpSuite
--	• Net-snmp
--	• tcl
--	• rotatelog
--	• xalan
--	• syslog client
--	• perl
DeleGate	• DeleGate
NIST	• Expect
ILOG	• JTGO • JViews

System and database backup

SSPFS lets you backup and restore the system and database. The information is backed up on a Digital Audio Tape (DAT) or a DVD-RW.

System backup

Applications and the system have several sets of configuration files with static information about the system configuration and operating parameters. This information is backed up in-service using standard Unix commands and a Solaris 8 feature called SNAPFS which takes a snapshot of the file system.

The file system layout for SSPFS-installed machines is as follows:

> ***Note:*** File systems “/”, “/var”, “/data”, “/opt”, and “/opt/nortel” are available on every system. The other file systems vary according to the applications installed on the system.

File system	Types of information stored in file system
/	operating system software and administrations
/var	operating system software and administrations
/data	application data in flat files
/opt	third-party software as Platform common services
/opt/nortel	Nortel applications
/data/oradata	Oracle data files (only present with the CS2M and APS)
/data/qca	QoS Collector Application (QCA) data (only present with the CS2M)
/data/mg9kem/logs	MG 9000 Manager logs (only present with MG 9000 Manager)
/PROV_data	audio transaction files before they are sent to the UAS (only present with APS)
/user_audio files	audio uploaded from the user desktop prior to its import into the database (only present with APS)
/audio_files	audio data that has been imported into the database (only present with APS)

Database backup

The Oracle database includes its own utilities to perform live backup and restore of the database. The database information is maintained on a Digital Audit Tape (DAT) or Digital Video Disk-Re-Writable (DVD-RW).

Backup schedules and recommended policies

This section contains backup schedules and recommended policies.

Application data in the Oracle database

The application data in the Oracle database is not automatically backed up. You can enable automated Oracle data backups, where the system backs up all application data in the Oracle database on a daily basis at a specified time to a DAT or DVD-RW. Refer to procedure “Configuring automated Oracle data backups” in the CS 2000 Management Tools Configuration Management document, NN10106-511.

Data on a DVD cannot be overwritten, therefore, you must insert a blank DVD prior to the next scheduled backup.

If you leave the same DAT in the drive, the contents of the DAT will be replaced with the new backup data when the backup is scheduled to run. If you want to preserve the daily backup of your application data, remove the DAT from the drive and insert a new one prior to the next scheduled backup. It is recommended that you label the DAT with the date, time and content (oracle backup data). You can restore all application data from this DAT at any time. Refer to procedure “Restoring application data to the Oracle database” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

ATTENTION

In order to maintain network functionality, the CS 2000 Management Tools persistent data in the Oracle database and the associated CORE/CM tables must match at all times. Therefore, it is recommended that the CS 2000 Management Tools support person modify the automated oracle data backup schedule to run in parallel to the customer's CORE Image Dump schedule. This will ensure that there are always CORE Images and CS 2000 Management Tools database backups that are 100% identical in configuration information.

To view or change the current configuration settings for automated backup of Oracle data, refer to procedure “Configuring automated Oracle data backups” in the CS 2000 Management Tools Configuration Management document, NN10106-511.

File systems

It is recommended you back up file systems after installing a new release of SSPFS software and all the Nortel Succession application software.

Sun Netra t1400

The t1400 server is a NEBS level 3 compliant computing platform that offers several configurations and performance points that can be expanded upon. It is based on the Ultra Sparc II processor clocked at 440 MHz. Up to 4 processors can be configured in a single server. It can also support up to 4 Gbytes of RAM and up to 4 disk drives on a SCSI internal bus that can be hot swapped.

The t1400 mounts in an OAME frame and has the following key features:

- 4 disks of 36 Gbytes each that are hot swappable. The disk drives are accessible from the front panel and are in-service Field Replaceable Units (FRUs).
- 2 Ultra SparcII processors at 440 MHz each with 4 Mbytes cache
- 2 Gbyte RAM
- 1 DVD ROM drive 10X
- 1 DDS-3 DAT drive
- 1 Quad Fast Ethernet card

Sun Netra 240

The Netra 240 server, also referred to as the Cabinetized Operations, Administration, and Maintenance (COAM) server, is a NEBS level 3 compliant computing platform that offers several configurations and performance points that can be expanded upon.

The COAM server, mounts in a COAM equipment cabinet, and has the following key features:

- 2 disks of 73 Gbytes each that are hot swappable. The disk drives are accessible from the front panel and are in-service Field Replaceable Units (FRUs).
- 2 Ultra Sparc IIIi processors at 440 MHz each with 4 Mbytes cache
- 2 Gbytes of RAM (basic model) or 4 Gbytes RAM
- 1 DVD/RW drive
- 3 PCI I/O slots
- 4 Ethernet ports 10/100/1000
- 1 SCSI port

The COAM servers can be provisioned as simplex units or as high availability (HA) pairs. The maximum number of COAM servers in a COAM equipment cabinet is six.

COAM servers provisioned in an HA pair, are referred to as a cluster. A cluster uses a minimum of three IP addresses; one for each COAM server and one for the cluster. While one of the cluster nodes is actively providing OAM&P services, the other remains on standby. An automatic failover takes place, when one of the following conditions occurs on the active node:

- power failure
- CPU failure
- double disk failure
- network inteface failure (all four network interfaces)
- system overheating
- memory failure

For maintenance or software upgrades, the user can also initiate a manual failover. Refer to procedure “Performing a manual failover” in the CS 2000 Management Tools Faults Management document, NN10084-911.

ATTENTION

During an automatic or manual failover, the HA cluster takes approximately 5 minutes to failover and bring up the standby node to Active state.

CS2000 Management Tools application

Overview

The CS2000 Management Tools application is a web-based GUI (graphical user interface) that provides the following capabilities:

- provision gateway controllers (GWCs), audio provisioning servers (APSs), universal audio servers (UASs), media gateways, carriers, media proxies, Network Address Translators (NATs), Policy Enforcement Point (PEP) servers, Quality of Service (QoS) collectors, and V5.2 interfaces (only in international version)
- view the topology and system faults, query and perform certain change operations
- perform line, trunk, and CS2K data integrity audits

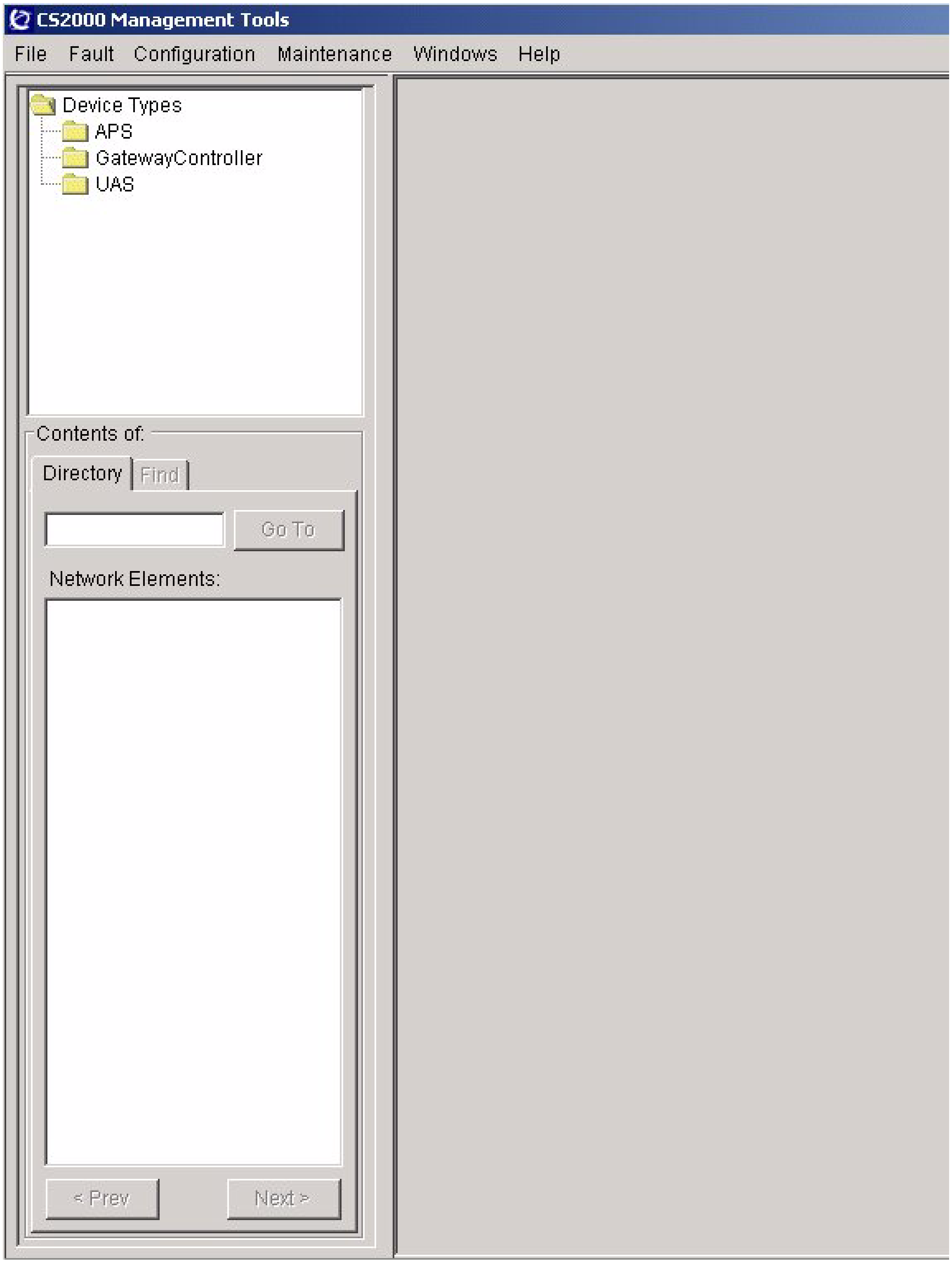
Note: To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 7.

User interface

The CS2000 Management Tools application GUI is accessed through the common launch page as previously described under Common launch page. To access the CS2000 Management Tools application GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

When the CS2000 Management Tools application is launched, a window, similar to the following is displayed:

CS2000 Management Tools GUI



Selecting a device under Device Types displays any provisioned network elements for that device under Contents of:.

Search capabilities for network elements of the selected device type, are provided through the Find tab and the Go to button, and scrolling capabilities are provided through the Prev (previous) and Next buttons.

The pane on the right side of the CS2000 Management Tools application GUI is a display area for device and network element information. The display varies according to the device type and associated network element selected. For details on each device type, refer to Audio Provisioning Server Manager application, CS 2000 GWC Manager, or Universal Audio Server Manager in this document.

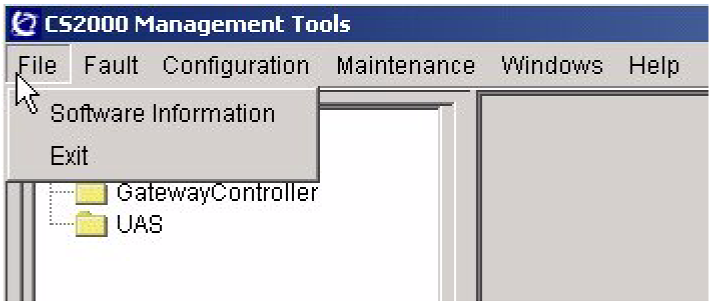
The sections that follow briefly describe the options available under each menu in the CS2000 Management Tools GUI.

> ***Note:*** Some of the options in the menus are available only when a device that uses the function is selected.

File

The File menu contains the options to view the software version information, and Exit the CS2000 Management Tools GUI.

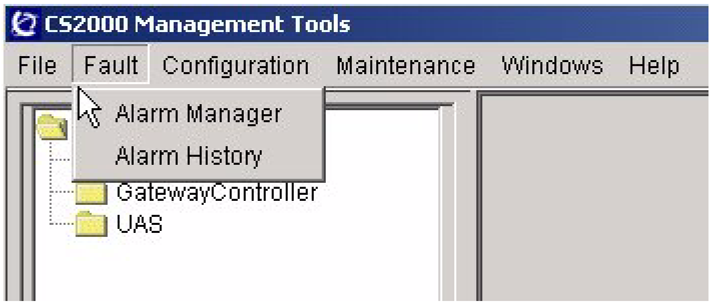
File menu



Fault

The Fault menu contains the options to open the Alarm Manager window and the Alarm History window used to manage alarms on the system. For more information, refer to the CS 2000 Management Tools Fault Management document, NN10084-911.

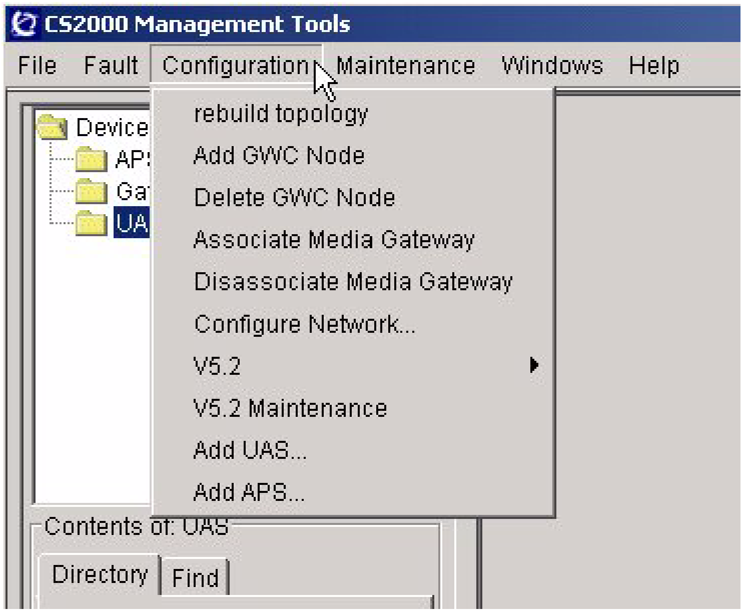
Fault menu



Configuration

The Configuration menu contains the options to rebuild the topology, add or delete network elements (GWC, UAS, and APS), associate or disassociate media gateways to or from GWCs, set network configuration parameters, such as bearer network type, compression codec, and packetized rate, and manage V5.2 interfaces (only in international version).

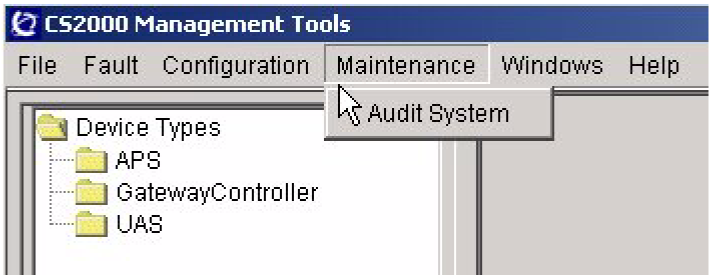
Configuration menu



Maintenance

The Maintenance menu contains the Audit System option used to perform a line data integrity, trunk data integrity or CS2K data integrity audit. The audits track the integrity of line-specific, trunk-specific, and node-specific data shared between the XA-Core and CS 2000 GWC Manager data in the database. Refer to procedure “Performing an audit” in the CS 2000 Management Tools Fault Management document, NN10084-911.

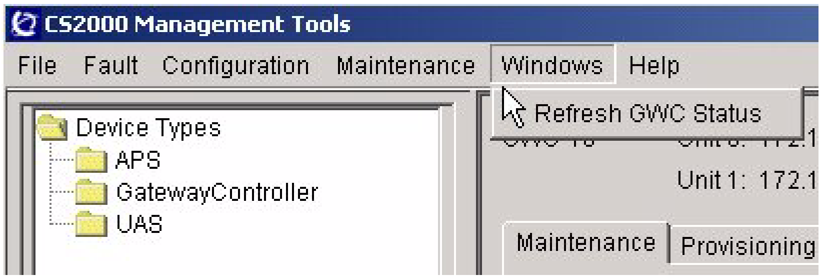
Maintenance menu



Windows

The Windows menu contains the option to refresh the status of a network element when one is selected. The example below shows the Windows menu option when a GWC network element is selected and displayed.

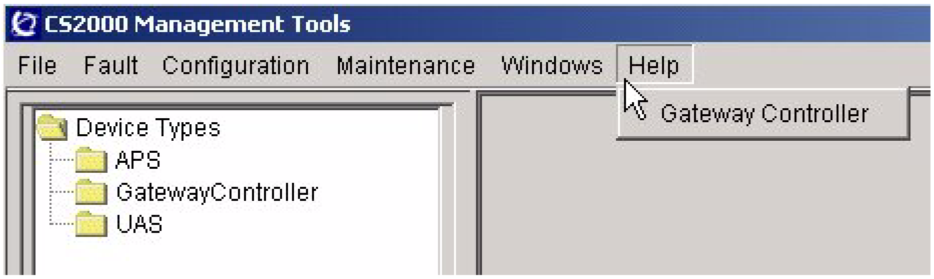
Windows menu



Help

The Help menu contains the option to display help information on the Gateway Controller.

Help menu



Audio Provisioning Server Manager application

Overview

The Audio Provisioning Server (APS) Manager application is available to view alarms and logs sent by the APS network elements (NEs). No management functionality is available from this application.

Note: To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 7.

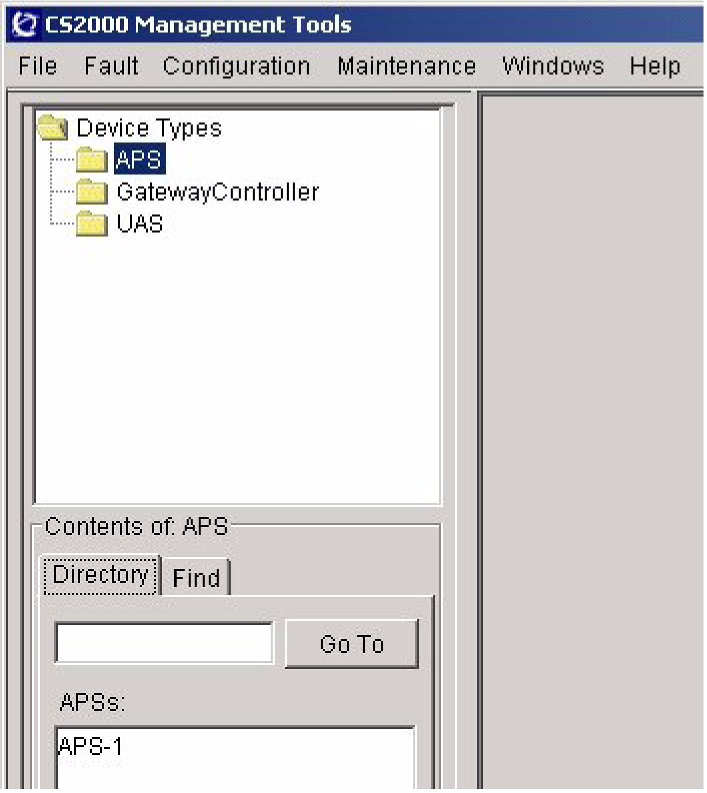
For procedures on how to provision and maintain APS NEs, refer to the UAS documentation suite.

User interface

The APS Manager application is a component of the CS2000 Management Tools application GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page. To access the CS2000 Management Tools application GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

When the APS device type is selected, a window, similar to the following is displayed:

Selecting APS



Adding or deleting an APS device to or from the network topology is done through the CS2000 Management Tools Configuration menu. Once an APS device is added to the topology, users can view APS alarms and logs through the Alarm Manager and Alarm History, which are accessed through the Fault menu. Refer to the CS 2000 Management Tools Fault document, NN10084-911.

CS 2000 GWC Manager

Overview

The CS 2000 GWC Manager is used to manage the GWC network elements (NEs) within a Succession Network.

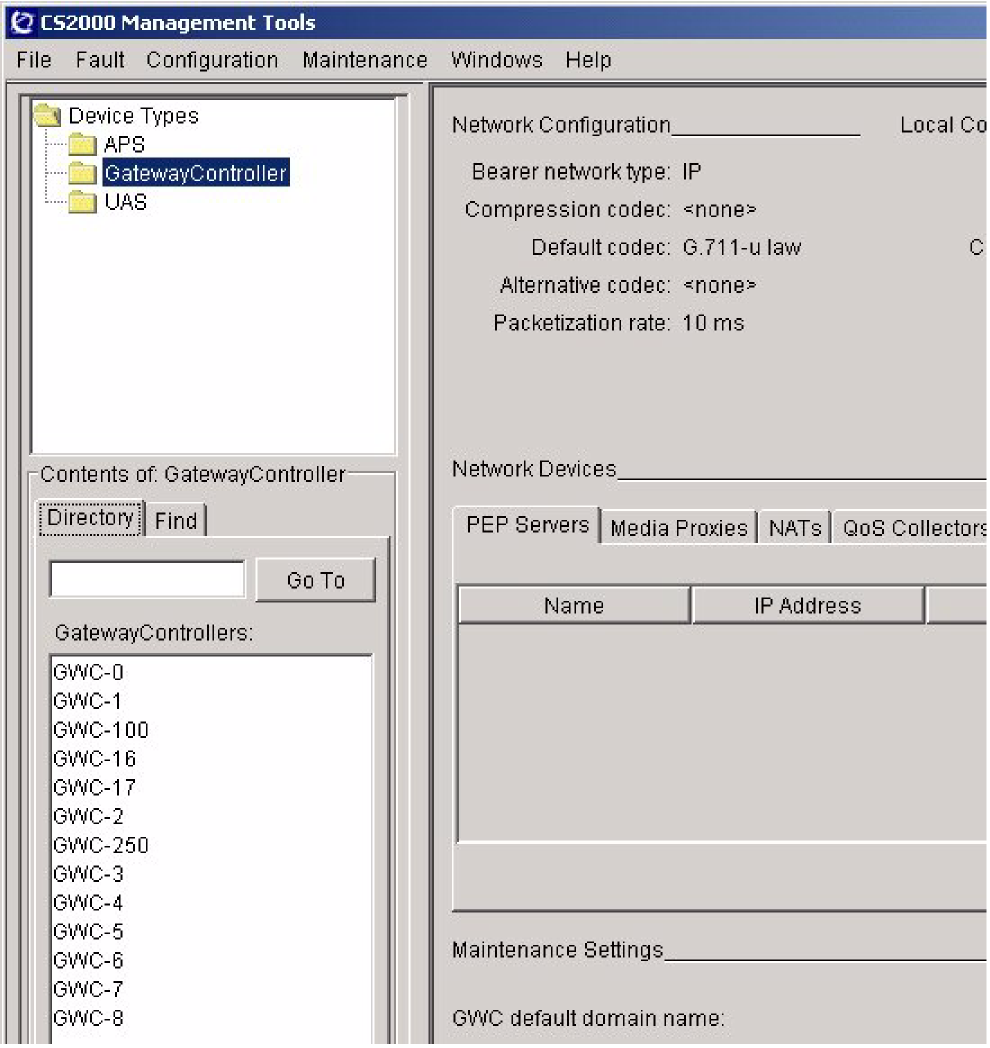
This section provides a brief overview of the CS 2000 GWC Manager. For procedures on how to provision and maintain GWC NEs using the CS 2000 GWC Manager, refer to the GWC documentation suite, or the GWC online help.

User interface

The CS 2000 GWC Manager is a component of the CS2000 Management Tools application GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page. To access the CS 2000 GWC Manager, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

When the GatewayController device type is selected, a window, similar to the following is displayed:

Selecting GatewayController



Bearer network type: IP
Compression codec: <none>
Default codec: G.711-u law
Alternative codec: <none>
Packetization rate: 10 ms

GatewayControllers:
GWC-0
GWC-1
GWC-100
GWC-16
GWC-17
GWC-2
GWC-250
GWC-3
GWC-4
GWC-5
GWC-6
GWC-7
GWC-8

GWC default domain name:

The right pane displays network configuration information, which applies to all GWC NEs in the network. Selecting a specifc GWC network element (NE) under Contents of: GatewayController, displays information about the selected GWC NE.

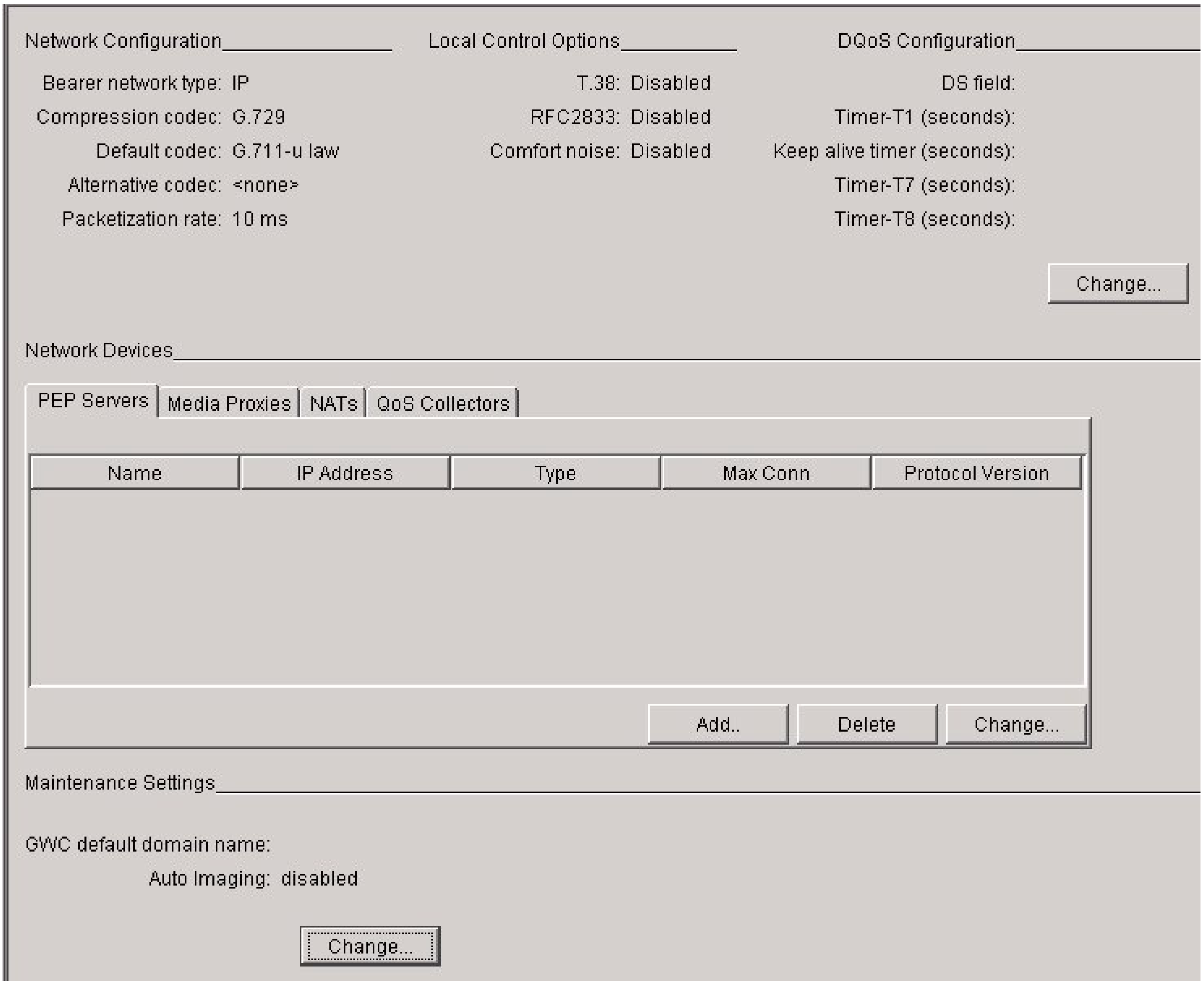
Managing the GWC NEs is done through the Network view and Node view of the CS 2000 GWC Manager, and some menu options in the CS2000 Management Tools application GUI as previously mentioned in CS2000 Management Tools application.

The sections that follow briefly describe the Network view and Node view.

Network view

The Network view, similar to the following, displays information related to all GWC NEs in the network.

Network view



Network Configuration

Bearer network type: IP
Compression codec: G.729
Default codec: G.711-u law
Alternative codec: <none>
Packetization rate: 10 ms

Local Control Options

T.38: Disabled
RFC2833: Disabled
Comfort noise: Disabled

DQoS Configuration

DS field:
Timer-T1 (seconds):
Keep alive timer (seconds):
Timer-T7 (seconds):
Timer-T8 (seconds):

Network Devices

Name	IP Address	Type	Max Conn	Protocol Version

Maintenance Settings

GWC default domain name:
Auto Imaging: disabled

From the Network view, you can perform any of the following activities:

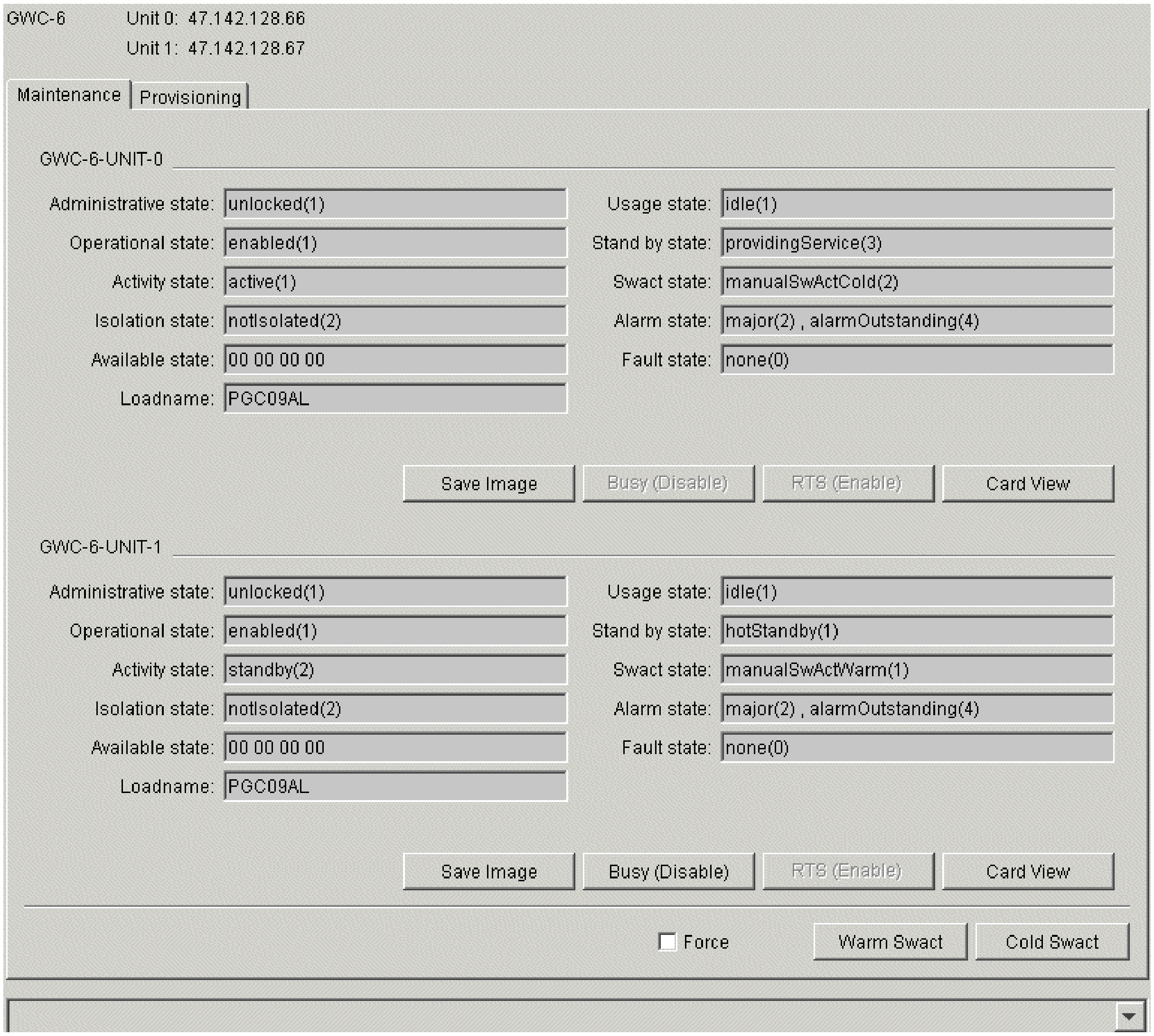
- Change button (in top right-hand corner) - Change the dynamic Quality of Service (DQoS) system policy data for the GWCs in the network.
- PEP Servers tab - Add or delete a Policy Enforcement Point (PEP) server to or from the network, or change the information of an existing PEP server. A PEP server communicates with the GWC to provide dynamic quality of service (DQoS) and other policy services for the associated gateways.
- Media Proxies tab - Add or delete a media proxy server to or from the network, or change the information of an existing media proxy server.
- NATs tab - Add or delete a Network Address Translations (NATs) device to or from the network.
- QoS Collectors tab - Add or delete a Quality of Service (QoS) collector to or from the network.
- Change button (in bottom left-hand corner) - Enable or disable periodic imaging of GWC loads automatically. It is recommended that auto imaging be enabled in order to prevent potential losses of patching applications.

Node view

The Node view displays information related to individual GWC NEs in the network. The Node view consists of a Maintenance tab and a Provisioning tab, as well as a status bar, located at the bottom of the main panel, which displays operation messages. You can display the previous twenty messages from the drop-down list.

The Maintenance tab, similar to the following, displays the details related to each GWC unit.

Maintenance tab



GWC-6 Unit 0: 47.142.128.66
Unit 1: 47.142.128.67

GWC-6-UNIT-0

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	providingService(3)
Activity state:	active(1)	Swact state:	manualSwActCold(2)
Isolation state:	notIsolated(2)	Alarm state:	major(2) , alarmOutstanding(4)
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGC09AL		

GWC-6-UNIT-1

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	hotStandby(1)
Activity state:	standby(2)	Swact state:	manualSwActWarm(1)
Isolation state:	notIsolated(2)	Alarm state:	major(2) , alarmOutstanding(4)
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGC09AL		

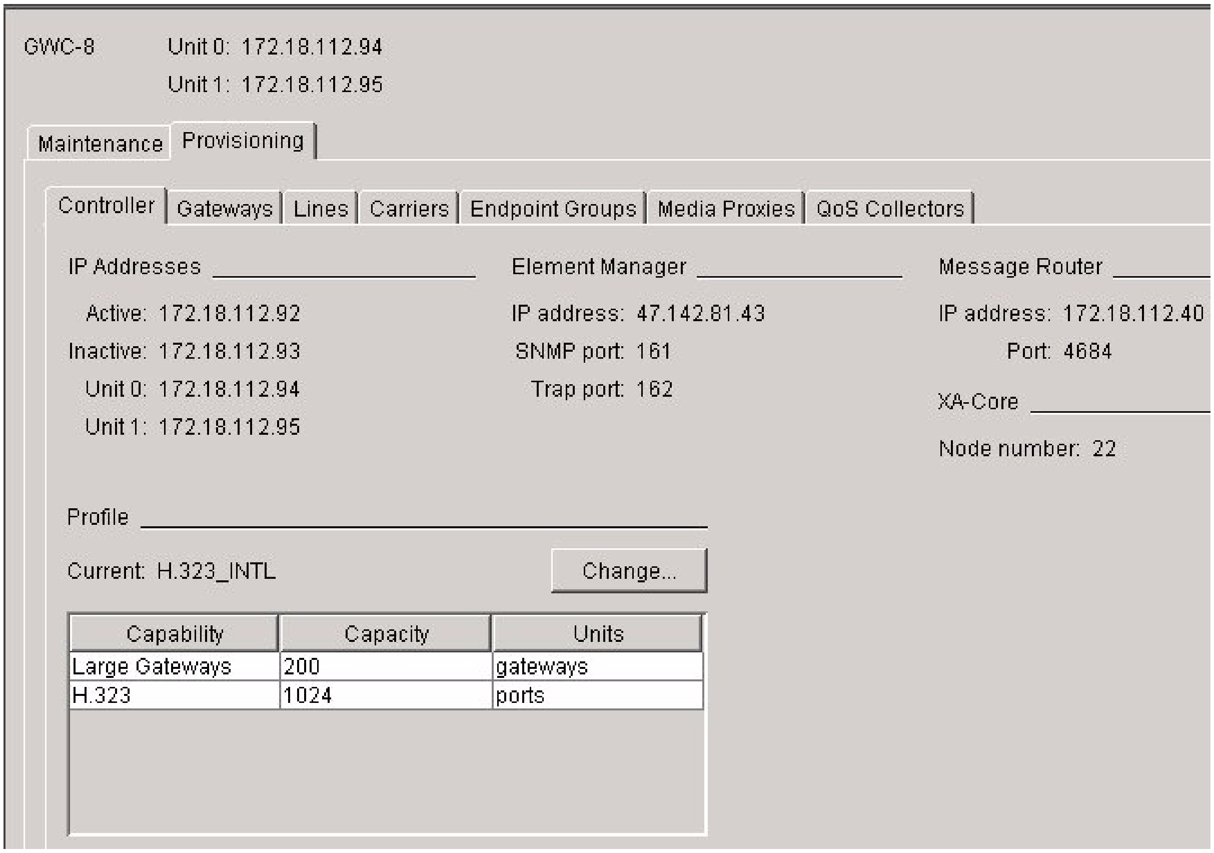
From the Maintenance tab you can perform any one of the following activities:

- Save Image button - save an image of each GWC unit
- Card View button - display the card view of each GWC unit
- Busy (Disable)/RTS (Enable) buttons - busy and return a GWC unit to service
- Warm Swact/Cold Swact buttons - perform a warm or cold switch of activity (Swact)

> ***Note:*** Selecting the Force option gives priority to the next maintenance request to override some pending operations.

The provisioning tab, similar to the following, displays configuration data associated with a GWC NE.

Provisioning tab



GWC-8 Unit 0: 172.18.112.94
Unit 1: 172.18.112.95

IP Addresses

Active: 172.18.112.92
Inactive: 172.18.112.93
Unit 0: 172.18.112.94
Unit 1: 172.18.112.95

Element Manager

IP address: 47.142.81.43
SNMP port: 161
Trap port: 162

Message Router

IP address: 172.18.112.40
Port: 4684

XA-Core

Node number: 22

Profile

Current: H.323_INTL

Capability	Capacity	Units
Large Gateways	200	gateways
H.323	1024	ports

From the Provisioning tab you can perform any one of the following activities:

- Controller tab - View the data specific to the selected gateway controller, including the profile that is currently provisioned and a list of capabilities associated with that profile, and change the profile if the provisioned profile supports change.
- Gateways tab - View a list of media gateways (MGs) associated with the GWC, associate or disassociate an MG to or from the GWC, or modify the MG configuration.
- Lines tab - View configuration data for lines associated with the selected gateway controller.
- Carriers tab - View configuration data for carriers associated with the selected gateway controller, add or delete a carrier to or from the selected gateway controller, and display the trunks for the selected carrier.
- Endpoint Groups tab - View the endpoint groups that were automatically created with the addition of an H.323 media gateway.

  Note: When an H.323 media gateway is removed, the associated endpoint groups are also removed.

- Media Proxies tab - View configuration data for media proxies associated with the selected gateway controller, and associate or disassociate a media proxy to or from the gateway controller.
- QoS Collectors tab - View configuration data for the QoS collectors associated with the selected gateway controller, associate or disassociate a QoS collector to and from the gateway controller, and enable or disable QoS collection on the gateway controller.

Universal Audio Server Manager

Overview

The Universal Audio Server (UAS) Manager application is used to manage the UAS network elements (NEs) within a Succession Network. With the UAS Manager application, users can view general information, perform various configuration and maintenance tasks, and view performance measurements for UAS NEs.

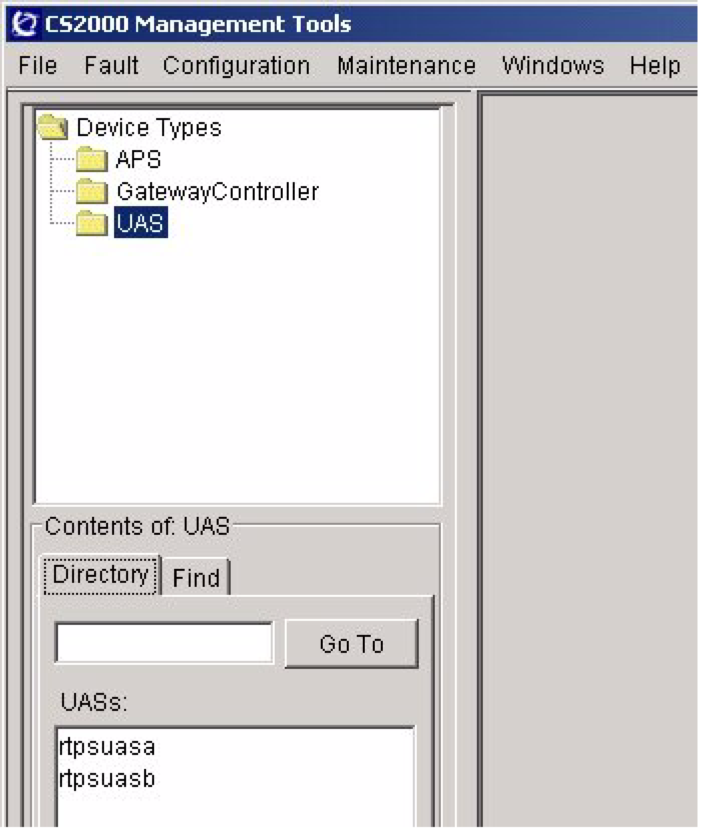
This section provides a brief overview of the UAS Manager. For procedures on how to provision and maintain UAS NEs using the UAS Manager, refer to the UAS documentation suite.

User interface

The UAS Manager is a component of the CS2000 Management Tools application GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page. To access the CS2000 Management Tools application GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

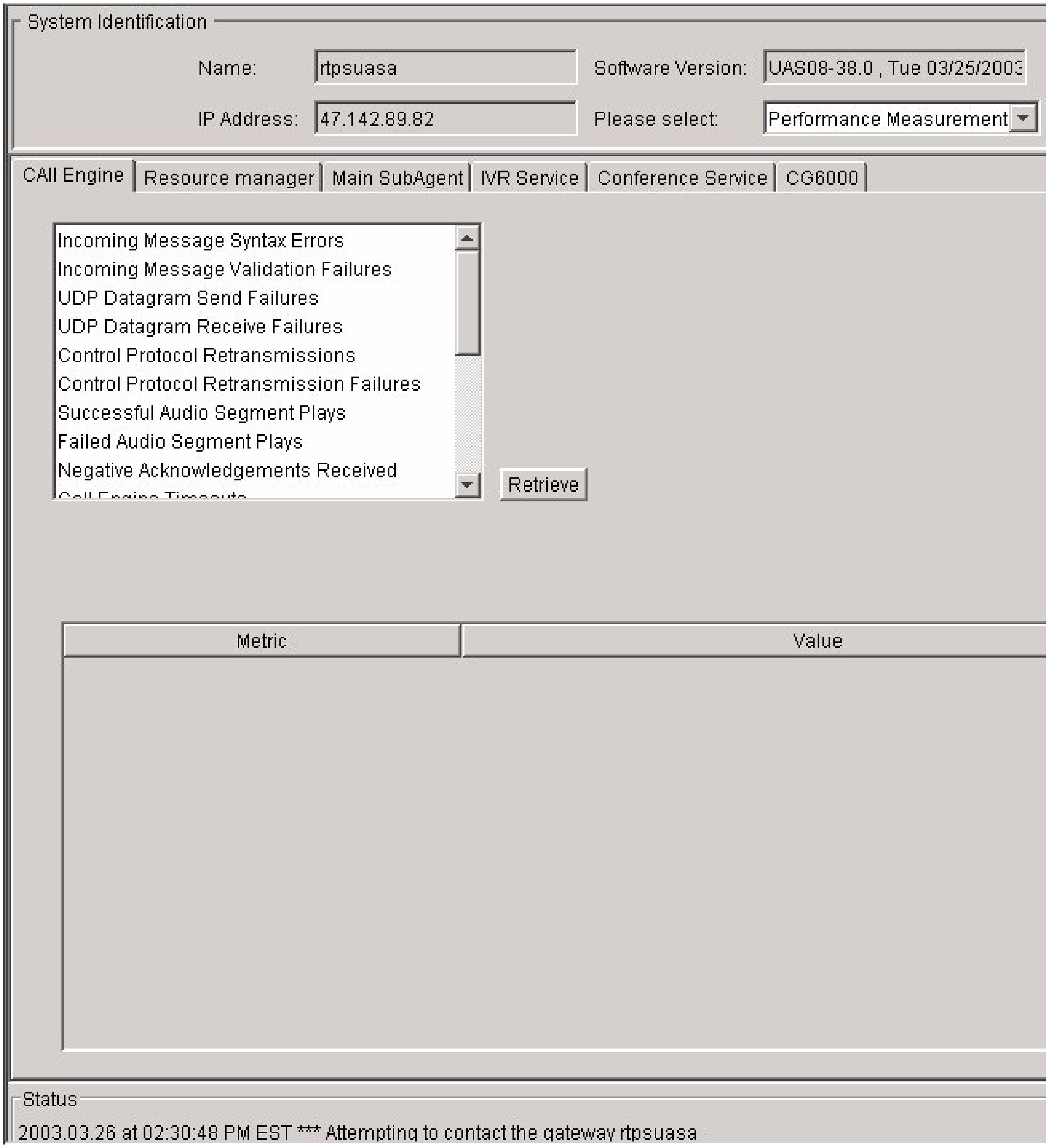
When the UAS device type is selected, a window, similar to the following is displayed:

Selecting UAS



Selecting a specifc UAS network element (NE) under Contents of: UAS, displays information about that UAS NE in the right pane of the CS2000 Management Tools GUI as shown in the following example:

Selecting a UAS network element


System Identification
CAll Engine
Resource manager
Main SubAgent
IVR Service
Conference Service
CG6000
Incoming Message Syntax Errors
Incoming Message Validation Failures
UDP Datagram Send Failures
UDP Datagram Receive Failures
Control Protocol Retransmissions
Control Protocol Retransmission Failures
Successful Audio Segment Plays
Failed Audio Segment Plays
Negative Acknowledgements Received
Call Engine Timeouts
Retrieve
Metric
Value
Status

Name: rtpsuasa

IP Address: 47.142.89.82

Software Version: UAS08-38.0 , Tue 03/25/2003

Please select: Performance Measurement

2003.03.26 at 02:30:48 PM EST *** Attempting to contact the gateway rtpsuasa

The top portion of the pane displays information about the selected UAS network element and provides a drop down menu where you select one of the following options; Performance Measurement, Maintenance, Configuration or SNMP Configuration.

The middle portion of the pane varies according to the option selected, and the bottom portion of the pane displays operation messages.

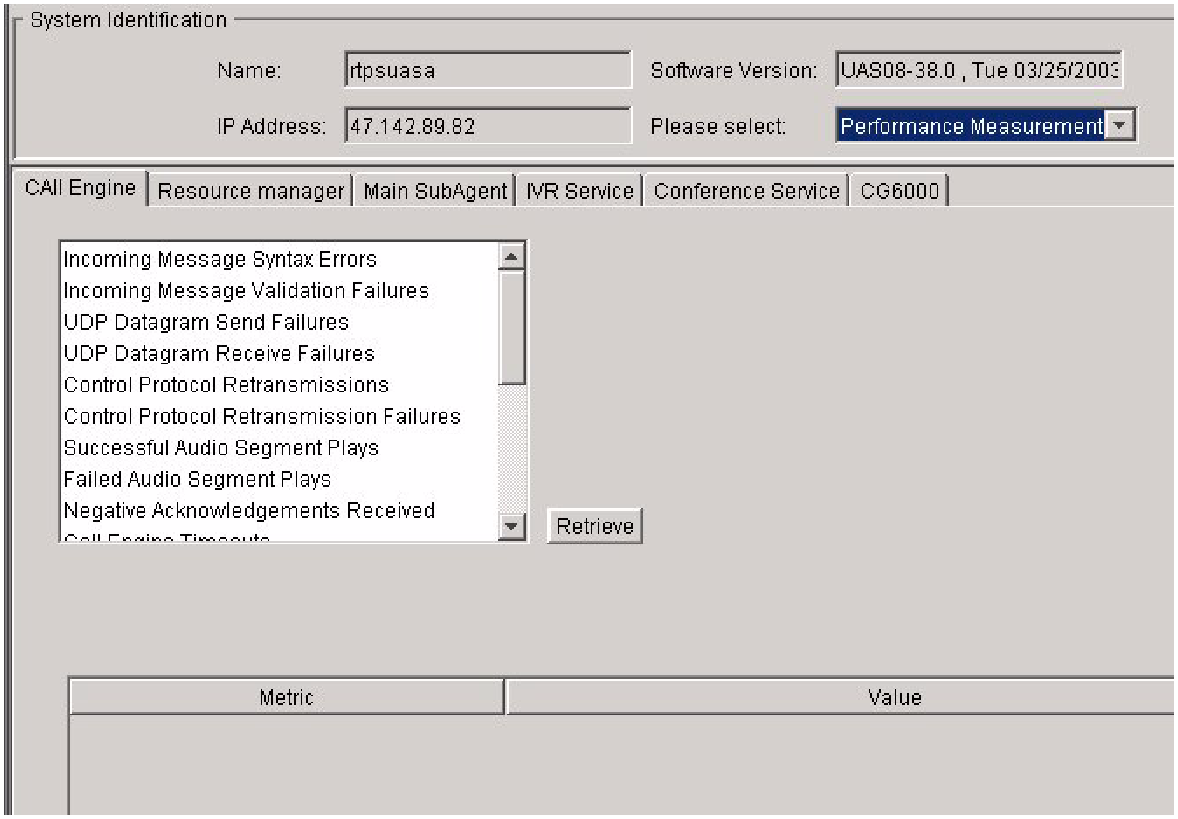
Managing UAS NEs is done through the Performance Measurement, Configuration, Maintenance, and SNMP Configuration options of the UAS Manager, and some menu options in the CS2000 Management Tools application GUI as previously mentioned in CS2000 Management Tools application.

The sections that follow briefly describes each of the options of the UAS Manager.

Performance Measurement

Selecting the Performance Measurement option from the drop-down menu, displays a window similar to the following.

Performance Measurement window



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Performance Measurement

Incoming Message Syntax Errors
Incoming Message Validation Failures
UDP Datagram Send Failures
UDP Datagram Receive Failures
Control Protocol Retransmissions
Control Protocol Retransmission Failures
Successful Audio Segment Plays
Failed Audio Segment Plays
Negative Acknowledgements Received
Call Engine Timeouts

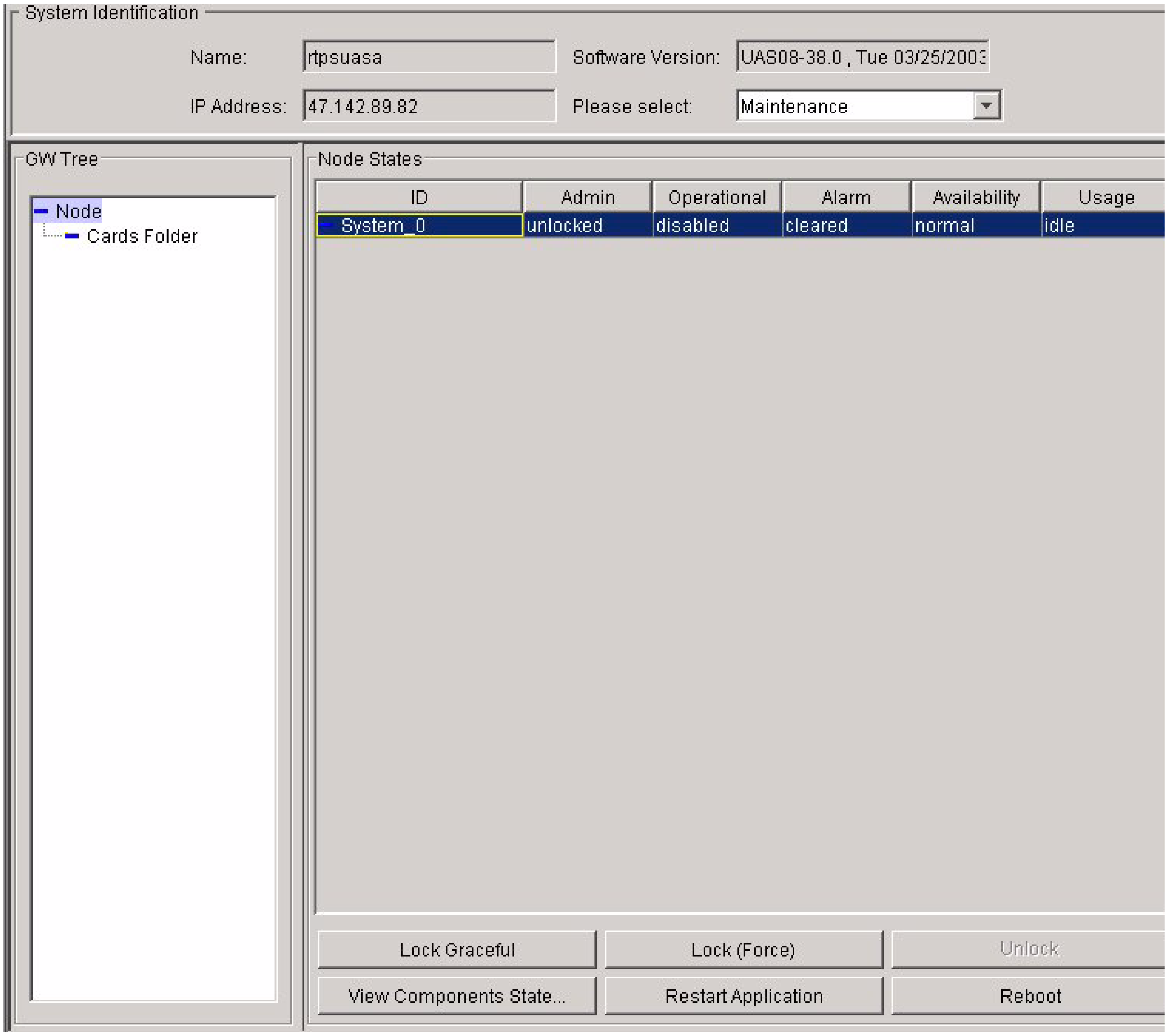
Metric	Value

From this window, you can view the statistics collected for the selected UAS node. The types of statistics you can view are in individual tabs as shown above. For details on the statistics you can view in each tab, refer to the UAS Performance Monitoring document, NN10139-711.

Maintenance

Selecting the Maintenance option from the drop-down menu and selecting Node from the GW Tree, displays a window similar to the following.

Maintenance (Node view)



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/200

IP Address: 47.142.89.82

Please select: Maintenance

GW Tree

- Node
  - Cards Folder

Node States

ID	Admin	Operational	Alarm	Availability	Usage
System_0	unlocked	disabled	cleared	normal	idle

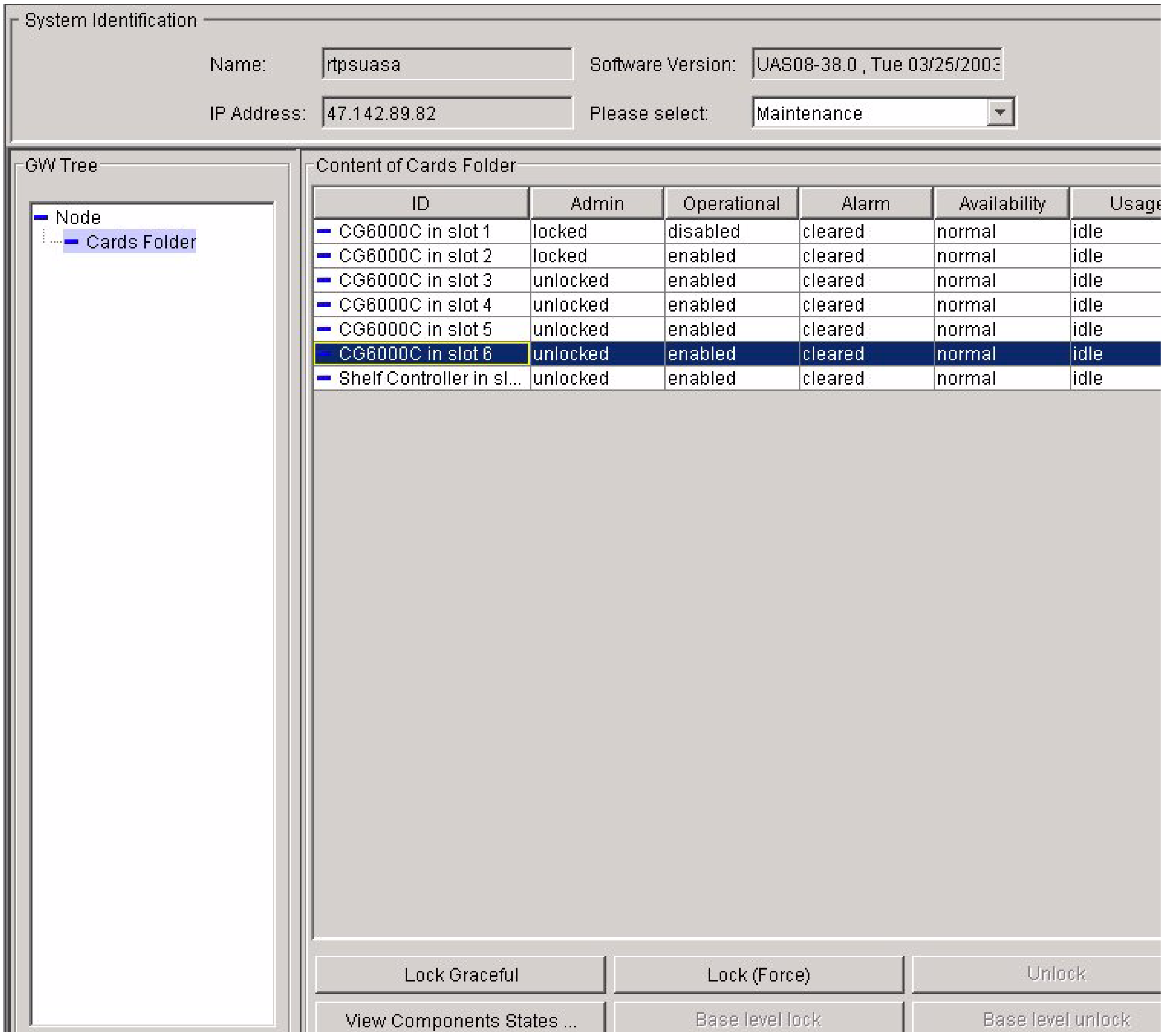
From this window, you can perform any one of the following activities: reboot the UAS, restart the UA

- Lock Graceful button - lock a UAS node
- Lock (Force) button - lock a UAS node (overriding any pending operations)
- Unlock button - unlock a UAS node

- View Component States... button - view component states associated with the selected UAS node
- Restart Application button - restart the UAS server application
- Reboot button - reboot the UAS node

Selecting Cards Folder from the GW Tree, displays a window similar to the following:

Maintenance (card view)



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Maintenance

GW Tree

- Node
  - Cards Folder

Content of Cards Folder

ID	Admin	Operational	Alarm	Availability	Usage
CG6000C in slot 1	locked	disabled	cleared	normal	idle
CG6000C in slot 2	locked	enabled	cleared	normal	idle
CG6000C in slot 3	unlocked	enabled	cleared	normal	idle
CG6000C in slot 4	unlocked	enabled	cleared	normal	idle
CG6000C in slot 5	unlocked	enabled	cleared	normal	idle
CG6000C in slot 6	unlocked	enabled	cleared	normal	idle
Shelf Controller in sl...	unlocked	enabled	cleared	normal	idle

From this window, you can perform any one of the following activities: reboot the UAS, restart the UA

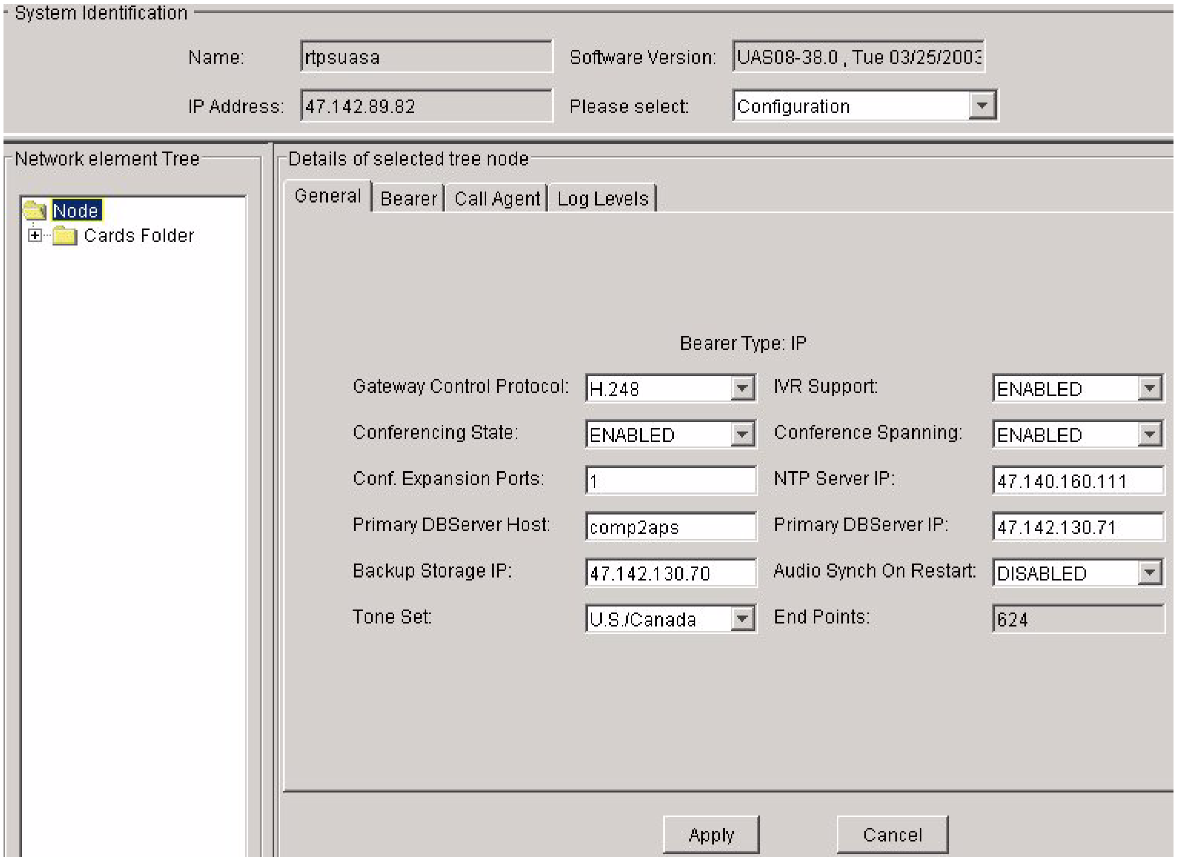
- Lock Graceful button - lock a card but not completety shut it down (used to perform some administrative tasks on the card)
- Lock (Force) button - lock a card (overriding any pending operations)
- Unlock button - unlock a card
- View Component States... button - view component states associated with the selected UAS node
- Base level lock button - lock a card and completely shut it down (used to replace or remove the card)
- Base level unlock button - unlock a card from a complete shut down

Note: The lock and unlock functions are only available for the CG6000 card type.

Configuration

Selecting the Configuration option from the drop-down menu and selecting Node from the Network element Tree, displays a window similar to the following.

Configuration (node view)



System Identification

Name:	rtpsuasa	Software Version:	UAS08-38.0 , Tue 03/25/2003
IP Address:	47.142.89.82	Please select:	Configuration

Bearer Type: IP

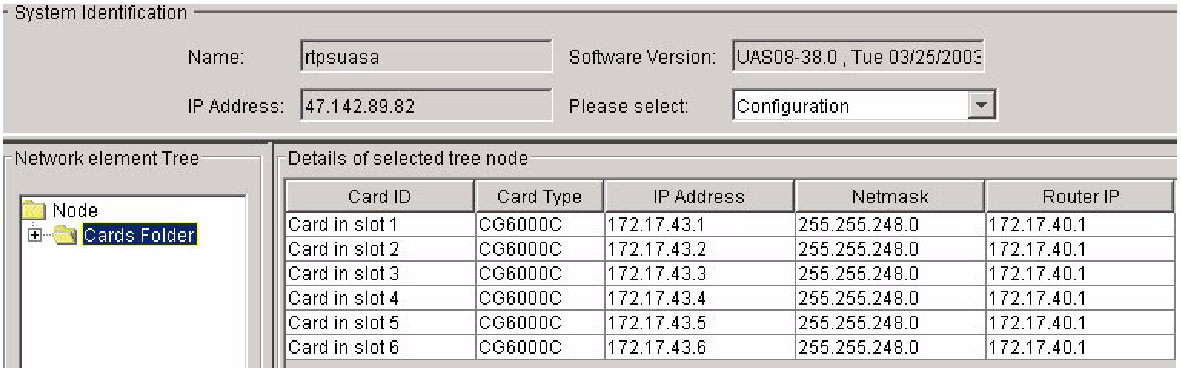
Gateway Control Protocol:	H.248	IVR Support:	ENABLED
Conferencing State:	ENABLED	Conference Spanning:	ENABLED
Conf. Expansion Ports:	1	NTP Server IP:	47.140.160.111
Primary DBServer Host:	comp2aps	Primary DBServer IP:	47.142.130.71
Backup Storage IP:	47.142.130.70	Audio Synch On Restart:	DISABLED
Tone Set:	U.S./Canada	End Points:	624

From this window, you can perform any one of the following activities:

- General tab - modify configuration data for the UAS node
- Bearer tab - modify configuration data for the bearer card associated with the selected UAS node
- Call Agent - modify the configuration data for the call agent associated with the selected UAS node
- Log Levels tab - modify the logs you want to have sent to the element management station
- Apply button - apply the configuration changes you made
- Cancel button - cancel the configuration changes you made and return the fields to their original value

Selecting Card Folder from the Network element Tree, displays a window similar to the following:

Configuration (card folder view)



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Configuration

Network element Tree

- Node
  - Cards Folder

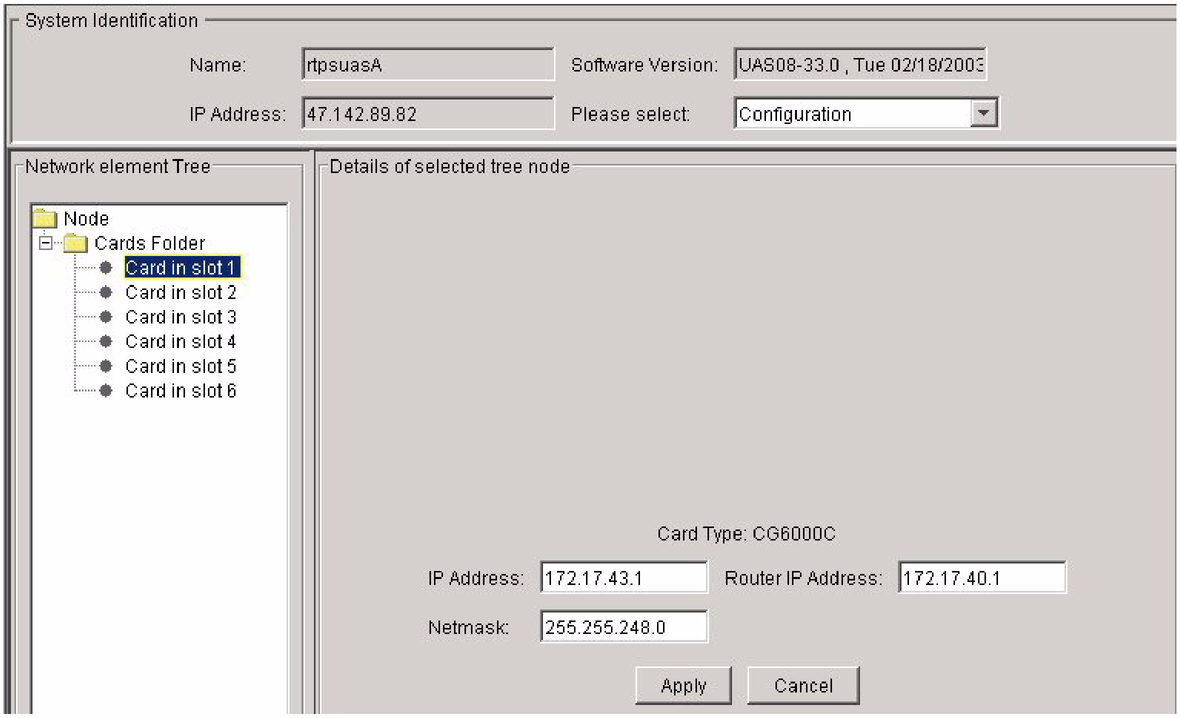
Details of selected tree node

Card ID	Card Type	IP Address	Netmask	Router IP
Card in slot 1	CG6000C	172.17.43.1	255.255.248.0	172.17.40.1
Card in slot 2	CG6000C	172.17.43.2	255.255.248.0	172.17.40.1
Card in slot 3	CG6000C	172.17.43.3	255.255.248.0	172.17.40.1
Card in slot 4	CG6000C	172.17.43.4	255.255.248.0	172.17.40.1
Card in slot 5	CG6000C	172.17.43.5	255.255.248.0	172.17.40.1
Card in slot 6	CG6000C	172.17.43.6	255.255.248.0	172.17.40.1

From this window you can view the configuration data for all the cards.

Expanding the Card Folder and selecting a card, displays a window similar to the following:

Configuration (card view)



System Identification

Name: rtpsuasA

Software Version: UAS08-33.0 , Tue 02/18/2003

IP Address: 47.142.89.82

Please select: Configuration

Network element Tree

- Node
  - Cards Folder
    - Card in slot 1
    - Card in slot 2
    - Card in slot 3
    - Card in slot 4
    - Card in slot 5
    - Card in slot 6

Details of selected tree node

Card Type: CG6000C

IP Address: 172.17.43.1

Router IP Address: 172.17.40.1

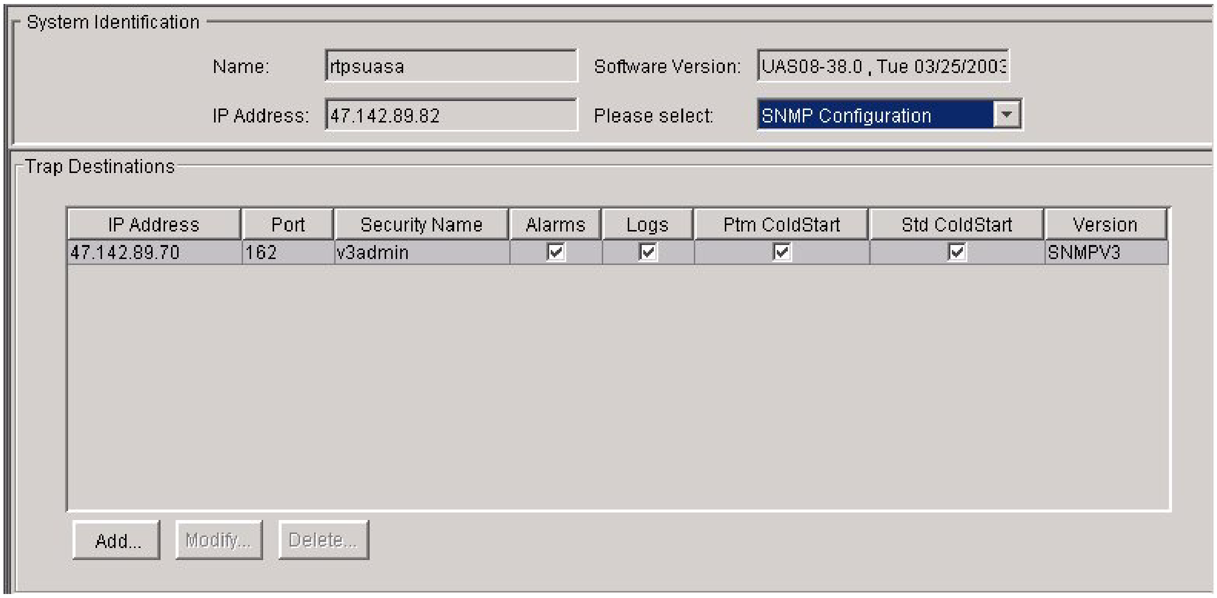
Netmask: 255.255.248.0

From this window you can modify the configuration data for the selected card.

SNMP Configuration

Selecting the SNMP Configuration option from the drop-down menu, displays a window similar to the following.

SNMP Configuration window



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: SNMP Configuration

Trap Destinations

IP Address	Port	Security Name	Alarms	Logs	Ptm ColdStart	Std ColdStart	Version
47.142.89.70	162	v3admin	☑	☑	☑	☑	SNMPV3

From this window, you can add, modify, or delete an SNMP trap destination for the selected UAS node.

V5.2 Configuration and Maintenance applications

Overview

The V5.2 Configuration and Maintenance applications are used to manage v5.2 interfaces within a Succession Network.

> ***Note:*** The V5.2 Configuration and Maintenance applications are only available in the international version of the software and not in the North American version.

A V5.2 interface consists of a grouping of E1 carriers on which V5.2 lines are carried. Assuming that at any given time only a portion of subscribers will use the interface, V5.2 supports concentration such that an Access Node (AN) can support more subscribers than there are available timeslots on the E1s connecting it to the Local Exchange (LE).

In the context of Succession Networks, Gateway Controllers can be provisioned with a V5.2 interface using the CS2000 Management Tools GUI.

This section provides a brief overview of the V5.2 Configuration and Maintenance applications. For procedures on how to provision and maintain v5.2 interfaces, refer to the GWC documentation suite.

User interface

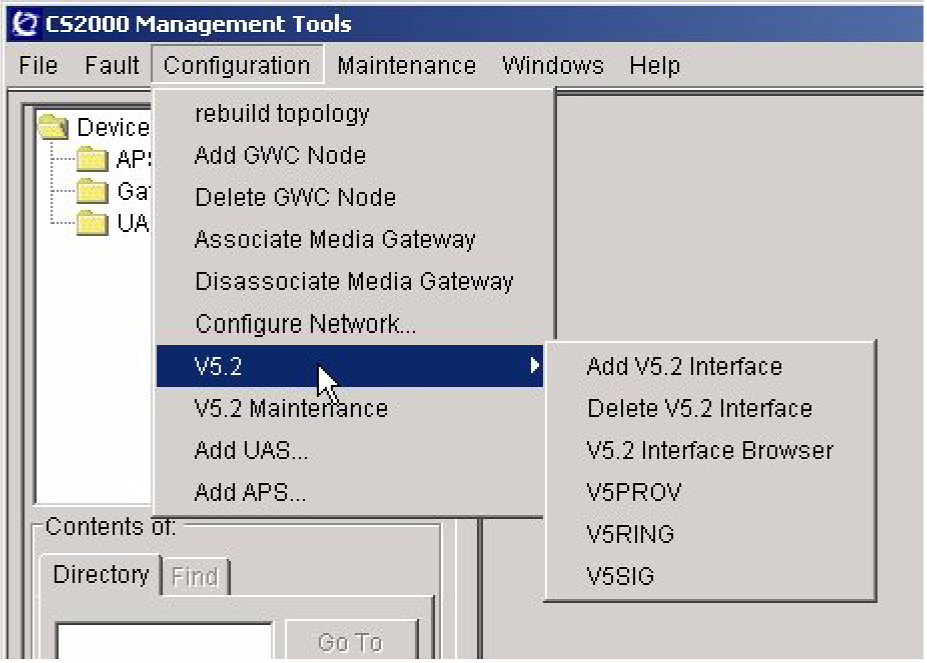
The V5.2 Configuration and Maintenance applications are components of the CS2000 Management Tools application GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page. To access the CS2000 Management Tools application GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Configuration and maintenance activities on V5.2 interfaces are done through the V5.2 option and V5.2 maintenance option on the Configuration menu of the CS2000 Management Tools application GUI.

V5.2 option

When the V5.2 option is selected from the Configuration menu, a sub-menu, similar to the following, is displayed.

Configuration menu items for V5.2



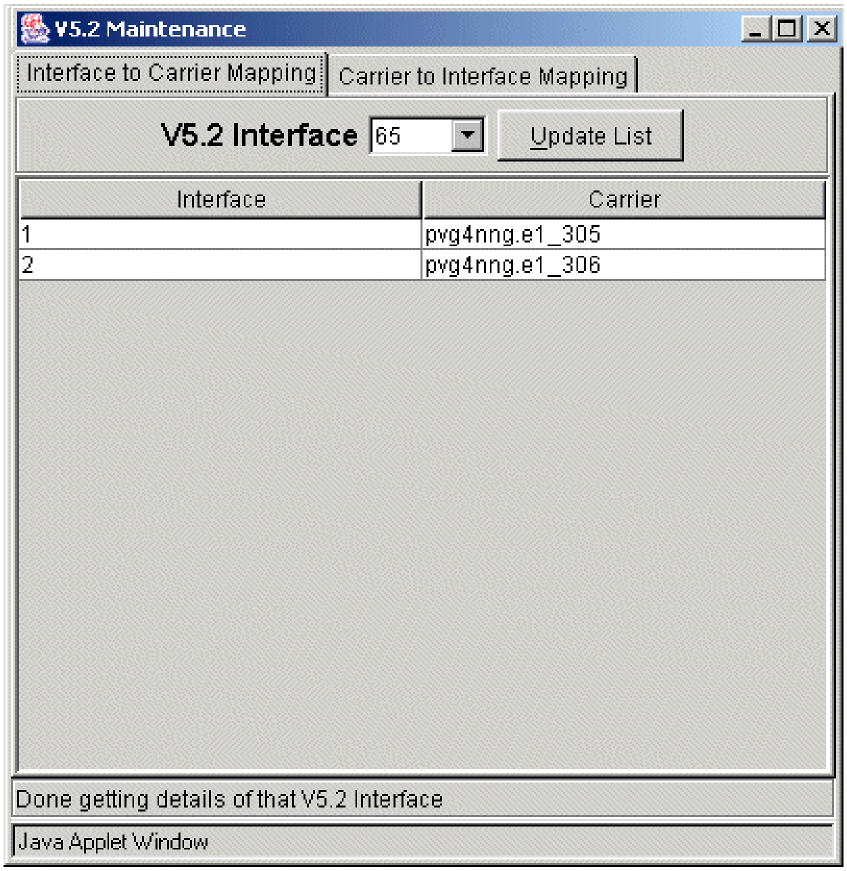
The options in this sub-menu, allow you to perform any of the following activities:

- Add V5.2 Interface - Add a V5.2 interface and associate physical E1 carriers to the interface, assign a ring plan, provision a profile, and a signaling profile.
- Delete V5.2 Interface - Delete a V5.2 interface when nothing is provisioned on it and it is no longer required.
- V5.2 Interface Browser - View the current information for the selected V5.2 interface, create a new V5.2 interface, modify the provisioning information for the selected V5.2 interface, delete the lines on the selected V5.2 interface, and refresh the Current V5.2 Interfaces table.
- V5PROV - Add, delete, review and modify V5.2 provisioning templates.
- V5RING - Add, delete, review and modify V5.2 ring templates. V5.2 ringing templates are a set of mappings between the ringing cadences known by the peripheral and the V5.2 protocol.
- V5SIG - Add, delete, review and modify V5.2 signaling templates

V5.2 Maintenance option

When the V5.2 Maintenance option is selected from the Configuration menu, a window similar to the following, is displayed.

V5.2 Maintenance



Interface	Carrier
1	pvg4nng.e1_305
2	pvg4nng.e1_306

Done getting details of that V5.2 Interface

Java Applet Window

The V5.2 Maintenance window provides a mechanism for viewing a V5.2 interface to Carrier mapping and a Carrier to V5.2 interface mapping.

Line Maintenance Manager

Overview

The Line Maintenance Manager (LMM) application is used to post lines and perform maintenance activities on them.

> ***Note 1:*** To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 7.
>
> ***Note 2:*** The LMM does not currently support hunt groups.

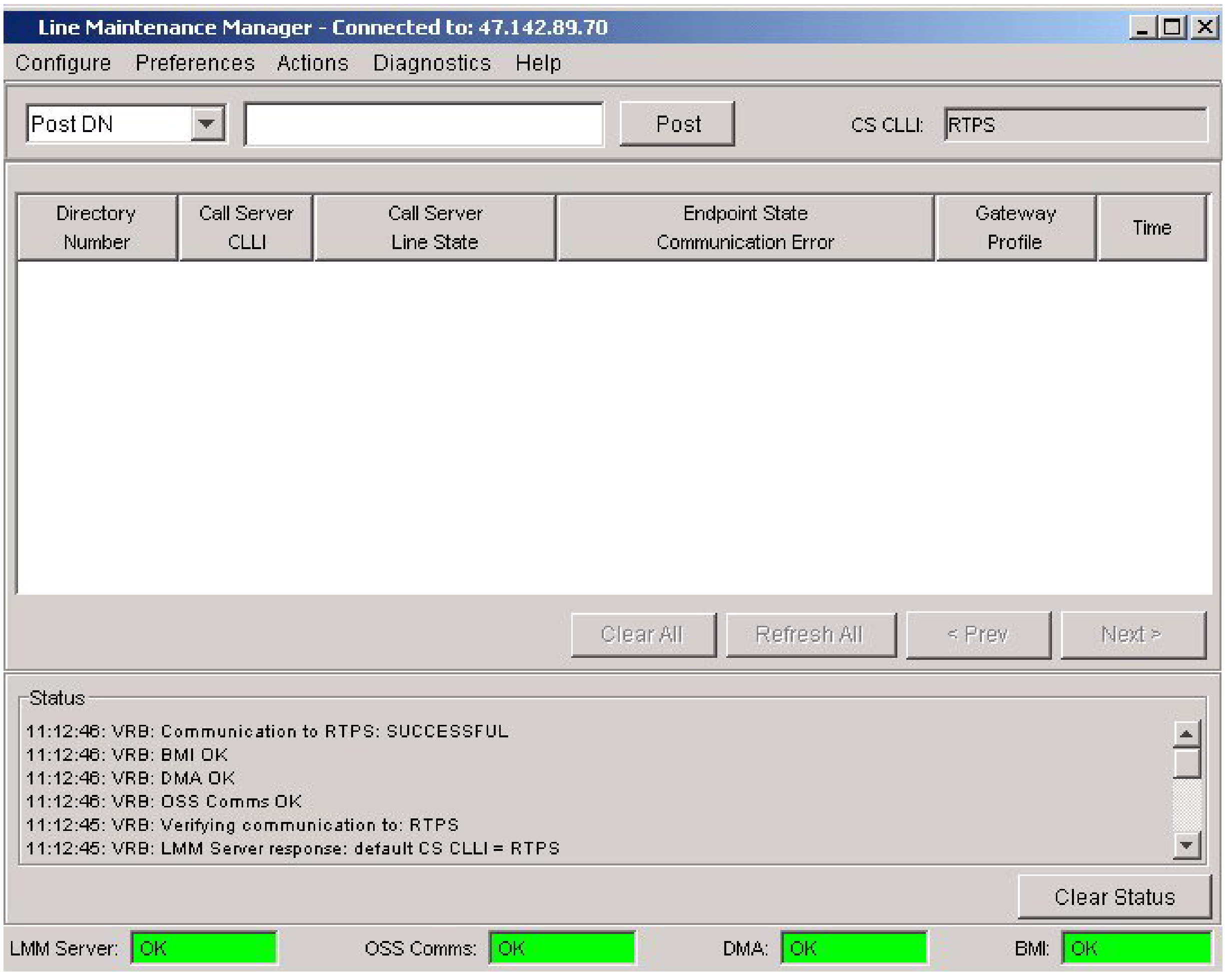
This section provides a brief overview of the LMM. For procedures on how to perform line maintenance activities using the LMM, refer to the CS 2000 Management Tools Fault Management document, NN10084-911.

User interface

The user interface for the LMM application is a web-based GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page. To access the LMM GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

When the Line Maintenance Manager is launched, a window, similar to the following is displayed:

Line Maintenance Manager GUI



CS CLLI: RTPS

```
11:12:46: VRB: Communication to RTPS: SUCCESSFUL
11:12:46: VRB: BMI OK
11:12:46: VRB: DMA OK
11:12:46: VRB: OSS Comms OK
11:12:45: VRB: Verifying communication to: RTPS
11:12:45: VRB: LMM Server response: default CS CLLI = RTPS
```

LMM Server: OK OSS Comms: OK DMA: OK BMI: OK

The main panel displays the following information:

- **CS CLLI** - The CLLI for the Communication Server 2000
- **Status** - Operation messages
- **LMM Server** - Status of the link between the LMM client and LMM server
- **OSS Comms** - Status of the OSS Comms Svcs application on the CS 2000 Core Manager.
- **DMA** - Status of the DMS Maintenance Application on the CS 2000 Core Manager
- **BMI** - Status of the Base Maintenance Interface application on the CS 2000 Core Manager

From the main panel, you can perform any of the following activities:

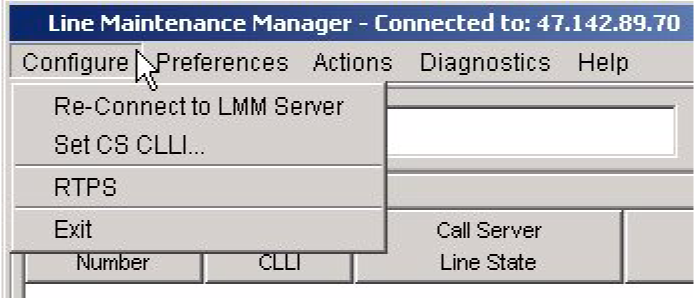
- **Post** - Post the lines according the selection in the pull down menu. Selecting Post DN, displays a line by its directory number (DN). Selecting Post by Gateway, displays the lines associated with the specific gateway.
- **Clear All** - Remove all posted lines from the display.
- **Refresh All** - Manually refresh the posted lines in the display, when auto-refresh is disabled.
- **Prev/Next** - Navigate from the current page to the previous or next page, respectively, when multiple screens are needed to show all the posted lines
- **Clear Status** - Clear the status information that is reported in the Status area

The sections that follow briefly describe the options available under each menu in the Line Maintenance Manager GUI.

Configure

The Configure menu contains the options to reconnect to the LMM server (used when the connection times out), set the CS CLLI, and exit the Line Maintenance Manager GUI.

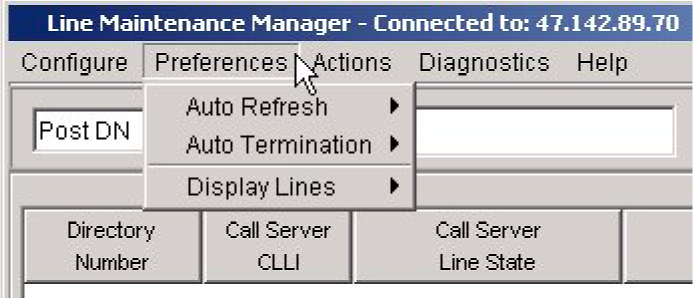
Configure menu



Preferences

The Preferences menu contains the options to turn Auto refresh on or off and set the Auto refresh value, turn Auto Termination on or off and set the Auto Termination timeout value, disable Auto refresh, cancel pending CPD requests, and display a fixed number of lines.

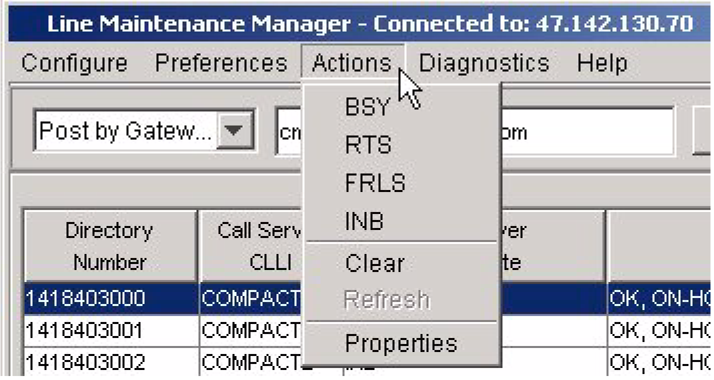
Preferences menu



Actions

The Actions menu contains the options to busy and return lines to service, force release a line, installation busy (INB) a line, clear or refresh the display of the posted lines, and display the properties of a line.

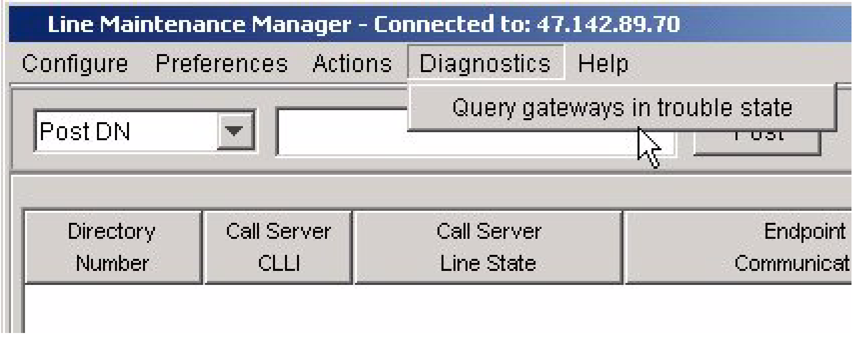
Actions menu


Line Maintenance Manager - Connected to: 47.142.130.70
Configure
Preferences
Actions
Diagnostics
Help
Post by Gatew...
cn
om
BSY
RTS
FRLS
INB
Clear
Refresh
Properties
Directory Number
Call Serv CLLI
ver te
1418403000 COMPACT OK, ON-H(
1418403001 COMPACT OK, ON-H(
1418403002 COMPACT OK, ON-H(

Diagnostics

The Diagnostics menu contains the option to query gateways in trouble state.

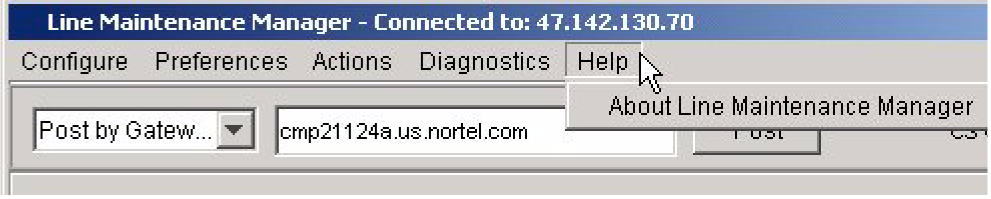
Diagnostics menu



Help

The Help menu contains an option to display LMM troubleshooting tips.

Help menu


Line Maintenance Manager - Connected to: 47.142.130.70
Configure
Preferences
Actions
Diagnostics
Help
About Line Maintenance Manager
Post by Gatew...
cmp21124a.us.nortel.com

Trunk Maintenance Manager

Overview

The Trunk Maintenance Manager (TMM) application is used to display trunks and perform maintenance activities on them.

> ***Note:*** To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 7.

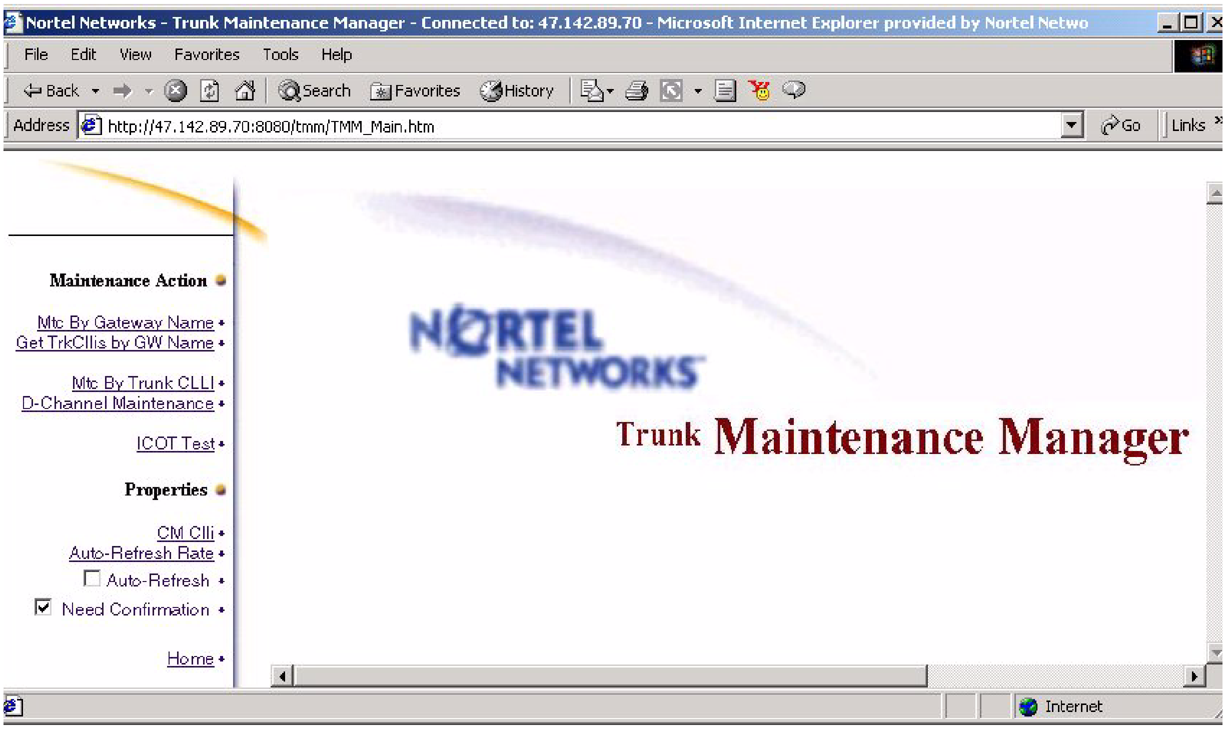
This section provides a brief overview of the TMM. For procedures on how to perform trunk maintenance activities using the TMM, refer to the CS 2000 Management Tools Fault Management document, NN10084-911.

User interface

The user interface for the TMM application is a web-based GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page. To access the Trunk Maintenance Manager, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

When the Trunk Maintenance Manager is launched, a window, similar to the following is displayed:

Trunk Maintenance Manager main window


Nortel Networks - Trunk Maintenance Manager - Connected to: 47.142.89.70 - Microsoft Internet Explorer provided by Nortel Netwo
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47.142.89.70:8080/tmm/TMM_Main.htm
Go Links
Maintenance Action
Mtc By Gateway Name
Get TrkCllis by GW Name
Mtc By Trunk CLLI
D-Channel Maintenance
ICOT Test
Properties
CM Clli
Auto-Refresh Rate
□ Auto-Refresh
☑ Need Confirmation
Home
NORTEL NETWORKS
Trunk Maintenance Manager
Internet

Using the Trunk Maintenance Manager GUI, you can perform any of the following activities:

- **Mtc By Gateway Name** - Perform the following maintenance actions on a selected gateway:
  - — query endpoint states
  - — post endpoints
  - — busy endpoints
  - — return endpoints to service
  - — force release endpoints
  - — installation busy endpoints
- **Get TrkCllis by GW Name** - Display a list of trunk CLLIs for a selected gateway.

- **Mtc By Trunk CLLI** - Perform the following maintenance actions on a selected trunks:
  - — post trunks
  - — busy trunks
  - — return trunks to service
  - — force release trunks
  - — installation busy trunks
- **D-Channel Maintenance** - Display statistics on D-channels for a selected PRI trunk.
- **ICOT Test** - Perform an ISUP (Integrated Services Digital Network User Part) continuity test on a trunk or group of trunks for a selected CLLI.
- **CM Clli** - Set the CM CLLI.
- **Auto-Refresh Rate** - Enable or disable the Auto refresh rate.
- **Need Confirmation** - Enable or disable confirmation on a request to busy an entire posted endpoint set (default is enabled where confirmation is required).
- **Home** - Return to the main window.

Batch provisioning tool

Overview

The batch provisioning tool (BPT) is included in the Succession Element and Sub-Network Manager (SESM) software package. The BPT provides users with the following capabilities:

- perform bulk configuration of Succession lines
- perform bulk flow through configuration of ADSL for MG 9000
- view the log and output files associated with each batch provisioning process
- delete the log and output files associated with each batch provisioning process

The batch provisioning commands are executed using a single OSSGate connection.

To perform provisioning activities using BPT, a user must be belong to user group “Inssprov”. Refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

For information on how to provision lines using the BPT, refer to the CS 2000 documentation suite.

User interface

The BPT is a command line user interface (CLUI). To access the BPT Refer to procedure “Starting the batch provisioning tool” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

A web browser interface, the Batch Configuration Monitor, is also provided for users to view output xml files in an easy readable format. The Batch Configuration Monitor is accessed through the common launch page as previously described under Common launch page. to access the Batch Configuration Monitor interface, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

Once logged in to the BPT, the Main menu, similar to the following, is displayed.

```
--------------------------------------------------
        ==================================
        Batch Provisioning Tool (BPT V1.0)
        ==================================

Username:ptm
Password:

Loging in process...

You are currently logged in as : ptm!

==========
Main Menu:
==========

     (1) Execute Batch File
     (2) Display Output
     (3) Display Logs
     (4) Delete Output or Log Files
     (h) Help

     (x) Exit

Selection: [1/2/3/4/h/x:1]
--------------------------------------------------
```

Execute Batch File

The Execute Batch File option allows you to execute batch provisioning commands. When you select this option, the Provisionining Input Entry Menu, similar to the following, is displayed.

```
--------------------------------------------------
==================================
Provisioning Input Entry Menu:
==================================


     (1) Lines
     (2) ADSL
     (3) Go to shell prompt
     (r) Return to the main menu.
     (x) Exit BPT.

Selection: [1/2/3/r/x:1]
--------------------------------------------------
```

- Lines - allows you to batch provision lines
- ADSL - allows you to batch provision ADSL
- Go to shell prompt - brings you to the command line where you can execute unix commands
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Display Output

The Display Output option allows you to view the output file associated with each batch provisioning process. When you select this option, the Display Output Menu, similar to the following, is displayed.

```
--------------------------------------------------
==================================
Display Output Menu:
==================================


     (1) Lines
     (2) ADSL
     (3) Go to shell prompt
     (r) Return to the main menu.
     (x) Exit BPT.

Selection: [1/2/3/r/x:1]
--------------------------------------------------
```

- Lines - allows you to view the output files that are currently in the Lines output directory
- ADSL - allows you to view the output files that are currently in the ADSL output directory
- Go to shell prompt - brings you to the command line where you can execute unix commands
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Display Logs

The Display Logs option allows you to view the log files associated with each batch provisioning process. When you select this option, the Display Log File Menu, similar to the following, is displayed.

```
--------------------------------------------------
==================================
Display Log File Menu:
==================================


     (1) Lines
     (2) ADSL
     (3) Go to shell prompt
     (r) Return to the main menu.
     (x) Exit BPT.

Selection: [1/2/3/r/x:1]
--------------------------------------------------
```

- Lines - allows you to view the log files that are currently in the Logs directory for lines
- ADSL - allows you to view the log files that are currently in the Logs directory for ADSL
- Go to shell prompt - brings you to the command line where you can execute unix commands
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Delete Output or Log Files

The Delete Output or Log Files option allows you to delete one or more output or log files from the Lines or ADSL directory. When you select this option, the Delete Files Menu, similar to the following, is displayed.

```
--------------------------------------------------
==================================
Delete Files Menu:
==================================


     (1) Lines
     (2) ADSL
     (3) Go to shell prompt
     (r) Return to the main menu.
     (x) Exit BPT.

Selection: [1/2/3/r/x:1]
--------------------------------------------------
```

- Lines - displays a menu with options to delete lines output files or lines log files
- ADSL - displays a menu with options to delete ADSL output files or ADSL log files
- Go to shell prompt - brings you to the command line where you can execute unix commands
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Help

The Help option displays information on the BPT, its menus and options.

Batch Configuration Monitor

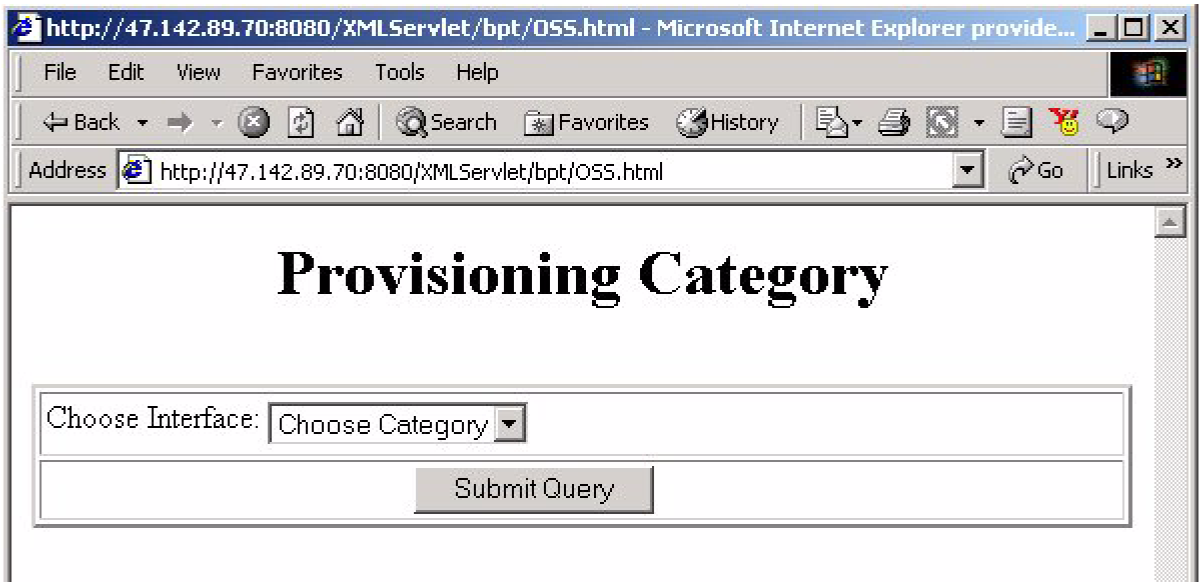
Overview

The Batch Configuration Monitor is a web browser interface to view provisioning output files in an easy readable format.

> ***Note:*** To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 7.

The Batch Configuration Monitor is accessed through the common launch page as previously described under Common launch page. To access the Batch Configuration Monitor interface, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

The web browser window is similar to following.


http://47.142.89.70:8080/XMLServlet/bpt/OSS.html - Microsoft Internet Explorer provide...
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
History
Address
http://47.142.89.70:8080/XMLServlet/bpt/OSS.html
Go
Links
Provisioning Category
Choose Interface:
Choose Category
Submit Query

From this window, you can select an interface and display a list of provisioning output files that are available in the output directory for the selected interface.

> ***Note:*** ADSL is the only interface supported in the SN06 release.

Network Patch Manager

Overview

The Network Patch Manager (NPM) is a patch management solution for Nortel Networks network-based products. Patching using the NPM is currently supported for the following components:

- CS 2000 Gateway Controller (GWC)
- Media Gateway 9000 (MG 9000)
- Media Gateway 9000 Manager (MG 9000 Manager)
- CS 2000 SAM 21 Element Manager (SAM21 EM)
- Patching Server Element (PSE)
- Succession Element and Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Network Patch Manager (NPM)

The NPM uses the Patch File Receipt System (PFRS) and the Patching Server Element (PSE) device.

Patch File Receipt System

The Patch File Receipt System (PFRS) provides an automated means of interacting with an upstream patch administration and delivery system, for example, the Regional Patch Selector (RPS), to make new patch files available to the NPM.

When installed, PFRS runs each of two tasks once every 24 hours. First, it generates a report specifying the patch and load content for each device in the site. Second, it detects newly available patch files and brings those patches into the NPM system (getpatch). The second task (getpatch) is typically run several hours after the first task (report).

The delay between execution of the tasks allows an upstream patch administration and delivery system time to view the day's report, calculate patches needed by the site, and download the needed patches to a designated "drop-off" location. When the PFRS getpatch task runs, the newly downloaded patch files are discovered and introduced into the NPM system.

The two tasks, the report and the getpatch, are run several hours apart. The status report is typically run in the evening (9:00 PM). The getpatch phase is typically done in the early morning hours (5:00 AM).

The PFRS 24-hour cycle typically uses the following schedule:

- PFRS generates the report showing the patch status of the site and puts the report file in the designated dropbox.
- Some time later, the upstream patch administration system gets the report from the dropbox.
- The upstream patch administration system uses the report to "calculate" which newly available patches are needed by the site.
- The upstream patch administration system downloads new patches to the site's dropbox.
- Some time later, PFRS executes the getpatch task which makes the new patches known to the NPM server and database, puts a copy of the each patch file in NPM's "Au" directory, and determines which devices can use the patch (i.e., creates a VA status where appropriate).

Note: PFRS does not automatically apply any patches.

The PFRS has the following requirements for use in the NPM:

- An interface server hosting an FTP server that is accessible using a userid and password with full read, write, and overwrite access, must be available.
- The default directory of the FTP user (1 unique user per site recommeded) on the FTP server must provide the location from which patch files are retrieved and to which reports are written.
- The PFRS can be configured at any time after NPM is installed, using the command line interface (CLI) tool.
- A CLLI name is required to configure PFRS. You can retrieve the CLLI name from table OFCENG.
- The IP address or host name of the interface server is required to configure PFRS.

Patching Server Element Device

The patching server element (PSE) device enables communication between the NPM and OAM devices to be patched on the SSPFS platform. The PSE also tracks patch data and information on each OAM device.

User interface

The NPM provides a graphical user interface (GUI) and a command line user interface (CLUI). Both interfaces offer the same functionality. Using the NPM GUI or CLUI, you can

- apply and remove patches
- activate and deactivate patches
- restart OAM devices
- perform file management, tracking, and reporting

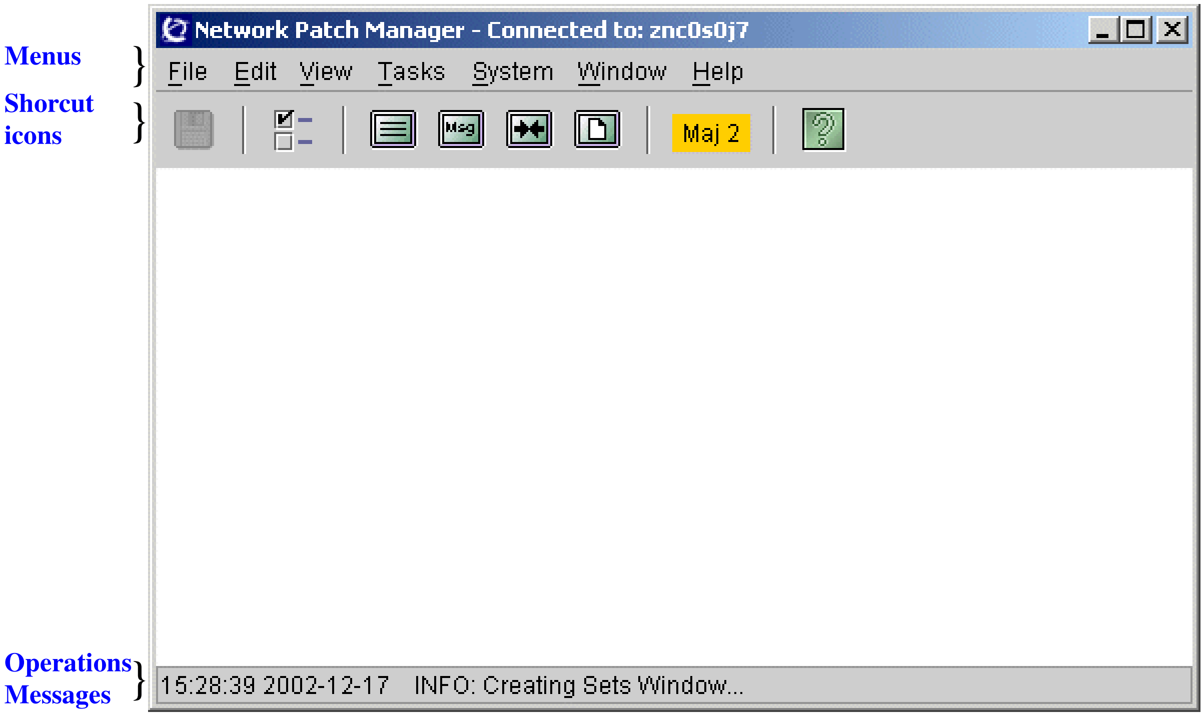
Users who need to perform patching activities using the NPM GUI or CLUI, need to belong to user group “emsadm”. Refer to procedure “Setting up users on a Sun server” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

NPM GUI

The NPM GUI is a Java^{TM} Web Start (JWS) application delivered through a web browser that provides full access to all patching functionality. The NPM GUI is accessed through the common launch page as previously described under Common launch page.To access the NPM GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

The following figure shows an example of the NPM GUI.

The NPM GUI


Menus
Shorcut icons
Operations Messages
Network Patch Manager - Connected to: znc0s0j7
File Edit View Tasks System Window Help
Msg
Maj 2

15:28:39 2002-12-17 INFO: Creating Sets Window...

The GUI provides menus along the top with shortcut icons for some of the menu items below. Placing your cursor over an icon indicates its function. Operation messages are displayed at the bottom of the window.

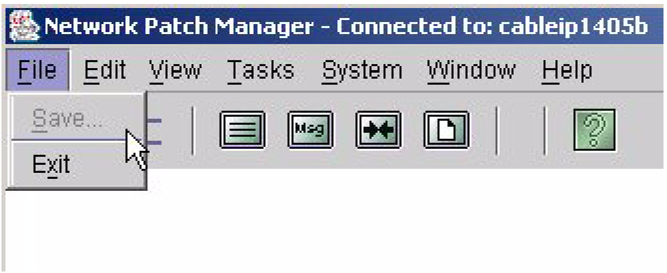
The sections that follow briefly describe the options available under each menu. More details are provided in the online help for the Network Patch Manager (see Help).

File

The File menu contains the following options:

- **Save** - save the data of the currently active window to a file
- **Exit** - exit the Network Patch Manager GUI

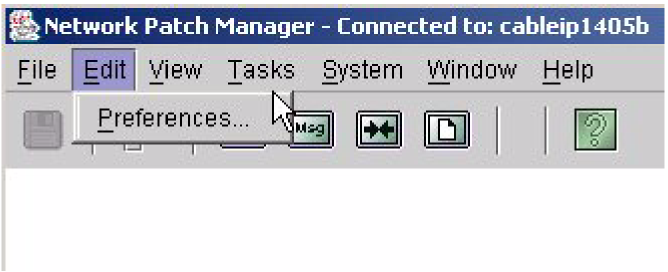
File menu



Edit

The Edit menu contains the **Preferences** option used to enable or disable the display of patching activity results, and enable or disable debug messages.

Edit menu

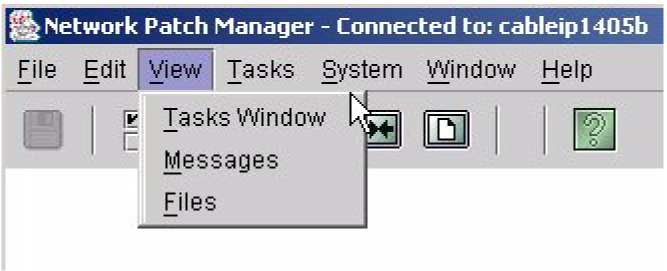


View

The View menu contains following options:

- **Tasks Window** - display maintenance tasks (apply, remove, and audit) and their current status
- **Messages** - display all system messages and responses received during the current session
- **Files** - view details of patch files

View menu

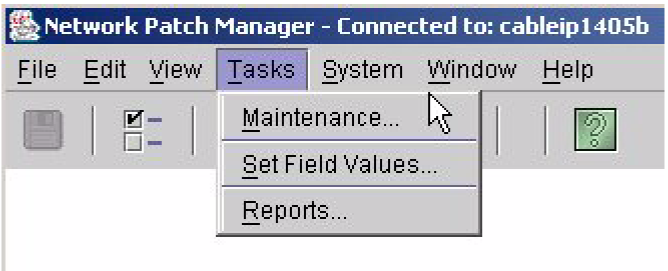

Network Patch Manager - Connected to: cableip1405b
File Edit View Tasks System Window Help
Tasks Window
Messages
Files

Tasks

The Tasks menu contains the following options:

- **Maintenance** - initiate patching tasks such as apply, remove, activate, and deactivate
- **Set Field Values** - set database field values such as PATCH.HOLD, and DEVICE.HOLD
- **Reports** - define and generate reports

Tasks menu

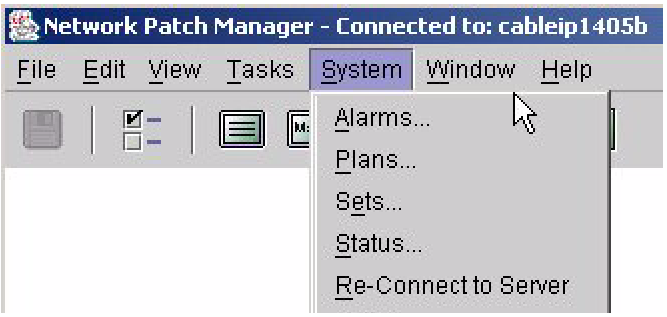

Network Patch Manager - Connected to: cableip1405b
File Edit View Tasks System Window Help
Maintenance...
Set Field Values...
Reports...

System

The System menu contains the following options:

- **Alarms** - define and manage alarms
- **Plans** - define, modify or delete a plan, which is a list of one or more tasks such as apply, remove, audit, reports, that can be executed according to a specified schedule
- **Sets** - define sets, which are groupings of patches and devices used in routine patching tasks
- **Status** - view details for currently active alarms
- **Re-Connect to Server** - reconnect to the server in the event the connection is lost

System menu

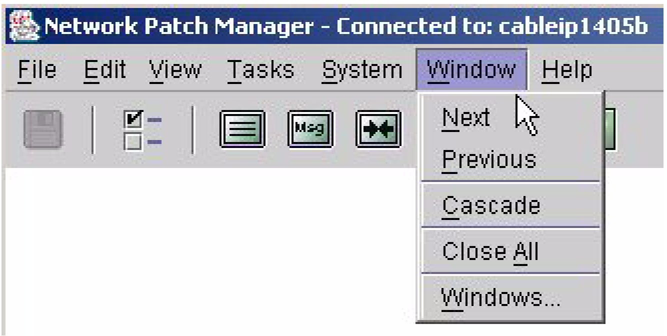


Window

The Window menu contains the following options:

- **Next/Previous** - activate the next or previous open window
- **Cascade** - auto-arrange all open windows on the desktop
- **Close All** - close all open windows
- **Windows** - view all open windows, and switch to or close an open window

Window menu

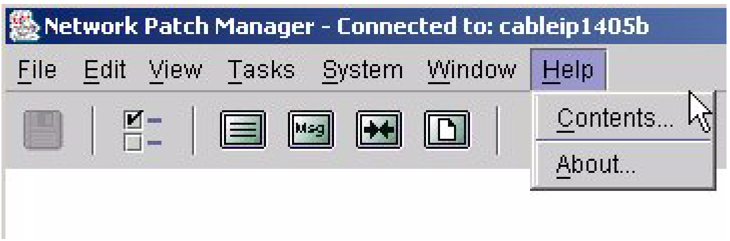


Help

The Help menu contains the following options:

- **Contents** - display online help information for the NPM
- **About** - display the version of the NPM GUI, NPM server application, and NPM database schema

Help menu



NPM CLUI

The CLUI offers the same functionality as the GUI, but in a command-line approach. Additionally, the CLUI services can be used as an Application Programming Interface (API) for scripts that need to access patching information or functions.

Alarms

The Network Patch Manager (NPM) includes a set of pre-defined system alarms at install. You cannot remove or modify these alarms, however, you can disable them (refer to procedure "Enabling and disabling alarms using the NPM" in the CS 2000 Management Tools Fault Management document, NN10084-911). By default, all system alarms are enabled.

The following table lists the NPM system alarms and provides a brief description of each.

NPM system alarms

Alarm name	Description	Severity
ACT_NOT_APP	Activatable patch not applied to all applicable devices	No alarm
ACT_NOT_ACT	Activatable patch applied to all applicable devices but not activated in all devices	No alarm
DEBUG_APP	Debug patches applied	Minor
DNR_NOT_APP	Do Not Remove (DNR) patches not applied	Critical
EMG_NOT_APP	Emergency (EMG) patches not applied	Critical
GEN_NOT_APP	General (GEN) patches not applied	No alarm
LTD_NOT_APP	Limited (LTD) patches not applied	No alarm
OBS_NOT_REMOVED	Obsolete (OBS) patches not removed	Major
OBE_NOT_REMOVED	Obsolete Emergency (OBE) patches not removed	Critical

NPM system alarms

Alarm name	Description	Severity
REMOVED_PATCHES	Removed patches which are not category OBS, OBE, or DBG	No alarm
PATCH_ONHOLD	Patches on hold	Minor
DEVICE_ONHOLD	Devices on hold	Minor
DEVICE_AUDITFAIL	Devices which have failed or not executed audits since registration	Major
DISABLED_APPLIED	OAM processor patch has been applied but not enabled	Major
ENABLED_REMOVED	OAM processor patch has been removed but not disabled	Major

In addition to the pre-defined system alarms, you can create your own alarms to match your specific criteria. Refer to procedure “Defining alarms using the NPM” in the CS 2000 Management Tools Fault Management document, NN10084-911.

Logs

The Network Patch Manager (NPM) generates logs, which can help in troubleshooting activities. The logs are saved into a local file “/data/npm/logs/custlogs”, but you can also send them into the customer’s log system through an Operations Support Systems Interface (OSSI).

The following figure shows an example of the log file.

Example NPM log file

```
  NPM600 APR29 16:36:54 0100 INFO General Information
     The Network Patch Manager Server has been started.

  NPM400 APR29 16:48:19 0200 SUMM Action Summary
     Patch ID, Device ID, Command, Pass/Fail, Time Complete
     ----------------------------------------------------
      NONE, gwc9 Unit 0 47.142.108.62, AUDIT, Pass, 4:48:19 PM

* NPM303 APR29 16:57:24 0300 TBL Device Audit Failure
     The audit of the following device was not successful
      device: gwc9 Unit 1 47.142.108.63

  NPM400 APR29 16:57:24 0400 SUMM Action Summary
     Patch ID, Device ID, Command, Pass/Fail, Time Complete
     ----------------------------------------------------
      NONE, gwc9 Unit 0 47.142.108.62, AUDIT, Pass, 4:57:24 PM
      NONE, gwc9 Unit 1 47.142.108.63, AUDIT, Fail, 4:57:24 PM

  NPM600 APR29 20:7:26 0500 OFFL General Information
     The NPM Server has shut down.
```

The NPM logs are grouped into logical sets based on the log number as follows:

- NPM300 to NPM399 - Trouble logs
- NPM400 to NPM499 - Service summary logs
- NPM600 to NPM699 - Information logs

Log severity is indicated by a number of asterisks at the beginning of the log.

- <none> - information
- * - minor
- ** - major
- *** - critical

For details on each of the NPM logs, refer to the Succession Fault Management Logs Reference document, NN10275-909.

CS 2000 SAM21 Manager

Overview

The CS 2000 SAM21 manager is a client-server application. The client application runs on either a Solaris or a Windows platform, and the server application runs on the CS 2000 Management Tools server (SSPFS platform).

> ***Note:*** In SN06.2, there are two clients; one that is used with the CS 2000 Core Manager during the upgrade only, and the other that will be used in SN06.2 with the SAM21 Manager server application running on the CS 2000 Management Tools server (SSPFS platform) after the upgrade.

The CS 2000 SAM21 Manager is used to manage the SAM21 network elements within a Succession Network. The SAM21 Manager allows remote device management of multiple SAM21 network elements at the card level through a single graphical user interface (GUI).

> ***Note:*** To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 7.

User interface

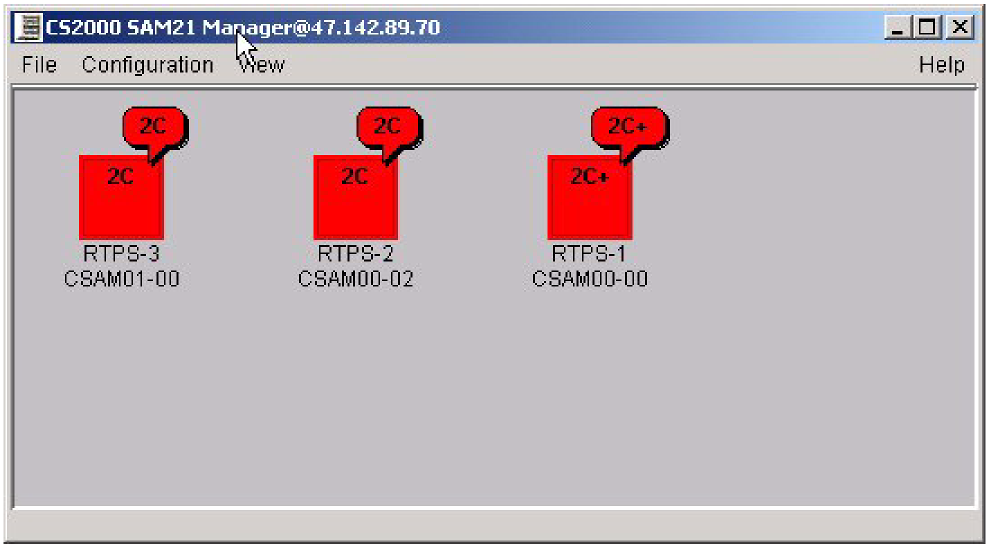
The user interface for the CS 2000 SAM21 Manager application is a web-based GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page. To access the CS 2000 SAM21 Manager GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the CS 2000 Management Tools Administration and Security document, NN10172-611.

The CS2000 SAM21 Manager GUI provides a Subnet view, a Shelf view, and a Card view.

Subnet view

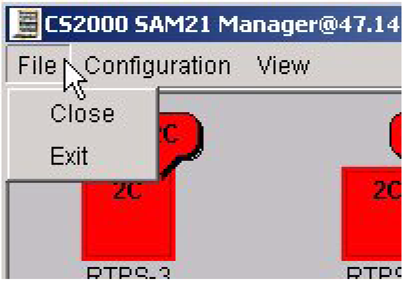
The subnet view, similar to the following, is displayed when the CS2000 SAM21 Manager GUI is launched.

CS2000 SAM21 Manager subnet view



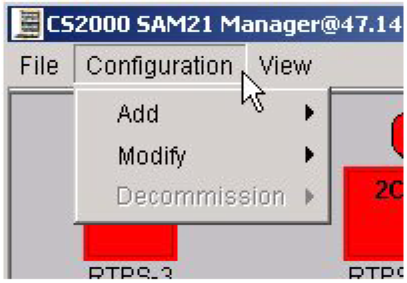
File menu

The File menu provides the options to Close or Exit the CS 2000 SAM21 Manager.



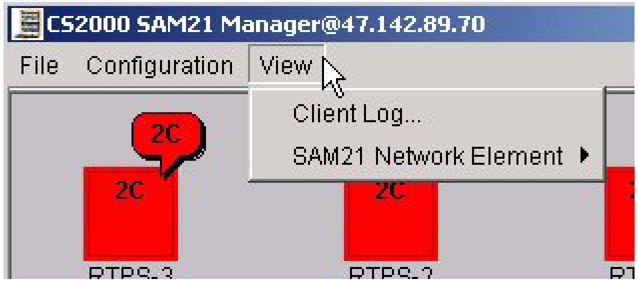
Configuration menu

The Configuration menu provides the options to Add, Modify, or Decommission a SAM21 network element.



View menu

The View menu provides the options to view the client log and display the shelf view of a SAM21 network element.

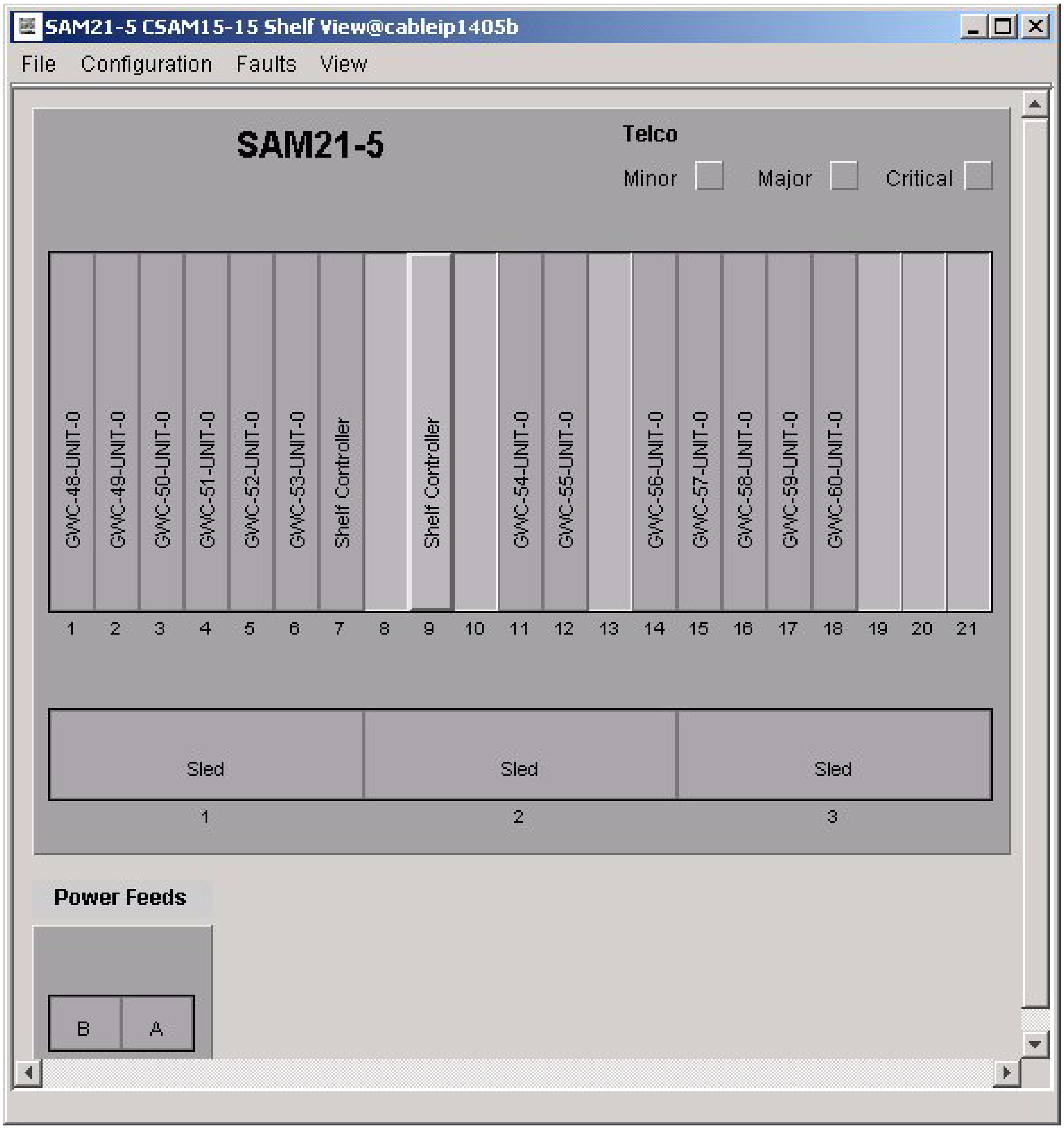


Note: You can also display the shelf view of a SAM21 network element by double clicking on the SAM21 network element icon in the GUI window.

Shelf view

The Shelf view, similar to the following, is displayed by selecting the SAM21 Network Element option from the View menu of the Subnet view.

Shelf view of a SAM21 network element



File

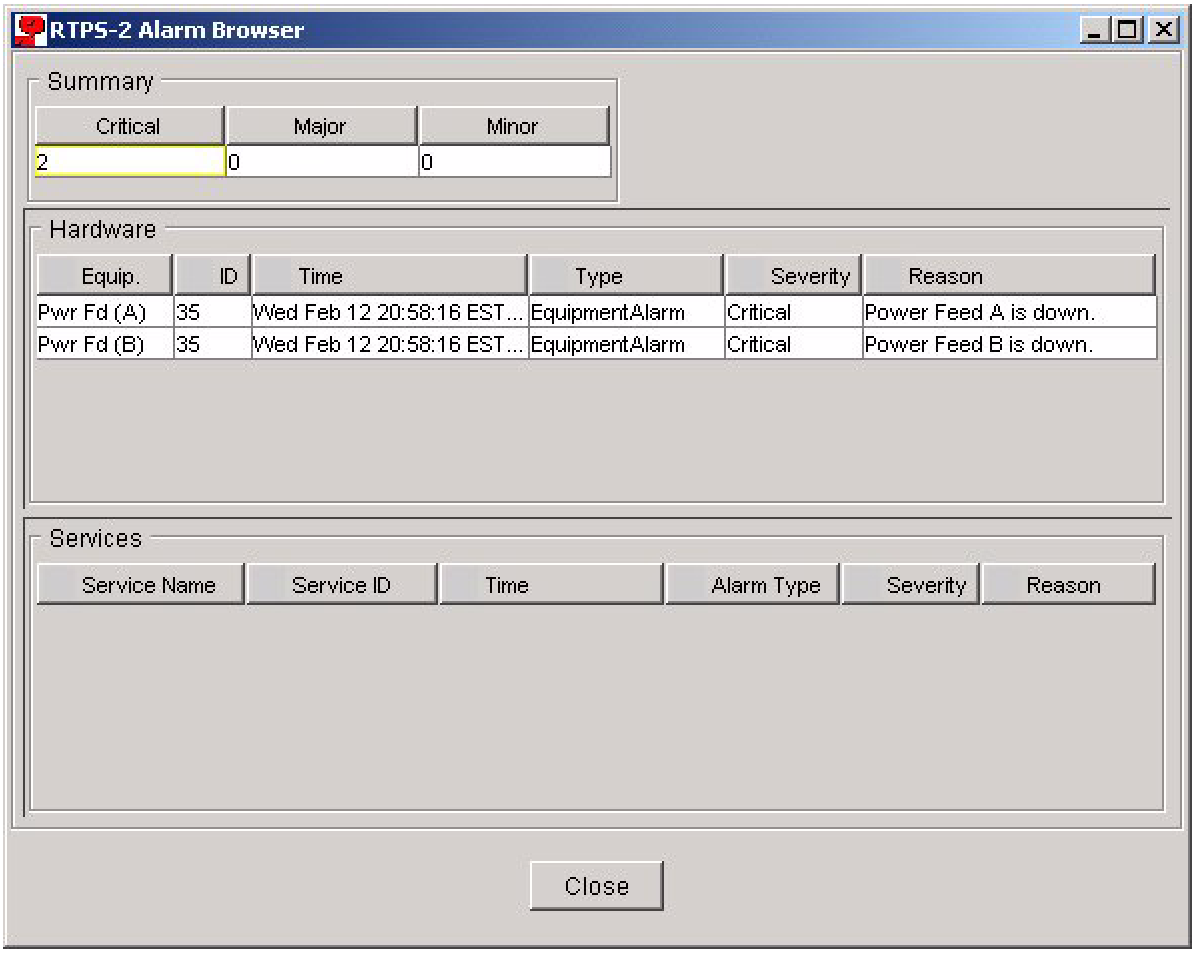
The File menu provides the option to close the shelf view.

Configuration

The Configuration menu provides the options to configure IPoA services and ATM PMC addresses.

Fault

The Fault menu provides the option to display the alarm browser, which shows alarm information for all cards in the SAM21 shelf. When the option is selected, a window similar to the following is displayed.



Critical	Major	Minor
2	0	0

Equip.	ID	Time	Type	Severity	Reason
Pwr Fd (A)	35	Wed Feb 12 20:58:16 EST...	EquipmentAlarm	Critical	Power Feed A is down.
Pwr Fd (B)	35	Wed Feb 12 20:58:16 EST...	EquipmentAlarm	Critical	Power Feed B is down.

Service Name	Service ID	Time	Alarm Type	Severity	Reason

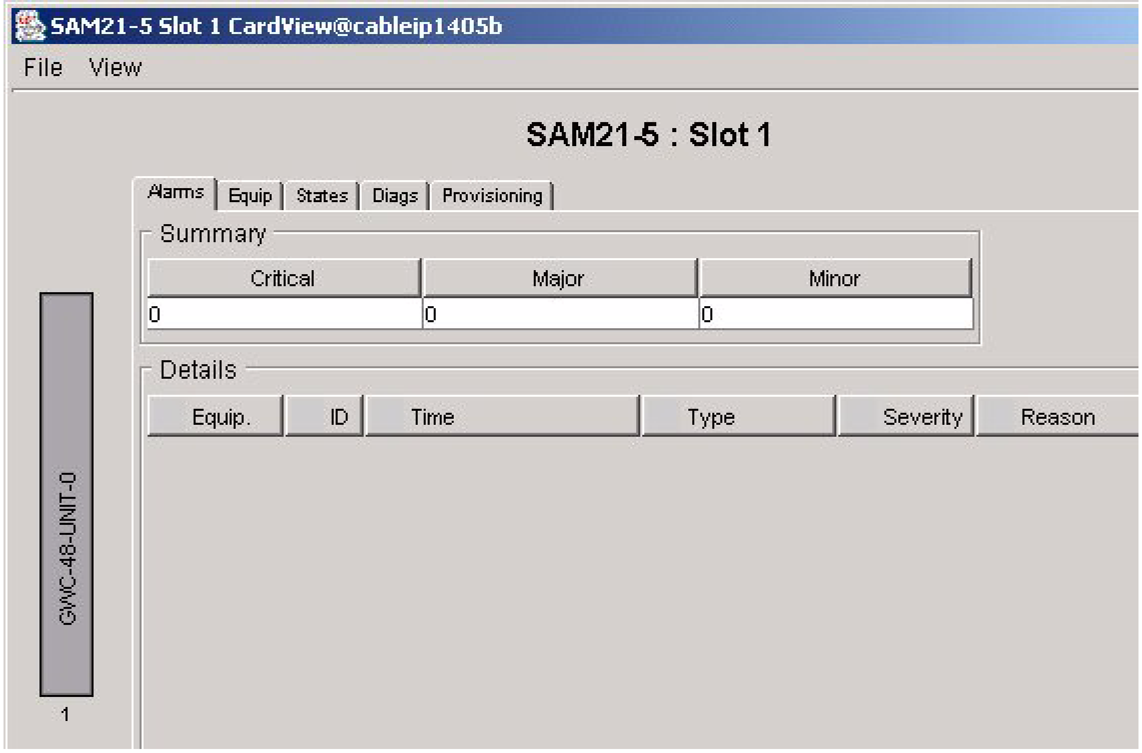
View

The View menu provides the options to display the client log, the card view, or the subnet view.

Card view

The Card view, similar to the following, is displayed by selecting the Card Views option from the View menu, by double clicking a card, or by right-clicking a card from the Shelf view and selecting the Card View... option.

Card view



SAM21-5 : Slot 1

Summary

Critical	Major	Minor
0	0	0

Details

Equip.	ID	Time	Type	Severity	Reason

Alarms tab

The Alarms tab displays the number of alarms on the card and the details on each alarm.

Equip tab

The Equip tab displays the type of card and memory size.

States tab

The States tab displays the current state of the card as well as a history of its state.

Diags tab

The Diags tab allows a user to perform brief or full diagnostics on the card and view status messages.

Provisioning tab

The Provisioning tab displays the provisioning details for the card.

QoS Collector application

Overview

The Quality of Service (QoS) Collector Application (QCA) collects QoS records and stores them. QoS records contain a set of QoS parameters collected on a per-call basis. The QoS parameters that are collected are

- packets sent
- packets received
- packet loss
- octets sent
- octets received
- inter-arrival latency
- jitter

The QCA receives binary QoS records from the Gateway Controllers (GWCs), converts these records to QCA Internet Protocol Detail Records (IPDRs), and stores them in a file. The OSS can obtain these QCA IPDRs and process them.

> ***Note:*** For details on the required disk space to store QCA data, refer to section Required disk space to store QCA data in this document.

The configuration details for the QCA are contained in a properties file on the CS 2000 Management Tools server. Users can modify the configuration details for the QCA through the QCA properties. The QCA must be stopped and restarted for any changes in the properties file to take place.

The Quality of Service (QoS) Collector Application (QCA) is installed when the the CS2M NCL software package is installed. The procedures available for the QCA are as follows:

- “Installing the QCA software package on a separate server” in the Upgrades document.

  Note: Nortel Networks recommends that you install a second instance of the QCA on another dedicated t1400 server to support in-service upgrades without loss of records.

- “Configuring the QoS Collector Application” in the Configuration Management document.
- “Starting the QoS Collector Application” in the Administration and Security document.

To add a QoS collector to the network and associate it with a gateway controller, refer to the GWC documentation suite.

Restriction and limitations

QoS reporting is applicable to more than just VoIP networks. It can also be used in ATM and hybrid networks. However, up to the SN06.2 release, QoS reporting has only been validated to GWC-driven GWs in Succession Cable solutions.

If you are interested in using QoS reporting in your non-Cable solution, please contact your Nortel Networks account prime for more information.

All gateways in SN06.2 VoIP solutions will report these statistics via end-of-call reporting mechanisms specific to the protocol used for MGC - VMG communication.

The GWs that are supported are listed below.

- UAS (H.248)
- Motorola CG4500 (NCS)
- PVG (Aspen/VSP2)
- PVG (Aspen/VSP3)
- PVG (H.248)
- Mediatrix (MGCP)
- Arris PacketPort (MGCP)
- Askey

Required disk space to store QCA data

The following table provides guidelines for the required disk space to store QCA data for one day.

Estimated average traffic rate (BHCA)	Minimum disk space required to store QoS records for 1 day (GB)
250K	0.504
500K	1.008
750K	1.512
1M	2.016
1.25M	2.52
1.5M	3.024
1.75M	3.528
2M	4.032

The required disk space indicated in the table, was calculated as follows:

- BHCA = 500K
- Calls per day = 10 hours of traffic per day x BHCS = 5M
- QoS records per day = 2 x calls per day = 10M
- Record size = 840 bytes
- Compression ratio = 88%
- Required disk space for 1 day = 10M x 840 = 8.4GB
- When using compression = 8.4GB x 0.12 = 1GB

> ***Note:*** If the storage period is greater than one day, the disk space must be increased accordingly.

To increase disk space of “/data/qca”, refer to procedure “Increasing the size of file systems” in the CS 2000 Management Tools Configuration Management document, NN10106-511.

OSSGate

Overview

OSSGate is an application that provides a machine interface for provisioning components within Succession. The main functionality of OSSGate is to act as a gateway to the Node, Carrier, Trunk, Line, ADSL Provisioning applications and the Trunk Maintenance application. It provides the end user with an alternative to the GUI (graphical user interface) as a method for provisioning succession components.

For detailed information on OSSGate, refer to the OSSGate User Guide.

PM poller

Overview

The Performance Monitoring (PM) Poller is delivered as a sub-package within the Succession Server Platform Foundation Software (SSPFS). The PM poller provides a simple network management protocol (SNMP)-based system to gather performance information from the gateway controller (GWC), Universal Audio Server (UAS), SAM21 shelf controller, Media Server 2010 (MS 2010), and the Succession Server Platform Foundation Software (SSPFS).

The PM poller is configured with server information that provides system attributes for the system to be monitored. The poller is also configured with a number of profiles that determine data collection. Profile information can include the type of data collected, how often the data is collected, and the device from which the data is collected. The PM poller can have many profiles, each defining a distinct set of polling characteristics.

To set up SNMP polling in your network, refer to procedure “Setting up the PM poller” in the CS 2000 Management Tools Configuration Management document, NN10106-511.

Data collection output

The data collected by the PM device pollers is output in Comma Separated Value (CSV) files to the “/data/oms” file output directory. The oms directory contains seven sub-directories (named 1 through 7), which in turn contain a day’s collection of CSV output files. The current day’s output files are always written to sub-directory ’1’. File rotation occurs just prior to midnight every 24 hour period. When file rotation occurs, the files in sub-directory ’7’ are removed, and the contents of each sub-directory are moved up one sub-directory. For example, the contents of sub-directory 6 are moved up to sub-directory 7.

Viewing output files

The CSV files can be loaded into a customer supplied text viewer or spreadsheet software to browse the raw data.

> ***Note:*** The CSV file format is not intended to be a user-friendly format for viewing the output using a standard text editor.

We recommend that you use an OSS tool to view the CSV output files. If you require a product to analyze and view performance data, contact your Nortel Networks account prime to allow Nortel staff to review and recommend a commercial solution.

Logs

The PM Poller uses the SSPFS syslog interface to log internal poller events. These events include the starting and stopping of the poller, polling session activities, and internal poller errors. These logs can be extremely useful in debugging PM Poller related issues. The command to monitor the PM poller syslog stream is as follows:

```
# tail -f /var/adm/messages
```

> ***Note:*** PM poller logs are preceded by “SNMPP”.

User interface

User interface tools, “snmpp_ctl” and “snmpp_cfg” are provided as part of the PM Poller package to control the state of the PM Server, Query configured data add or modify polled device configuration data attributes.

OMPUSH application

Overview

The OMPUSH application is delivered as a sub-package within the Succession Server Platform Foundation Software (SSPFS). The OMPUSH application is used to make scheduled OM (CSV/SSV) file transfers to predefined remote servers using File Transfer Protocol (FTP) or Secure FTP (SFTP).

The OMPUSH application does not create the OM files, but transfers them. The OMPUSH application can tranfer two types of OM files:

- MG 9000 OM files, which are collected by the MG 9000 OM collector
- SSPFS, GWC, UAS, and SAM21 SC OM files, which are collected by the SNMP PM poller.

> ***Note:*** All OM files to be transferred must reside on the server where OMPUSH is installed.

User interface

The OMPUSH application is a command line user interface (CLUI) with the following tools:

- OMPUSH application control tool.
- OMPUSH session configuration tool.

OMPUSH application control tool

The OMPUSH application control tool (**ompush_ctl**) is used to start, stop, and query the state of the OMPUSH server application. When the OMPUSH server application is running, the query also returns the status of existing OMPUSH sessions.

For a list of the sub-commands available with this tool, refer to Commands for the OMPUSH application control tool.

Commands for the OMPUSH application control tool

The following table lists the tasks you can perform with the OMPUSH application control tool, and their associated command.

Task	Command
Start the OMPUSH server application.	**ompush_ctl -start**
Stop the OMPUSH server application.	**ompush_ctl -stop**
Re-synchronize the OMPUSH server application with the configuration data. ***Note:*** You can also re-synchronize by stopping and starting the OMPUSH server application.	**`ompush_ctl -sync`**
Query the status of the OMPUSH server application, as well as the status of existing OMPUSH sessions (only provided when the OMPUSH server application is running)	**`ompush_ctl -status`**
Display help information for the OMPUSH application control tool	**`ompush_ctl -help`**

OMPUSH session configuration tool

The OMPUSH session configuration tool (**ompush_cfg**) is used to

- create a new session
- modify a session
- query a session
- delete a session
- activate or deactivate a session

Only one instance of the OMPUSH session configuration tool (ompush_cfg) is supported at one time.

The OMPUSH session configuration tool provides the following two interface types:

- full-screen menu mode that steps you through the provisioning process
- a command line interface (CLI) for provisioning data with batch scripts

  For a list of the sub-commands available from the command line, refer to Commands for the OMPUSH session configuration tool.

Commands for the OMPUSH session configuration tool

The following table lists the tasks you can perform with the OMPUSH session configuration tool CLI, and their associated command.

> ***Note:*** It is recommended not to use the “Home”, “End”, “Insert”, “Delete”, and “Break” keys when using the OMPUSH session configuration tool CLI, as they may have a different function for different terminals and cause some unexpected errors.

Task	Command
Access the OMPUSH full-screen configuration mode.	**ompush_cfg -menu**
Create a new OMPUSH session.	**ompush_cfg -create <SessionName> <Attribute=Value ... >**
Modify an OMPUSH session.	**ompush_cfg -modify <SessionName> <Attribute=Modify ... >**
Activate an OMPUSHsession.	**ompush_cfg -activate <SessionName>**
Deactivate an OMPUSH session.	**ompush_cfg -deactivate <SessionName>**
Display details of an OMPUSH session.	**ompush_cfg -query <SessionName>** ***Note:*** If no value is entered for <SessionName>, all sessions will be displayed.

Task	Command
Delete an OMPUSH session.	`ompush_cfg -delete <SessionName>`
Display help information for the OMPUSH session configuration tool.	`ompush_cfg -help`

Logs

The OMPUSH application uses Syslog to log events such as starting and stopping the OMPUSH server application, configuration file errors, file push session activities, and internal push errors . All OMPUSH logs are preceded by "OMPUSH". To view OMPUSH logs, refer to procedure "Viewing OMPUSH logs" in the CS 2000 Management Tools Fault Management document, NN10084-911.

Additional information

The following procedures are available for the OMPUSH application:

- "Starting the OMPUSH server application" in the Administration and Security document.
- "Stopping the OMPUSH server application" in the Administration and Security document.
- "Creating an OMPUSH session" in the Configuration Management document.
- "Modifying an OMPUSH session" in the Configuration Management document.
- "Deleting an OMPUSH session" in the Configuration Management document.
- "Activating or deactivating an OMPUSH session" in the Configuration Management document.
- "Querying OMPUSH session attributes" in the Configuration Management document.
- "Viewing OMPUSH logs" in the Fault Management document.

Resource monitor

Overview

The resource monitor (RESMON) application is included with the Succession Server Platform Foundation Software (SSPFS). It is automatically started when the SSPFS server is started.

The resource monitor can detect the following hardware and software faults:

- fan failure
- disk failure
- loss of network connectivity
- power supply unit (PSU) failure
- temperature exceeding a defined threshold
- file system usage exceeding a defined threshold

The resource monitor generates a log when a fault occurs, as well as when a fault is cleared. For log details, refer to the CS 2000 Managemen Tools Fault Management document, NN10084-911.

The resource monitor also triggers the corresponding fault light to go on when a fault occurs, or off when a fault is cleared.

Media Server 2000 Series Configuration Tool

The Media Server 2000 Series Configuration Tool, commonly referred to as MS 2010 CLUI, is the primary tool used for normal MS 2010 configuration activities.

For details, refer to *MS 2000 Series Configuration Management* NTP NN10340-511.