Carrier VoIP

Nortel ATM/IP Solution-level Configuration

NN10409-500

Document status: Standard
Document version: 04.03
Document date: 20 October 2006

Nortel ATM/IP Solution-level Configuration

New in this release

(I)SN09U is an extension of the (I)SN09 software release and supersedes both (I)SN09 and (I)SN09FF for CVoIP applications. (I)SN09 continues to be supported for TDM-only applications. The (I)SN09U software release incorporates all capabilities of (I)SN09, (I)SN09FF, and additional corrective content delivered as part of Nortel's (I)SN09 software robustness program. (I)SN09, (I)SN09FF, and (I)SN09U are valid terms for use within the (I)SN09U software release.

The following table highlights the (I)SN09U features that affect configuration management.

(I)SN09U ATM/IP features

Feature descriptions
SIP Lines MADN Support (CHS) The purpose of this feature is to interwork a specific set of Session Initiation Protocol (SIP) clients into IBN/RES network-based Multiple Appearance Directory Number (MADN) Single Call Arrangement (SCA) features.
Pass Phrase Protected Keys for SSH (IAW, IAC, PT-IP, UA-IP, ATM) This feature enhances the existing secure outbound file transfer functionality by introducing the key-based (public key) authentication. The key-based authentication mechanism is provided as an additional option for the user. Hence, the user can select to use either the password-based or the key-based authentication while adding and changing the secure file transfer schedules in the SBA (billmtc) or OMDD (omui) user interface programs.
CS 2000 features
Enhanced ESA for International MG9000 (UA-IP) This activity allows the download of information necessary to support International Emergency Stand Alone (ESA) call processing across all native (non ABI) and ABI lines served by a single MG9000 for intra and internodal ESA.
ACD Call Recording Phase I (ATM, UA-IP, PT-IP, IAC, IAW, CHS)

Feature descriptions

This feature provides trunk information in the ICM (Intelligent Call Management) protocol to facilitate call recording functionality in a TDM environment.

UUI NI-2 PRI over SCAI (ATM, UA-IP, PT-IP, IAC, IAW, CHS)

This feature supports only the “Preferred UUS” option which is an existing option in table LTDATA. User-to-User Service (UUS) starts with UUS option datafilled against a given LTID in table LTDATA. The UUS option is already available for tuples in table LTDATA. At present, it is enabled for NI-2 LTIDS on GWC. This feature enables UUS as an option for NI-2 LTIDS on SPM and XPM(DTCI).

Carrier Hosted SVCS\Applications (PT-IP)

This feature is a development of an (I)SN09 feature which limited the direct networking between two CS2K using SIP network. This featurenow allows the following:

Session Initiation Protocol (SIP) based network message waiting service (NMS) support based on RFC 3842 interworking with tandem solutions.
Testing of message waiting indication (MWI) and NMS with RFC 3842 compliant SIP based 3rd party VM/UM.
Testing of the MWI and NMS with RFC 3842 compliant SIP based open source VM/UM system

Gateway Controller features

G729 CODEC FOR AAL2 (UA-AAL1)

This feature supports SESM provisioning to allow G.729 in AAL2 solution .

GWC EM Support for Siren (PT-IP. UA-IP, IAW, IAC, intl IAW, intl IAC, intl PT-IP, intl UA-IP)

This feature modifies the GWC provisioning to support Siren and simplifies it for CVoIP.

ABI SMU Support (UA-AAL1)

This activity adds support for the SMU (Subscriber Module Urban) and its subtending RCU (Remote Concentrator Urban) to the list of legacy PMs supported by the ABI program. The ABI program allows legacy host XPMs to be connected to the packet network without use of an ENET and an I/W Bridge.

MG 9000 features

International MG9000 Line Test Support (intl UA-IP)

This feature provides support for MG9K Line Testing for International markets. Line Testing and troubleshooting are done using Maintenance and Administration Position (MAP) user interface at the levels under LNS MAP level. The LNS MAP level contains the lines test position (LTP) menu commands, the automatic line testing (ALT) menu commands and the lines service trouble (LNSTRBL) commands.

MG9KEM support for GLC12 coin line card (UA-AAL1, UA-IP)

This feature introduces the GLC12 card that is replacing the existing SAA12 card. This card has to support all the capabilities of the SAA card inclusive of the coin telephone support.

MG9K PKI Development (UA-IP)

Feature descriptions

This feature calls for using some functions of Public Key Infrastructure (PKI) to manage the generation and distribution of keys used to authenticate nodes participating in an IPSec session.

Integrated Element Management System (IEMS) features

IEMS - MS20X0 IPSEC CONFIGURATION SUPPORT (UA-IP)

This feature adds IPSec and IKE configuration capabilities to the MS 2000 node configuration tool. This will allow the craftsperson to enable IPSec for secure messaging between the IEMS and MS 2000 as well as configure the IPSec and IKE parameters necessary for the MS 2000 to securely send and receive messages to and from the GWC.

CS2K SS Integration (UA-IP)

In (I)SN07 and (I)SN08, IEMS manages the Multimedia Communication Server Manager (MCS Manager). The MCS Manager when added can have as its managing type either an MCS/CSE MX NE or Media Proxy NE. When an MCS Manager is added to they IEMS, the MCS/CSE MX NE or Media Proxy NE is added as a map symbol under the Network Elements. The MCS System Manager is added as an element in the Element Managers map.

SPFS features

Disabling Non-secure Network Services in SPFS

This activity provides some configuration tools to assist customer in configuring the server based on their security policy. Upon completion of the fresh system installation or upgrade, the customer (security administrator) has the possibility to apply the security policy on the server via a command line interface.

SESM features

SESM: SIP Lines - Data Sync Audit (MCS)

The Line Audit feature component will add auditing coverage of SIP line data on the SS-EM. The data to be audited on the SS-EM includes the Directory Number(DN), the termination name, the Virtual Media Gateway (VMG), and the HUNT/MADN group name information.

Geographic Survivability features

Compact Call Agent: Geo Support for GIGE (PT-IP, UA-AAL1, UA-IP, IAW, IAC, intl IAW)

The Line Audit feature component will add auditing coverage of SIP line data on the SS-EM. The data to be audited on the SS-EM includes the Directory Number (DN), the termination name, the Virtual Media Gateway (VMG), and the HUNT/MADN group name information.

ATM/IP Solution-level Configuration Overview

ATTENTION

This document addresses all Nortel Carrier VoIP solutions. Some statements may not apply to your solution. The North American IAW solution is not included in the (I)SN09 release.

This document describes performance management for the following solutions

Solution name	
International IP solutions	Integrated Access Wireline (IAW) Integrated Access-Cable Media (IAC) Packet Transit-IP (PT-IP) Universal Access-IP (UA-IP)
International ATM solutions	Packet Transit-AAL2 (PT-AAL2)
North American IP solutions	Packet Trunking-IP (PT-IP) or Packet Trunking-AAL2 (PT-AAL2) Integrated Access-Cable Media (IAC) Universal Access-IP (UA-IP)
North American ATM solutions (see Note) ***Note:*** Collectively, these two Carrier VoIP solutions are referred to as ATM solutions.	Universal Packet Access (UA-AAL1)
	Packet Trunking-AAL1 (PT-AAL1) There are three distinct architectures supported within the PT-AAL1 solution: • Packet Trunking-AAL1 (PT-AAL1) • Packet Trunking on XA-Core (PT-XA Core) • Packet Trunking on SN70EM (PT-SN70)

Nortel performs initial installation and commissioning of the solution for you (the customer). Once installation and commissioning are completed, you can begin to configure your system to make it fully operational. The term ‘configuration management’ is used to encompass all of these functions and activities.

In this document, the term "configuration" refers to the activities required to activate a network element or service such as the number, type, and position of circuit packs within a shelf for installation and commissioning.

In this document, the term ‘provisioning’ refers to the line or trunk services associated with provisionable circuit packs such as the carriers provisioned on a specific circuit pack. Within the network, both of these activities involve specifying and storing data in a database and are commonly called translations, datafill, or service activation.

ATTENTION

Nortel delivers Carrier VoIP Solutions on a pre-configured basis. All components within these pre-defined configurations and components not included can be ordered separately. Process and tool development is geared to this strategy. As a result, custom engineering is only offered at an additional cost through Nortel Global Professional Services.

Use the following checklist to verify that base commissioning has been completed before you begin configuration management.

Configuration management checklist

Checkpoint	Completed (yes/no)
Have all appropriate hardware equipment and correct software loads have been installed and loaded? These include the following components and related software: • Call Server components • Packet bearer path components • Management components	
Is the network connected?	
Are all cards installed?	
Is grounding implemented for safety?	
Is all network topology (physical characteristics) implemented as planned?	
Have the steps for datafilling the network, translation, service activation of trunks, internal customer testing, additional services, applications, and features been planned?	
Are installation validation procedures complete and components operational? For example, when you install and load software and turn pieces of equipment on, is the equipment commissioned?	

Customer configuration prerequisites

After all installation and base commissioning is completed by Nortel perform the following configuration tasks:

- Configure and complete translations to enable voice and trunk services as applicable
- Configure any additional services, applications, and features that Nortel is not contracted to perform
- Complete installation of clients or add client software for the following management interfaces as applicable:
  - CS 2000 Core Manager - provides FCAPS tasks related to CS 2000, MG 4000, and IW SPM
  - Multiservice Data Manager (MDM) - provides FCAPS tasks for the Multiservice Switch 15000 and Media Gateway 7400/15000
  - Device Manager for Ethernet Routing Switch 8600 - provides FCAPS tasks for the Communication Server LAN
  - CS 2000 Gateway Controller Manager - provides FCAPS tasks for the Gateway Controller
  - Universal Audio Server Manager - provides FCAPS tasks for the Universal Audio Server
  - Universal Signaling Point Manager - provides FCAPS tasks for the Universal Signaling Point
  - CS 2000 SAM21 Manager - provides FCAPS tasks for the CS 2000 SAM21
  - MG 9000 Manager - provides FCAPS tasks for the MG 9000
  - IEMS - provides a single interface for consolidating fault, performance, and security of a series of network elements and element management systems (EMS)

Trunking solution configuration overview

The trunking solutions are made up of a composite network consisting of a TDM-based digital multiplex system (DMS) subsystem which combines with asynchronous transfer mode (ATM) network elements through a set of interworking elements. The merging of the TDM/DMS and ATM technologies enables voice calls to directly use the transport and switching capabilities of an ATM network. This network multiplexes the trunk traffic for different destinations and transparently carries it over a common ATM infrastructure to time division multiplexing (TDM) end offices.

ATM/IP solution configuration overview

The following sections outline configuration functionality.

ATM/IP solutions configuration functionality

The following functionality is provided for commissioning:

- CS 2000 Core and CS 2000 - Compact commissioning via MAPCI
- XA-Core, GWC, SAM21, UAS/SAM16, Media Gateway 7400/15000, CICM, MG 9000, MCS, Ethernet Routing Switch 8600 commissioning for initial install via Command Line Interface (CLI) and respective element managers
- Media Gateway 7400/15000 provisioning via the Multiservice Data Manager (MDM) GUI
- GWC equipment provisioning via GWC manager
- SAM21 equipment provisioning via SAM21 manager
- MG 9000 equipment provisioning via MG 9000 Manager GUI
- USP configuration via USP Manager GUI
- UAS/SAM16 configuration via UAS CLI. UAS configuration via APS configurator.
- CICM configuration via CICM Manager
- IEMS addition of network elements, EMSs, EMS platforms, or EMS applications via the IEMS wizard
- Nortel Media Server 2000 (MS 2000) configuration via MS 2000 Series Configuration Tool
- Auto hardware discovery of UAS to the UAS Manager
- Ethernet Routing Switch 8600 configuration via Ethernet Routing Switch 8600 CLI or via Device Manager GUI. Device Manager is not available for the PT-IP solution.
- Configurable primary TFTP server for SAM21, Call Agent, and GWC load retrieval
- Call Agent Manager (CS 2000 - Compact specific) commissioning via CI level and MAPCI level of a MAP session established via Telnet.
- H.232 VPN configuration via GWC Manager

- SAM21 Manager support for GWC provisioning across multiple SAM shelves on the same frame. One SAM21 Manager client desktop can access multiple SAM21 Manager servers.
- Alternate Bootp Server on SPFS
- Element management for Media Proxy
  - Internet Transparency Provisioning through GWC manager
- Storage Manager (STORM) commissioning via the STORage Management Manager (STORM Manager) CS 2000 - Compact specific

  Note: STORM Manager provides the Server application for provisioning the STORM card.
- Where one Session Server supports a series of call servers, the minimum release for the supported call servers must be (I)SN06. Session Server is not backwards compatible to (I)SN05 or earlier call servers.

ATM/IP solutions service activation functionality

The following base functionality is provided for service activation:

- Nodes and Carrier provisioning for V5.2 lines, Dynamic Packet Trunks (DPT) via OSS (XML) and OSSGate
  - For GUI Gateway Controller (GWC), Service Application Module (SAM21), Universal Audio Server (UAS), Media Gateway 15000, CS 2000 Core Manager, and Universal Signaling Point (USP)
  - For MAPCI XA-Core and CS 2000 Core Manager
- Trunk provisioning is a multi-step process that includes steps in the XA-Core, GWC, and Gateway
- Line provisioning is a multi-step process for the cable solution that includes steps for the cable MTA, DNS/DHCP server, GWC and XA Core
- UAS Audio service configuration via Audio Provisioning Server (APS) configurator
- CS 2000 lines provisioning via SERVORD+ and XML interfaces for flow-through provisioning
- Provisioning support of SITE parameter for media gateways
- CS 2000 Gateway Controller Manager support of change to number of gateway endpoints
- PEP configuration support for DQoS
- Reduced number of service activation interfaces through redirecting Media Gateway Controllers (MGC) for non-IPSec gateways

- SERVORD+ support for hybrid solutions
- Flow-through provisioning for ADSL data service on Media Gateway 9000 (MG 9000)
- Service Data Integrity verification tools for trunk and line data for GWC and CS 2000
- OSSGATE Batch Provisioning Tool
- LEN-based provisioning for MG 9000 lines
- CICM supports automated provisioning via an XML interface
- MCS supports flow-through provisioning through an XML interface

The following optional functionality for service activation is included:

- Preside Service Provisioning (PSP) for trunk and translations management
  - — manages IP trunking and translations
  - — enhances XA-Core PRS to include GWC and Universal Signaling Point (USP)
  - — coordinates provisioning between GWC and tables TRKMEM and TRKSGRP for trunking
  - — coordinates provisioning between USP and XA-Core tables for SS7
  - — uses a single Work Order (WO) to create changes on XA-Core, GWC, and USP
- NML applications availability of:
  - — Telepath for XA-Core trunk, routing, billing, and translations provisioning
  - — Optivity for Ethernet Routing Switch 8600
- CS 2000 trunk provisioning through the integrated XML interface for IP solutions (TRKMEM and TRKSGRP for PRI)

ATM/IP solutions software management functionality

The following functionality is provided for software management:

- Software delivery via tape or DVDs or electronically to the target device. Format is device dependent.
- ESD planned to first point in customer's network for some devices (Customer-provided repository server)
- Manual transfer from repository to elements
- CS 2000 Core patching via Post Release Software Manager (PRSM)

- GWC and MG 9000 patching via Network Patch Manager

  Note: Network Patch Manager (NPM) is a software application used for patch administration. It is Java-based and requires the Server Platform Foundation Software (SPFS) platform. It enables application, removal, reporting, auditing and alarming. Its capabilities also include automatic patch file delivery and application.

- Other element loading and patching differs with each element manager
- No central load and patch management
- Auto ONP for PT-IP
- Auto-imaging for GWC
- APS fix delivery to allow APS upgrades without maintenance non-computing loads (MNCL)
- MG 9000 Manager fix delivery to allow MG 9000 upgrades without MNCLs
- System Manager GUI is used to deploy software to the MCS core components (centralized distribution)
- Automatic patch restart for OAM&P patches

The Integrated Element Management System (IEMS) is an application which ties all the OAM&P managers into a single integrated desktop environment. IEMS is distributed as a separate NCL (IEMS) and runs co-resident with the CS 2000 Management Components NCL (CS2M) on Sun Netra t1400 servers or the new Sun Netra 240 servers.

Component documentation

For additional details on commissioning of hardware and service activation, refer to the following component documentation:

- Call Agent Configuration Management, NN10109-511
- CICM Configuration Management, NN10240-511
- CS 2000 Configuration Management, NN10105-511
- CS 2000 Product Overview, NN10109-111
- GWC Configuration Management, NN10205-511
- IEMS Configuration Management, NN10330-511
- MG9000 Configuration Management, NN10096-511
- MS 2000 Series Configuration Management, NN10340-511
- MG 3200 H.248 User's Manual, LTRT-72704
- MG 3200 Gateway Configuration Guide, LTRT-72904

- MG 3200 H.248 Fast Track Installation Guide, LTRT-73804
- MG 3500 EMS User's Manual, LTRT-74004
- MG 3500 EMS Product Description, LTRT-74104
- MG 3500 EMS Server Installation and Maintenance Manual, LTRT-74204
- MG 3500 Gateway Installation, Operation & Maintenance, LTRT-74504
- MG 3500 Gateway Product Description, LTRT-74604
- Nortel Multiservice Switch 15000/20000 Hardware Description, NN10600-120
- Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade, NN10600-130
- SAM21 Manager Configuration Management, NN10111-511
- Session Server Configuration Management, NN10338-511
- Policy Controller Configuration Management, NN10432-511
- STORage Management Configuration Management, NN10110-511
- UAS Configuration Management, NN10095-511
- USP Configuration Management, NN10093-511

Configuration sequences

This section lists the configuration sequences for both ATM-based and IP-based solutions, excluding Packet Trunking AAL1.

IP solution configuration sequence

Perform IP network configuration tasks in the following order:

Note: Ensure that the IP core network and cable MTAs/Media Gateways and IAD devices are configured prior to performing the following configuration sequence.

- Communication Server 2000 (CS 2000) and the CS 2000 Core Manager

  or

  Call Agent and Call Agent Manager
- CS 2000 Communication Server LAN (Ethernet Routing Switch 8600 and Device Manager)
- Universal Signalling Point and Universal Signalling Point Manager
- Media Gateway and Nortel MDM
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller Manager
- Universal Audio Server Manager
- Storage Management (STORM) and STORM Manager
- Service Application Module 21 (SAM21)
- Gateway Controller
- Session Server
- Policy Controller
- Universal Audio Server/Media Server 2000

PT-XA Core or PT-SN70 configuration sequence

Configuration for PT-XA Core, or PT-SN70 is performed in the following order:

- configure the SuperNode Data Manager (SDM) if your switch includes one
- provision network data for DMS and SPM-based equipment
  - — provision DPT SPM
  - — provision SS7 trunks to the SS7 network

— provision office parameter table OFCOPT, and OFCSDT

— provision DPTs (Dynamic Packet Trunks)

— provision office parameter table OFCVAR

Note: When datafilling table C7NETWRK, you can define up to 16 pointcodes for a Service Switching Point (SSP). In other words you can provision multiple logical SSP nodes for a single network indicator (NI) on a single Carrier VoIP office. When a TCAP application is initialized by the system, the application chooses the first available national network indicator from table C7NETWRK, and this is the node that is used by the system for the application. This capability allows one Carrier VoIP office to appear as several SS7 signaling nodes in an SS7 signaling network. For information on provisioning table C7NETWRK, see *DPT SPM (ATM) Configuration Management,* NN10099-511.

UA-AAL1 configuration sequence

Perform component network configuration tasks in the following order:

- Communication Server 2000 (CS 2000) and the CS 2000 Core Manager
- CS 2000 Communication Server LAN (Ethernet Routing Switch 8600 and Device Manager)
- Universal Signalling Point and Universal Signalling Point Manager
- ATM core network and element management (Media Gateway 7480/15000 and MDM)
- Interworking Spectrum Peripheral Module (IW SPM)
- Multi-Service Gateway 4000 (MG 4000)
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller Manager
- Universal Audio Server Manager
- Media Gateway 9000 Manager
- Service Application Module 21 (SAM21)
- Gateway Controller
- Universal Audio Server
- Media Gateway 9000

Configuration task flows

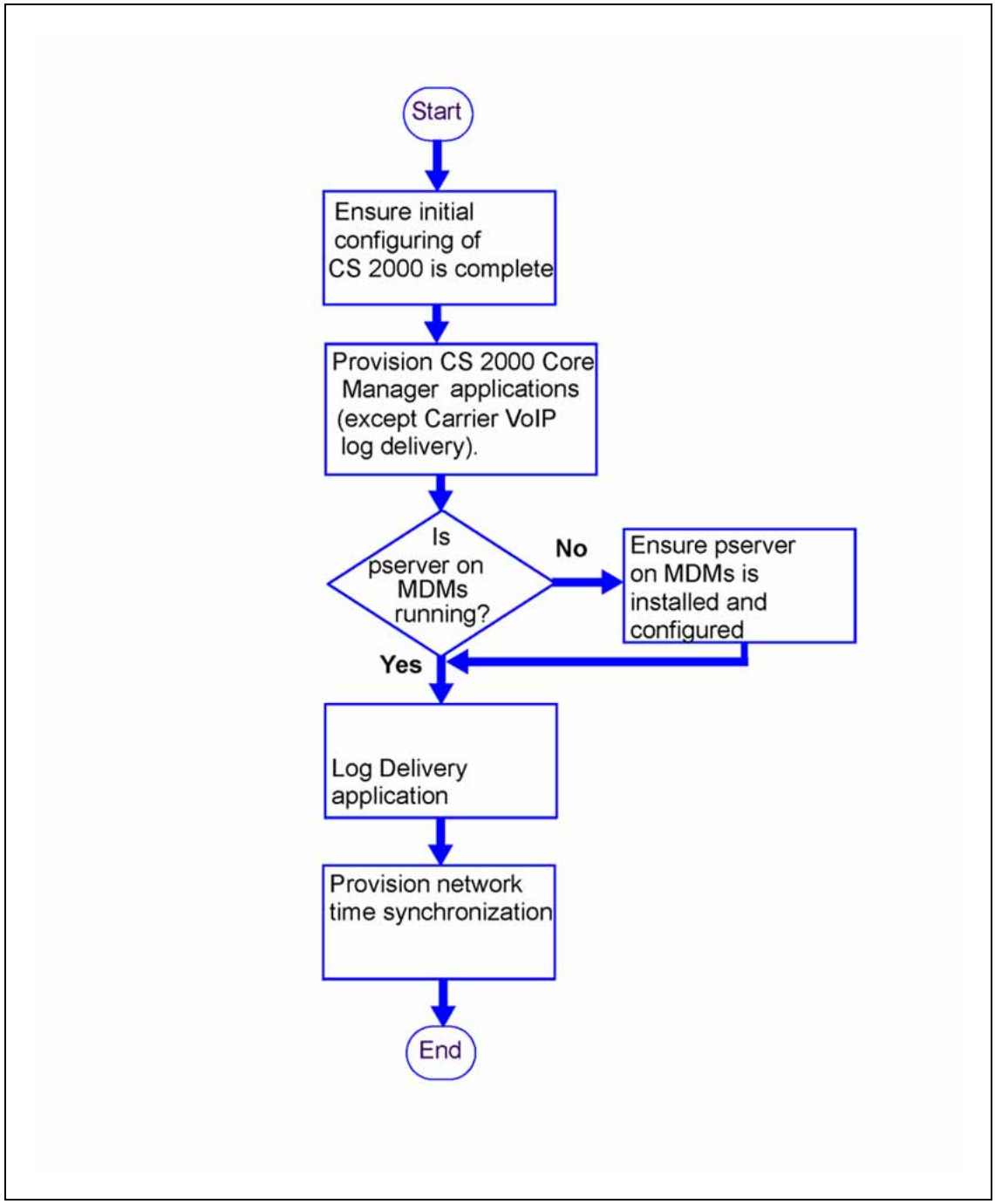
This section presents configuration task flows for the following ATM-based network elements:

Universal Access AAL1

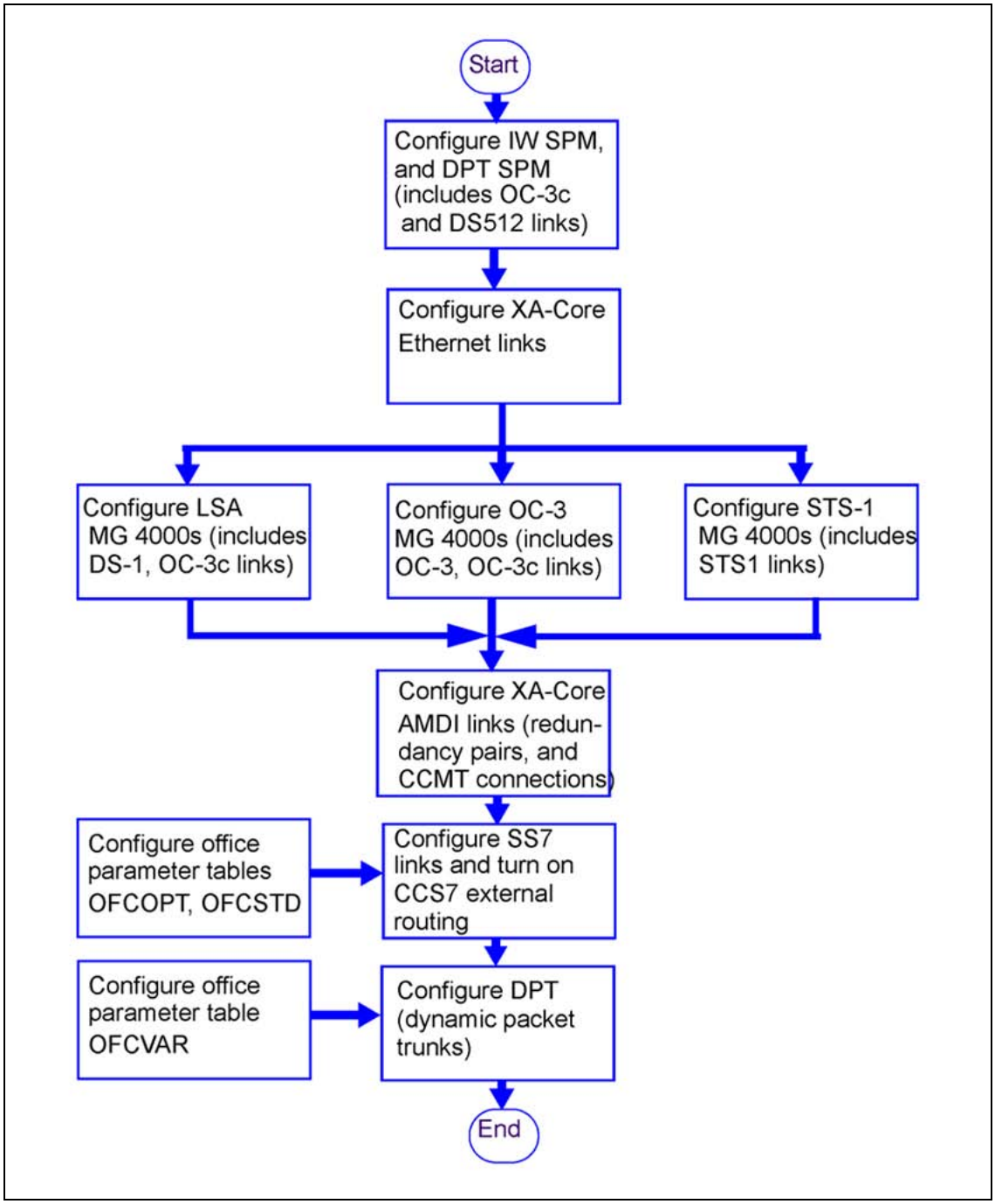
- "Configuration tasks for CS 2000 Core Manager" (page 17)
- "Configuration tasks for CS 2000, IW SPM, DPT SPM, and MG 4000" (page 18)
- "Configuration tasks for Media Gateway 7400/15000 and MDM" (page 19)

Note: Please see the table located just after the UA-AAL1 task flows for a list of detailed configuration procedures for each network element in the solution.

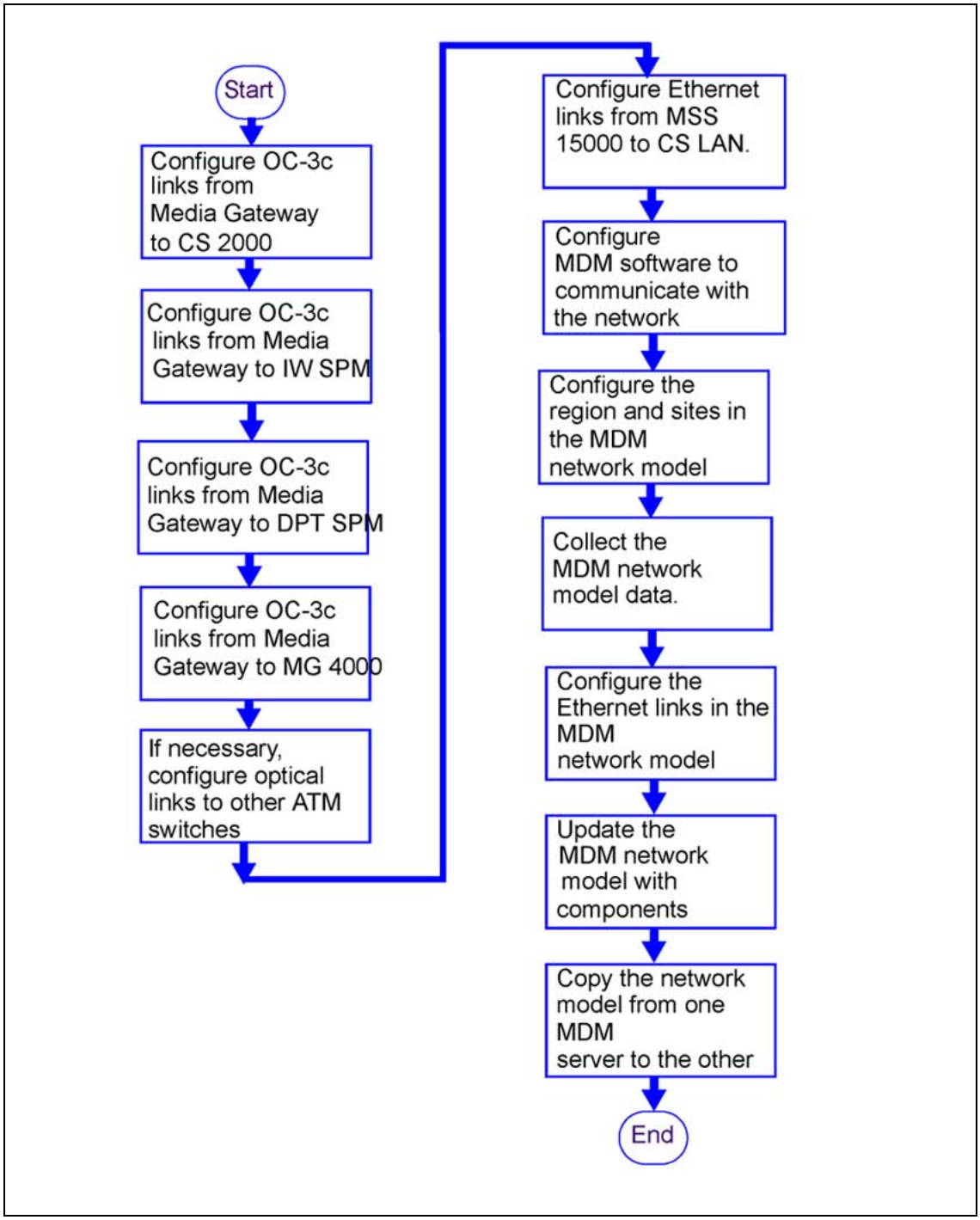
Configuration tasks for CS 2000 Core Manager



Configuration tasks for CS 2000, IW SPM, DPT SPM, and MG 4000



Configuration tasks for Media Gateway 7400/15000 and MDM



Detailed configuration procedures

Network element	Configuration procedure location
NETWORK INTELLIGENCE	
CS 2000	Communication Server 2000 Configuration Management, NN10201-511
Call Agent	Call Agent Configuration Management, NN10109-511
CS 2000 Communication Server LAN/Ethernet Routing Switch 8600	Configuring Switching and Routing Operations for the Ethernet Routing Switch 8000 Series Switch Using the Command Line Interface Release 3.2, 313191A Configuring Switching and Routing Operations for the Ethernet Routing Switch 8000 Series Switch Using Device Manager Release5.5.x, 313193A
SAM21	SAM21 Shelf Controller Configuration Management, NN10111-511
Gateway Controller	Gateway Controller Configuration Management, NN10205-511
Universal Audio Server	Universal Audio Server Configuration Management, NN10095-511
Media Server 2000	Media Sever 2000 Series Configuration Management, NN10340-511
Storage Management	Storage Management Configuration Management, NN10110-511
Universal Signalling Point	USP Configuration Management, NN10093-511
Universal Signalling Point Compact	USPc (compact) Configuration Management, NN10094-511
Border Control Point	Border Control Point Basics, NN10367-111
CICM	CICM Configuration Management, NN10240-511
Session Server	Session Server Configuration Management, NN10338-511
Policy Controller	Policy Controller Configuration Management, NN10432-511
CORE NETWORK	
Multiservice Switch 15000, Media Gateway 15000	Nortel Multiservice Switch 15000, Media Gateway 15000 and MDM in Carrier VoIP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP, NN10114-511
GATEWAYS	
MG 9000	MG 9000 Configuration Management, NN10096-511

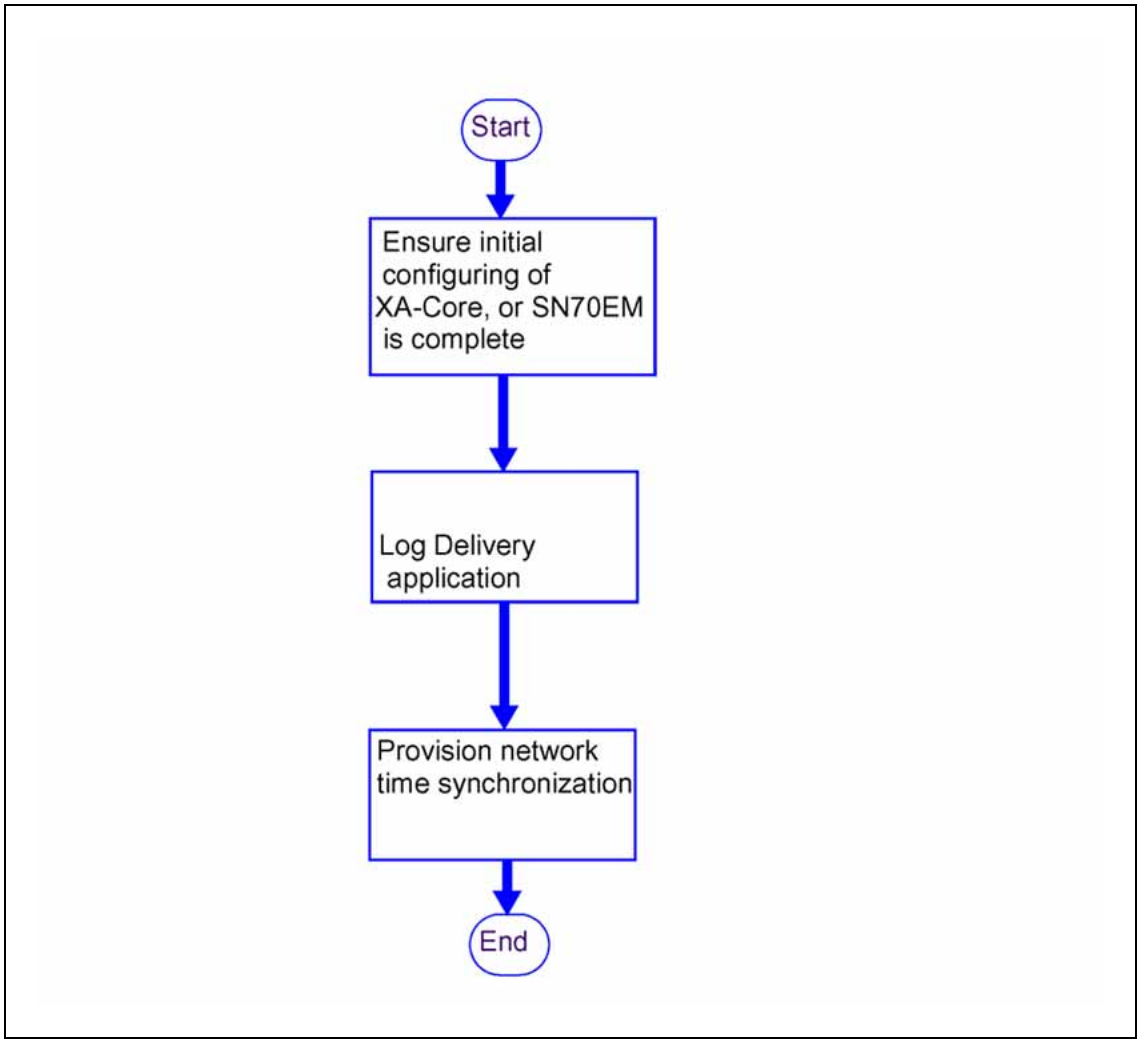
Network element	Configuration procedure location
MG 4000	MG 4000 Configuration Management, NN10098-511
IW SPM ATM	IW SPM ATM Configuration Management, NN10099-511
IW SPM IP	IW SPM IP Configuration Management, NN10100-511
NETWORK MANAGEMENT	
CS 2000 Core Manager	CS 2000 Core Manager Configuration Management, NN10104-511
CS 2000 SAM21 Manager	ATM/IP Solution-level Configuration Management module, NN10409-500
CS 2000 GWC Manager and Universal Audio Server Manager	ATM/IP Solution-level Configuration Management module, NN10409-500
Universal Signalling Point Manager	USP Configuration Management, NN10093-511
Integrated Element Management System	IEMS Configuration Management, NN10330-511
Nortel Multiservice Data Manager	Nortel Multiservice Switch 15000, Media Gateway 15000 and MDM in Carrier VoIP Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP, NN10114-511
MG 9000 Manager	MG 9000 Configuration Management, NN10096-511
Ethernet Routing Switch 8600 and Device Manager	Configuring Switching and Routing Operations for the Ethernet Routing Switch 8000 Series Switch Using the Command Line Interface Release 3.2, 313191A Configuring Switching and Routing Operations for the Ethernet Routing Switch 8000 Series Switch Using Device Manager Release5.5.x, 313193A

Packet Trunking XA Core or Packet Trunking SN70

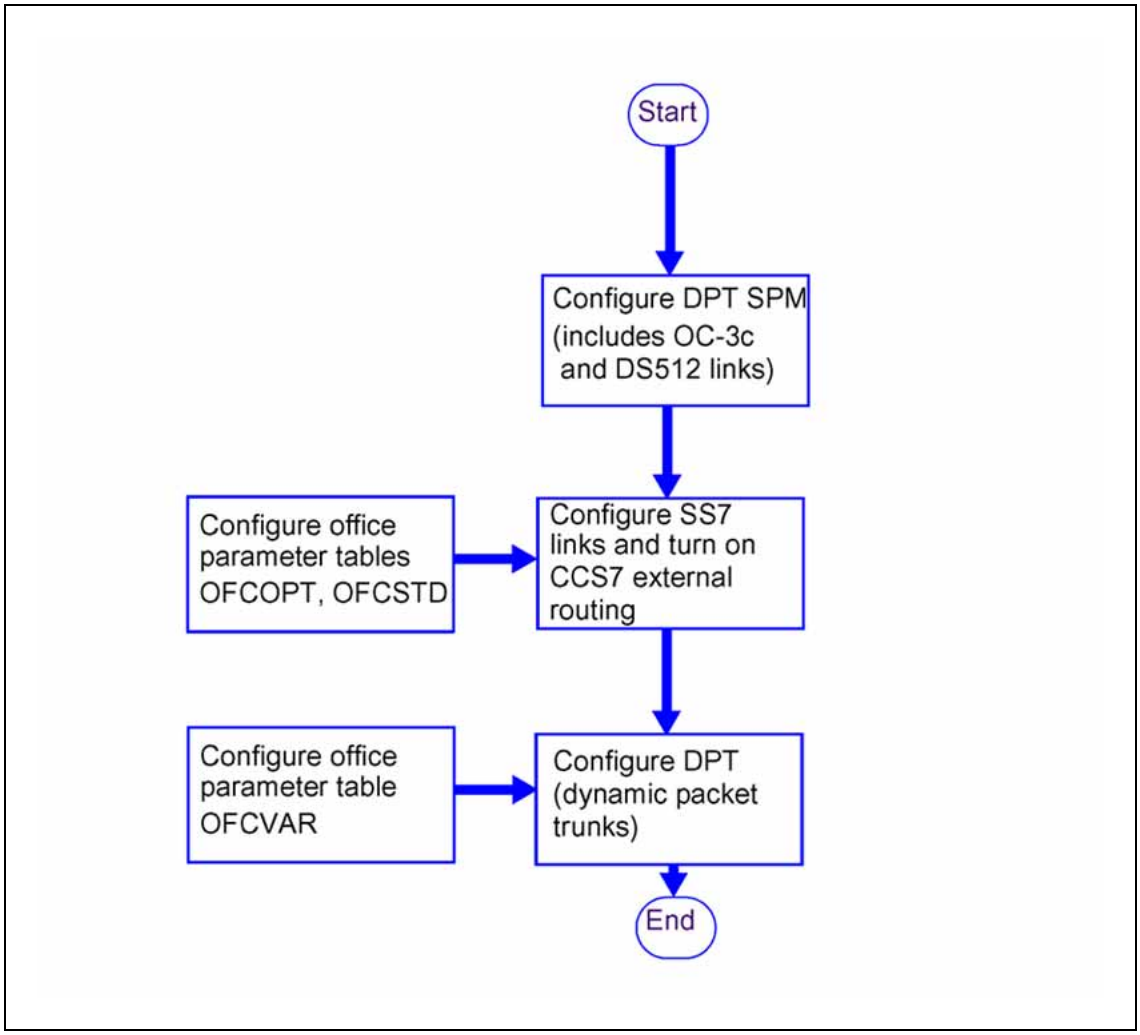
- "Configuration tasks for SDM" (page 22)
- "Configuration tasks for XA-Core, or SN70EM, and DPT SPM" (page 23)

Note: The table located just after the task flows lists detailed configuration procedures for each network element included in the PT-XA Core, or PT-SN70 product.

Configuration tasks for SDM



Configuration tasks for XA-Core, or SN70EM, and DPT SPM



The following table lists detailed configuration procedures for each network element in the PT-XA Core or PT-SN70 solutions.

Detailed configuration procedures

Network element	Where to find the configuration procedures
DPT SPM	*DPT SPM ATM Configuration Management*, NN10102-511
XA-Core, or SN70EM (including DPT, and SS7 links)	*DPT SPM ATM Configuration Management*, NN10102-511
SDM	*CS 2000 Core Manager Configuration Management*, NN10104-511

Trunk and line provisioning overview

ATTENTION

This section includes general information about CS 2000 trunk and line provisioning.

For detailed procedures, please refer to the Adobe Acrobat bookmark list.

Provisioning of trunk and line services for different Carrier VoIP solutions varies by access type, either by trunk or line.

Trunk provisioning

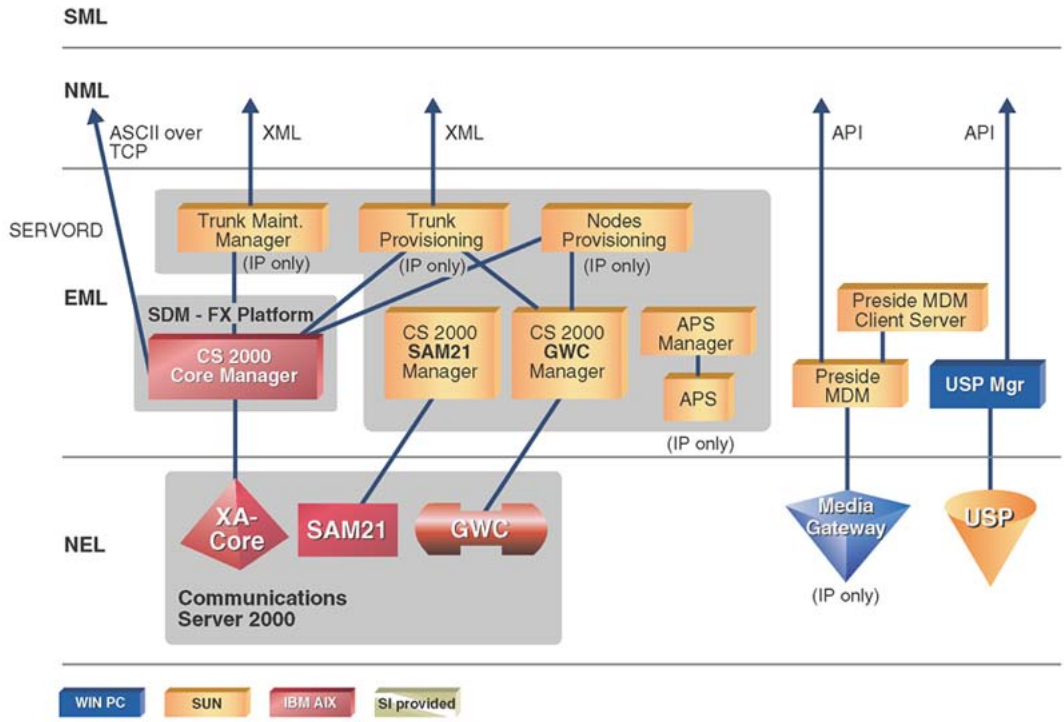
Trunk provisioning or trunk service activation involves creation, change, or deletion of trunk groups or individual trunks. This is required for the trunks of every solution. The steps required will be different for different solutions however.

For the MG 4000 gateways, the steps are very similar to the SPM in the DMS-100F. Service activation is performed via Table Editor. The ATM connections are configured in the Multiservice Switch 15000 as a commissioning step.

For the Media Gateway, the GW cards must be assigned to the GWC using the GWC GUI or an XML command via OSSGate. Then the carrier endpoints must be assigned for each T-1 or E-1 facility. This is done using the GWC Manager or an XML command via OSSGate also. Finally the same trunking tables must be datafilled using Table Editor. These are defined in the appropriate sections of the North American DMS-100 Translations Guide, Volumes 1 through 25 (297-8021-350P1 through 297-8021-350P25).

The following figure shows the configuration management architecture for trunking solutions for the CS 2000 network.

CS 2000 Trunk architecture



Note 1: This interface is used for translations and dial plan provisioning.

Note 2: Service Activation is identical for both CS 2000 and CS 2000 compact.

When all components are installed and commissioned, the following configuration and provisioning tasks can be performed as needed.

Adding a trunk

Note: For supported third party trunk gateways, the gateway must be configured before starting this procedure.

Step	Action
1	Add the GWC to CS 2000 using the CS 2000 GWC Manager. ***Note:*** This step is performed by the Nortel installation team.
2	Add the trunk gateway to the GWC using the CS 2000 GWC Manager or OSS gate using XML.
3	Provision the endpoints in the trunk gateway using the CS 2000 GWC Manager or OSS gate using XML.

4 Provision the trunk in the CS 2000 using the Table Editor.

5 Return the trunk to service using MAP CI or Trunk Maintenance Manager (TMM).

—End—

Deleting a trunk

Step	Action
1	Remove trunks from service using the Trunk Maintenance Manager (TMM) or TTP level of MAP.
2	Delete CS 2000 trunk datafill using the CS 2000 Core Manager.
3	Delete endpoint/carrier datafill in the GWC using the CS 2000 GWC Manager or OSS gate using XML. ***Note:*** This step is not applicable for the MG 4000 and other supported gateways.
4	Delete endpoint/carrier datafill in the Media Gateway using MDM.

—End—

Changing trunk group data

- Change CS 2000 trunk group datafill using the CS 2000 Core Manager.

  Note 1: Dependencies: Customers who wish to have trunking survivability during a Media Gateway upgrade must configure trunk groups or route lists across multiple Media Gateways in an n+1 configuration. Media Gateway upgrades are done after the CS 2000 upgrade is completed.

  Note 2: Mixed trunk subgroups (that is, trunk members on a legacy peripheral such as DTC or SPM in the same trunk subgroup as trunk members on a packet-based gateway such as Media Gateway) are not supported. Trunk members on a legacy peripheral should be combined in one subgroup and trunk members on a packet-based gateway should be combined in a second trunk subgroup if you both types are needed in the same trunk group. A notification message is generated during provisioning if a mixed trunk subgroup is detected.

For additional details about adding, deleting, changing, and activating trunks, refer to the following core and component documentation:

- CS 2000 Configuration Management, NN10105-511
- SAM21 Manager Configuration Management, NN10111-511
- Gateway Controller Configuration Management, NN10205-511
- UAS Configuration Management, NN10095-511
- Nortel Multiservice Switch 7400/15000/20000 Components Reference, NN10600-060
- Nortel Multiservice Switch 15000/20000 Hardware Description, NN10600-120
- Nortel Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade, NN10600-130
- Getting Started with the Ethernet Routing Switch 8600 Management Software Part #209663-C
- Reference for the Ethernet Routing Switch 8600 Series Management Software Routing Operations 207415-C
- XML Schema for Carrier Provisioning (OSSGate User Guide, NE10004-512)

Translations

For details on datafilling translations, and for information on additional services, applications, and features, refer to the following documentation through Helmsman:

- UCS 250 General Description, 297-2621-100
- North American DMS-100 Translations Guide, Volumes 1 - 25, 297-8021-350P1 through 297-8021-350P25

Routing

For details on configuring routing or for adjusting and changing routing, refer to the following documentation through Helmsman:

- UCS 250 General Description, 297-2621-100
- North American DMS-100 Translations Guide, Volumes 1 - 25, 297-8021-350P1 through 297-8021-350P25

Line provisioning

Line provisioning or line service activation involves creation, change, or deletion of line service. This is required for the lines of every solution.

Line provisioning requires updates to be made to the data stored by some or all of the following components:

- CS 2000 Core
- GWCs
- Line media gateways for the MG9000
- Trunk gateways configured to support V5.2 interfaces

  Note: The stages for provisioning V5.2 lines are as follows:

  — provision a set of trunk gateway E1s as V5.2

  — define the V5.2 interface using the V5.2 configuration manager

  — use MAPCI to add entries manually in LNINV

  — use SERVORD or SERVORD+ or provision IBNLINES

Two applications are provided to help ensure that these separate updates are coordinated: lines provisioning application and nodes provisioning application (also used in trunk provisioning).

The lines provisioning and nodes provisioning applications support different interfaces for handling provisioning data:

- The lines provisioning application supports the proprietary SERVORD+ (Service Order) interface. The SERVORD+ ADO (Add Option) command is used to assign features to lines. The SERVORD+ NEW command specifies for each line

  — the DN to be assigned to the line

  — the gateway endpoint serving the line

- The nodes provisioning application supports an XML (Extensible Markup Language) interface.

The lines and nodes provisioning applications can both be accessed by a provisioning system through OSSGate, which provides a single access point for Carrier VoIP provisioning applications. Each application uses lines provisioning input to generate two types of output:

- ASCII over TCP, which is provided to the CS 2000 Manager on the SDM and used by it to update CS 2000 Core datafill
- Corba data, which is provided to the GWC Manager and used by it to update GWC data.

Provisioning of line service for different Carrier VoIP solutions varies by access type. The optional Lines Maintenance Manager (LMM) application provides additional maintenance capabilities.

Some solutions use large line gateways with many lines and some use small line gateways with only one or two lines per gateway. A lines solution requires additional steps per line. Small line gateways require a gateway for each subscriber and additional steps are necessary to turn up service for each line. Similar steps apply for large line gateways where it is necessary to perform these steps once for a large number of subscribers. In all cases the line gateway must be added to its element manager. This is referred to as the nodes provisioning transaction. The phone number, a gateway controller endpoint and any features must be assigned through SERVORD+. This is referred to as the SERVORD+ transaction. Any additional service provisioning such as DSL data or cable modem service must be provisioned. DNS/DHCP assignments may be added as well. The gateway assignment can be performed via GWC EM GUI or XML command. This applies to IAC and IAW solutions.

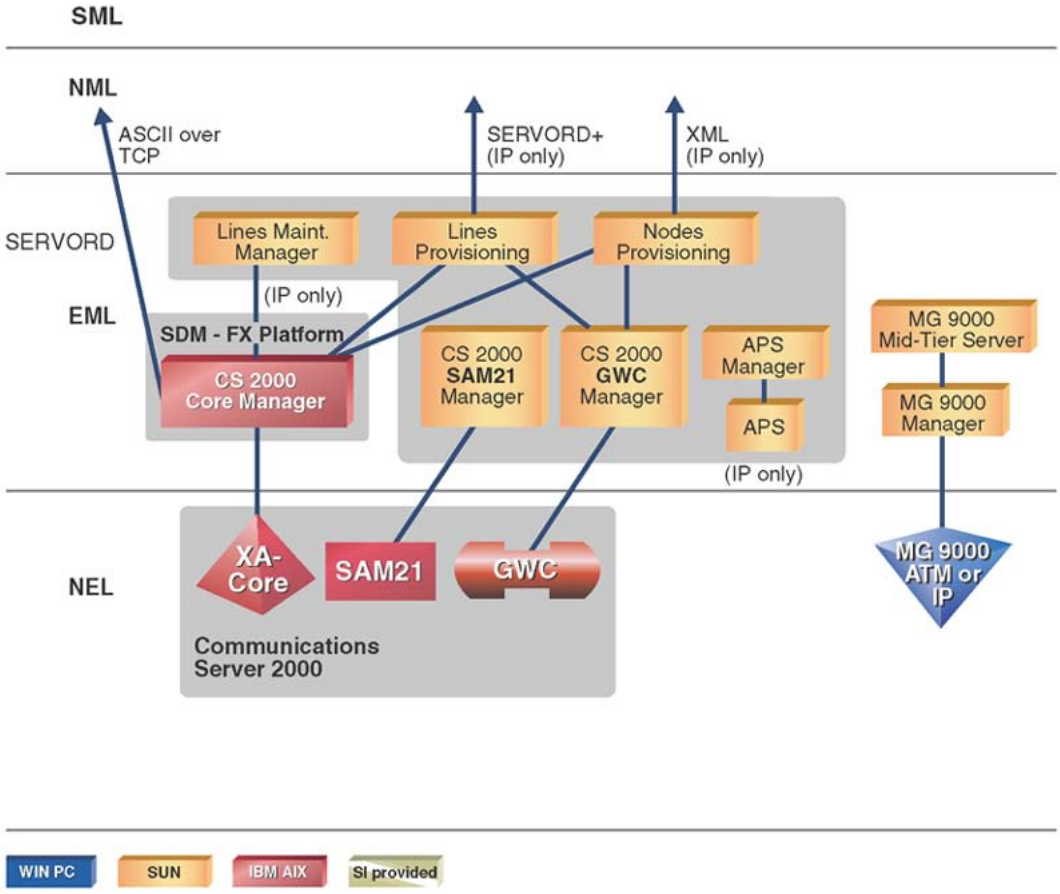
> ***Note:*** In a CS 2000 lines solution, in common with many DMS/XPM-based line access solutions, a moment of ringback may be heard prior to an announcement being played. This is designed to fill in quiet periods of audio while the connected equipment prepares and connects the announcement resources to the user channel.

The steps required will be different for different solutions however. In general it is necessary to assign the line gateway to the GWC and activate it, then provision the individual lines. For the MG 9000, the assignment of the gateway to the GWC is a commissioning activity done at installation time. Activation of the line simply requires the use of **SERVORD** or **SERVORD+** commands.

Changes to individual lines can be performed through the use of the appropriate **SERVORD** or **SERVORD+** commands. The Add option, delete option, or change feature are examples of these types of changes. The deletion of a line involves the DELETE command. For small line gateways used in IAC or IAW, it may also be necessary to delete the small line gateway from the GWC as well.

The following figure shows the CS 2000 Base Line architecture.

CS 2000 Base Lines operational configuration architecture



Note 1: This interface is used for translations and dial plan provisioning.

Note 2: Service Activation is identical for both CS 2000 and CS 2000 compact.

Adding a line

The following is a high-level view of the steps described in the previous section.

Step	Action
	From the CS 2000 Management Tool
1	Associate GW to GWC (for IAC and IAW solutions only).
2	Create the line assignment as follows: • Connect to the OSSGate telnet interface

- Send a **servord+** command to assign a telephone number and endpoint, plus any feature options

3 **For IAC solutions only, do the following:**

a. Log onto EMS and provision the new MTA or to assign the GW to GW EMS.

b. To assign the GWC address to the cable MTA, enter an IP address to indicate to the MTA what gateway controller to obtain service from.

c. To assign DNS/DHCP, provision the IP address of the MTA in the DHCP server.

—End—

Deleting a line

The following is a list of high-level steps for deleting a line. For details, see

Step	Action
	From the CS 2000 Management Tool
1	Make a telnet connection to OSSGate.
2	Send the **SERVORD+ OUT** command to delete service.
3	**For IAC solutions only, do the following:** a. Change to XML format (CTRL B) and send dissociate GW command in XML format or login to CS 2000 GWC Manager GUI and dissociate GW from GWC. b. Login to GW EMS and delete GW from system. c. Login to DNS/DHCP system and delete entry for the GW.

—End—

Changing a line

The following is a list of high-level tasks for deleting a line:

- Feature changes are made using the CHF (change feature) command

For IAC and IAW solutions only:

- Changing IP address requires deleting and re-adding the GW (unless DNS service is used). The line is automatically brought into service when the **SERVORD+** transaction is completed successfully.

Routing and translations

For details on configuring routing or for adjusting and changing routing, refer to "Translations" (page 27) and "Routing" (page 27).

Provisioning UA-AAL1 echo cancellation

An office parameter named ECAN_EDGE_STRATEGY in table OFCENG controls network-wide echo cancellation (ECAN) in packet networks.

As described in the following sections, there are two available ECAN strategies: ‘region’ or ‘edge’. The region strategy applies by default. To employ the edge strategy, follow the procedure explained in "Provisioning rules" (page 33).

Region strategy (ECAN_EDGE_STRATEGY = N)

The region strategy is the default in TDM networks. The network is divided into regions and only calls crossing region boundaries require ECAN. The region strategy can be implemented by providing ECAN in both directions for every trunk group that crosses a regional boundary.

Edge strategy (ECAN_EDGE_STRATEGY = Y)

The edge strategy always cancels echo before it enters the packet network. This strategy ensures that ECAN is performed in both directions for all packet calls. The edge strategy also eliminates the need for echo cancellation after calls have passed over the packet network.

The edge strategy office parameter determines whether ECAN is performed on an IW SPM for MG 4000 trunks and line GWC interfaces. ECAN datafill for MG 4000s must be configured as in (I)SN05.

Provisioning rules

Step	Action
	Edge strategy
1	Provision access mode ECAN using the SPMECIDX in TRKSGRP on MG 4000 TDM trunk groups which require ECAN based on a network delay analysis. Access mode ECAN is specified in a SPMECAN tuple by setting FAREC to N and BK2BK to N.
2	Provision IW SPMs with echo cancellers based on engineering guidelines.
3	Enable the echo cancellers on the IW SPM by adding the SPMECIDX option in table MNNODE.
4	Set the ECAN_EDGE_STRATEGY office parameter to Y.

Note: DPT calls are inter-call server and therefore are unaffected by the edge strategy. If ECAN is required on DPT trunks, add the appropriate ECAN datafill in TRKSGRP.

—End—

Configuring a Trunk-only solution

Application

Use this procedure to configure the solution as a trunk-only solution..

Prerequisites

This procedure has no prerequisites.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password. In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command. For detailed steps, refer to procedure "Logging in to an SPFS-based server".
2	Launch the configuration tool by typing: `# configure` and pressing the Enter key.
3	From the resulting menu, select the number against the “SESM provisioning configuration” menu option, and press the Enter key.
4	From the resulting menu, select the number against the “Office Provisioning Type configuration” menu option, and press the Enter key. **Example response**

```
SESM Provisioning Type Selection
Will line gateways be provisioned in this office?
[y/n]:
```

5 Enter **n** at the prompt to indicate that the solution will not use line gateways, and press the Enter Key.

6 Exit each menu level of the configuration tool by typing

```
select - x
```

and pressing the Enter key.

7 Restart the SESM application by typing

```
# servstart SESMservice
```

8 You have completed this procedure.

—End—

Provisioning the QoS collector application

In all North American and International IP solutions, you can configure QoS collector applications (QCA). A QCA collects quality-of-service (QoS) data and forward it to an operations support system (OSS).

The QoS data is for calls handled by GWC-driven gateways. The gateways report per-call QoS information to the GWCs. Each GWC can log on to a QCA and forward the QoS data.

The QCA is an application that runs on a computer that must be connected to the CO LAN. The computer can be the same one on which the CS 2000 Management Tools are running, or it can be a separate computer.

There can be one or more QCAs running on computers on the CO LAN.

When a QCA receives QoS data from a GWC, it formats the data into XML format and forwards it to the operating company's OSS. The OSS processes the QoS data according to the operating company's wishes.

To configure QoS reporting, you must complete the following tasks:

- Provision the QCA. You must specify values in the QCA properties file, and set up the input and output directories that the QCA will use. Refer to procedure 'Configuring the QoS Collector Application' in your solution's Configuration Management document.
- In the GWC Management Tools interface, you must
  - set the network QoS configuration parameters
  - add the QoS collectors
  - associate each GWC with a maximum of two QCAs
  - enable reporting on a per-GWC basis, so the GWCs will be able to send the QoS data to the QCA

  To find directions to the procedures for performing these tasks, refer to the procedural flowchart for QoS in the overview section of the GWC configuration document.
- Optionally, in the MAP interface, you can update table AMAOPTS to enable the QoS-reporting software to append correlation identifiers (CIDs) to billing records. If there are CIDs in the billing records, the OSS can locate the QoS statistics for individual calls.

  For instructions for updating table AMAOPTS, see the procedure covering provisioning in support of QoS reporting, in Communication Server 2000 Configuration Management, NN10284-511.

CICM element manager integration with PAM+ proxy

Overview

Carrier VoIP (CVoIP) user authentication services can use a single centralized third party server which provides authentication services to CVoIP management systems via a pluggable authentication module (PAM) on the IEMS platform.

From (I)SN07 onwards, the CICM element manager is integrated into the CVoIP centralized user authentication strategy. The CICM element manager interfaces to PAM via the HTTPS PAM+ proxy on IEMS.

Prior to (I)SN07, the user name and password supplied when logging into the element manager corresponded to local user accounts on the CICM element manager. From (I)SN07 onwards, the user name and password can be configured to be a global CVoIP account managed on a centralized authentication database which interfaces to CVoIP management tools via the PAM+ proxy located on the IEMS.

Centralized user authentication via the SSPFS PAM proxy is not available to TDM deployments of CICM or if connectivity is lost between the CICM element manager and the SSPFS platform.

- For TDM deployments, the authentication functionality passes control of the authentication back to the standard mechanism used for CICM.
- For CVoIP deployments, a method of local user authentication is also provided for use when connectivity is lost to the IEMS platform. Users can select local authentication by prefixing their user name with a period (.). This allows users to access their local user account in the CICM element manager when the PAM proxy is out of service.

For more information on CICM integration with PAM+ proxy, see *CICM Configuration Management*, NN10240-511.

Overview of Core Element Manager integration with IEMS

This feature integrates the functionality of Core Element Manager (CEM) to the Integrated Element Management System (IEMS). CEM is an element manager for the CS 2000 core and Call Agent core. It provides Resource Discovery (RD), Fault Management (FM) and Performance Management (PM) support for the core. You can add, delete, and manage CEM from IEMS.

The Core Element Manager system is an Element Management System which provides the following:

- an exchange of data between a management application (CEM) and a core network element (SDM or CBM). The Core Element Manager is installed on a Sun platform.
- mediation functionality (data accumulation, filtering, manipulation, and transfer) between the CS 2000 Core or Call Agent Core network elements and the CEM workstation

CEM components

The CEM software includes the Core Element Manager GUI, the CEM Server, and the OMC-S in SDM/CBM. The following three components perform the performance management, configuration management, fault management, and security management functionality for the CS 2000 core or Call Agent core.

- The Core Element Manager browser runs on a PC or Sun platform. OAM&P personnel can use the GUI to manage the network elements.
- The Core Element Manager Server runs on a Sun Solaris platform.
- SDM/CBM is the mediation device which connects to the network element and gets raw data such as OMs, logs and also table data. SDM/CBM passes this information to the CEM server software.

The CEM store and forward process (SAF) framework:

- stores and forwards the SDM/CBM data on to the appropriate CEM server process
- synchronizes after disconnection from the CEM server process and the SDM/CBM

By default, the SAF process on the SDM/CBM is not in service after CEM is installed. The SAF process must be switched to the in service state.

For more information about the CEM SAF process, see CS 2000 Core Manager Overview, NN10018-111.

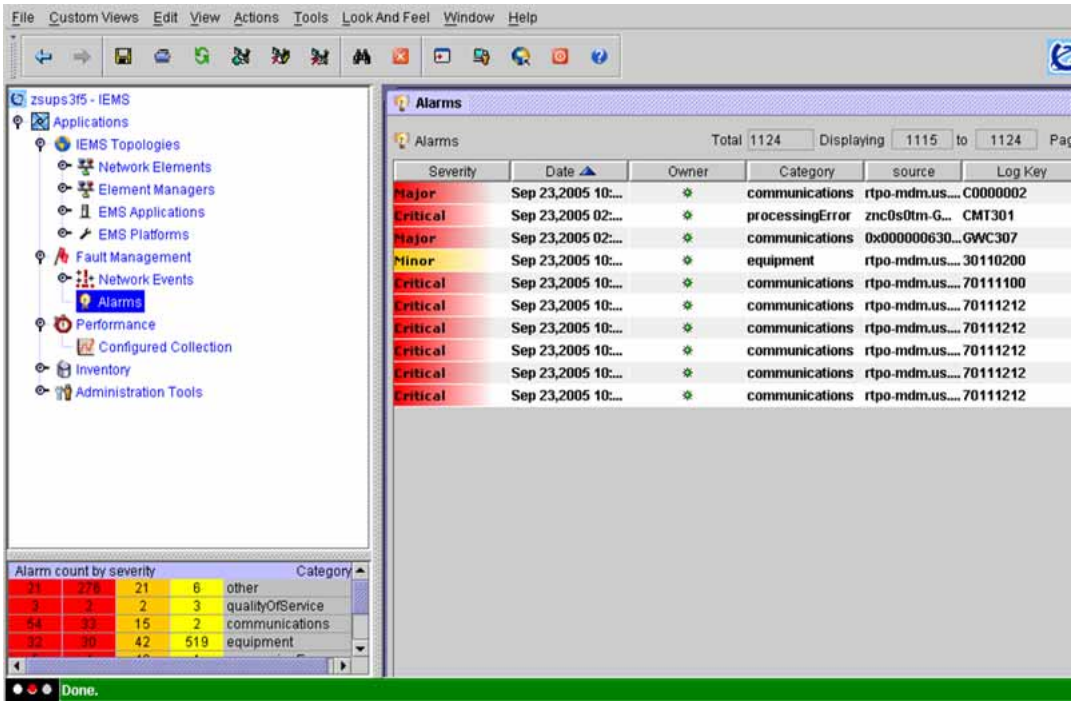
CEM GUI description

Fault Management

The Fault Management function (FM) displays logs of alarm or fault events that occur within the network, usually within a switch node. These alarms or events may have an impact on the overall service of the network element. The Fault Management function provides information about the network element so that you can perform further maintenance operations. Fault Management provides the following capabilities:

- displays alarms for a specific switch node. When a repeated alarm occurs for the same problem and the same resource, the most current alarm is shown. The previous alarms are stored as cleared alarms.
- displays a time-based histogram of alarm activity for time periods of 1 to 30 days. By default, the retention period is 30 days for uncleared alarms and 7 days for cleared alarms.
- displays alarms by selected severities (Critical, Major, Minor, Warning, unknown, or any combination)
- displays the element color to reflect the current alarm status
- displays alarms for specific filters
- provides alarm notifications as they occur
- exports alarm data to file
- prints alarm data
- provides filter criteria for alarms
- provides actions triggered by alarm

Fault management window



Configuration Management

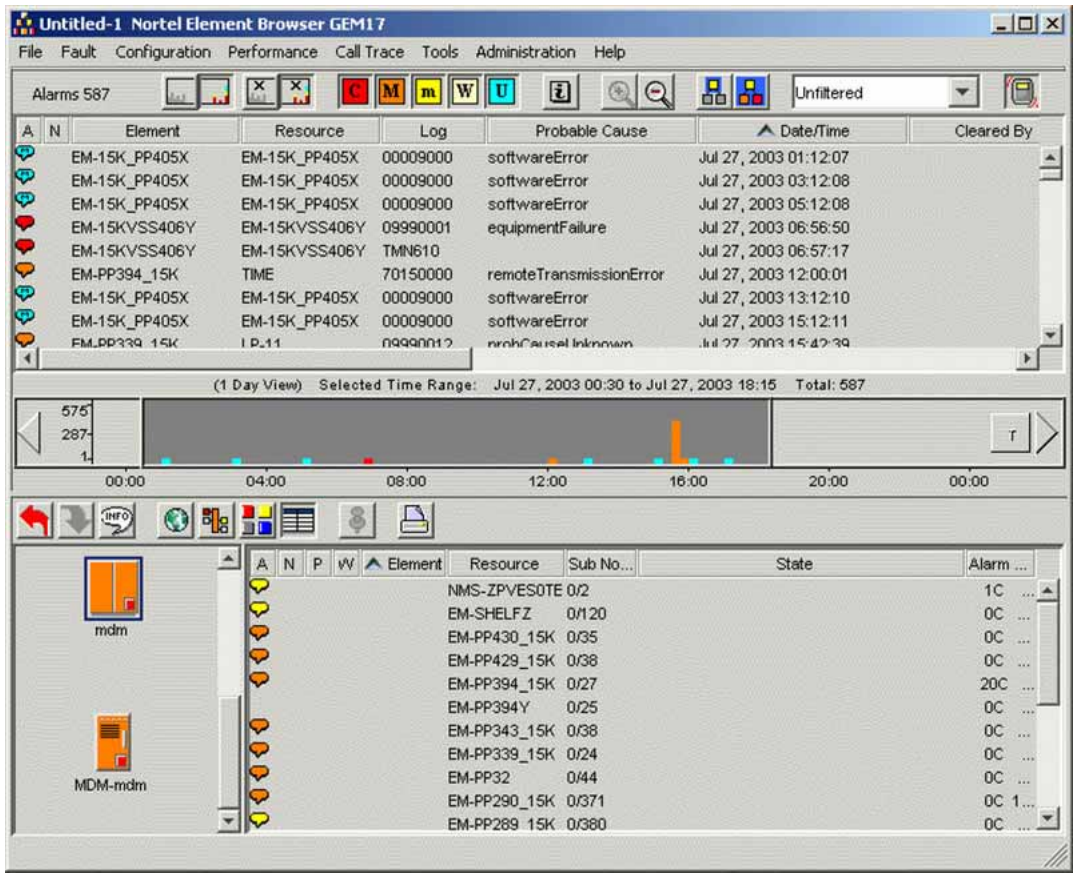
The Configuration Management function allows you to manage network elements within a circuit core network. The Configuration Management function identifies the configuration and status of the network when it is initialized. The network elements are identified by icons and are arranged according to the network hierarchy. The CEM displays complete information for each target network element and its subordinate elements. The configuration display is updated automatically by the Configuration Manager to maintain consistency between the Element Manager display and its managed objects. This display is called the containment tree.

The Configuration Manager includes the following features:

- Physical, Logical, Icon or List views from the Element Manager
- Pin and Unpin nodes
- nodes sorted by name or severity
- find carriers and linksets
- saving and retrieving of notes for nodes
- table access (add/read/delete/modify tuple operations)
- customs wizards to create/modify/delete trunks and other table access operations
- integration with performance management

- launch the Threshold Management window for a PM resource
- threshold management information for PM resources
- threshold crossed information
- performance management information for PM resources (pmCurrentData)
- print support for the Configuration Management window

Configuration Management window in list mode



Performance Management

The Operational Measurements (OM) system provides the following measurements for the Circuit Core Networks (CCN) Call Server:

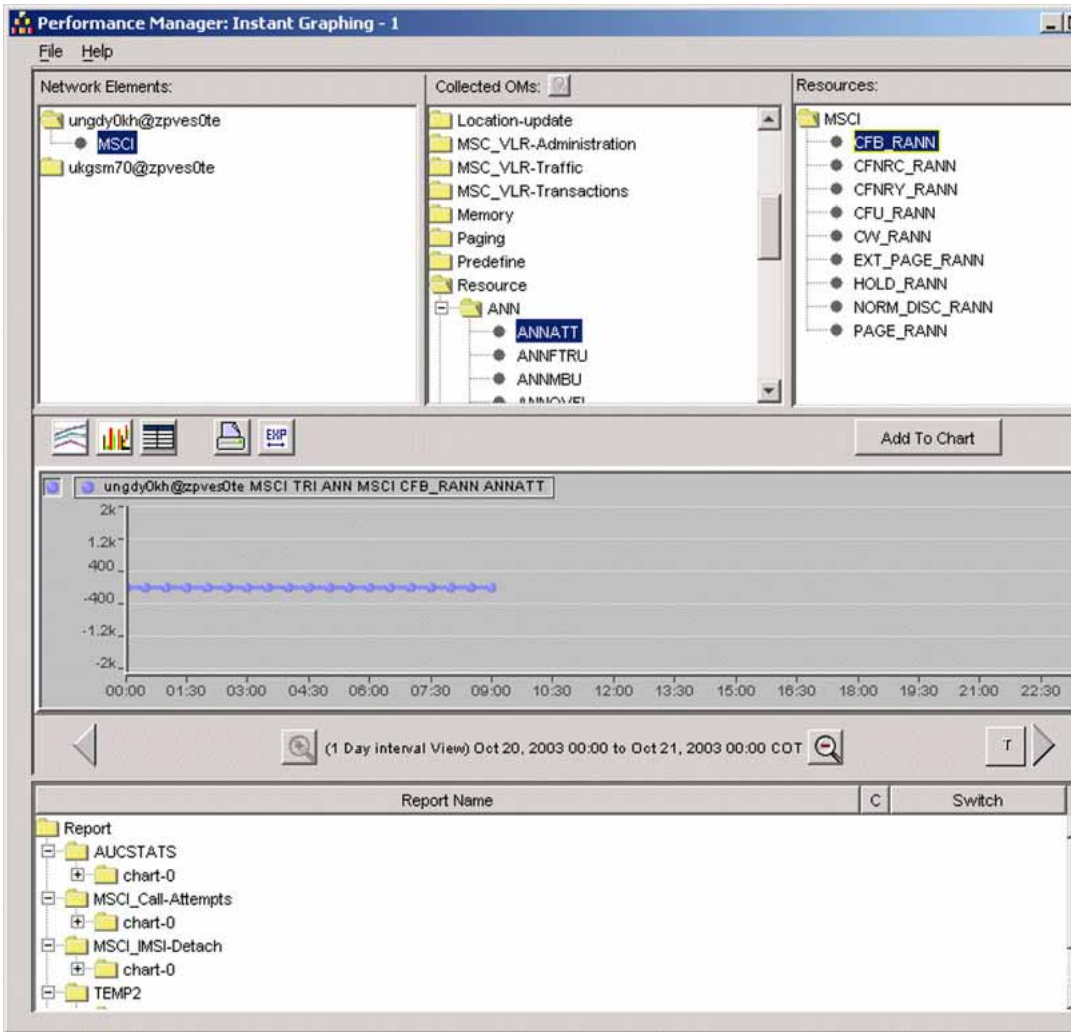
- traffic measurements
- service data

You can view OM records to ensure that the CS switch operates at its fullest potential with optimum efficiency. New OM data is transferred from the switch every transfer period.

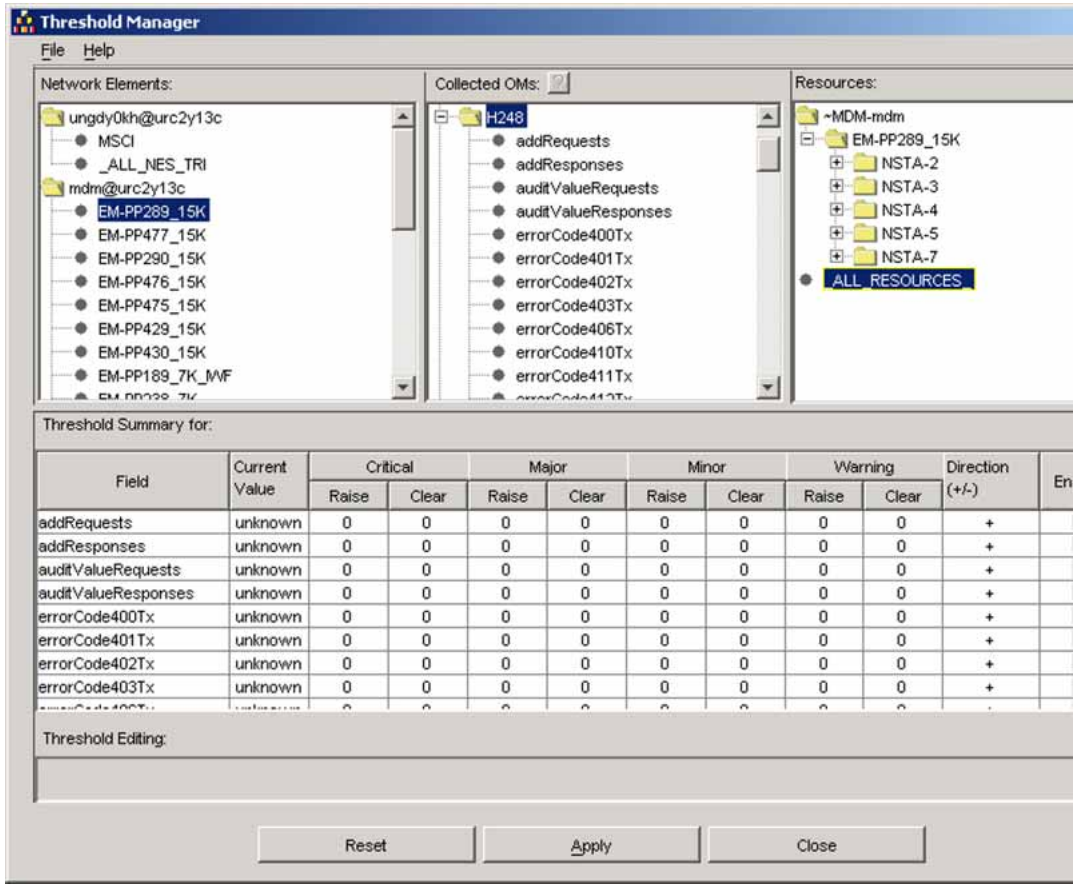
The Performance Management functionality does the following:

- provides access to OMs in predefined measurement groups
- displays OMs in operator-configurable studies, including a graph of specific OMs over a given time frame
- configures real-time updates of OMs with the CS transfer period as the minimum update frequency
- displays data from multiple network elements on the same graph
- displays errors such as incomplete OM data for the requested study
- sends the output display to print
- allows OM threshold settings
- displays summary reports on network elements

Performance Management: Instant graphing window



Performance Management: Threshold Manager window

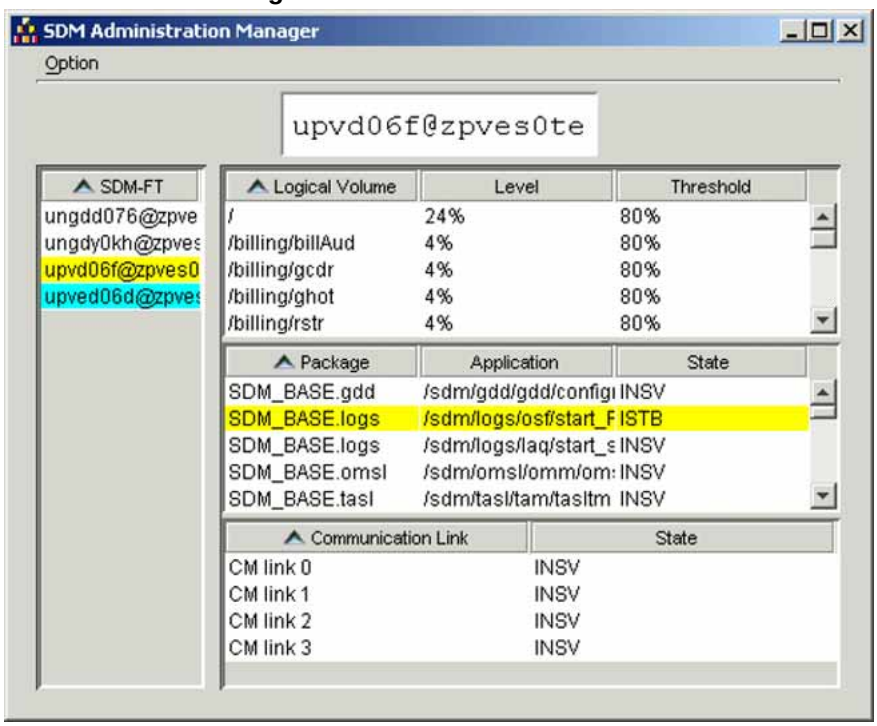


Security Management

It is necessary to restrict access to the CEM browser to only users with valid login credentials. The security framework on the CEM system is provisioned with the functionality such as the following:

- login to access the CEM browser
- encrypted login credentials
- account lockout due to consecutive failed login attempts
- change password capability
- configuration of the telnet or FTP session
- time-out interval periods
- generates security alarms and event logs

Administration Manager main window



Commissioning Manager

After installing the CEM package onto a Sun server, you must set up managed node instances in order to manage network elements. The Commissioning Manager is used to configure coreEMS managed node instances, such as to create, reconfigure and delete a managed node instance. Use the Commissioning Manager command line user interface to configure managed node instances.

For details about how to launch the Commissioning Manager CLI, see "Launching a CEM Commissioning Manager CLI" (page 46). For details about creating and deleting managed node instances, see Creating a CEM managed node instance and Deleting a CEM managed node instance in *IEMS Configuration*, NN10330-511.

Launching a CEM Commissioning Manager CLI

Application

Use this procedure to launch the CEM Commissioning Manager application. Commissioning Manager can be used for configuration of network elements which are represented within the Commissioning Manager system as a set of managed node instances. You can use Commissioning Manager CLI to create, edit, and delete managed node instances.

Prerequisites

To perform this procedure you must have root privileges.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the IEMS server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the server where IEMS resides
2	When prompted, enter your user ID and password.
3	Change to the root user by typing: `$ su - root` and pressing the Enter key.
4	When prompted, enter the root password.
5	Change the directory by typing `# cd /opt/nortel/cem/data/coreEMS/nodes/server/bin` and pressing the Enter key.
6	Launch the CLI by typing `# ./configCEMS -c` and pressing the Enter key.

7 You have completed this procedure.

—End—

Creating a CEM managed node instance

Application

Use this procedure to set up a managed node instance of CEM in order to manage network elements.

Use the Commissioning Manager CLI to configure CEM managed node instances. After installing the CEM package onto a Sun server, users need to set up managed node instances in order to manage network elements. The Commissioning Manager is used to configure coreEMS managed node instances, such as to create, reconfigure and delete a managed node instance. Users should only use the Commissioning Manager to configure managed node instances. Manually editing configuration files is highly discouraged unless the user is absolutely sure of the effect of their action.

Prerequisites

This procedure has the following prerequisites:

- The DMS needs an SDM/CBM with CEM SAF packages installed and services enabled. For details on configuring CEM packages in SDM/CBM, see the *CBM850 Commissioning for UCBM23*, IM 24-2610 and *SDM/FT Installation and Commissioning SDM15 - SDM17, CS2A0002 - CS2E0009*, IM-24-0193, or contact your Nortel representative for instructions.
- The version of CEM on the SDM/CBM must be the same as the target CEM version on the IEMS server.
- You must know the target SDM/CBM IP address.

Action

Step	Action

At your workstation

1 Launch the CEM Commissioning Manager CLI. See Launching the CEM Commissioning Manager CLI in *IEMS Overview*, NN10329-111.

The Commissioning Manager CLI main menu is displayed.

Example response

```
Nortel Networks coreEMS Commissioning Manager
Main menu
1 - Commission a new node
2 - Reconfigure an existing node
3 - Delete an existing node
```

```
4 - Add a mated pair monitor
5 - Delete a mated pair monitor
6 - SDM to CBM migration
0 - Exit
Selection :
```

2 Enter the number next to Commission a new node in the menu.

Example response

```
Configure a Node Instance
1 - DMS
2 - HLR200
3 - MDM
4 - NSP
5 - SESM
6 - USP_NES
7 - DS
Select a new device type for the new node:
```

3 Select the DMS device type for the new node instance by entering the number next to DMS in the menu.

DMS is the only supported option in this configuration.

Example response

```
Hint:  Input a string up to 15 characters drawn
from "-a-z0-9".  The 1st character must be an alpha
character; the last one must not be a minus sign.
Element name cannot be "server", "localhost", "loghost"
or the hostname of the local host.
Mandatory input.
Element Name :
```

4 Enter the name for the new node at the Element Name prompt.

The name can be a string of up to 15 alphanumeric characters and the minus sign (-). The first character must be alphanumeric and the last character must not be a minus sign. The element name cannot be server, localhost, loghost, or the hostname of the local host.

Example response

```
Hint:  Enter the region path to the node or select
one from the list.  Valid path characters include
alpha-numeric and the '/' characters.  Mandatory input.
List of existing regions:
Nortel
Region :
```

5 Enter the region name at the Region prompt.

Example response

```
Hint:  Choose a software version.
```

```
Mandatory input.
[1] GEM18
Software Release (1):
```

6 Select GEM18 for the new node by entering 1 at the Software Release prompt.

Example response

```
Hint:  Input a dot-decimal representation of an IP
address or the string "localhost".
Mandatory input.
Target SDM IP Address:
```

7 Enter the target IP address at the Target SDM IP Address prompt.

The target IP address must be in dot-decimal format.

Example response

```
Hint:  Answer Yes if the SDM has Call Trace installed,
otherwise answer No.
Mandatory input.
1 - Yes
2 - No
Enable Call Trace (1) :
```

8 Enter the number next to No at the Enable Call Trace prompt.

No is the only supported option in this configuration.

Example response

```
Hint:  Answer Yes if this DMS has an MSC/TriNode, No if
this DMS is an HLR.
Mandatory input.
1 - Yes
2 - No
Install Billing Manager(1) :
```

9 Enter the number next to No at the Install Billing Manager prompt.

No is the only supported option in this configuration.

Example response

```
Hint:  Answer Yes if this DMS has USP, otherwise answer
No.  Not valid if Billing Manager = Yes
Mandatory input.
1 - Yes
2 - No
Does This DMS Have USP (2) :
```

10 Enter the number next to No at the Does This DMS Have USP prompt.

No is the only supported option in this configuration.

Example response

```
Proceed to create this node?  [y/n] (n):
```

11 Enter y at the proceed to create this node prompt.

Example response

```
Commissioning node, please wait...
Commissioning node completed successfully!
Is sdma2 already in server mode?  [y/n] (n):
```

12 Enter y at the prompt.

Example response

```
Start all applications of node <nodename>?  [y/n] (n):
```

13 Enter y at the prompt to start the node applications.

14 Wait until the following message appears.

Example response

```
Returning to service all applications of node
<nodename>.
This action may take a few minutes.
Please wait...
Busy/Rts action completed!
```

The Nortel Networks core EMS Commissioning Manager Main menu appears.

```
Nortel Networks coreEMS Commissioning Manager
Main menu
1 - Commission a new node
2 - Reconfigure an existing node
3 - Delete an existing node
4 - Add a mated pair monitor
5 - Delete a mated pair monitor
6 - SDM to CBM migration
0 - Exit
Selection -
```

15 Exit the Commissioning Manager CLI by entering the number next to Exit in the Nortel Networks core EMS Commissioning Manager Main menu.

You have completed this procedure.

—End—

Deleting a CEM managed node instance

Application

Use this procedure to delete a managed node instance of CEM.

Action

Step	Action
	At your workstation

1	Launch the CEM Commissioning Manager. See Launching the CEM Commissioning Manager CLI in *IEMS Overview*, NN10329-111.
	The Commissioning Manager CLI main menu is displayed.
	Example response
	`Nortel Networks coreEMS Commissioning Manager`
	`Main menu`
	`1 - Commission a new node`
	`2 - Reconfigure an existing node`
	`3 - Delete an existing node`
	`4 - Add a mated pair monitor`
	`5 - Delete a mated pair monitor`
	`6 - SDM to CBM migration`
	`0 - Exit`
	`Selection -`

2	Enter the number next to Delete an existing node in the menu.
3	Select the node you want to delete. *Example response* `Proceed to delete this node?  :`

4	Enter y at the prompt to delete this node.
	The Nortel Networks core EMS Commissioning Manager Main menu appears.
	`Nortel Networks coreEMS Commissioning Manager Main menu`
	`1 - Commission a new node`
	`2 - Reconfigure an existing node`
	`3 - Delete an existing node`
	`4 - Add a mated pair monitor`
	`5 - Delete a mated pair monitor`
	`6 - SDM to CBM migration`
	`0 - Exit`
	`Selection -`

5 Exit the Commissioning Manager CLI by entering the number next to Exit in the Nortel Networks core EMS Commissioning Manager Main menu.

You have completed this procedure.

—End—

Packet Media Anchor functionality overview

Many services and call processing capabilities on SIP/SIPt require interaction with a call's bearer path to provide progress indications (that is, tones) in to or to collect digits out of the bearer stream. DPT endpoints are logical entities and do not have physical bearer facilities of their own. As well, SIP/SIPt signaling has limited capability to convey tone and/or digit collection requests to preceding offices. Due to this limitation the SIP specification allows for the introduction of a media server into a call topology to perform media functions. The Packet Media Anchor is Nortel's solution to tone insertion and digit extraction on SIP/SIPt.

The Media Server 2010 is used as the packet gateway to supply media anchoring functionality. The Packet Media Anchor solution uses the bearer channel tandeming (BCT) capability of the AMS to provide media stream anchoring functionality. The media anchor is directed by the CS 2000, which is responsible for managing call topology, resource allocation/deallocation and resource usage. Media anchoring through the AMS does not require conversion from packet to TDM back to packet again, thus impact on bearer path latency will be minimal.

The bearer channel tandeming (BCT) capability of the AMS is provisioned in table SERVSINV. The Packet Media Anchor shares the resources with Lawful Intercept (ALTTERMS), however the Packet Media Anchor resources must be provisioned as a separate Subtending Application on a particular GWC. Packet Media Anchor also requires audio resources, thus an audio application must also be provisioned on the same GWC with the BCT applications.

The packet media anchor will be inserted into SIP/SIPt calls that require bearer facility interaction. Some of these scenarios include:

- Local Treatment on a SIP trunk (tone treatment only)
- Digit collection (for example, DISA service, Auth/Account Codes, CFRA)
- Interactions with CS 2000 line or network services. For example, IN Send-To-Resource could request digit collection on the trunk, or Blind Call Transfer or ACD queuing could request audible ringback on a SIP Trunk after the SIP session has been established. After successful SIP session setup any inband application of tones must be accomplished via Packet Media Anchor.

For the procedure to configure the Packet Media Anchor (PKTMA) for the Dynamic Packet Trunking SIP/SIPt application, see "Configuring Packet Media Anchor functionality" (page 55).

Configuring Packet Media Anchor functionality

Application

Use this procedure to configure the Packet Media Anchor (PKTMA) for the Dynamic Packet Trunking SIP/SIPt application. The role of the Media Anchor is to provide tone, digit collection and bearer path anchoring capabilities for SIP/SIPt call types.

Prerequisites

This procedure has the following prerequisites:

- Table TONES must be datafilled with the appropriate values of FNTONID for the proper tones to be played. For further details, see Carrier Voice over IP Operational Configuration: Data Schema Reference, NN10324-509.
- you must have a Media Server 2010 for Packet Media Anchor functionality
- both BCT and Audio resources must be provisioned on each Media Server 2010 that will be used for the PKTMA
- the device will register with a CS 2000 GWC and it is expected that multiple Media Server 2000 Series devices will be used in the pool of available resources required
- a GWC may support a maximum of one BCT node for Lawful Intercept (ALTTERMS) and one BCT node for the Packet Media Anchor (PKTMA_MAX_CALLS). Multiple instances of either option on a single GWC is not permitted.
- table SERVSINV is the only table that must be provisioned to enable Media Anchor endpoints
- Table TONES must be datafilled with the appropriate values of FNTONID for the proper tones to be played. For further details, see Carrier Voice over IP Operational Configuration: Data Schema Reference, NN10324-509.

Note: The UAS does not support Packet Media Anchor functionality.

Action

Perform the following steps to complete this procedure.

Step	Action
1	Identify the maximum number of anchored calls to support.

2 Provision the Dynamic Packet Media Anchor tuple in table SERVSINV with the maximum number of simultaneous calls to support. See "Provisioning a packet media anchor in table SERVSINV" (page 57).

3 In the GWC element manager provision the following.

For more details, see *GWC Configuration*, NN10205-511.

a. The Network Codec Profile must contain either PCMU or PCMA (G.711)

b. If both PCMU and PCMA are provisioned, then whichever is higher on the preferred list will be used

c. The PMA will ignore other codecs and codec parameters

4 In the Media Server 2000 Series manager provision the following.

For more details, see *MS 2000 Configuration Management*, NN10340-511.

a. Three (3) BCT resources for each anchored call. That is, three times the maximum number of simultaneous anchored calls.

b. One (1) Audio resource for each anchored call.

5 Cold SWACT the ACC GWC or re-initialize all the Media Server gateways.

6 You have completed this procedure.

—End—

Provisioning a packet media anchor in table SERVSINV

Use this procedure to update table SERVSINV to provision a packet media anchor. You must make the following updates:

- You must add a 'BCT' tuple. The BCT tuple specifies the bearer-channel-tandeming capability as a subtending application of the GWC, and also specifies the PKTMA_MAX_CALLS value, that is, the maximum number of anchored calls that the BCT subtending application will support.

  Note: The BCT capability is provided by the MS-2000-series device, which is provisioned as one of the gateways controlled by the GWC.

- You must change the 'AUD' tuple. The AUD tuple specifies the MS-2000-series device. In that tuple, you must increase the value specified for the ANNC option, which specifies number of announcement resources. You increase the ANNC value by adding to it the PKTMA_MAX_CALLS value specified in the BCT tuple.

Prerequisites

You must know the maximum number of anchored calls to be supported by the bearer-channel-tandeming capability of the MS-2000-series device.

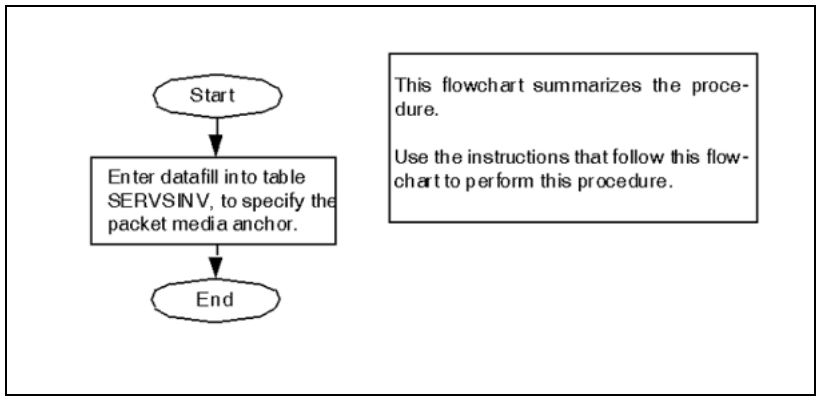
Common procedures

None.

Action

The following flowchart summarizes this procedure.

Provisioning the packet media anchor in table SERVSINV



Provisioning the packet media anchor in table SERVSINV

Step	Action

At the MAP terminal

1 Start the table editor to edit table SERVSINV. At the user interface prompt on any MAP screen type.

```
>TABLE SERVSINV
```

and press the Enter key.

Example of system response:

```
TABLE: SERVSINV
```

2 Indicate that you intend to add a tuple. Type

```
>ADD
```

and press the Enter key.

Example of system response:

```
SERVSNAME:
```

3 Specify the value for the SRVSNAME field. This is the name of the BCT subtending application. Type

```
>BCT <pm-number>
```

and press the Enter key

where

BCT stands for bearer channel tandeming, a subtending application of the GWC

> ***Note:*** The system will use bearer-channel-tandeming capability provided by the MS-2000-series device.

<pm-number> is an integer in the range 0 to 255, representing the unique peripheral-module number of the bearer-channel-tandeming subtending application

For example, type

```
>BCT 5
```

and press the Enter key.

Example of system response:

```
SVRNAME:
```

4 Specify the value for the SRVRNAME (server subtending name) field. This is the name of the gateway controller that uses the bearer-channel-tandeming capability of the MS-2000-series device. Type

>GWC <n>

and press the Enter key

where

<n> is an integer

Note: The GWC name was specified when the gateway controller was configured.

For example, type

>GWC 20

and press the Enter key.

Example of system response:

```
NUMTERMS:
```

5 Specify the value for the NUMTERMS (number of terminals) field. Type

>4095

and press the Enter key.

Example of system response:

```
OPTION:
```

6 Specify the PKTMA-MAX_CALLS value. Type

>PKTMA_MAX_CALLS <n>

and press the Enter key

where

<n> is an integer specifying the maximum number of anchored calls that can be supported by the bearer-channel-tandeming subtending application

Note: You must provision a number of ports on the MS 2000-series device to support anchored calls. The number of ports provisioned for that purpose must be three times the maximum number of anchored calls.

Example of system response:

```
OPTION:
```

7 Indicate that you have finished specifying options. Type:

>$

and press the Enter key.

Example of system response:

```
TUPLE TO BE ADDED:
BCT 5 GWC 20 4095 (PKTMA_MAX_CALLS 300) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

8 Confirm the addition. Type

>Y

and press the Enter key.

Example of system response:

```
TUPLE ADDED.
```

9 Use the POS command to move to the AUD tuple, which is the tuple for the audio-controlling device for the MS-2000-series device. Type

>POS AUD <pm-number>

and press the Enter key

where

AUD specifies the audio-controlling segment of the GWC

<pm-number> is an integer in the range 0 to 255, representing the unique peripheral-module number of the audio-controlling device

For example, type

>POS AUD 4

and press the Enter key.

Example of system response:

```
AUD 4 GWC 20  (6PORT 30)  (ANNC 400)  $:
```

10 Make note of how many options are specified in the tuple, and whether the ANNC option is first option, the last option, or if it occurs elsewhere in the sequence. The options follow the GWC-name. For example, in the system response shown in step 9, the GWC-name is ‘GWC 20, and the ANNC option is the last option specified in the tuple.

11 Indicate that you intend to change the tuple. Type

>CHA

and press the Enter key.

Example of system response:

```
SERVRNAME: GWC 20:
```

12 Press the Enter key to retain the existing value for the SRVRNAME (server name) field.

Example of system response:

```
NUMTERMS: 4095
```

13 Press the Enter key to retain the existing value for the NUMTERMS (number of terminals) field.

14 Choose the next step as follows:.

If the ANNC option	Do
was the first option specified in the tuple, as you noted in step 10	step 16
was not the first option specified in the tuple, as you noted in step 10	step 15

15 The system prompts you to supply a new value for each option that precedes the ANNC option, one option at a time. For each option, press the Enter key to retain the existing value.

Continue to press Enter until the system prompts for a new value for the ANNC option.

Example of system response:

```
ANNC: 400
```

16 Specify a new value for the ANNC (announcement resources) option. Type

`>ANNC <new-value>`

and press the Enter key

where

`<new-value>` is the sum of the previous value of the ANNC option and the value of the PKTMA_MAX_CALLS option (which was specified in step 6)

For example, according to the sample datafill shown in step 9, the previous value of ANNC is 400, and in step 6 we specified 300 as the PKTMA_MAX_CALLS value, so we now type

`>ANNC 700`

and press the Enter key.

17 Choose next step as follows:.

If the ANNC option	Do
was the last option specified in the tuple, as you noted in step 10	step 19
was not the last option specified in the tuple, as you noted in step 10	step 18

18 The system prompts you to supply a new value for each option that follows the ANNC option, one option at a time. For each option, press the Enter key to retain the existing value.

Continue to press Enter until the system prompts you to specify a new option.

Example of system response:

```
OPTION:
```

19 Indicate that you do not wish to specify any more options. Type

>$

and press the Enter key.

Example of system response:

```
AUD 4 GWC 20  (6PORT 30)  (ANNC 700)  $:
```

20 Confirm the change. Type

>Y

and press the Enter key.

Example of system response:

```
TUPLE CHANGED.
```

21 Exit from the table editor. Type

>QUIT

and press the Enter key.

22 You have completed the procedure.

—End—

The following figure shows part of the contents of table SERVSINV. The table now contains a BCT tuple, which specifies the bearer-channel-tandeming subtending application. The table now contains an updated value for the ANNC option in the AUD tuple. In the figure, the new and changed specifications are shown in bold type.

```
SCRSNAME   SVRNAME   NUMTERMS  OPTIONS
-------------------------------------------------------
AUD 4      GWC 20    4095      (6PORT 30) (ANNC 700) $
DPT 6      GWC 15    2048      (SIPT) $
BCT 4      GWC 20    1024      (ALLTERMS 90) $
BCT 5      GWC 20    2095      (PKTMA_MAX_CALLS 300) $
```

MTA signal timeout settings

This section lists the signal timeout values that must be included in the IAC configuration files. The default timeout values for the MTA must be increased. The MTA gateway tone timeouts must be longer than the CS 2000 timeouts to allow the CS 2000 to remain in control.

The following table lists the tone timeouts that are recommended for MTAs.

Tone	Packet Cable default duration (seconds)	Recommended duration (seconds)
Busy	30	Highest possible value
Dialtone	16	25
Message waiting indicator	16	25
Off hook warning tone	0	Highest possible value
Audible ringback	180	Highest possible value
Reorder tone	30	Highest possible value
Stutter dialtone	16	25

The MIBs for these parameters are included in the PacketCable Signaling MIB Specification (www.packetcable.com). These MIBs must be set for each endpoint in the MTA configuration file. The MIBs are:

- pktcNcsEndPntConfigBusyToneTO
- pktcNcsEndPntDialToneTO
- pktcNcsEndPntConfigMessageWaitingTO
- pktcNcsEndPntOffHookWarnToneTO
- pktcNcsEndPntConfigRingingToneTO
- pktcNcsEndPntRingBackToneTO
- pktcNcsEndPntReorderToneTO
- pktcNcsEndPntStutterDialToneTO
- pktcNcsEndPntConfigCallWaitingMaxRep = 0
- pktcNcsEndPntConfigCallWaitingDelay = 0

Configuration management tools and utilities

This section lists tools and utilities used for operational configuration of Carrier VoIP solutions.

Universal Access-AAL1

The Universal Access-AAL1 network includes the following element managers that share all network fault, configuration, accounting, performance, and security (FCAPS) tasks:

UA-AAL1 configuration tools and utilities

Component	Tools
CS 2000, MG 4000, and IW SPM	CS 2000 Core Manager
Multiservice Switch 15000	Nortel MDM
Communication Server LAN	Device Manager for Ethernet Routing Switch 8600
Gateway Controller	CS 2000 Gateway Controller Manager
Universal Audio Server	Universal Audio Server Manager
Universal Signaling Point	Universal Signaling Point Manager
SAM21	CS 2000 SAM21 Manager
MG 9000	MG 9000 Manager

Packet Trunking XA Core and Packet Trunking SN70 solutions

If your switch architecture includes an SDM, then the SDM manages the XA-Core, (or SN70EM) and the subtending TDM components of the XA-Core, or SN70EM. The SDM is an optional piece of equipment. If your switch does not include an SDM, then the XA-Core, or SN70EM, and the MAP provide element management capabilities. The SDM or the MAP is responsible for FCAPS tasks related to XA-Core, (or SN70EM) SPM, and DPT SPM.

The following table lists the tools and utilities used for PT-XA Core or PT-SN70 operational configuration:

PT-XA Core and PT-SN70 configuration tools and utilities

Component	Tools and utilities
Solutions with SDM	
XA-Core and subtending components	SDM
Solutions without SDM	

Component	Tools and utilities
XA-Core or SN70 Manager	MAP
SPM	MAP
DPT SPM	MAP

Packet Trunking IP solution

The following table lists the tools and utilities used for PT-IP operational configuration:

PT-IP configuration tools and utilities

Component	Tools and utilities
XA-Core	MAP
GWC	CS 2000 GWC Manager; XML via OSS gate
SAM21	CS 2000 SAM21 Manager
UAS	Local Config GUI APS for audio provisioning
MS 2000	MS 2000 Series Configuration Tool
APS	SNMP configure_agent tool
USP	USP Mgr GUI
Media Gateway	Nortel MDM, API/EPI
Ethernet Routing Switch 8600	Ethernet Routing Switch 8600 Device Manager

Network management control of dynamic packet trunks

In general, network management control is the real-time surveillance and control of the telephone switching network to ensure maximum traffic flow under overload conditions or network failures. Specifically, in the context of this document, network management control allows you to control the allocation of DPTs (dynamic packet trunks) during overload conditions or during network failure.

In UA-AAL1 networks, you can use these controls to alter or restrict the normal telephone DPT traffic pattern between a given CS 2000 and those CS 2000s to which the first CS 2000 is connected. Using network management control, you can make effective use of network resource during exceptional circumstances and ensure that traffic congestion does not spread through the network.

In PT-XA Core or PT-SN70 solutions, you can use these controls to alter or restrict the normal telephone DPT traffic pattern between a given PT-XA Core, or PT-SN70 office and those BICC CS1 offices (PT-XA Core, PT-SN70 or UA-AAL1) to which the first BICC CS1 office is transmitting DPT bearer traffic. A BICC CS1 (bear independent call control capability set 1) office is an office that supports the BICC CS1 (or ISUP +) signaling standard. Included in the UA-AAL1 solution, there are three office types that support BICC CS1 signaling: PT-XA Core; PT-SN70, and UA-AAL1. Using network management control, you can make effective use of network resource during exceptional circumstances and ensure that traffic congestion does not spread through the network.

Dynamic packet trunks (DPTs) are Nortel implementation of the ATM packet trunk based on BICC CS1 standards. BICC CS1 means bearer independent call control capability set 1 (or ISUP +). DPT hardware ports are not dedicated, nor allocated to any office in the network except during a call. For TDM (time division multiplex) trunks, the logical resources (CICs or trunk members) are statistically associated with the physical resources (terminal identifiers or TIDs) through provisioning. Trunk reservation for TDM is done by reserving a number of idle trunks in the group. Since DPT trunks draw TIDs from a central pool as the need arises, a different form of trunk reservation is needed. Since TDM trunks do not share TIDs, trunk priority is not an issue. However, for DPTs a mechanism is needed to control allocation of TIDs among DPT trunks when traffic is high.

You can apply DPT network management controls in one of two ways:

- by manually inputting commands at the Trunk Group Control (GRPCTRL) and DPT Control (DPTCTRL) levels of the MAPCI

- by using an offline processor such as EADAS (Engineering and Administration Data Acquisition System) or Netminder

Trunk Group Control (GRPCTRL) level of the MAPCI

The GRPCTRl level of the MAPCI is used for TDM (time division multiplex) trunks as well as DPT trunks (see "GRPCTRL level of the MAPCI" (page 68)). At the GRPCTRL level of MAPCI, there are five network management controls that can be used with DPTs:

- DPTP (DPT Priority)
- CANT (Cancel To)
- CANF (Cancel From)
- SKIP (Skip)
- FRR (Flexible ReRoute)

Note 1: Some of the network management controls may only be available for IXC (inter exchange carrier) switches, while other commands are available for both IXC, and ILEC (incumbent local exchange carrier switches. For instance, DPTP is an ILEC and IXC command, while CANT, CANF, SKIP, and FRR are IXC commands.

Note 2: As well as showing the menu controls and commands available at this MAPCI level, "GRPCTRL level of the MAPCI" (page 68) shows the results of applying DPT Priority (_DPTP_) to a select trunk group. The select command has been used after applying DPT Priority to illustrate how DPT Priority is now listed under Ctrls for trunk group EAN820C7DR01.

Note 3: The following controls, at the GRPCTRL level, are not supported for use with DPTs: DRE, PRE, STR, ITB, BRC and TASI.

GRPCTRL level of the MAPCI

```
GrpCtrl      GrpCtrl     Selected Group:   SPDA28     EAN820C7DR01      2W
 0 QUIT_       DRE     PRE    CanT   CanF    Skip    ITB      STR  DPTP
 2              0       0      0      0       0       0        0    1
 3 _DPTP_
 4 LIST_          FRR                  BSSKIP
 5 APPLY_          0                     0
 6 REMOVE_
 7 _DRE_        select    EAN820C7DR01
 8 _PRE_       SCLLI   CLLI              Ofrd      Ovf
   ACH  CCH   ICCH  CCS  Defl
 9 _CANT_      EAN820  EAN820C7DR01   0     0   0%    0     0       0       0
   0
10 _CANF_                                  Ctrls: DPTP
11 _SKIP_
12 _ITB_
13 _STR_
14 _FRR_
15
16
```

DPT Priority control for bandwidth directionalization

The DPT Priority control is one of the following three features that are collectively referred to as Bandwidth Directionalization sub-features: DPT TID Limit Refinement; DPT Reservation; and DPT Priority. DPT Bandwidth Directionalization is a feature offering that is enabled by SOC (software optionality control CS2B0003) and should only be enabled on offices using BICC CS1. DPT Priority allows you to assign priorities to DPT groups in order to control which calls are completed during periods of high call volumes. For example, you can assign a higher priority to DPTs between several CS 2000s (BICC CS1 offices in PT-XA Core or PT SN70 solutions) in close proximity to have a higher priority than other DPT groups in order to reserve bandwidth for calls within a region.

> ***Note:*** For information on setting or removing the DPT priority control, see CS 2000 Operational Configuration, NN10201-511.

When the DPT Priority control is activated, each selected trunk group is assigned a specific threshold, which is stated as a percentage of the TIDs (terminal identifiers) which are idle. The idle percentage of TIDs used for DPT Priority is calculated as follows:

Idle% = ((DPT TID limit DPT TIDs in use) / (DPT TID Limit)) x 100

Since the percentage of TIDs is calculated in the same way for DPT Priority as it is for DPT Reservations (another Bandwidth Directionalization feature), you can see how the value of DPT limit influences the behavior of DPT Priority. For information on the DPT reservation feature, see "DPT Reservation control for bandwidth directionalization" (page 86).

All trunk groups without specific thresholds are assigned an office threshold which defaults to zero percentage (0%) but can be set, if desired. When the percentage of idle terminal identifiers drops below the threshold for a trunk group, calls are blocked, in other words incoming calls are released and outgoing calls attempt to use the next route on the route list. When calls are blocked on a trunk group, registers NWMTGAFF, and NWMTGATT (operational measurements group NWMTGCNT), and register DEFLDCA (OM group TRK) are pegged. When calls are not blocked, only register NWMTGATT is pegged. The figure "Example 1 showing the impact of DPT Priority on TID allocation" (page 70) describes the operation of DPT Priority in terms of a flowchart.

Note 1: The DPT Priority feature must be used with care. If all trunk groups and office thresholds have a DPT Priority greater than zero (0), then the lowest percentage for DPT Priority would effectively represent the percentage of TIDs which would never be used.

Note 2: In order for DPT Bandwidth Directionalization controls to be effective, you must provision office parameter DPT_MAX_PORTS first and set this office parameter through table control. (The default value is 1.)For information on setting this parameter, see CS 2000 Operational Configuration, NN10201-511.

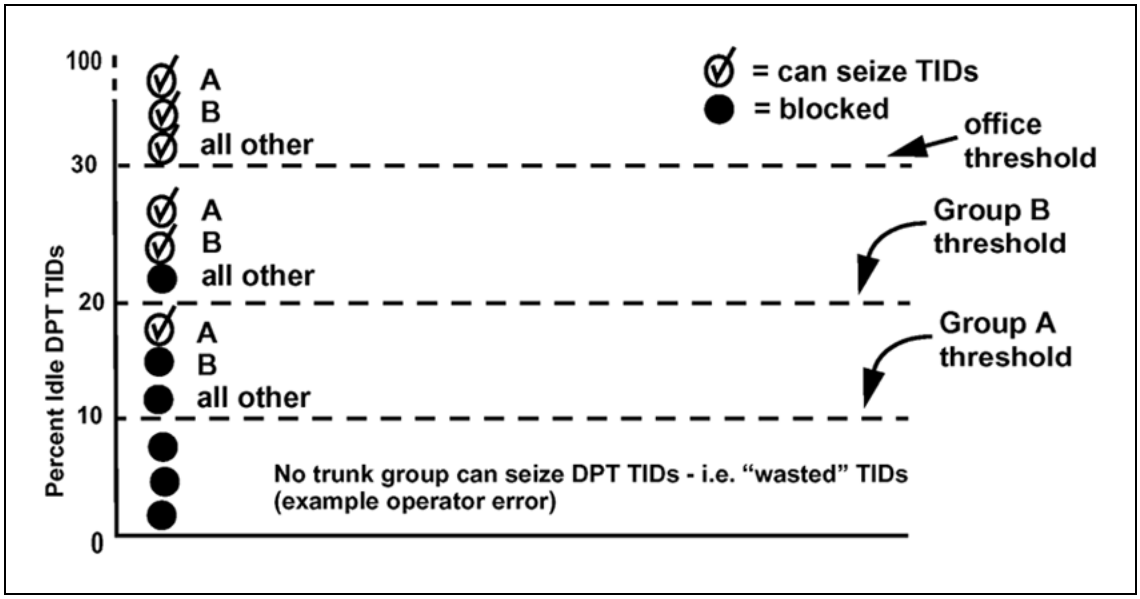
Note 3: For information on the order of precedence for DPT Priority and DPT Reservation, see "Order of precedence for DPT Reservation and DPT Priority" (page 88).

Although the operation of DPT Priority appears simple, the implications of using this control on multiple trunk groups are not immediately apparent. DPT Priority is a powerful control that you can use in more ways than one. To further illustrate the use of this control, three examples are supplied.

Example 1: Using DPT Priority to give an advantage to certain trunk groups

In this example, the office threshold is set to 30% and trunk groups A and B are given thresholds of 10% and 20% respectively. The figure shows which trunk groups can seize DPT TIDs at different levels of DPT business or idleness.

Example 1 showing the impact of DPT Priority on TID allocation



Notice in the figure that the phenomenon of 'wasted TIDs' can be prevented simply by setting the threshold of the highest priority trunk group to zero percent (0%) rather than 10% (shown above) whenever the office threshold is explicitly set and not 0%.

In the case of example 1, if the percentage of idle TIDs stays between 20% and 30% for several minutes or more, all DPT traffic is focused onto trunk groups A and B, assuming that these trunk groups together have sufficient CICs (carrier identification codes) and incoming traffic to sustain the 30% idle condition.

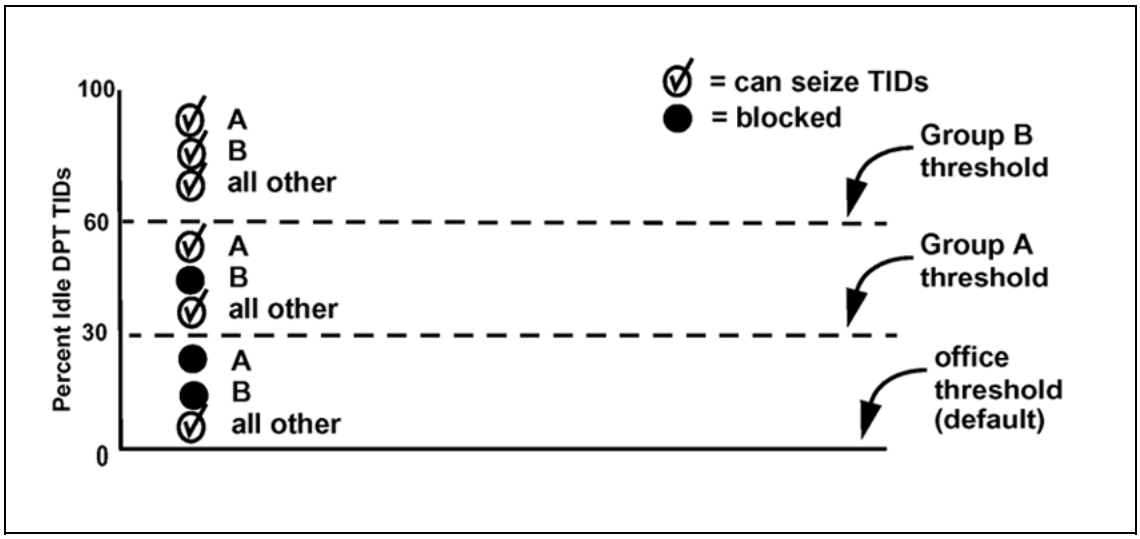
Also, if the percentage of idle TIDs stays less than 20% for several minutes or more, all DPT TIDs are allocated to trunk group A, assuming this trunk group alone has sufficient CICs and incoming traffic to sustain this degree of business or idleness.

If in example 1, trunk group A can only support 6% of the total DPT capacity due to insufficient CICs or incoming traffic, then 14% of the TIDs are unusable. Ten percent of the 14% is attributable to trunk group A (the highest priority trunk group) because trunk group A is assigned a 10% threshold rather than 0%. The remaining 4% is attributable to the gap between the 10% exclusive use zone for trunk group A and the fact that trunk group A can only use 6%.

Example 2: Using DPT Priority to place certain trunk groups at a disadvantage

In example 2, the office threshold is left at the default value of 0% and trunk groups A and B are given thresholds of 30% and 60% respectively. The figure shows which trunk groups can seize DPT TIDs at different levels of DPT business or idleness.

Example 2 showing the impact of DPT Priority on TID allocation



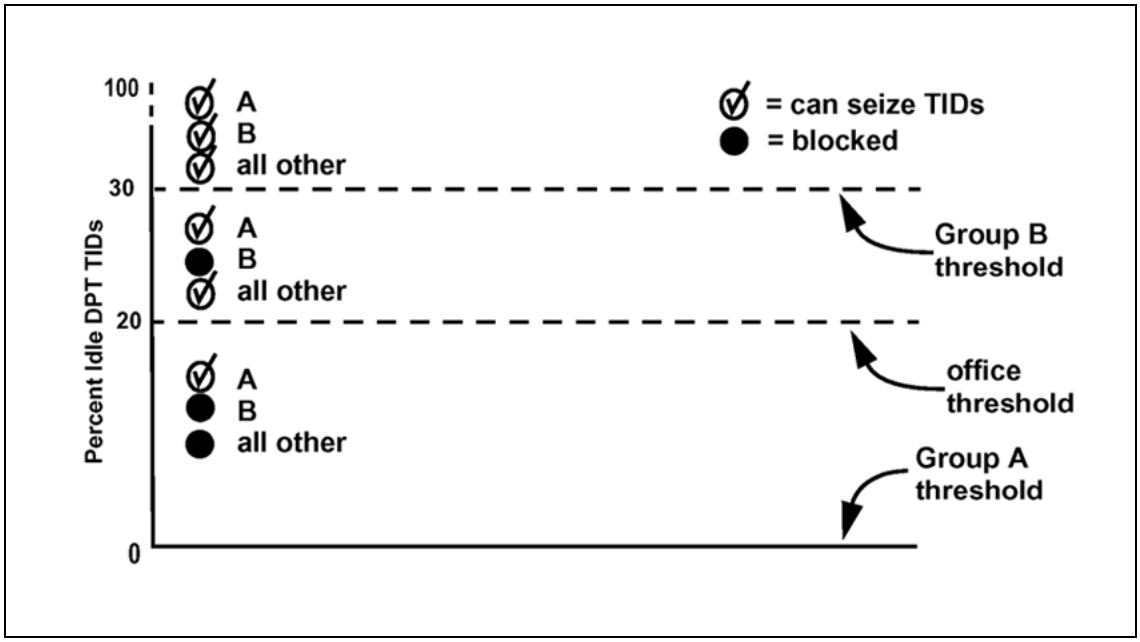
In example 2, if the idle TIDs stay between 30% and 60% for several minutes or more, then, all traffic through trunk group B has been ‘squeezed out’ in favor of DPT traffic through trunk group A and all other trunk groups.

Likewise, if the percentage of idle TIDs stays less than 30% for several minutes or more, traffic for both trunk groups A and B is suppressed in favor of all other trunk groups.

Example 3: The hybrid approach of using DPT Priority

In example 3, the office threshold is specifically set to 20%, trunk group A is set to 0%, and trunk group B is set to 30%.

Example 3 showing the impact of DPT Priority on TID allocation



In example 3, since the office threshold is greater than the threshold for trunk group A, trunk group A has an advantage relative to all other trunk groups. Since the office threshold is less than the threshold for trunk group B, trunk group B has a disadvantage relative to all other trunk groups.

In example 3, if trunk group A can only support 8% of the total DPT capacity due to insufficient CICs, or incoming traffic, then 12% of DPT TIDs are effectively unusable.

Cancel To control for DPTs

The CANT (Cancel To) control is one of the following five DPT network management controls that you can access from the GRPCTRL level of MAPCI: DPTP, CANT, CANF, SKIP, FRR. The CANT control is a protective network management trunk group control that limits a preset percentage of traffic offered to a selected trunk group. The CANT control limits traffic on one-way out-going and two-way trunk groups. This control can cancel any percentage of alternate route (AR) traffic exclusively or all alternate route traffic and a percentage of direct route (DR) traffic. Percentages of traffic the CANT control cancels range from 1 to 100% in one percent increments.

Note 1: The CANT control is only available for IXC switches.

Note 2: For information on setting or removing the DPT CANT control, see CS 2000 Operational Configuration, NN10201-511.

Activation of the CANT control blocks a percentage of the traffic offered to a particular trunk group, and routes the traffic to one of the following treatments:

- No circuit announcement (NCA)
- Emergency announcement 1 (EA1)
- Emergency announcement 2 (EA2)

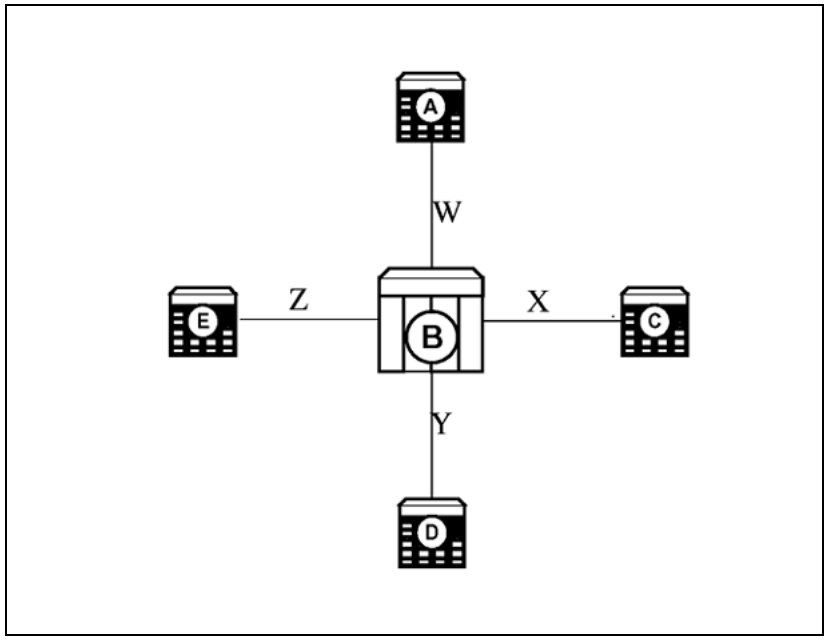
Enhanced Cancel To control for DPTs

The enhanced CANT (Cancel To) control is enabled by software optionality control (SOC) OAM00012. When SOC OAM00012 is turned on, enhanced CANT is active, and when the SOC is off standard CANT control is active. The enhanced CANT control, when implemented in an originating CS 2000 (BICC CS1 offices), cancels a percentage of traffic to a terminating CS 2000 (BICC CS1 offices). This activity allows you to apply different threshold percentages for Hard To Reach (HTR) traffic and Easy To Reach (ETR) traffic. A code is tagged Hard To Reach when the probability of call completion is extremely low. A code is tagged Easy To Reach when the probability of call completion is close to 100%. The CANT control cancels a percentage of the calls out of an originating CS 2000 (BICC CS1 offices in PT-XA Core or PT SN70 solutions) to a specified terminating CS 2000 (BICC CS1 offices). You can use this control during periods of heavy calling to protect the terminating CS 2000 (BICC CS1 offices) and the signaling network from overload (see "Enhanced CANT control applied to a terminating trunk" (page 74)).

Note 1: The CANT control is only available for IXC switches.

Note 2: For information on setting or removing the DPT CANT control, see CS 2000 Operational Configuration, NN10201-511.

Enhanced CANT control applied to a terminating trunk



In the figure, CS 2000 B is the congested switch. To regulate traffic, you can throttle traffic on trunk X and Y using the enhanced CANT option. You can specify different traffic thresholds for HTR, and ETR codes on the CS 2000 switches C and D.

Cancel From control for DPTs

The CANF (Cancel From) control, at the GRPCTRL level of MAPCI, is a protective network management trunk group control. The CANF control prevents overflow traffic (both DR or direct route, and AR or alternate route), that is coming from selected one-way out-going or two-way trunk groups, from continuing to the next trunk group within the route list of trunks.

The CANF control acts in a similar way to the CANT control by blocking a preset level from both direct and alternate-routed (DAR) traffic. Note that DR or direct route traffic, plus AR or alternate route traffic, equals DAR traffic. The blocked calls are routed to treatments NCA, EA1, or EA2. The percentages of traffic, that the CANF control cancels, ranges from 1 to 100% in one percent increments.

Note 1: The CANF control is only available for IXC switches.

Note 2: For information on setting or removing the DPT CANF control, see CS 2000 Operational Configuration, NN10201-511.

Enhanced Cancel From for DPTs

The enhanced CANF (Cancel From) control is enabled by software optionality control (SOC) OAM00012. When SOC OAM00012 is turned on, enhanced CANF is active, and when SOC is off standard CANF control is active. The enhanced CANF control applies to traffic overflowing or skipping a trunk group. The enhanced CANF control gives you the option of controlling a percentage of calls that are denied in-chain route advance. The enhanced CANF control can control at the same percentage levels as the enhanced CANT control. These percentage levels apply to overflow traffic offered to a trunk group as AR (alternate route) or DR (direct route) traffic. It can also control HTR (Hard To Reach) traffic for AR and DR.

Skip control for DPTs

The SKIP (Skip) control, at the GRPCTRL level of MAPCI, affects traffic on one-way out-going and two-way trunk groups. The system can deny access to any percentage of direct route (DR) or alternate route (AR) traffic to the trunk group. The system redirects that traffic percentage to the next in-chain route that has the SKIP control. Affected percentages of traffic range from 1 to 100%, in one percent increments. In all the trunk groups in the routing chain are exhausted, the call is sent to treatment.

Note 1: The Skip control is only available for IXC switches.

Note 2: For information on setting or removing the DPT Skip control, see CS 2000 Operational Configuration, NN10201-511.

Enhanced skip control for DPTs

The enhanced SKIP (Skip) control is enabled by software optionality control (SOC) OAM00012. When SOC OAM00012 is turned on, enhanced SKIP control is active, and when SOC is off standard SKIP control is active. The enhanced SKIP control allows a call to take an alternate route by way of the next trunk group in the routing pattern. If a SKIP control and a post hunt control are applied to the same trunk group simultaneously, the skipped traffic is subjected to overflow reroute and or CANF control. SKIP control also controls at the same percentage levels as CANT control for both ETR and HTR AR or DR traffic.

Note 1: The Skip control is only available for IXC switches.

Note 2: For information on setting or removing the DPT Skip control, see CS 2000 Operational Configuration, NN10201-511.

Flexible ReRoute control for DPTs

The FRR (Flexible ReRoute) control, at the GRPCTRL level of MAPCI, enhances network management by allowing you to reroute calls from an in-chain route to a VIA route without modifying the datafill in the DMS (Digital Multiplex System) tables.

Note 1: The FRR control is only available for IXC switches.

Note 2: For information on setting or removing the DPT FRR control, see CS 2000 Operational Configuration, NN10201-511.

In the past, you would have had to change provisioning before reroutes could be made. The FRR control allows you to reroute traffic without modifying provisioning. As a result, traffic control can be activated quickly and when needed. FRR allows you to respond immediately and effectively to traffic overload and congestion within the network.

The FRR control uses an office route table (OFRT, OFR2, OFR3, OFR4) to provide an alternate routing scheme, so that all selectors are supported (selectors N, ST, T and so on). In other words, instead of specifying trunk groups as the VIA route in network management commands, an office route table and a route reference are identified as the VIA route of a trunk group.

The FRR control functions in the following way: you select a trunk group, then, point the traffic to a replacement trunk group, or point the traffic to the routing table of a trunk group.

The FRR control is an expansive network management trunk group control. When you use the FRR control, you associate two trunk groups:

- The first trunk group (the in-chain route) is the trunk group to which the FRR control is applied. This trunk group is also referred to as the controlled trunk group.
- The second trunk group (the VIA route) is a standard route (standard digit manipulation). Calls that cannot be carried over the controlled route are offered to the VIA route.

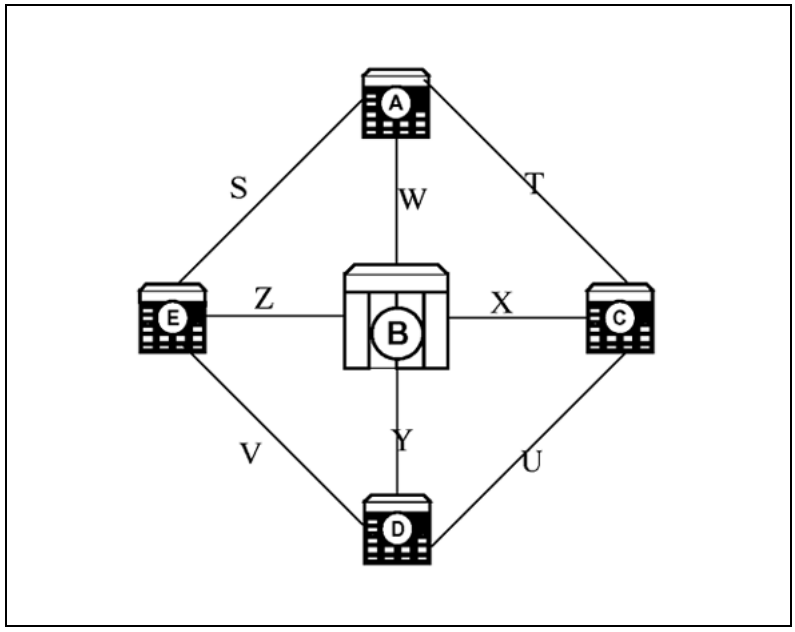
Enhanced Flexible ReRoute control for DPTs

The enhanced Flexible ReRoute (FRR) control is enabled by software optionality control (SOC) OAM00012. When SOC OAM00012 is turned on, enhanced the FRR control is active, and when SOC is off standard FRR control is active. The enhanced FRR control is implemented on an originating CS 2000. This control allows you to specify an alternate route for the traffic to the terminating CS 2000.

For each call going on this trunk group the destination directory number is compared with the codes (up to a max. of 15 digit) that you specify in the enhanced FRR control. The enhanced FRR control can support a maximum of 16 codes for each FRR control. You can specify different traffic thresholds

for ETR & HTR traffic. Enhanced FRR control request supports a prefix field that allows you to reroute the traffic based on the type of call. (The call types that are supported is limited to national or international calls.)

Enhanced FRR control applied to a terminating trunk



In the figure, CS 2000 A is the originating office and CS 2000 D is the terminating office. In the event of CS 2000 B being congested, a percentage of calls made from office A to office D, (assuming it follows path W to CS 2000 B to Y) should be rerouted through an alternate route. (For example, T to CS 2000 C to U.) Routing the traffic through the alternate route, reduces the load and alleviates the congestion on CS 2000 B.

Using the GRPCTRL commands to issue the DPT network management controls

As has already been mentioned, there are five DPT network management controls at the MAPCI;NWM;GRPCTRL level:

- DPTP (DPT Priority)
- CANT (Cancel To)
- CANF (Cancel From)
- SKIP (Skip)
- FRR (Flexible ReRoute)

At the GRPCTRL level there are three commands that you can use to manage these five DPT network management controls (see "GRPCRTL level after applying DPT Priority" (page 78)):

- Apply
- List
- Remove

GRPCRTL level after applying DPT Priority

```
GrpCtrl        GrpCtrl      Selected Group:    SPDA28      EAN820C7DR01
      2W
 0 QUIT_         DRE     PRE    CanT   CanF    Skip    ITB      STR  DPTP
 2                0       0       0      0       0      0        0   1
 3 _DPTP_
 4 LIST_             FRR                   BSSKIP
 5 APPLY_             0                      0
 6 REMOVE_
 7 _DRE_           select    EAN820C7DR01
 8 _PRE_           SCLLI     CLLI                Ofrd      Ovf
   ACH   CCH    ICCH   CCS   Defl
 9 _CANT_          EAN820    EAN820C7DR01   0     0   0%    0      0       0
     0      0
10 _CANF_                                        Ctrls: DPTP
11 _SKIP_
12 _ITB_
13 _STR_
14 _FRR_
15
```

Using the Apply command with the DPTP (DPT Priority) control

The following table shows the syntax for the APPLY command used with the DPTP control. This control is only available when SOC CS2B0003 is on. (See "GRPCRTL level after applying DPT Priority" (page 78).)

APPLY command with DPT Priority control

Command, control and variables
APPLY DPTP ppct otheppct
where

Command, control and variables	
<ppct>	is a percentage (0 to 100) indicating the threshold level for the selected trunk group. Once the percentage of remaining TIDs falls below this mark, calls on this trunk group are blocked. This is a mandatory parameter.
<otheppct>	is a percentage (0 to 100) indicating the threshold level for all other trunk groups. This is an optional parameter.

Using the APPLY command with the CANT (Cancel To) control

The CANT control on the GRPCTRL level of MAPCI works in the same way for DPT trunks as for TDM (time division multiplex) trunks. For additional information on the CANT control see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

Using the APPLY command with the enhanced CANT (Cancel To) control

The following table shows the syntax for the APPLY command used with the enhanced CANT control. This control is only available when SOC OAM00012 is on. For additional information on the CANT control see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

APPLY command with enhanced CANT control

Command, control and variables	
APPLY CANT dr_pct ar_pct htr_dr_pct htr_ar_pct ann	
where	
<dr_pct>	is a percentage (0 to 100) for ETR (Easy to Reach) direct-routed calls.
<ar_pct>	is a percentage (0 to 100) for ETR (Easy to Reach) alternate-routed calls.
<htr_dr_pct>	is a percentage (0 to 100) for HTR (Hard to Reach) direct-routed calls.
<htr_ar_pct>	is a percentage (0 to 100) for HTR (Hard to Reach) alternate-routed calls.
<ann>	is NCA, EA1, EA2 to specify the announcement to which blocked calls are connected. A treatment is given to a call when the traffic exceeds the threshold percentage level.

Using the APPLY command with the CANF (Cancel From) control

The CANF control on the GRPCTRL level of MAPCI works in the same way for DPT trunks as for TDM (time division multiplex) trunks. For additional information on the CANF control see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

Using the APPLY command with the enhanced CANF (Cancel From) control

The following table shows the syntax for the APPLY command used with the enhanced CANF control. This control is only available when SOC OAM00012 is on. For additional information on the CANF control see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

APPLY command with CANF control

Command, control and variables	
APPLY CANF dr_pct ar_pct htr_dr_pct htr_ar_pct ann	
where	
<dr_pct>	is a percentage (0 to 100) for ETR (Easy to Reach) direct-routed calls.
<ar_pct>	is a percentage (0 to 100) for ETR (Easy to Reach) alternate-routed calls.
<htr_dr_pct>	is a percentage (0 to 100) for HTR (Hard to Reach) direct-routed calls.
<htr_ar_pct>	is a percentage (0 to 100) for HTR (Hard to Reach) alternate-routed calls.
<ann>	is NCA, EA1, EA2 to specify the announcement to which blocked calls are connected. A treatment is given to a call when the traffic exceeds the threshold percentage level.

Using the APPLY command with the SKIP (Skip) control

The SKIP control on the GRPCTRL level of MAPCI works in the same way for DPT trunks as for TDM (time division multiplex) trunks. For additional information on the SKIP control see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

Using the APPLY command with the enhanced SKIP (Skip) control

The following table shows the syntax for the APPLY command used with the enhanced SKIP control. This control is only available when SOC OAM00012 is on. For additional information on the SKIP control see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

APPLY command with enhanced SKIP control

Command, control and variables	
APPLY SKIP dr_pct ar_pct htr_dr_pct htr_ar_pct	
where	
<dr_pct>	is a percentage (0 to 100) for ETR (Easy to Reach) direct-routed calls.
<ar_pct>	is a percentage (0 to 100) for ETR (Easy to Reach) alternate-routed calls.
<htr_dr_pct>	is a percentage (0 to 100) for HTR (Hard to Reach) direct-routed calls.
<htr_ar_pct>	is a percentage (0 to 100) for HTR (Hard to Reach) alternate-routed calls.

Using the APPLY command with the FRR (Flexible ReRoute) control

The FRR control on the GRPCTRL level of MAPCI works in the same way for DPT trunks as for TDM (time division multiplex) trunks. For additional information on the FRR control see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

Using the APPLY command with the enhanced FRR (Flexible ReRoute) control

The following table shows the syntax for the APPLY command used with the FRR control. This control is only available when SOC OAM00012 is on. For additional information on the FRR control see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

APPLY command with enhanced FRR control

Command, control and variables	
APPLY FRR dr_pct ar_pct htr_dr_pct htr_ar_pct ctrlopt [htropt] [eaopt] [cicropt] viaopt no_csrcodes	
where	
<dr_pct>	is a percentage (0 to 100) for ETR (Easy to Reach) direct-routed calls.
<ar_pct>	is a percentage (0 to 100) for ETR (Easy to Reach) alternate-routed calls.
<htr_dr_pct>	is a percentage (0 to 100) for HTR (Hard to Reach) direct-routed calls.
<htr_ar_pct>	is a percentage (0 to 100) for HTR (Hard to Reach) alternate-routed calls.

Command, control and variables	
<ctrlopt>	specifies the Immediate Reroute (IRR), Regular ReRoute (RRR), or Table ReRoute (TRR) control. The TRR option provides the capability to reroute traffic to an office route table (OFRT, OFR2, OFR3, OFR4). If the TRR option is used, VIAOFC must be entered as the VIA option (via_opt).
<htropt>	specifies that only Hard To Reach (HTR) calls are affected by the FRR control.
<eaopt>	specifies whether only Equal Access (EA) calls or only Non Equal (NEA) calls are affected by the FRR control.
<cicropt>	specifies the Cancel InChain Return (CICR) control. CICR specifies that calls rerouted by the FRR control should be sent to treatment once the out-of-chain route list for those calls is exhausted. Omission of the CICR specifies that calls rerouted by FRR should not be sent to treatment once the out-of-chain route list is exhausted. Instead these calls are returned to the next route in the in-chain route list.
<viaopt>	specifies the VIA routes (trunk groups) to which calls (with the FRR control activated) are routed.
<no_csrcodes>	specifies the number of Code Specific Reroute (CSR) codes. Depending on the number of CSR codes, the remaining command document is displayed.

The following figure shows the output for the APPLY command.

APPLY command with enhanced CANT, CANF, SKIP, and FRR controls

```
Ctrl   ITS    RADR       CPU     Init     IDOC     CS   DCR          Fs
G...     0      0%         0%      .        .        .                  0

GrpCtrl          GrpCtrl      Selected   Group:       IBNT2M      IBNT2MF
         2W
 0 QUIT_         DRE    PRE    CanT   CanF      Skip      ITB         STR
       DPTP
 2                 0      0      1      1         1        0           0              0
 3 _DPTP_
 4 LIST_          FRR
 5 APPLY_           1
 6 REMOVE_
 7 _DRE_
 8 _PRE_
 9 _CANT_
10 _CANF_
11 _SKIP_
12 _ITB_
13 _STR_
14 _FRR_
15
```

Using the LIST command with DPT network management controls

The LIST command allows you to list a particular network management trunk group control for either selected trunk groups or for all trunk groups. The LIST command (at the GRPCTRL level) operates in the same way for DPTs as for TDM trunks. For DPTs, the DPT Priority (DPTP) control is added to the possible control types that you can list. For additional information on the LIST command see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

Using the REMOVE command with DPT network management controls

The REMOVE command allows you to remove a particular network management trunk group control from a selected trunk group. The REMOVE command (at the GRPCTRL level) operates in the same way for DPTs as for TDM trunks. For DPTs, the DPT Priority (DPTP) control is added to the possible control types that you can operate on with the REMOVE command. For additional information on the LIST command see, the Network Management System Reference Manual, 297-1001-453 on Helmsman.

DPT Control (DPTCTRL) level of the MAPCI

There are two network management controls at the MAPCI;NWM;DPTCTRL level that can be used with DPTs (see "DPTCTRL level of MAPCI" (page 84)):

- DPTR (DPT Priority)
- MAXTID (Maximum number of TIDs)

At the DPTCTRL level there are three commands that you can use to manage these two controls:

- LIST_
- APPLY_
- REMOVE_

Note: As well as showing the menu controls and commands available at this MAPCI level, "DPTCTRL level of MAPCI" (page 84) shows the results of applying DPT Reservation (_DPTR_) to a select trunk group.

DPTCTRL level of MAPCI

```
DptCtrl                DptCtrl
 0 QUIT_                     DPTR        MaxTid
 2                            ON           OFF
 3
 4 LIST_
 5 APPLY_
 6 REMOVE_
 7 _DPTR_
 8 _MAXTID_
 9
10
11
12
13
14
15
16
17
18 PAGE
```

DPT TID Limit Refinement control for bandwidth directionalization

The DPT Reservation control is one of three features that are collectively referred to as Bandwidth Directionalization sub-features. The three Bandwidth Directionalization features are: DPT TID Limit Refinement (MAXTID); DPT Reservation; and DPT Priority. DPT Bandwidth Directionalization is a feature offering that is enabled by SOC (software optionality control CS2B0003) and should only be enabled on offices using BICC CS1. The DPT TID Limit Refinement control (MAXTID on MAPCI), and the DPT Reservation control are both available from the DPTCTRL level of MACPI. The DPT Priority control is available at the GRPCTRL level.

The DPT TID (terminal identifier) Limit Refinement control provides a network management interface for updating the number of DPT TIDs that a PT-XA Core, PT SN70 solutions or CS 2000 supports. Each DPT TID represents the ATM (asynchronous transfer mode) bandwidth needed to carry a single DPT trunk call. The DPT TID limit can be used to ensure that the ATM bandwidth required by DPT trunks does not exceed the ATM bandwidth provided by the ATM links that connect the PT-XA Core, PT SN70 solutions or CS 2000 to the rest of the ATM network. A nominal value for the TID limit can be engineered and provisioned, but over time this value may need to be refined to reflect temporary conditions, for example, a subset of the ATM links being temporarily down.

> ***Note:*** For information on setting or removing the DPT maximum TID limit control, see CS 2000 Operational Configuration, NN10201-511.

In order to understand how the DPT TID Limit Refinement control works, it is necessary to define the following four values:

- DPT_MAX_PORTS the provisioned value for the maximum number of DPT TIDs. This value is entered through table OFCVAR.
- NWM_DPT_MAXTIDS the network management supplied value for the maximum number of DPT TIDs. You enter this value through the MAPCI level MAPCI;NWM;DTPCTRL (using the MAXTID command).
- TOTAL_INSERVICE_TRMS this value is updated as needed by the PT-XA Core, PT SN70 solutions or CS 2000 and represents the total number of DPT terminals in-service on the PT-XA Core, PT SN70 solutions or CS 2000 at any point in time.
- DPT TID Limitis the maximum number of DPT TIDs actually used by the call processing logic.

The DPT TID Limit Refinement control does not directly influence call processing. Instead, it directly affects the value of DPT TID Limit which in turn affects the behavior of DPT Reservation, DPT Priority, and the call processing behavior of office parameter DPT_MAX_PORTS in table OFCVAR. The way the DPT TID Limit affects DPT Reservation and DPT Priority is described in the following sections.

The rules that relate the values of DPT_MAX_PORTS, NWM_DPT_MAX-TIDS, and TOTAL_INSERVICE_TRMS to DPT TID Limit Refinement are:

- If DPT_MAX_PORTS is set and NWM_DPT_MAXTIDS is applied (as opposed to OFF), the maximum number of DPT TIDs allowed is the minimum of DPT_MAX_PORTS, NWM_DPT_MAXTIDS, and TOTAL_INSERVICE_TRMS. (This rule reflects the role of DPT_MAX_PORTS as an upper bound, NWM_DPT_MAXTIDS as a temporary reduction to the upper bound, and TOTAL_INSERVICE _TRMS as a continuously up to date physical limit.)
- If DPT_MAX_PORTS is set and NWM_DPT_MAXTIDS is not applied then the minimum of DPT_MAX_PORTS and TOTAL_INSERVICE_TRMS is used for DPT TID Limit.
- If DPT_MAX_PORTS is un-set then DPT TID Limit is assigned value 0 and treated as un-set. In other words, DPT Bandwidth Directionalization controls have no effect.

DPT Reservation control for bandwidth directionalization

The DPT Reservation control is one of three features that are collectively referred to as Bandwidth Directionalization features. The three Bandwidth Directionalization feature are: DPT TID Limit Refinement; DPT Reservation; and DPT Priority. DPT Bandwidth Directionalization is a feature offering that is enabled by SOC (software optionality control CS2B0003) and should only be enabled on offices using BICC CS1 (bearer independent call control capability set 1).

Note: For information on setting or removing the DPT reservation level, see CS 2000 Operational Configuration, NN10201-511.

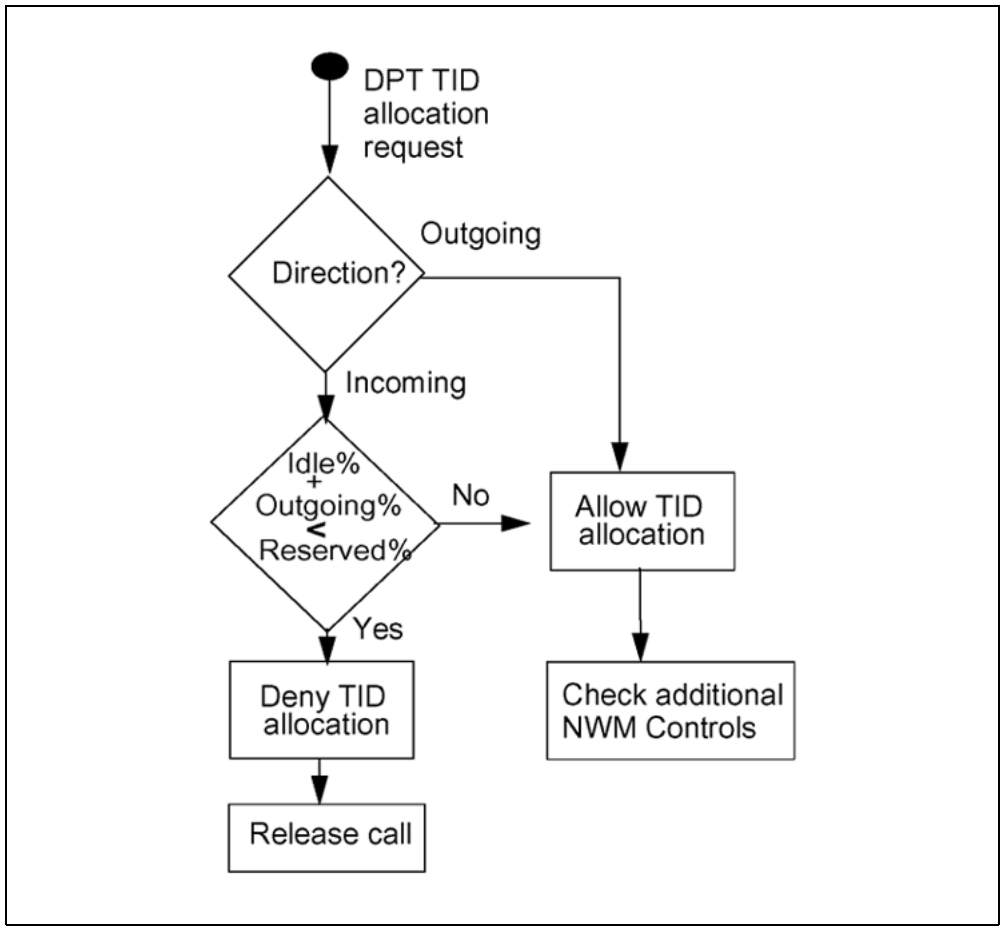
DPT Reservation allows you to reserve a percentage of usable TIDs (terminal identifiers) for outgoing DPT calls during a mass calling event. For example, during a natural disaster, you can reserve bandwidth for outgoing calls from a disaster area, while blocking an excess of calls incoming to the area. To enforce the reservation, incoming calls may be blocked. On outgoing calls, no blocking is required. Normally, when the terminating CS 2000 receives the BICC CS1 IAM (ISUP initial address) message, the terminating CS 2000 must pick an initial MG 4000 for the call and select an idle DPT TID (terminal identifier). However, with DPT Reservation, the allocation of the TID may be denied.

To determine whether or not to block, the CS 2000 software uses three percentages:

Percentage	How the percentage is derived
Outgoing % =	((DPT TIDs in use for outgoing calls)/(DPT TID Limit)) x 100
Idle% =	((DPT TID Limit DPT TIDs in use)/(DPT TID Limit)) x 100
Reservation% =	the desired percentage of TIDs reserved for outgoing calls

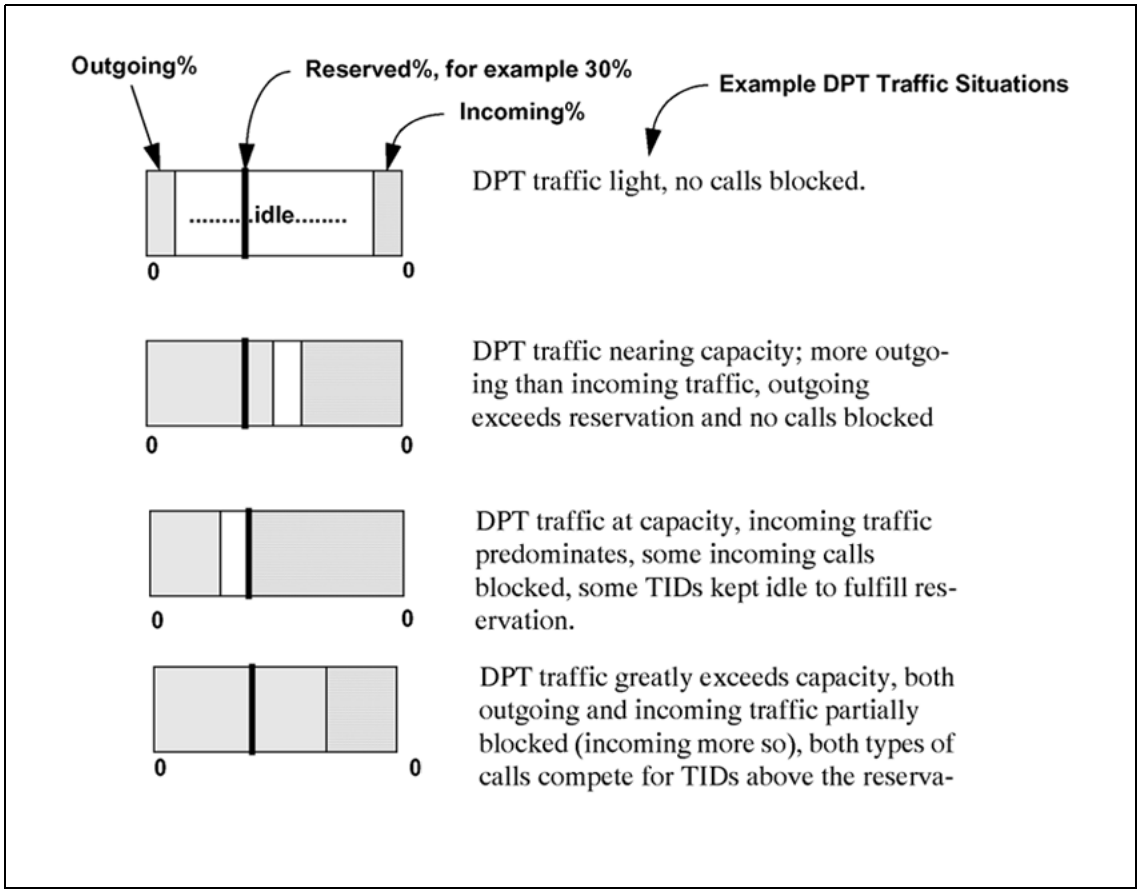
Assume that the outgoing percentage (Outgoing%) plus the idle percentage (Idle%) is less than the reservation percentage. This would indicate that completing the call would violate the reservation. As a result, the CS 2000 clears the call by sending a release message to the originating CS 2000 and pegs OM register DPTR (in OM Group OFZ2). The operation of the DPT Reservation control is illustrated in "DPT Reservation operation" (page 87).

DPT Reservation operation



The consequence of this TID allocation policy is illustrated by a "Effect of DPT Reservation on TID distribution" (page 88) that shows outgoing TIDs on the left, idle TIDs in the middle, and incoming TIDs on the right. A reference line is added to show the percentage reserved for outgoing calls. "Effect of DPT Reservation on TID distribution" (page 88) shows the effect of the DPT Reservation control in the following four situations: with light DPT traffic, when DPT traffic nearing capacity; with DPT traffic at capacity; when DPT traffic exceeds capacity.

Effect of DPT Reservation on TID distribution



Order of precedence for DPT Reservation and DPT Priority

This section defines the order of precedence for DPT network management controls in relation to existing network management controls. The order of precedence is examined for both incoming and outgoing calls.

For incoming calls, where a DPT is the originator, the order of precedence from highest to lowest is as follows:

1. The DPT Reservation
2. DPT Priority

For outgoing calls, where a DPT trunk is the terminator, the order of precedence from highest to lowest is as follows:

1. FRR and IRR (Flexible ReRoute and Immediate ReRoute)
2. DPT Priority
3. CANT (Cancel To)
4. SKIP
5. FRR and RRR (Flexible ReRoute and Regular ReRoute)
6. CANF (Cancel From)

Using the DPTCTRL commands to issue the DPT network management controls

As has already been mentioned, there are two DPT network management controls at the MAPCI;NWM;DPTCTRL MAPCI level:

- _DPTR_ (DPT Reservation)
- _MAXTID_ (DPT TID Limit Refinement)

At the DPTCTRL level there are three principal commands that you can use to manage the two DPT network management controls (see "GRPCRTL level after applying DPT Reservation" (page 90)):

- LIST_
- APPLY_
- Remove_

GRPCRTL level after applying DPT Reservation

```
DptCtrl                DptCtrl
 0 QUIT_                    DPTR        MaxTid
 2                           ON           OFF
 3
 4 LIST_
 5 APPLY_
 6 REMOVE_
 7 _DPTR_
 8 _MAXTID_
 9
10
11
12
13
14
15
16
17
18 PAGE
 C
```

Using the Apply command with the DPTR (DPT Reservation) control

The table below shows the syntax for the APPLY command used with the DPTR control. This control is only available when SOC CS2B0003 is on. Also see "GRPCRTL level after applying DPT Reservation" (page 90).

APPLY command with the DPT Reservation control

Command, control and variables	
APPLY DPTR thpct	
where	
<thpct>	is the reservation percentage (0 to 100). This is a mandatory parameter.

Using the Apply command with the MAXTID (DPT TID Limit Refinement) control

The following table shows the syntax for the APPLY command used with the MAXTID control. This control is only available when SOC CS2B0003 is on. Also see "GRPCRTL level after applying DPT Reservation" (page 90).

APPLY command with the DPT MAXTID control

Command, control and variables	
APPLY MAXTID maxtid	
where	
<maxtid>	is the maximum number of DPT TIDs available in the CS 2000 from the ATM backbone point of view. This is a mandatory parameter.

Using the LIST command with DPT network management controls

The LIST command allows you to list the DPT Reservation and maximum DPT TID (MAXTID) controls.

Using the REMOVE command with DPT network management controls

The REMOVE command allows you to remove the DPT Reservation control or the MAXTID control.

Using EADAS or Netminder

EADAS (Engineering and Administration Data Acquisition System) and Netminder are third-party alternatives to Nortel MAPCI for applying, removing and establishing settings for the Bandwidth Directionalization sub features. EADAS is based on Telecordia standard TR-746. Nortel has developed enhancements to TR-746 to support Bandwidth Directionalization. The enhancements to TR-746 fall into two categories:

- extensions generated specifically for Bandwidth Directionalization
- extensions shared with other Nortel network management features

For more information on the use of EADAS and Netminder with DPT network management control see the following Nortel functional descriptions:

- DPT Bandwidth Directionalization, 59028933
- Cancel To and Cancel From for DPTs, 59028903
- AT&T Specific Network Management Control Enhancements, 59028697.
- EADAS Support for DPT Bandwidth Directionalization, 59035929

Enhanced log information for SPM ATM and CARR logs

The Enhanced Logs feature provides additional text for the ATM (asynchronous transfer mode) and CARR (carrier) series logs (for example ATM300, and CARR310). The ATM, and CARR logs provide information on the four SPM (Spectrum peripheral module) network elements: IW SPM, DPT SPM, MG 4000 and legacy SPMs. The additional text, in the ATM and CARR logs, consists of the SPM location and SPM type.

For the ATM, and CARR logs, the location and type field only appears in the (I)SN05 software release and only if the office parameter SPM_ENHANCED_OUTPUT in table OFCVAR is set to ON. If the office parameter SPM_ENHANCED_OUTPUT is set to OFF, the location and type fields do not appear on the ATM and CARR logs. All ATM, and CARR logs created in (I)SN05 or later display the location and type fields by default.

For detailed information about setting office parameters SPM_ENHANCED_OUTPUT in table OFCVAR see, the following:

- MG 4000 Configuration Management, NN10098-511, or
- IW SPM-ATM Configuration Management, NN10099-511, or
- DPT SPM ATM Configuration Management, NN10102-511.

For additional information about the Enhanced Logs feature, see

- MG 4000 Fault Management, NN10076-911, or
- IW SPM-ATM Fault Management, NN10077-911, or
- DPT SPM-ATM Fault Management, NN10080-911

Provisioning ECAN for MG 4000 PTS trunks

To provision ECAN for MG 4000 PTS trunks, you must datafill option SPMECIDX (in table TRKSGRP) for each of the supported PTS trunk types. For a list of supported PTS trunk types see ‘ECAN support for legacy line to MG 4000 PTS trunks’.

The option SPMECIDX provides an index into table SPMECAN. The ECAN resource parameters are defined in table SPMECAN.

> ***Note:*** You can provision ECAN functionality in access mode, network mode, and back-to-back mode. However, Nortel recommends that you provision MG 4000 PTS trunks (that interwork with legacy lines) in access mode only.

For detailed procedural information about provisioning ECAN for MG 4000 PTS trunks, see the following:

- MG 4000 Configuration Management, NN10098-511
- ECAN support for legacy line to MG 4000 PTS trunks

Support for AB bit signaling on SPM ISUP trunks

There is support for AB signaling on ISUP trunks from an SPM to an external ECAN (echo canceler). Field ABCNTL in table TRKSGRP allows you to enable AB signaling. Normally, ISUP trunking does not use the bearer channel to transmit signaling information. If this feature is enabled, then the channel bandwidth for the ISUP trunk decreases from 64 kbps to 56 kbps for all trunks using the trunk subgroup.

For information about configuring this option in table TRKSGRP, see SPM Configuration Management, NN10097-511.

Random ascending or descending algorithm for CIC selection

Office parameter DPT_OPTIMIZED_CIC_SELECTION in table OFCVAR turns on or off the random ascending or descending algorithm for CIC selection. To minimize XA-Core blocking and glare, this algorithm combines the random CIC selection algorithm with the ascending or descending algorithm. The CIC range is divided into several CIC blocks. A block is selected randomly for each call. Within that block, the CIC is picked sequentially, ascending for one office, and descending for the network counterpart of that office.

The default value for this office parameter is set to YES for the XA-Core platform, and NO for the BRISK platform. Nortel recommends that you always use the default YES setting for the XA-Core platform and the default NO setting for the BRISK platform.

For information about provisioning office parameters in table OFCVAR, see Communication Server 2000 Configuration Management, NN10201-511.

CS 2000 Management Tools Configuration Procedures

System Audit

The following table lists the configuration procedures available for the system audit.

System Audit procedures

Procedure
"Configuring an Audit Schedule" (page 98)

QoS Collector Application (QCA)

The following table lists the configuration procedures available for the QCA.

QCA procedures

Procedure
"Modifying the QoS Collector Application" (page 102)

Line Maintenance Manager (LMM)

The following table lists the configuration procedures available for the LMM.

LMM procedures

Procedure
"Setting the CM CLLI on the LMM" (page 107)
"Reconnecting to LMM server" (page 109)
"Canceling pending CPD requests with LMM" (page 111)
"Setting the LMM auto refresh rate" (page 112)
"Disabling the LMM auto refresh" (page 114)
"Setting the LMM auto termination value" (page 115)
"Controlling the number of lines displayed by the LMM GUI" (page 117)
"Configuring a query for line gateways in a trouble state" (page 119)

Network Patch Manager (NPM)

The following table lists the configuration procedures available for the NPM.

NPM procedures

Procedure
"Configuring the Patching Server Element on an SPFS-Based Server" (page 122)
"Configuring NPM for Automatic Patch File Delivery" (page 126)

Server Platform Foundation Software (SPFS)

The following table lists the configuration procedures available for the SPFS.

SPFS procedures

Activity
"Setting the MSC Server 1000 CLLI on the Sun server" (page 167)
"Configuring a Timing Provider on an SPFS-Based Server" (page 184)
"Adding IP Addresses for FTP Proxy and Restricted Shell Access" (page 188)
"Configuring the Time Zone on an SPFS-Based Server" (page 191)
"Configuring Domain Name Service on an SPFS-Based Server" (page 194)
"Configuring Client/Server Ports on an SPFS-Based Server for Secure Firewall Communications" (page 210)
"Configuring a Virtual IP Address on an SPFS-Based Server" (page 215)
"Setting the CS 2000MSC Server 1000 IP Address on an SPFS-Based Server" (page 221)
"Creating or Modifying the Login Greeting Message on an SPFS-Based Server" (page 225)
"Setting a limit for login retries on an SSPFS-based server" (page 406)
"Configuring the Apache Web Server for HTTPS Proxy" (page 228)
"Configuring Automated Data Backups on an SPFS-Based Server" (page 231)
"Setting the Threshold for File Systems on an SSPFS-Based Server" (page 235)
"Configuring Dark Office Backups on an SPFS-Based Server" (page 409)
Unconfiguring DCE on an SSPFS-based server
Unconfiguring DCE on an SSPFS-based server
"Configuring the destination for SNMP traps" (page 237)
"Configuring Client Session Monitor" (page 172)

Succession Element and Sub-network Manager (SESM)

The following table lists the configuration procedures available for the SESM.

SESM procedures

Procedure
"Configuring the SESM Server Application" (page 241)

PM Poller

The following table lists the configuration procedures available for the PM Poller.

PM poller procedures

Procedure
" Setting up the PM Poller on an SSPFS-Based Server" (page 244)
"Configuring the SNMP Defaults for a Poller Profile and Setting the Polling Interval" (page 250)
"Viewing the Configuration Data for a Profile or Device" (page 255)
"Deleting a Device from a PM Poller Profile" (page 257)

OMPUSH

The following table lists the configuration procedures available for OMPUSH.

OMPUSH procedures

Procedure
"Creating an OMPUSH Session" (page 260)
"Activating or Deactivating an OMPUSH Session" (page 266)
"Modifying an OMPUSH Session" (page 271)
"Deleting an OMPUSH Session" (page 277)
"Querying OMPUSH Session Attributes" (page 282)

Trunk Maintenance Manager (TMM)

The following table lists the configuration procedures available for the TMM.

TMM procedures

Procedure
"Setting the CM CLLI on the TMM" (page 287)
"Setting the TMM Auto-Refresh Value" (page 289)

Procedure
"Turning TMM Auto-Refresh On or Off" (page 290)
"Setting the TMM Confirmation for the Busy Command" (page 291)

Configuring an Audit Schedule

Application

Use this procedure to schedule any of the following audits to occur at specified times:

- CS 2000 data audit
- Trunk audit
- V5.2 audit (only available in the international version of the software and not in the North American)

ATTENTION

Nortel recommends scheduling multiple audits to run at separate times. Scheduling multiple audits to run at the same time causes the audits to run sequentially (one after the other) and not at their scheduled time (the timestamp in the audit report indicates the actual time the audit started).

When the auto-apply task is enabled, do not run audits at the same time as the auto-apply task.

When scheduling audits please keep in mind that the system is locked and no provisioning changes are allowed when an audit is already running on a node.

For more information refer to procedure "Performing an audit" in *ATM/IP Solution-level Fault Management* (NN10408-900).

Prerequisites

You must be logged in to the CS2000 Management Tools application GUI. For more information refer to procedure "Launching the CS2000 Management Tools and NPM client applications" in *ATM/IP Security and Administration* (NN10402-600).

You must be assigned to user group "mgcadm" to configure an audit schedule. For more information refer to procedure "Setting up local user accounts on an SPFS-based server" in *ATM/IP Security and Administration* (NN10402-600).

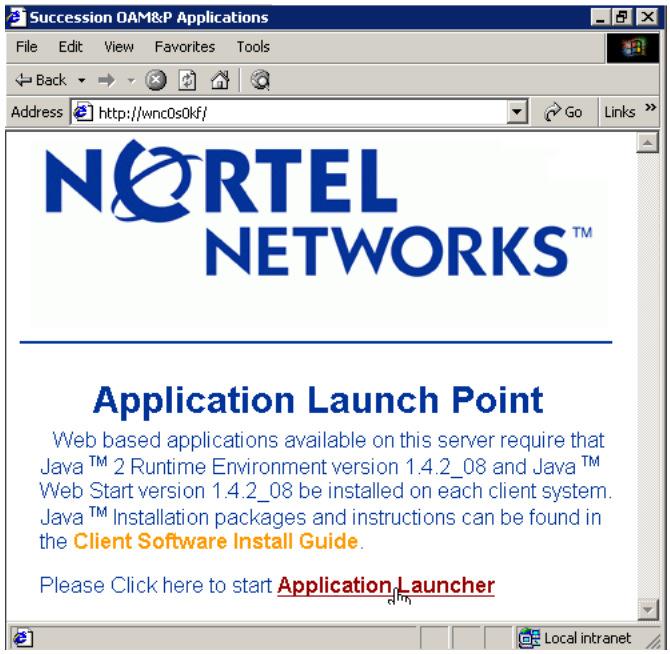
Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation:
1	Launch the CS2000 Management Tools GUI.

Refer to the "Launch applications from a web browser" (page 294) procedure for more information.

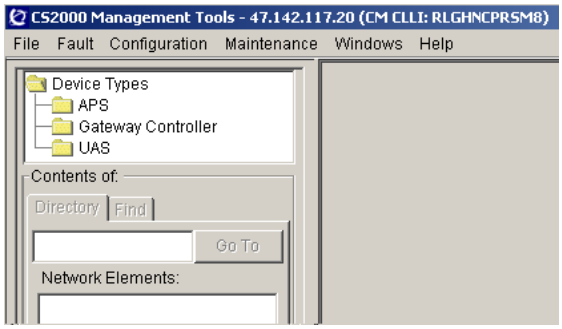
System response:



2 Click on **Application Launcher** to access the available web-based applications.

3 Click on **CS 2000 Management Tools**.

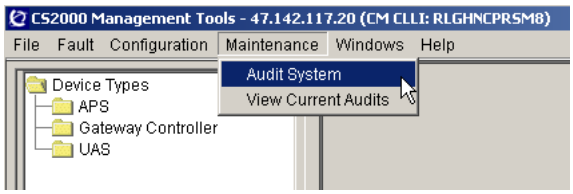
System response:



Using the CMT GUI:

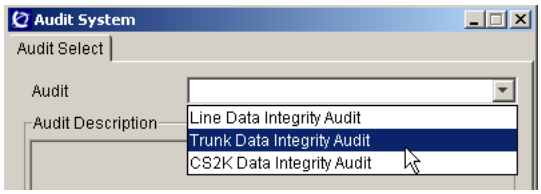
4 On the **Maintenance** menu, click **Audit** System.

System response:



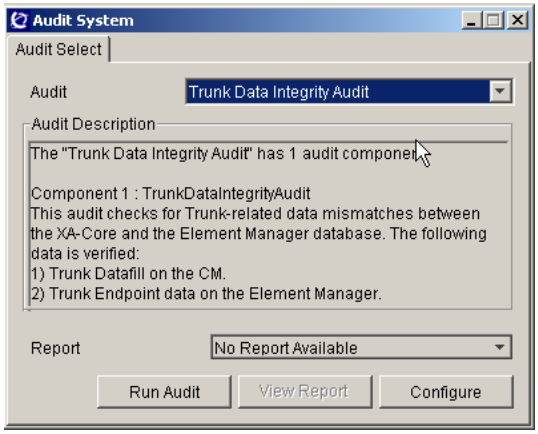
5 In the **Audit** list, select the audit type of your choice.

System response:



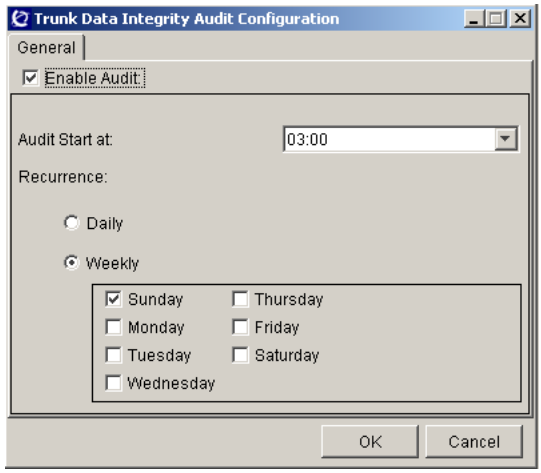
6 Click **Configure**.

System response:



7 Click the **Enable Audit** check box, and schedule the desired start time and recurrence of the audit .

System response:



8 Click **OK**

—End—

Modifying the QoS Collector Application

Application

Use this procedure to modify the configuration details for the QoS Collector Application (QCA) on the SPFS-based server.

QCA is applicable to AAL2 solutions starting with SN09U.

In a two-server configuration, you must perform this procedure on both the active and inactive servers.

Prerequisites

You need the root user ID and password to log in to the server where the QCA software resides.

Action

Step	Action

At your workstation

1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the hostname or IP address of the server

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

d. When prompted, enter the root password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the hostname or IP address of the server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

4 Edit the QCA properties file by typing

```
# vi /opt/nortel/qca/properties/qca.properties
```

and pressing the Enter key.

Example response

```
# QCA Properties file
# The QCA will have to be restarted for changes in the properties
# file to be reflected in the application's operation.

# port name to start application on.
# Default is 20000
portNumber=20001

# The maximum size of a file, in MBytes, before it is closed
# Range is 1 to 100
# Default is 1
MaxFileSize=10

# The maximum time, in minutes, a file can be open before it is
# closed
# Range is 1 to 240
# Default is 15
MaxFileTime=10

# How long, in days, the files are kept before deleting
# Range 1 to 30.
# Default is 5
RetainFileTime=3

# Hour of the day that the directory structure is recycled
# Range 0 (12:00 AM) to 23 (11:00 PM) Do NOT specify minutes.
# Default is 0
recycleToD=14

# File Extension used in the QCA output file name.
# Default is xml
fileExt=xml

# Node name to be used in the QCA output file name.
# Default in QCA.
nodeName=CS2K1

# 'true' or 'false' value indicating whether the output file
# should be compressed when closed. Default is true.
closedFileCompression=true

# 'true' or 'false' value indicating whether the file should be
# compressed at the first directory recycle
# Note: If closedFileCompression is true the value of the
# oldFileCompression property is negated as the files will have
# already been compressed. Default is true.
oldFileCompression=true
```

5 Modify the desired properties. The properties you can modify are described in the table below.

Name	Description	Range	Default
Port number	The port number the QCA accepts connections on. A range of port numbers is provided for flexibility. The main use is for upgrade purposes where two QCA instances may be running on a single host. Multiple QCA instances, and therefore port numbers, should not be used to segregate QCA traffic	20000 to 20004	20000

Name	Description	Range	Default
MaxFileSize	The maximum size an output file can be added, before it is closed. It is recommended to set this value to 10 MBytes. This reduces the number of file rotation during high traffic period.	1 to 100 MBytes	1
MaxFileTime	The maximum time the output file can be open before it is closed.	1 to 240 minutes	15
RetainFileTime	The length of time the output files should be retained.	1 to 30 days	5
RecycleToD	The hour in the day the directories are to be recycled. It is recommended to set this value to a time of day when the traffic is low, such as 2.	0 to 23 hours	0
FileExt	The output file extension.	string	xml
NodeName	The node name to be used in the output files.	string	QCA
ClosedFileCompression	The file should be compressed when closed and moved to today. File compression may be required as there is limited disk space to store QCA IPDRs.	true or false	true
OldFileCompression	The files should be compressed at the first directory recycle. File compression may be required as there is limited disk space to store QCA IPDRs. If ClosedFileCompression is true, the value of the *OldFileCompression* is negated as the files will have already been compressed.	true or false	true

6 Exit the edit session and save the changes by typing

```
zz
```

and pressing the Enter key.

7 Stop and restart the QCA for the changes in the QCA properties file to take place. If required, refer to procedure "Starting and stopping the QoS Collector Application" in ATM/IP *Security and Administration*, NN1402-600.

8 In a two-server configuration, repeat steps step 1 through step 7 on the other server.

You have completed this procedure.

—End—

Setting the CM CLLI on the LMM

Application

Use this procedure to set the CLLI of the Communication Server 2000 on the Line Maintenance Manager (LMM) by setting the IP address of the core manager (SDM/CBM), which automatically retrieves the associated CM CLLI. If there are no communication problems with the Communication Server 2000, the IP address of the core manager (SDM/CBM) and the associated CM CLLI are automatically set during the LMM GUI startup.

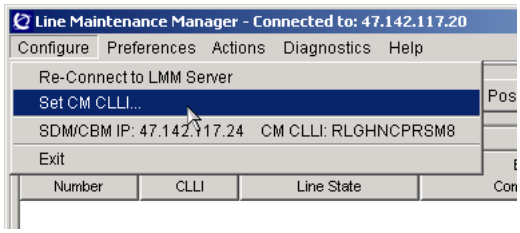
Prerequisites

You need the IP address of the core manager (SDM/CBM).

Action

Perform the following steps to complete this procedure.

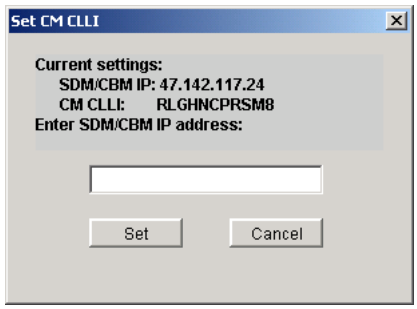
Step	Action
	At your workstation
1	Access the LMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM client applications" (page 292) in this document, if required.
	At the LMM GUI
2	On the Configure menu, click Set CM CLLI.



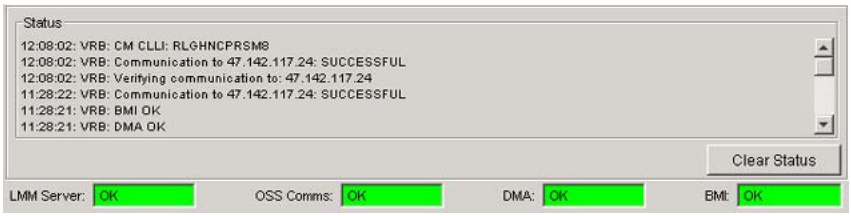
The CM CLLI window opens.

3 Enter the IP address for the core manager (SDM/CBM), and click **Set**.

The CM CLLI associated with the IP address for the core manager (SDM/CBM) is automatically retrieved.



4 Verify that the connection completes by reviewing the messages in the status area, and ensuring the status fields read "**OK**".



If the connection fails, a window opens to indicate the error.

5 You have completed this procedure.

—End—

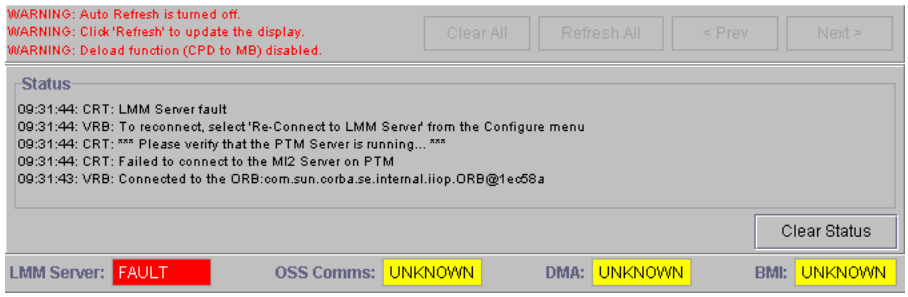
Reconnecting to LMM server

Application

Use this procedure to reconnect to the LMM server.

A lost connection is indicated by a Red LMM status button. If a server fault occurs during GUI startup (a case when the server where the CS 2000 Management Tools reside is down), the CS CLLI will not be set automatically. The CLLI field at the top right corner of the GUI will be blank.

Example of lost connection



Prerequisites

The server where the CS 2000 Management Tools reside must be running and the applications in ready status.

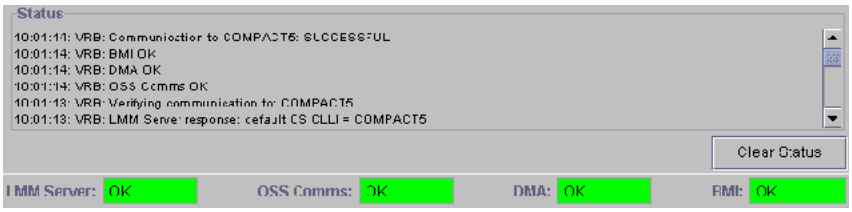
Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the LMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM client applications" (page 292) in this document, if required.
	At the LMM GUI
2	On the **Configure** menu, click **Re-Connect to LMM Server** to establish a connection with the LMM server again.

If the server fault occurred during GUI startup, performing this step will automatically connect to the default CLLI. Once connected, the default CLLI will show up on the top right corner of the GUI.

3 Check the status of the **LMM Server** box, which is green when the connection is re-established, as shown below.



4 You have completed this procedure.

—End—

Canceling pending CPD requests with LMM

Application

Use this procedure to cancel pending CPD requests. This option is effective only when the Auto Termination timer runs out.

Prerequisites

Auto Termination must be enabled.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the LMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM client applications" (page 292) in this document, if required.
	At the LMM GUI
2	On the **Preferences** menu, click **Auto Termination** then **Cancel pending CPD requests**. 
3	You have completed this procedure.

—End—

Setting the LMM auto refresh rate

Application

Use this procedure to set the auto refresh rate.

Prerequisites

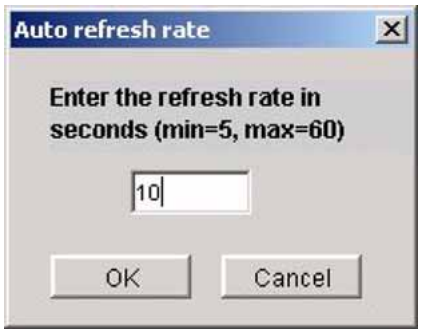
None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the LMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM client applications" (page 292) in this document, if required.
	At the LMM GUI
2	On the **Preferences** menu, click **Auto Refresh** then **Set Auto Refresh value** to open the Auto refresh rate window.

3	Enter the new value and click **OK**.
	The minimum is 5 seconds, and the maximum is 60 seconds.



4 You have completed this procedure.

—End—

Disabling the LMM auto refresh

Application

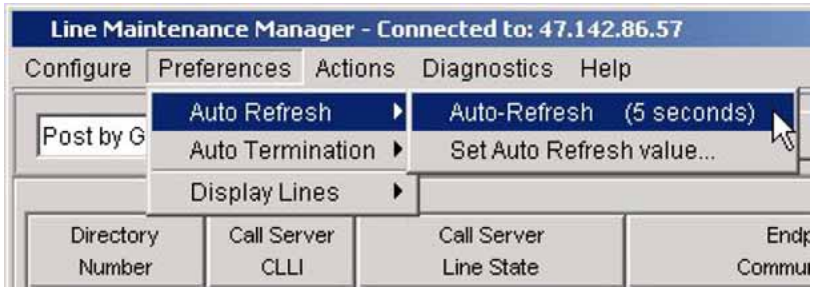
Use this procedure to disable the auto refresh.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the LMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM client applications" (page 292) in this document, if required.
	At the LMM GUI
2	On the **Preferences** menu, click **Auto Refresh** then **Auto-Refresh (value)** to disable automatic refresh of the display. 
3	Verify that automatic refresh is disabled by viewing the Status window and the warning messages. 
4	You have completed this procedure.

—End—

Setting the LMM auto termination value

Application

An auto termination timer is started when there is no activity on the LMM GUI. When the timer expires, lines are no longer refreshed and pending CPD requests are cancelled. Use this procedure to set the auto termination value.

Prerequisites

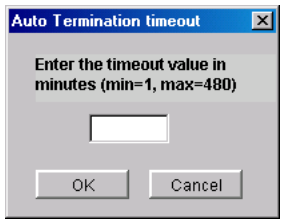
None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the LMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM client applications" (page 292) in this document, if required.
	At the LMM GUI
2	On the **Preferences** menu, click **Auto Termination** then **Set Auto Termination value...**.

	The **Auto Termination timeout** window opens.
3	Enter a new value for the timeout and click **OK.**
	The minimum is 1 minutes, and the maximum is 480 minutes.



4 You have completed this procedure.

—End—

Controlling the number of lines displayed by the LMM GUI

Application

The LMM allows you to control the number of lines that appear in the LMM GUI. You can choose from 6, 24, or 31 lines. With auto-refresh enabled, only the lines posted and visible at the GUI will be refreshed As the user navigates using the "Next" and "Prev" buttons, the corresponding posted visible set will be refreshed. Use this procedure to modify the number of displayed lines in the LMM GUI.

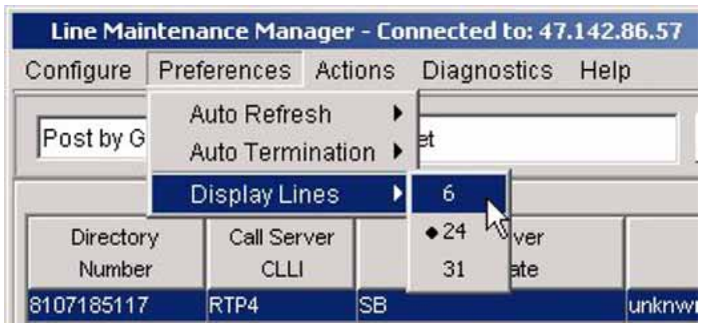
Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the LMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM client applications" (page 292) in this document, if required.
	At the LMM GUI
2	On the **Preferences** menu, click **Display Lines** then select the number of lines to display (6, 24, or 31).



If the number of displayed lines on GUI is larger than the value you chose in the previous step, the "Next" and "Prev" buttons will be automatically enabled, if they are not already enabled. Use the "Next" and "Prev" buttons to verify that the new display settings become effective.

If the number of displayed lines on GUI is less than the value you chose in the previous step, the "Next" and "Prev" buttons will be enabled when the set value is reached.

3 You have completed this procedure.

—End—

Configuring a query for line gateways in a trouble state

Application

This procedure describes how to configure a query for line gateways in a trouble state.

Use this procedure to have queries run on a regular basis and generate reports of line gateways in a trouble state. To manually perform a query and view reports, refer to procedure "Performing a query on line gateways in trouble state and viewing reports" in the ATM/IP Solution-level Fault Management document, NN10408-900.

Prerequisites

The LMM Server status field must be Green (OK) in order to configure a query.

Action

Perform the following steps to complete this procedure.

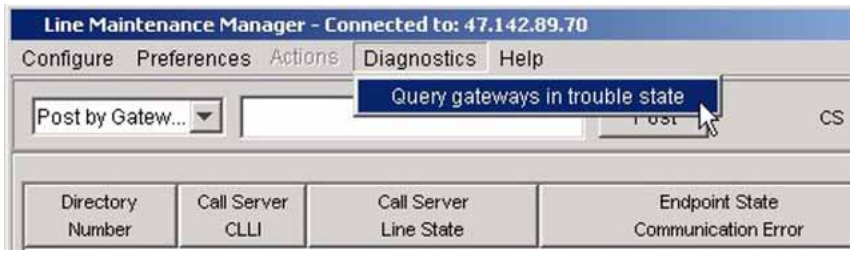
Step	Action

At your workstation

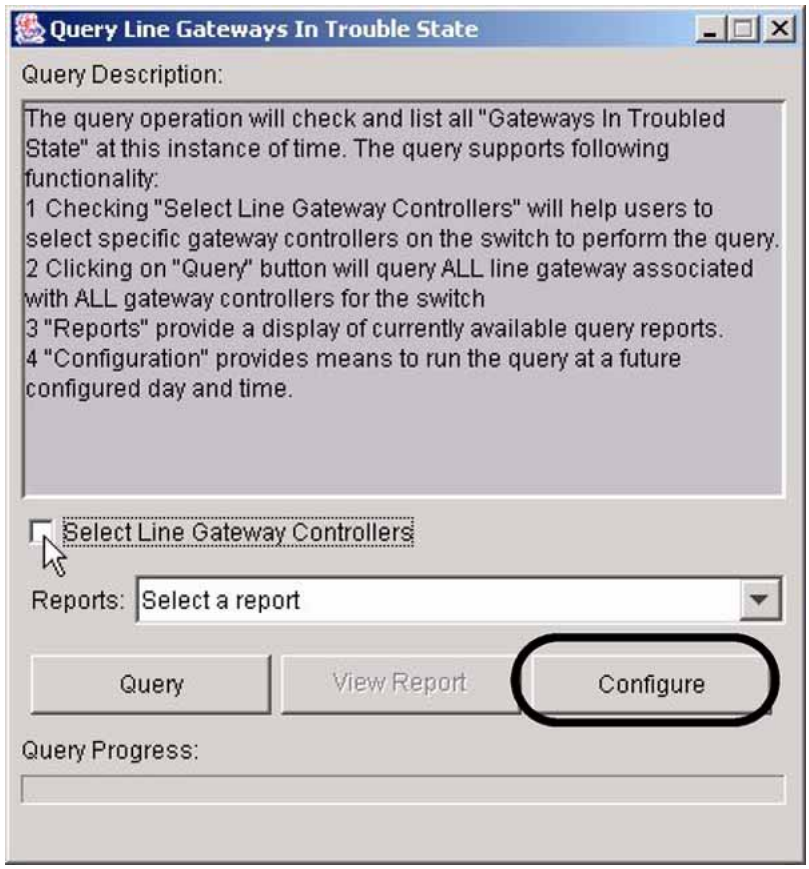
1 Access the LMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM client applications" (page 292) in this document, if required.

At the LMM GUI

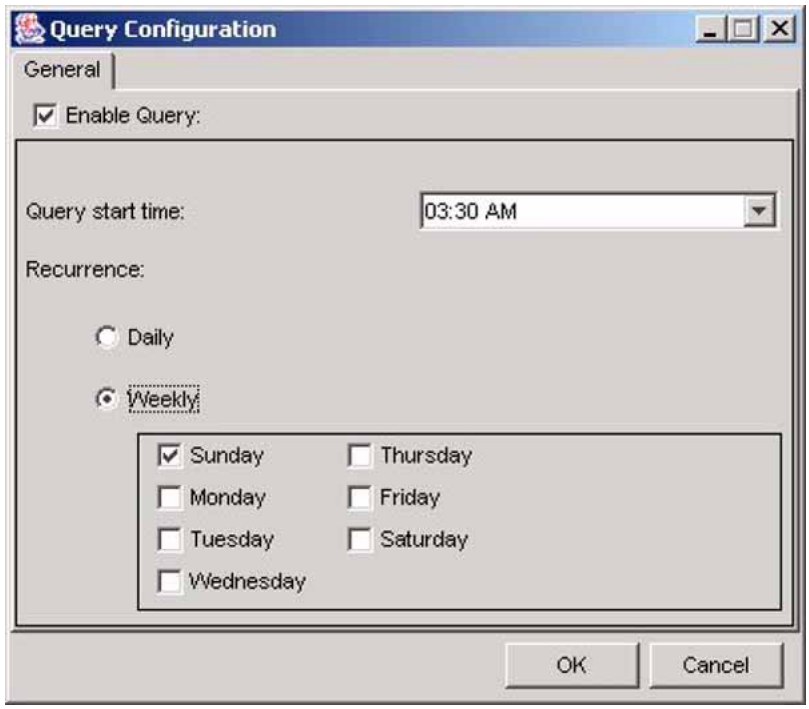
2 On the **Diagnostics** menu, click **Query gateways in trouble state**.



3 Click **Configure**.



4 Click the **Enable Query** check box, then click **Daily**, or **Weekly** with the day of the week, set the time, and click **OK**.



5 You have completed this procedure.

—End—

Configuring the Patching Server Element on an SPFS-Based Server

Application

Use this procedure to configure the Patching Server Element (PSE) on a Server Platform Foundation Software (SPFS) based server. Configuring the PSE involves specifying the location of the NPM server application so the PSE can communicate with the NPM server application.

ATTENTION

Only perform this procedure after an upgrade if a new SPFS-based server is added to the network with the PSE on it, or the NPM is moved to another SPFS-based server.

Prerequisites

The SPFS upgrade is complete.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you are configuring PSE
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su -` and pressing the Enter key.
4	When prompted, enter the root password.
5	Access the command line interface by typing `# cli` and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - DCE Configuration
  4 - OAMP Application Configuration
  5 - CORBA Configuration
  6 - IP Configuration
  7 - DNS Configuration
  8 - Syslog Configuration
  9 - Remote Backup Configuration
 10 - Database Configuration
 11 - NFS Configuration
 12 - Bootp Configuration
 13 - Restricted Shell Configuration
 14 - Security Services Configuration
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the number next to the "Succession Element Configuration" option in the menu.

Example response

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
  9 - OMPUSH Application Configuration
 10 - RESMON Application Configuration
X - exit
```

```
select -
```

8 Enter the number next to the “PSE Application Configuration” option in the menu.

Example response

```
PSE Application Configuration
1 - View_NPM_host_or_ip <View NPM hostname/ip address
location>
2 - Update_NPM_host_or_ip <Update NPM hostname/ip
address location>
3 - Create_PSE_Database (Initialize or re-unitize the
PSE database)
4 - Update_Patch_Corba_Mirroring (Mirror the NPM patch
CORBA name reference)
5 - Remove_Patch_Corba_Mirroring (Remove the NPM patch
CORBA name mirror re...)
6 - Unconfigure_PSE (Remove PSE as a system process.)
X - exit
select -
```

9 Enter the number next to the "Update_NPM_host_or_ip" option in the menu.

Example Response:

```
Enter the hostname (preferred) or the IP address
of the SPFS-based machine that contains the Network
Patch Manger (NPM) server.  If this machine is part
of a duplex/clustered configuration, please enter the
cluster hostname or IP address.
Enter NPM hostname or IP address:
```

10 When prompted, enter the host name or IP address of the SPFS-based server where the NPM resides.

If the NPM is installed on a server in a cluster (two-server configuration), enter the host name or IP address of the cluster.

Example response:

```
Checking communication to 124.12.54.3.  This may take
up to ten seconds.
Is host/ip 124.12.54.3 acceptable?  [y] [y,n,?,q]
```

11 When prompted, confirm the host name or IP address by typing

y

and pressing the Enter key.

Example response:

```
==="Update_NPM_host_or_ip" completed successfully
```

12 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Configuring NPM for automatic patch file delivery

Application

Use this procedure to configure the Network Patch Manager (NPM) for automatic patch file delivery, which consists of configuring the Patch File Receipt System (PFRS). You can configure PFRS using one of the following two NPM interfaces:

- "Using the NPM CLUI" (page 126)
- "Configure the NPM GUI" (page 129)

Once the PFRS is configured, patches are automatically delivered to the NPM database and retrieved for processing on a daily basis.

An option is provided to delete patch files from the drop-off server after they have been retrieved.

Prerequisites

To configure the PFRS, you need the following information:

- the hostname or IP address of the patch file drop-off server
- the user ID and password to connect to the patch file drop-off server

Action

Perform the following steps to complete this procedure.

Using the NPM CLUI

Step	Action
	At your workstation
1	Access the NPM CLUI. `# npm` When prompted, enter your **`username`** and **`password`**. If required, refer to the "Accessing the Network Patch Manager CLUI" (page 303) procedure for more information.
	At the NPM CLUI
2	Configure the PFRS by typing **`npm> setpfrs <drop-off server> <userID> <delete patches>`** and pressing the Enter key.

where

drop-off server is the IP address or hostname of the drop-off server where patch files are to be delivered
userID is the user ID that will be used to connect to the drop-off server
delete patches is either Y or N to indicate whether you want the patch files to be deleted from the drop-off server after they have been retrieved

The user ID must have read, write, and overwrite privileges in the FTP user's default directory on this server.

Example response:

```
Enter password for drop box:
```

3 When prompted, enter the password associated with the user ID that will be used to connect to the drop-off server.

Example response:

```
WARNING: You are about to set/reset the Patch File
Retrieval System settings.  If these values are
incorrect they may interfere with automatic delivery of
patches to this site.
Do you wish to continue Yes (Y) or N (N)?
```

4 When prompted, confirm you want to continue if acceptable by typing

y

and pressing the Enter key.

5 Review the PFRS settings if required by typing

npm> viewpfrs

and pressing the Enter key.

6 Enable the GENREPORT plan by typing

npm> enableplan genreport

and pressing the Enter key.

Ensure that the response is:

```
Plan enabled successfully.
```

If you receive any other response, contact your next level of support.

7 Check the plan status for genreport by typing

```
npm> vplan genreport
```

and pressing the Enter key.

The value for **Enabled** must be set to **Y**.

Expected response:

```
Name            : GENREPORT
Description     : PFRS Inform list report generation
Status          : SCHED
Enabled         : Y
Frequency       : Daily
Execute Time    : Wed Jan 25 12:00:00 GMT-03:00 2006
Max Execut Time:  No_Limit
Tasks/Reports   : [TASK:PFRSGENREPORT]
System Defined :  true
```

If genreport is not enabled, contact your next level of support.

8 Enable the GETPATCH plan by typing

```
npm> enableplan getpatch
```

and pressing the Enter key.

Ensure that the response is:

```
Plan enabled successfully.
```

If you receive any other response, contact your next level of support.

9 Check the plan status for getpatch by typing

```
npm> vplan getpatch
```

and pressing the Enter key.

The value for **Enabled** must be set to **Y**.

Expected response:

```
Name            : GETPATCH
Description     : Patch file retrieval
Status          : SCHED
Enabled         : Y
Frequency       : Daily
Execute Time    : Thu Jan 26 01:00:00 GMT-03:00 2006
Max Execut Time:  No_Limit
Tasks/Reports   : [TASK:PFRSGETPATCH]
System Defined :  true
```

If getpatch is not enabled, contact your next level of support.

10 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Configure the NPM GUI

Step	Action

At your workstation

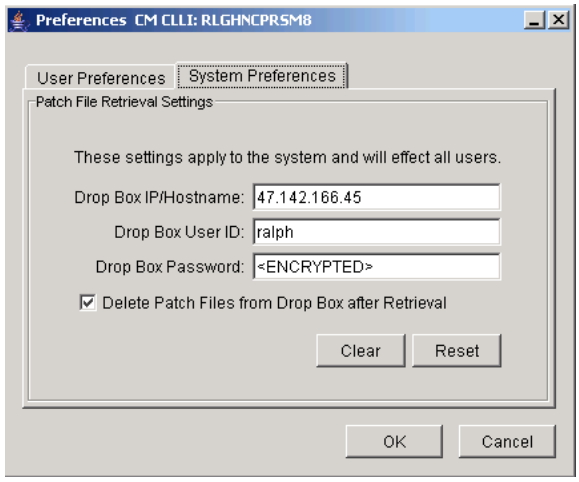
1 Access the NPM GUI. If required, refer to procedure "Launching CS 2000 Management Tools and NPM Client Applications" (page 292).

At the NPM GUI

2 On the Edit menu, click **Preferences...**.

The Preferences window is displayed.

3 Click the **System Preferences** tab.



4 In the Drop Box IP/Hostname field, enter the host name or IP address of the drop-off server where patch files are to be delivered.

5 In the Drop Box User ID field, enter the user ID that will be used to connect to the drop-off server.

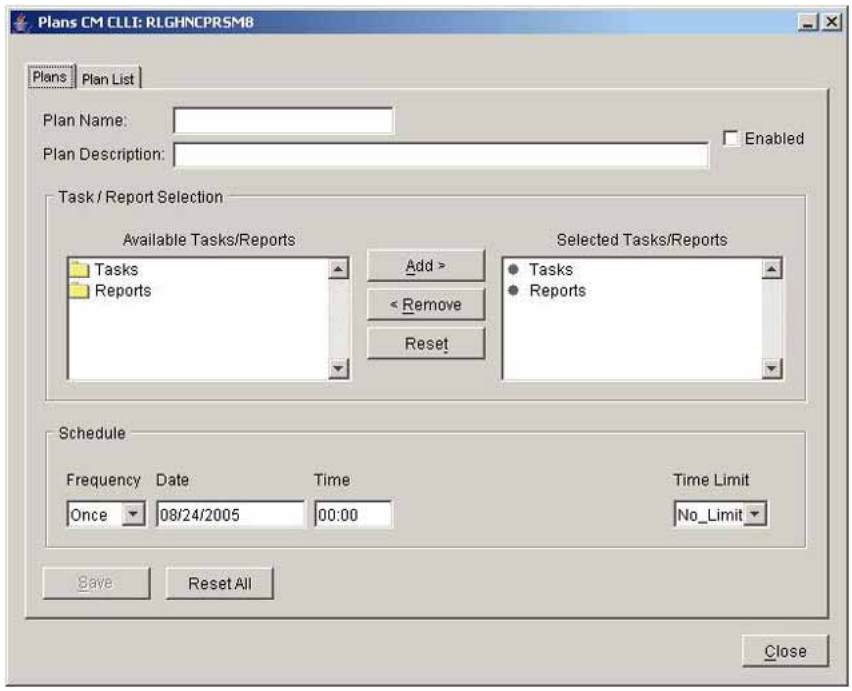
The user ID must have read, write, and overwrite privileges in the FTP default directory for the user on this server.

6 In the Drop Box Password field, enter the password associated with the user ID that will be used to connect to the drop-off server.

7 Click the Delete Patch Files from Drop Box after Retrieval box if you want the patch files to be deleted from the drop-off server after they have been retrieved, otherwise, leave it blank.

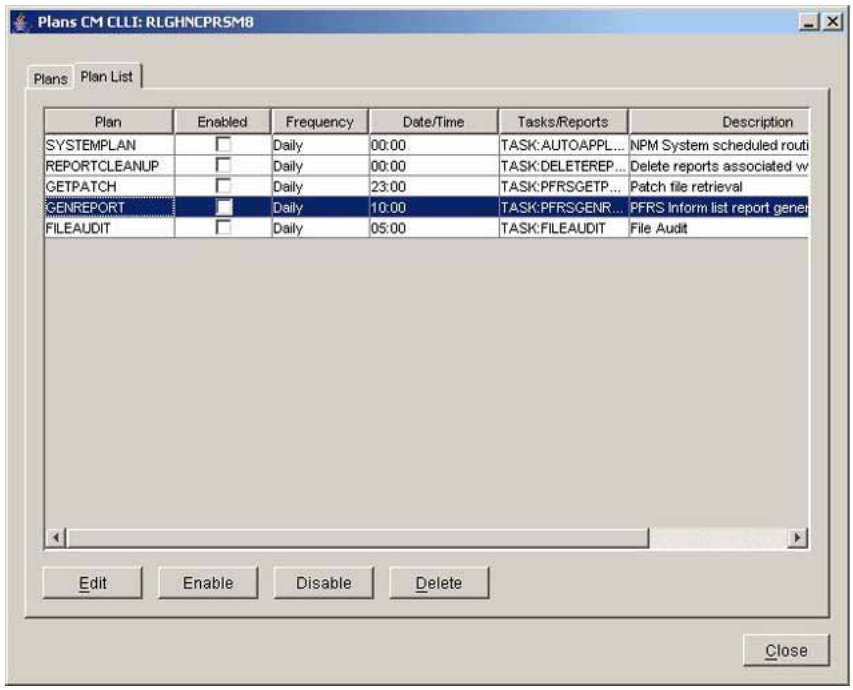
8 Click **OK** to complete the PFRS configuration.

9 On the System menu, select **Plans....**



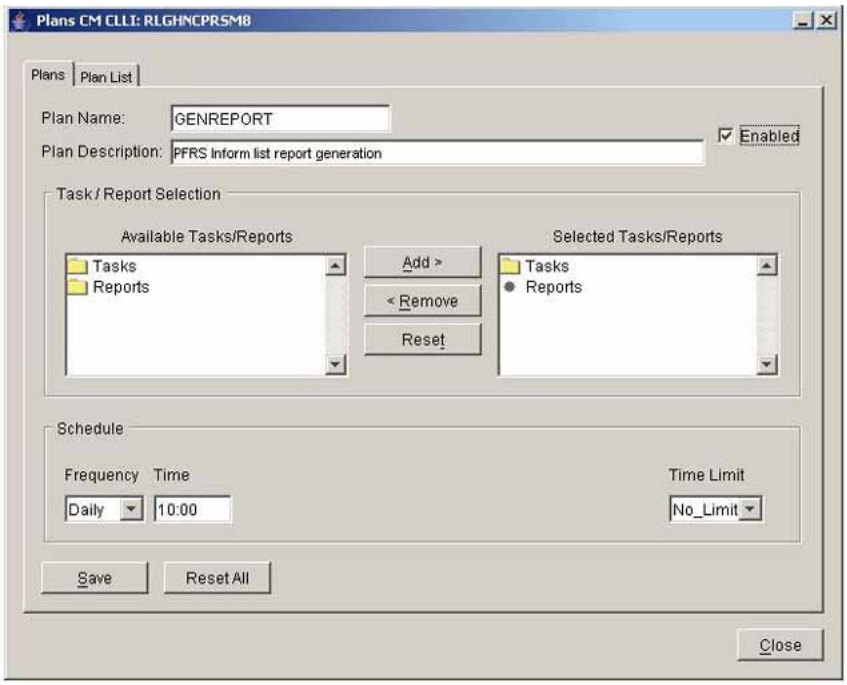
The Plans window is displayed.

10 Click **Plan List** tab.



The Plan List window is displayed.

11 Select the GENREPORT task and click **Edit**.



12 Click the Enabled checkbox, verify the schedule for the plan, and then click **Save**.

13 Repeat step 10 through to step 12 but select the GETPATCH task this time.

14 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

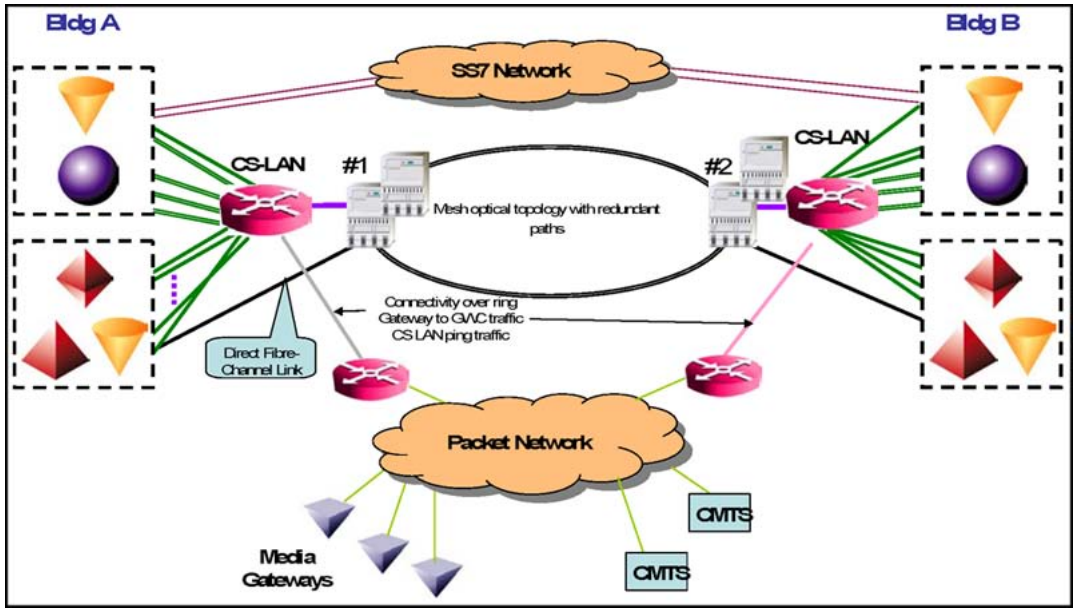
—End—

Geographic survivability

Geographic survivability is the distribution of components across a geographic area to ensure services continue in the event of a disaster. A disaster can include fire, flood, tropical storm, or act of terrorism. Geographic survivability includes the distribution of hardware across multiple locations.

The following figure shows the topology for CS 2000 - Compact support for geographic survivability.

Geographic survivability topology



The CS 2000 - Compact supports geographic survivability through the fail-over and sparing functionality of individual nodes. The configuration for the CS 2000 Management Tools (CMT) and Integrated Element Management System (IEMS) servers and the Core and Billing Manager (CBM) 850 is as follows:

- Site A is configured with the CMT and IEMS high-availability (HA) server pairs
- Site B is configured with the CBM 850 HA server pairs (referred to as CBM 850 HA u0 and u1)
- Site A is configured with an additional CBM in to be used in the event of disaster at Site B (referred to as CBM 850 standby u0)
- Site B is configured with an additional server for the CMT and IEMS in the event of disaster at Site A

For a communication server, geographic survivability requires that redundant components (other than OAM components) must reside at different sites (referred to as Site A and Site B).

For OAM components, the Automatic Backup and Accelerated restore feature (known as remote backup) remotely backs up all data on the target unit. This provides a standby backup system ready to provide service should the primary system or cluster be unavailable for an extended period of time (for example, catastrophic site loss). The remote backup can assume the identity of the target system with data and files accurate to the last sync and will be located at a different site from the target system. Remote backup performs the backup via TCP/IP connection and stores an exact copy on the standby server which can be quickly and remotely activated. This remote backup copies all files in each file system marked for backup using the same behavior as a full system backup.

A remote backup configuration tool is provided to set the necessary parameters and schedule for automatic backup which can be scheduled to automatically occur from once a day to four times per day. This tool also provides a facility for manually initiating a backup and monitoring its progress. The standby server has an identical copy of files from the last backup, so it can become the primary system via changing the boot pointer and rebooting. When the primary site is again available, the remote backup feature can be reused to transfer current system configuration back to the primary site and system.

ATTENTION

If configuration, provisioning, patching or other “write”-type operations occurred since the last remote backup, the remote backup system can be out of sync compared to the data in network elements and/or the primary OAM system

When initiating a switchover to a remote backup OAM server, do not execute configuration, provisioning, patching or other “write”-type operations through the remote backup OAM system until out-of-sync conditions are cleared.

Take actions before initiating the switchover to a remote backup OAM server (that is, response to a geographic or other prolonged outage of the primary OAM system) to halt or prevent “write”-type operations by OSSs and operations personnel until an in-sync status is achieved.

If a site outage is imminent (for example, threatening severe weather conditions), consider precautionary preparations to discontinue “write”-type operations. Make manual backups to the remote backup OAM servers to ensure data synchronization of the remote OAM server before performing a switchover.

Apply similar precautions when initiating a recovery back to the primary cluster. In this more controlled scenario, “write”-type operations must be discontinued before initiating this procedure

Site failure in a geographic survivable configuration

There are two scenarios for recovery of a geographic survivable network configuration:

- "Site A failure" (page 135)
- "Site B failure" (page 135)

Site A failure

A loss of Site A would include a loss of the CS 2000 Management Tools and IEMS servers. This loss would result in the following losses of functionality:

- all OAM&P functions of the CS 2000 Management Tools and Integrate EMS, including GUI access, element management, alarms, and non-Core logs
- access to the CS 2000-Compact Core Manager on the CBM 850

The responsive action in this scenario is to initiate a switchover to the standby CMT and IEMS servers at Site B.

Site B failure

A loss of Site B would include a loss of the CBM 850 servers. This loss would result in the following losses of functionality:

- transfer of billing records from the Core to the CBM 850
- billing records resident in the CBM 850 that had not been offloaded to an OSS
- ability to receive scheduled Core OMs and logs (resulting in them being discarded)
- access to the CS 2000-Compact Core Manager
- backup bootp load repository

The responsive action in this scenario is to initiate a switchover to the standby CMT and IEMS servers at Site A.

Fresh pre-install of CBM 850 cold u0

To reduce the duration of downtime during an outage, it is recommended that the CBM 850 cold u0 be pre-installed. Contact your next level of support for this task.

Maintaining sites in a geographic survivable configuration

The following procedures contain information for OA&M auto backup and accelerated restore capability:

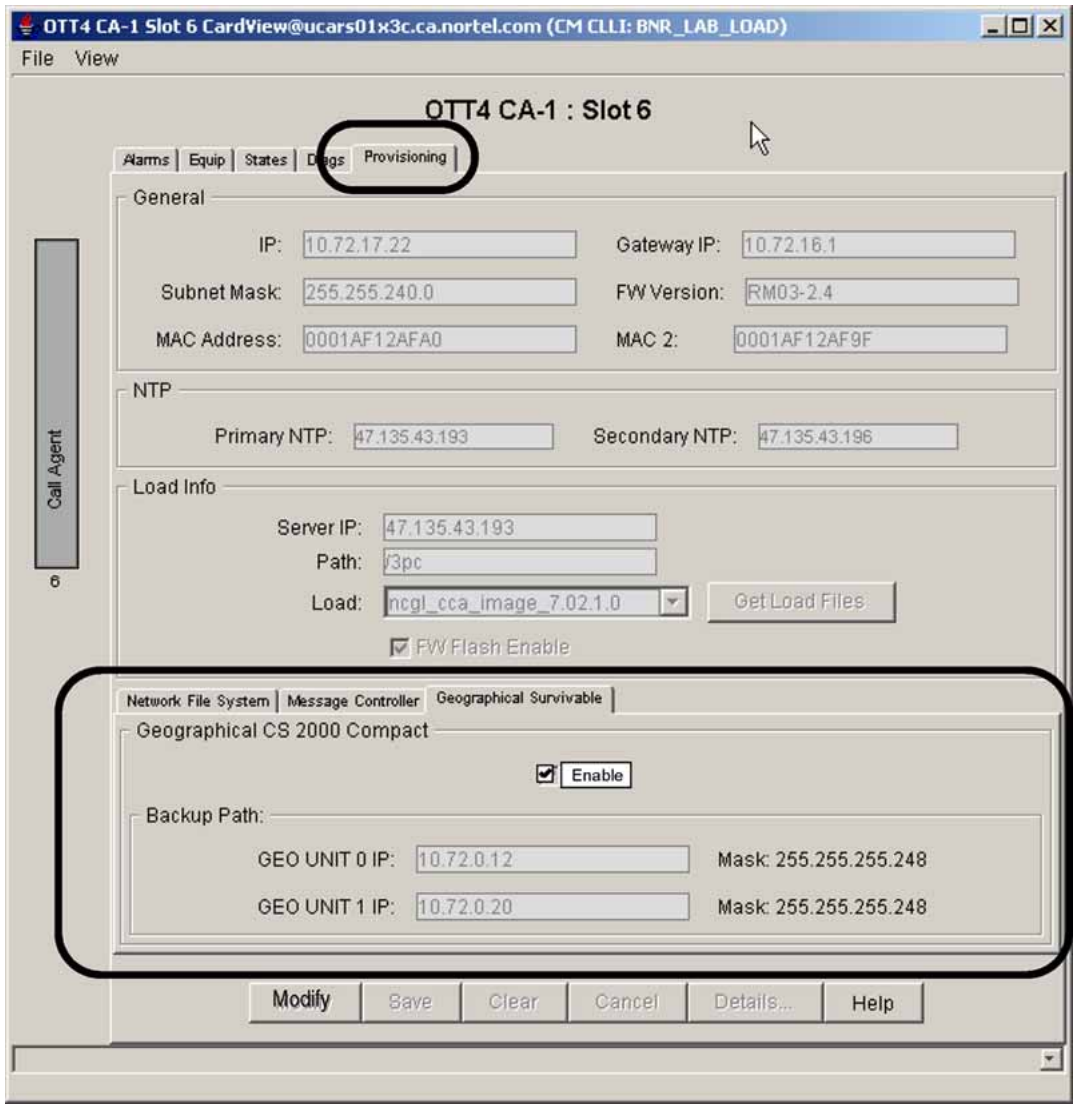
- "Installing the remote backup server" (page 148)
- "Scheduling automatic backups on the remote server" (page 155)

- "Viewing configuration information for remote server backups" (page 158)
- "Performing a manual backup of the target server" (page 160)
- "Viewing logs from a remote backup" (page 162)
- "Initiating a recovery back to the cluster" (page 163)
- "Initiating a switch over to the remote backup server" (page 165)

Geographical Survivability impacts to CS 2000-Compact

The Geographic Survivability feature allows services to continue in the event of a natural or man-made disaster. A sub-panel to the Call Agent Card View Provisioning panel (tab) allows you to enable or disable the feature. The following figure shows an example configuration with Geographic Survivability enabled.

Call Agent Card View Provisioning panel: Geographic Survivability enabled



Failure scenarios

The following table provides summaries of system responses during various failure scenarios when Geographical Survivability is enabled. The scenarios assume redundant configurations are located in two separate sites.

System response summaries

Scenario	Response
Ethernet Routing Switch 8600 failure at one site	***At the site with the failed routing switch:*** • All nodes lose mate connectivity via Ethernet. • The Call Agent loses WAN backup connectivity.

Scenario	Response
	• FC or GigE call data sync link remains up until the Call Agent resets. • The Call Agent resets itself approximately 1 minute after losing network connectivity and tries to boot from the network. The Call Agent keeps trying to boot until the network recovers and the boot is successful. • The Call Agent detects IST loss, but cannot disable ERS 8600 routing. • USPc detects isolation and takes down SS7 links at the site with the 8600 failure. ***At the site with the in-service routing switch:*** • The Call Agent remains active if it is already active. No outage occurs. If the Call Agent was not active, it takes activity within 2 seconds. • SOS goes through a warm or restart (approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor and 30 seconds for the NTRX51GZ card with the MPCN765 processor). • Other nodes go active and follow the Call Agent example after losing mate connectivity. • If Site B has the in-service router, the standby CMT server must be brought into service. Consider using this option based on the estimated time to recover the fault or failure of the CS LAN versus time and effort to bring up the cold standby system and recover the high availability (HA) pair afterward. For example, if the time to recover the CS LAN is estimated to be 10 hours, it might not be worth activating the cold standby CMT server or CBM. • If Site A has the in-service router, the standby CBM must be brought into service. See procedure *Initiating a switchover to the remote backup server.*

Scenario	Response
Optical frame failure at one site	***At the site with the failed optical frame:*** • All nodes lose mate connectivity via Ethernet. • Call Agent FC or GigE call data link connectivity is lost. • WAN backup remains up. • The active Call Agent remains active, but without sync. No outage occurs *The remainder of this scenario assumes the active Call Agent is at this site*. • If not already active, other nodes co-located with the active Call Agent are expected to go active after losing mate connectivity. If not already inactive, other nodes co-located with the inactive Call Agent are expected to go inactive after losing mate connectivity. (Done without mate connectivity.) ***At the site with the in-service optical frame:*** • The inactive Call Agent detects IST loss. For an ERS 8600 CS LAN using OSPF, the Call Agent disables OSPF. For an ERS 8600 CS LAN using Border Gateway Protocol (BGP) or for a third-party CS LAN using either OSPF or BGP, execute manual action to disable routing at the site with the inactive Call Agent. See section *Disabling Border Gateway Protocol (BGP)* for instructions of disabling and enabling BGP. • Other nodes go inactive and follow the Call Agent example after losing mate connectivity. (Done without mate connectivity.) • USPc detects isolation from the active Call Agent, and takes down SS7 links at the site with the inactive USP. • If Site B has the failed optical frame, the standby CBM must be brought into service at Site A. • If Site A has the failed optical frame, the standby CMT must be brought into service at Site B. Consider using this option based on the estimated time to recover the fault or failure of the CS LAN versus time and effort to bring up the standby system and recover the HA pair afterward. For example, if the time to recover the CS LAN is estimated to be 10 hours, it might not be worth activating the cold standby CMT server or CBM.

Scenario	Response
One site is destroyed in a catastrophic event	***At the site that is destroyed:*** • There is no activity. • The SS7 network takes down the links to the destroyed building. ***At the site that is not destroyed:*** • All nodes lose mate connectivity. • The Call Agent loses all mate connectivity, including the backup WAN link, and drops sync. • If the Call Agent is active, it remains active. No outage occurs. If the Call Agent is not active, it takes activity within 2 seconds. • If the Call Agent is inactive, it takes activity within 2 seconds followed by a warm or SOS restart (approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor). • Other nodes go active, and follow the Call Agent example after losing mate connectivity. • If Site B was destroyed, initiate a switchover to the standby CBM at Site A. • If Site A was destroyed, initiate a switchover to the standby CMT at Site B.
Active Call Agent card fails at one site	***At the site with the failed Call Agent:*** • All nodes at the site can communicate with their mates. ***At the site with the mate Call Agent:*** • All nodes in the site can communicate with their mates. • The (inactive) Call Agent detects loss of connectivity with the mate, detects local and WAN connectivity, takes activity, and restarts the SOS. • Other nodes experience disconnection from the SOS for approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor (normal restart behavior)

Scenario	Response
Inactive Call Agent card fails at one site	***At the site with the failed inactive Call Agent:*** • All nodes in the site can communicate with their mates. ***At the site with the mate Call Agent:*** • All nodes in the site can communicate with their mates. • The (active) Call Agent detects loss of connectivity with the mate, detects local and WAN connectivity, and stays active. • No SWACT or restart is required.
Recovery from isolation split brain (Active/Inactive)	***At both sites:*** • Once the Call Agents can communicate with their mates, they recognize that both are active. The Call Agent that was inactive backs down, leaving the other Call Agent active. The fallout is to force Unit 0 active and Unit 1 inactive. • Other nodes can communicate with their mates, negotiate activity, and resume normal operations.

System impact of failures

Failures could cause the following system impacts:

- When negotiating activity, the Call Agent preference is always to remain on the same side, if that side supports activity.
- If failover of the Call Agent is necessary, the Call Agent switches activity in less than 2 seconds. When the Callp Application performs a restart, call processing is interrupted for approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor (normal restart behavior). Failovers of other Callp nodes follow the Call Agent failover within 2 seconds.
- In Enterprise-only configurations where the solution contains Message Controller (MC) cards connected to Message Switches (MS), ENET and TDM peripherals, the MC and MS cards are co-located in one of the main geographically redundant sites.
- During site isolation, when determining the appropriate master site, preference is given to the site that contains the MC cards. This assumes that the site is able to take activity. If necessary, activity is switched to this side during the activity negotiation.

Recovery scenarios

The following table provides a summary of system responses during recovery.

System response summary

Scenario	Response
Recovery from isolation split brain (Active/Inactive)	• When Call Agents can communicate with their mates, they recognize that both are active. The Call Agent that was inactive before the failure backs down, leaving the other Call Agent active. The fallout is to force Unit 0 active, and Unit 1 inactive. • Other nodes can communicate with their mates, negotiate activity and resume normal operations.
General recovery behavior	All elements: • continually monitor connections with their mates, and with other network elements with which they normally communicate. When connectivity is not present, they continue to monitor the connections for restored connectivity. (The elements continue monitoring regardless of their activity state.) • negotiate activity and services when connectivity recovers, and resume normal operations.

System impact of recovery

Recovery could cause the following system impacts:

- When negotiating activity, the Call Agent preference is always to leave activity on the same side. When recovering to a full system configuration, activity remains on the same unit, without impact.
- During recovery from a split system (caused by incorrect message routing), node activity resolves in a few seconds. Call processing could require up to 15 minutes to recover completely.
- If an inactive call agent is not in service when the IST goes down, OSPF on the Ethernet Routing Switch 8600 is not disabled on the site of the inactive call agent, potentially resulting in failed calls due to misdirected messages. This condition can occur on site recovery after the Ethernet Routing Switch 8600 returns to service and the optical ring is still recovering. In the event that this outage occurs, manually disable OSPF on the Ethernet Routing Switch 8600 or disconnect the links to the WAN on the site of the inactive call agent until it returns to its operational state.

Disabling Border Gateway Protocol (BGP)

This section applies only to CS-LAN routers configured with Ethernet Routing Switch 8600s using BGP.

Similar to protocols OSPF and IS-IS, but providing more scalability and reliability, BGP serves as an interdomain protocol to distribute routing information between endpoints in an Geographic Survivability configuration.

Recall that the CS-LAN consists of dual Ethernet Routing Switch 8600s running as layer 2/3 switches. For redundancy, a pair of upstream routers must be deployed on the Core network edge as the entrance to the CS-LAN.

Nortel supports a square CS-LAN topology configuration, in which each Ethernet Routing Switch 8600 is connected to one of two upstream routers. Each Ethernet Routing Switch 8600 includes two BGP neighbors. One BGP neighbor is the eBGP peer to the wide area network (WAN) Core router. The other BGP neighbor is the iBGP peer to its Ethernet Routing Switch 8600 mate.

Routing policies

The following routing policies control the way in which the CS-LAN routers advertise CS-LAN prefixes to the BGP peers.

- one policy is used during normal operations
- one policy is used during a failure condition

When the system detects a communication failure condition, the routing policy to the external peer (that is, the eBGP peer) changes to control which prefixes are advertised.

A third policy could be required if BGP is used as the routing protocol between the network operations center (NOC) and the CS-LAN.

Nortel recommends using command network to advertise the backup path prefix.

Example

```
ip bgp network 172.30.242.169/29 add
```

Normal operations policy A policy is used on each Ethernet Routing Switch 8600 to redistribute all locally connected subnets to its peers: the iBGP peer (that is, the other Ethernet Routing Switch 8600) and the eBGP peer (the WAN router).

All prefixes to be redistributed are defined in a prefix list. The routing policy uses and applies the prefix list to the BGP peer. On any Ethernet Routing Switch 8600, a routing policy contains the prefix for the default route and other prefix that was advertised originally by the other Ethernet Routing Switch 8600.

Nortel recommends setting the name of the normal operations policy to “RoutesToDistribute.”

Normal operations policy example The following example shows entries in a typical normal operations policy prefix list:

Example

```
ip prefix-list "LocalPrefixes:  add-prefix 0.0.0.0/0
ip prefix-list "LocalPrefixes:  add-prefix 172.16.0.0/20
```

The following example shows a typical definition of a routing policy to be applied to the WAN eBGP peer:

Example

```
ip route-policy "RoutesToDistribute" seq 30 create
ip route-policy "RoutesToDistribute" seq 30 enable
ip route-policy "RoutesToDistribute" seq 30 action permit
ip route-policy "RoutesToDistribute" seq 30 match-network
"LocalPrefixes"
```

Failure condition policy When a failure condition interrupts connectivity between two halves of the CS-LAN, the system must react and change the routing policy. On each Ethernet Routing Switch 8600, a policy is applied to redistribute only the prefix for the backup path to the eBGP peer (that is, the WAN router).

As with the normal operations policy, all prefixes are redistributed and defined in a prefix list. The routing policy uses and applies the prefix list to the BGP peer.

Nortel recommends setting the name of the failure condition policy to "GeoBackupPath."

Failure condition policy example The following example shows an entry in a typical failure condition policy prefix list:

Example

```
ip prefix-list "GeoBackupPath" add-prefix 172.30.242.168
/29
```

The following example shows a typical definition of a routing policy to be applied to the WAN eBGP peer during a failure condition:

Example

```
ip route-policy "GeoBackupPath" seq 30 create
ip route-policy "GeoBackupPath" seq 30 enable
ip route-policy "GeoBackupPath" seq 30 action permit
ip route-policy "GeoBackupPath" seq 30 match-network
"GeoBackupPath"
```

Manual actions to disable and re-enable BGP When a failure occurs at the site with the in-service optical frame, adhere to the following sections to disable and re-enable routing at the site with the inactive call agent.

Disabling BGP during a failure condition When two call control agents (CCA) lose communication with one another through fiber channel/multi-link trunking (MLT), the CCA that does not assume mastership changes the redistribution policy (that is, from “RoutesToDistribute” to “GeoBackupPath”). Only the backup path prefix is advertised to the next hop WAN router.

Enter the following commands to advertise only the backup path prefix to the WAN router:

```
ip bgp neighbor 172.30.252.1 route-policy out “GeoBackupPath” add
```

```
ip bgp neighbor 172.30.252.1 restart soft-reconfiguration out
```

This action results in a new policy replacing the existing policy. Execute a soft restart of the peering session for this action to take effect.

Re-enabling BGP during a system recovery When the optical outage has been addressed and the master CCA recognizes that communication has been re-established with the backup CCA through fiber channel/MLTs, the backup CCA reverts the routing policy to normal steady-state (that is, from “GeoBackupPath” to “RoutesToDistribute”).

Enter the following commands to advertise all CS-LAN prefixes to the WAN router:

```
ip bgp neighbor 172.30.252.1 route-policy out “RoutesToDistribute” add
```

```
ip bgp neighbor 172.30.252.1 restart soft-reconfiguration out
```

This action results in a new policy replacing the existing policy. Execute a soft restart of the peering session for this action to take effect

Limitations and restrictions

The following limitations and restrictions apply to the Geographic Survivability feature:

- The physical distance between active and standby sites is limited to 120 KM/75 miles.
- Geographic survivability requires the USP - Compact.
- Each site must have a single Ethernet Routing Switch 8600 with dual switch fabric and CPU blades or third-party equivalent.

- Synchronization of data between two CCA blades over GigE links applies to the CS 2100 market with reduced capabilities. This configuration applies just to Enterprise solutions.
- In Enterprise hybrid configurations (with TDM equipment homed at one site), the TDM equipment is not geographically redundant. In determining the master site, preference is given to the TDM side only when either side can support Callp. If necessary, perform a SWACT to the TDM side to allow Callp on that side.
- Because the Call Agent interacts with the Ethernet Routing Switch 8600, the feature requires that each site have only one routing switch and IST links configured between sites. Dual ERS 8600s at each site and SMLT links between sites are not supported. Interactions between the Call Agent and the CS LAN are supported to prevent split brain scenarios (by disabling OSPF) when the ERS 8600s are used for the CS LAN. Upgrades from previous releases in an Enterprise geographic survivable configuration (which have dual ERS 8600's at each site) require that the dual ERS 8600s be migrated to a single ERS 8600 site.
- When a total loss of communication between sites occurs (that is, all three master links are down), the two Call Agents cannot negotiate activity decision. The decision is based on connectivity check from each site the WAN network.
  - While unlikely, it could be possible to have an active/active (split brain) scenario, or an inactive/inactive scenario (no processing).
  - The WAN backup path mitigates the risk of optical ring failure. The WAN connection check helps resolve activity when the backup path is down.
- CS 2000 - Compact supports only a single time zone setting. If the two physical sites are in different time zones, Nortel recommends that the time zone be set to either GMT or the time zone of one of the sites.
- Both Session Server units of a pair are located at the same site. For offices with Message Controllers, Nortel recommends that the Session Servers be located at the same site as the TDM components.
- For maximum redundancy, the WAN backup path must be configured separately from the optical network, as follows:
  - special vlans configured on Ethernet Routing Switch 8600 for backup path use only
  - vlans route over the WAN network instead of over the optical ring
  - vlans are not disabled with OSPF disable
  - alarm generated for lack of connectivity

- Gateways and services node components of CS 2000 - Compact are single units, and are not geographically redundant. Where the nodes are located and how they are connected to the network affects whether they survive a failure. Although the same nodes are supported in configurations with and without Geographic Survivability, there is no change in configuration or connection in the configuration with the Geographic Survivability configuration.

Installing the remote backup server

Target

Use this procedure to install the remote backup server for Geographic Survivability. Backing up the remote server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with data and files accurate to the last synchronization.

Prequisites

You must have the root user ID and password to perform this procedure.

Use the following table to ensure that you have the information ready for input during this procedure.

System Variable	Actual value
Hostname	
IP address (remote backup server)	
Netmask	
Router (default gateway IP)	
DNS (Yes, No)	
Unit 0 IP address (IP of primary cluster unit 0)	
Daily backup (up to four) in format:**HH:MM** where **HH = hours (00-23)** **MM = minute (00-59)**	
DNS domain	
IP address (DNS server[s])	
DNS search domain(s)	

DNS variables apply only when a DNS server has been configured.

Action

Installing the remote backup server on a Geographic Survivability standby server

At your workstation or the remote server console

Step **Action**

1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -1 root <server> and press the Enter key. Go to step 2
telnet	Type telnet <server> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 Log in to the server through the console (port A) and when prompted, enter the root user ID and password.

3 Bring the system to the {0} OK prompt by typing:

```
# init 0
```

4 Enter the following command to verify that the auto-boot option is set to true.

```
{0} ok printenv auto-boot?
```

If it is set to false, enter the following command.

```
{0} ok setenv auto-boot?=true
```

5 Insert disk 1 of the SPFS0** (090) CD set into the DVD drive on the standby unit.

6 Install the remote backup server for Geographic Survivability.

```
{0} OK boot cdrom - rbackup
```

7 Type OK and press Enter to acknowledge restriction on your use of the software.

8 Select the rbackup server profile for the system.

9 Enter no to not select the default settings. The N240 server must be connected to the network and must have access to the default

gateway. This allows you to enter the server's settings for the installation.

10 Enter site-specific information in response to the following prompts. (Refer to the information entered in the table at the beginning of this procedure.)

```
Enter the hostname for this system.
Enter the IP address for the remote backup server.
Enter the subnet mask for this network.
Enter the IP address for this network's router.
Enter the timezone for this system.
```

The default timezone is US/Eastern. Enter ? for a list of supported time zones.

```
Will this system use DNS?
```

11 Enter yes or no. If you answer yes, you are prompted for the DNS domain name, name server IP addresses, and the search domains. You can enter several name servers and search domains. To stop entry, enter a blank line

12 Enter OK to accept current settings.

The installation of the first CD takes approximately 25 minutes. No action is required until the following system response displays:

```
Media:

1.  CD/DVD
2.  Network File System
3.  Skip
Media[1]:
```

13 Enter 1 and then press Enter to select CD/DVD as the Media type for the installation of Solaris 9.

The system ejects disk 1 CD automatically.

14 Remove SPFS disk 1 CD from the server.

15 Insert SPFS disk 2 CD (the second SPFS CD in the set of 3 disks) into the DVD drive and then press Enter.

This step takes approximately 15 minutes to complete.

16 Enter 2 to continue with the installation.

17 Press Enter to reboot the system.

The installation of the Solaris Patches starts after the system reboots.

18 The installation of the second CD takes approximately 20 minutes. No action is required until the system prompts you to enter the third CD.

```
Done Installing Solaris Patches...
Insert SSPFS Deadstart CD ROM Disk 3 in the Drive.
Type "ok" when Ready.
```

19 Remove SPFS disk 2 CD from the server.

20 Insert SPFS disk 3 CD (the third SPFS CD in the set of 3 disks) into the DVD drive.

21 Enter OK and then press Enter to start the installation of the third CD.

The installation of the third CD takes approximately 50 minutes. You could be required to press Enter to reprint the login prompt to the screen after the reboot.

```
<Hostname> console login:
```

22 Log in to the server using the root user ID and password.

23 Remove SPFS disk 3 CD from the server.

```
eject cdrom
```

24 Enter the command line interface (CLI) tool.

```
cli
```

25 Enter the number next to the Configuration option in the menu.

26 Enter the number next to the Succession Element Configuration option in the menu.

27 Enter the number next to the PSE Application Configuration option in the menu.

28 Enter the number next to the Configure PSE option in the menu.

29 Enter the primary/cluster IP address of CS 2000 Management Tools server. This is the address of the NPM server.

30 Enter Y to confirm the IP address.

Ignore the following error message if it displays.

```
Can't configure PSE on remote backup unit to enable NPM
```

31 Enter X to exit each level until you have exited from the cli tool.

32 Start the PSE server.

```
# pse start
```

33 Verify that the server has started. If the server does not start, contact your next level of support.

```
# pse status
```

34 If an SPFS MNCL CD is to be installed, refer to the documentation included with the CD for complete installation instructions.

35 Enter NPM on the CS 2000 Management Tools server and follow patching procedures to apply all relevant patches.

—End—

Canceling a running remote backup process

Application

Use this procedure to cancel an existing remote backup process.

Prerequisites

This procedure has no prerequisites.

You must have the root user ID and password to log into the server.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Establish a connection to the server that is hosting the CS 2000 Management Tools through telnet or SSH, and log in using the root user ID and password. In a two-server configuration, log in to the active server using the physical IP address of the active server, and ensure you are on the active server using the `ubmstat` command. For detailed steps, refer to procedure "Logging in to an SPFS-based server".
2	Launch the command line interface tool by typing `# cli` and pressing the Enter key.
3	From the resulting menu, select the number against the “Configuration” menu option, and press the Enter key.

4 From the resulting menu, select the number against the “Remote Backup Configuration” menu option, and press the Enter key.

5 From the resulting menu, select the number against the “rbackup_cancel (Cancel Running Remote Backup)” menu option, and press the Enter key.

Example response

```
=== Executing "rbackup_cancel"
cleaning up files
unmounting /tmp/.snap/var /tmp/.snap/user_audio_files
/tmp/.snap/opt/nortel /tmp/.snap/opt /tmp/.snap/data/
qca
/tmp/.snap/data/oradata/arch /tmp/.snap/data/oradata
/tmp/.snap/data
/tmp/.snap/backup /tmp/.snap
removing scratch /tmp/.backing_store d99
=== "rbackup_cancel" execution completed
```

6 Exit each menu level of the command line interface tool by typing

```
select - x
```

and pressing the Enter key.

7 You have completed this procedure.

—End—

Scheduling automatic backups on the remote server

Target

Use this procedure to schedule automatic backups to the remote server. Backing up the primary server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with data and files accurate to the last synchronization.

ATTENTION
This procedure is for use with Geographic Survivability only.

Action

Scheduling automatic backups of the remote server

At your workstation or the remote server console

Step **Action**

1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -l <server> and press the Enter key. Go to step 2
telnet	Type telnet <server> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 When prompted, enter the root password.

3 Start the command line interface tool by entering:

```
cli
```

4 Select the Configuration menu.

The system displays the Configuration menu.

5 Select the Remote Backup option.

Response:

```
Remote Backup Configuration
```

```
1 - rbackup_display (Display Remote Backup Configurati
on)
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
4 - rbackup_cancel (Cancel Running Remote Backup)
X-exit
```

6 Select:

```
2-rbackup_config (Remote Backup Configuration)
```

The system responds with the IP address of the primary server that is currently configured as the remote server, and the times that are currently configured for automatic backups.

7 Enter the unit 0 IP address of the primary server to be backed up.

```
<nnn.nnn.nnn.nnn> is alive
```

where

nnn.nnn.nnn.nnn is the IP address that you entered.

8 Use the following table to determine your next step.

If the system	Do
prompts you to accept the ssh key	Enter yes. Go to step 9
does not prompt you to accept the ssh key	Go to step 9

```
Enter a time for a daily backup to occur (HH:MM):
```

where

HH is hours. Valid values are 00 to 23.
MM are minutes. Valid values are 00 to 59.

9 Enter the first time for a daily backup to occur

You can configure up to four times for daily backup to occur.

Response:

```
Enter a second time for a daily backup to occur (HH:MM)
or enter "x" to stop provisioning backup times:
```

10 Use the following table to determine your next step

If you	Do
want to enter another time for a remote backup to occur	Enter a second time for a daily backup to occur. Go to step 11
do not want to enter another time for a remote backup to occur	Enter x. Go to step 13

11 Use the following table to determine your next step

If you	Do
want to enter another time for a remote backup to occur	Enter a third time for a daily backup to occur. Go to step 12
do not want to enter another time for a remote backup to occur	Enter x. Go to step 13

12 Use the following table to determine your next step

If you	Do
want to enter another time for a remote backup to occur	Enter a fourth time for a daily backup to occur. Go to step 13
do not want to enter another time for a remote backup to occur	Enter x. Go to step 13

13 Use the following table to determine your next step

If you want to	Do
commit changes	Go to step 14
exit	Enter quit. Go to step 15
re-enter settings	Enter anything other than ok or quit. Go to step 9

14 Enter

```
ok
```

```
=== "rbackup_config"completed successfully
```

15 Exit the Remote Backup Configuration level.

```
x
```

—End—

Viewing configuration information for remote server backups

Target

Use this procedure to view the current configuration information for remote server backups. The system displays the IP address of the target system and the times in which automatic backups of the target system will occur.

ATTENTION
This procedure is for use with Geographic Survivability only.

Action

Viewing configuration information for remote server backups

At your workstation or the remote server console

Step	Action
1	Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -l <server> and press the Enter key. Go to step 2
telnet	Type telnet <telnet> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 Start the command line interface tool by entering:

```
cli
```

The system responds by displaying a menu.

3 Select the Configuration menu.

The system displays the Configuration menu.

4 Select the Remote Backup option.

Response:

```
Remote Backup Configuration
1-rbackup_display (Display Remote Backup Configuration)
```

```
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
4 - rbackup_cancel (Cancel Running Remote Backup)
X-exit
```

5 Select

```
1-rbackup_display (Display Remote Backup Configuration)
```

Response:

```
Current settings:
Target system is:  <nnn.nnn.nnn.nnn>
Back up times are:  <Time 1>...<Time n>
```

where

<nnn.nnn.nnn.nnn> is the IP address of the remote server

where

<Time 1>...<Time n> is the set of times at which automated backups occur.

6 Exit the Remote Backup Configuration level by typing:

x

—End—

Performing a manual backup of the target server

Target

Use this procedure to perform a manual backup of the primary server. Backing up the primary server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with system configuration data and files accurate to the last synchronization.

ATTENTION
This procedure is for use with Geographic Survivability only.

Action

Performing a manual backup of the remote server

At your workstation or the remote server console

Step **Action**

1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -l root <server> and press the Enter key. Go to step 2
telnet	Type telnet <server> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 When prompted, enter the root password.

3 Start the command line interface tool.

```
cli
```

The system responds by displaying a menu.

4 Select the Configuration menu.

The system displays the Configuration menu.

5 Select the Remote Backup option.

```
Remote Backup Configuration
1-rbackup_display (Display Remote Backup Configuration)
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
4 - rbackup_cancel (Cancel Running Remote Backup)
X-exit
```

6 Select

```
3-rbackup_exec (Execute Remote Backup Now)
```

7 An automatic backup is made.

Pressing 4 during execution of the backup halts the process and performs necessary clean-up operations.

8 Exit the Remote Backup Configuration level.

```
x
```

—End—

Viewing logs from a remote backup

Target

Use this procedure to view logs associated with a backup of the remote server. Logs are created during automatic and manual backups of the remote server.

Action

Viewing logs from a remote backup

At your workstation or the remote server console

Step **Action**

1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server.

If you want to log in by means of	Do
ssh	Type ssh -l <server> and press the Enter key. Go to step 2
telnet	Type telnet <server> and press the Enter key. Go to step 2
the remote server console	step 2

where

`server` is the name of the N240 server.

2 Enter:

```
less /var/adm/messages
```

The system responds by displaying the contents of the log file.

3 The procedure is complete.

—End—

Initiating a recovery back to the cluster

Prerequisites

It is expected that the primary server is in the shut-down mode.

If the server was previously a CBM and contains billing files not already sent to a down-stream billing server, using the cluster server, these files should be copied to a downstream server prior to performing "Installing the remote backup server" (page 149). Otherwise these files and the billing records will be lost. Contact next level of support for assistance

Target

When completed, this procedure will restore the HA cluster and backup server.

Action

Initiating a recovery back to the cluster

At your workstation

Initiating a recovery back to the cluster

Step	Action
1	Follow the "Installing the remote backup server" (page 149) procedure. In this case, the unit0 server of the cluster is used as a remote backup server. Use the same hostname and IP address that was used to configure the remote backup server in the first place.
2	Follow the "Scheduling automatic backups on the remote server" (page 155) procedure. Use only one automated schedule and make sure to select a time that will not be invoked shortly.
3	Follow the "Performing a manual backup of the target server" (page 160) procedure.
4	Bring down the machine currently active by following the procedure ‘Two-server (cluster) configuration’ in chapter ‘Shutting down an SPFS-based server’ of the document ATM/IP Solution-level Fault Management NN10408-900.
5	Follow the "Initiating a switch over to the remote backup server" (page 165) procedure to bring the services back to unit0 of the cluster.

6 Follow the ‘Cloning the image of one server in a cluster to the other server’ procedure of the document ATM/IP Solution-level Security and Administration NN10402-600.

7 If the server was previously a CBM and contains billing files not already sent to a down-stream billing server, using the remote backup server, these files MUST be copied to a downstream server prior to performing "Installing the remote backup server" (page 149) Otherwise these files and the billing records will be lost. Contact next level of support for assistance.

8 Reinstall the backup server following the "Installing the remote backup server" (page 149) procedure.

9 Reconfigure the backup server following the "Scheduling automatic backups on the remote server" (page 155) procedure.

10 The procedure is complete.

—End—

Initiating a switch over to the remote backup server

Prerequisites

Prior to starting this procedure, shut down the Cluster machine.

Refer to section *Two-server (cluster) configuration* in chapter *Shutting down an SPFS-based server* in NTP NN10408-900, *ATM/IP Solution-level Fault Management*.

The user must be logged in as the root user in order to initiate the switch command.

CAUTION

If configuration, provisioning, patching or other “write”-type operations occurred since the last remote backup, the remote backup system can be out of sync compared to the data in network elements and/or the primary OAM system.

Take actions before initiating the switchover to a remote backup OAM server (that is, response to a geographic or other prolonged outage of the primary OAM system) to halt or prevent “write”-type operations by OSSs and operations personnel until an in-sync status is achieved.

When initiating a switchover to a remote backup OAM server, do not execute configuration, provisioning, patching or other “write”-type operations through the remote backup OAM system until out-of-sync conditions are cleared.

Target

When completed, this procedure reboots the remote backup server as the unit0 of the cluster.

Action

Initiating a switch over to the remote backup server

At your workstation

Step	Action
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where

server is the IP address or host name of the SPFS-based remote backup server.

2 When prompted, enter your user ID and password.

3 Change to the root user.

```
su - root
```

4 When prompted, enter the root password.

5 Invoke the switch by typing:

```
$ /opt/sspfs/rbks/switch
```

6 When ready, indicate you want to proceed by typing:

```
OK
```

—End—

Setting the MSC Server 1000 CLLI on the Sun server

Application

The SDM IP address automatically retrieves the CM CLLI from the Communication Server 2000 (CS 2000).

Use this procedure to rediscover the CM CLLI on a Server Platform Foundation Software (SPFS) based server when the SDM IP has already been configured.

ATTENTION

The steps to configure the SDM IP are also provided in the event it has not already been configured. The CM CLLI can be configured or unconfigured on an SPFS-based server that hosts the Core and Billing Manager (CBM), but cannot be configured or unconfigured on an SPFS-based server that hosts the following components:

- CS 2000 Management Tools and Audio Provisioning Server (APS)
- CS 2000 Management Tools, Integrated Element Management System (IEMS), or both
- Media Gateway 9000 Manager

To set the CM CLLI on an SPFS-based server that hosts the CBM, refer to the CBM Configuration Management document (NN10353-511) .Use this procedure to set the CLLI for the MSC Server 1000 XA-Core (CM CLLI) on a server that uses Server Platform Foundation Software (SPFS). You can also use this procedure to remove the MSC Server 1000 CLLI from the server.

Make sure your system is patch-current before performing this procedure. If the system is not patch-current, changing or unconfiguring the CM CLLI can cause loss of configuration data on the system. If you are not sure whether the patch that corrects this issue is applied, contact your next level of support before you proceed.

Prerequisites

- Be prepared to configure the SDM IP address in the event the address is not already configured.
- You must have the CLLI for the CS 2000 that is associated with the SPFS-based server on which you are setting the CLLI.

ATTENTION

The CS 2000 CLLI is listed in table OFCENG.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server on which you are setting the CS 2000 CLLI

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3- OAMP Application Configuration
  4- CORBA Configuration
  5- IP Configuration
  6- DNS Configuration
  7- Syslog Configuration
  8- Remote Backup Configuration
 9 - Database Configuration
```

```
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "OAMP Application Configuration" option in the menu.

Example response

```
OAMP Application Configuration
  1 - sdm_conf (Configure SDM IP Address)
  2 - sdm_unconf (Unconfigure SDM IP Address)
  3 - sdmuser_conf (Configure SDM User)
  4 - sdmuser_unconf (Unconfigure SDM User)
  5 - cmClli_rediscovery (Re-discover the CM
CLLI by SDM IP)
  6 - cmClli_conf (Configure CM_CLLI Address)
  7 - cmClli_unconf (Unconfigure CM_CLLI IP Address)
  8 - cm_conf (Configure CM IP Address)
  9 - cm_unconf (Unconfigure CM IP Address)
X - exit
select -
```

8 Enter the number next to the "cmClli_rediscovery" option in the menu.

Example response

```
=== Executing "cmClli_rediscovery"
Retrieve CM CLLI by SDM IP <ip address>.  Please
wait......
CM CLLI old value:  TESTCLLI
CM CLLI new value:  TESTCLLI
CM CLLI has not changed.
=== "cmClli_rediscovery" completed successfully
```

If the system response …	Do
…provides the CM CLLI value	step 12
…indicates the SDM IP is not configured	step 9

9 Enter the number next to the "sdm_conf" option in the menu.

Example response

```
Enter the ip address of the SDM
```

10 When prompted, enter the SDM IP address.

Example response

```
Retrieving CM CLLI. Please wait.....
SDM IP: 45.123.456.89
CM CLLI: TESTCLLI
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

11 When prompted, commit the changes if acceptable by typing

ok

and pressing the Enter key.

Example response

```
You must log out and log back in to the new SDM
environment settings to take place.
SDM IP and CM CLLI have been successfully configured.
```

12 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - x

and pressing the Enter key.

13 Log out and log back in to the server to reflect the CLLI environment changes as follows:

a. Exit the root user level by typing

 # exit

and pressing the Enter key.

b. Exit the maintenance user level by typing

$ exit

and pressing the Enter key.

c. Log in to the server by typing

> telnet <server>

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

d. When prompted, enter your user ID and password.

ATTENTION

If the Network Patch Manager (NPM) server application is running on this SPFS-based server, you must stop it and start it now. If required, refer to procedures "Stopping the NPM server application" and "Starting the NPM server application" in the document titled *ATM/IP Security and Administration* (NN10402-600) .

You have completed this procedure.

—End—

Configuring Client Session Monitor

Application

Use the following procedures to change the default settings and customize the Client Session Monitor (CSM) application:

- "Configuring the display criteria for a CSM report" (page 172)
- "Configuring the CSMonitor Audit using CLI" (page 174)

Refer to Launching Client Session Monitor in the IEMS Basics document, NN10329-111 for details on accessing the CSM.

Prerequisites

For a security end user to perform "Configuring the display criteria for a CSM report" (page 172) using the GUI, the IEMS Central SS software must be installed.

The following prerequisites apply for "Configuring the CSMonitor Audit using CLI" (page 174):

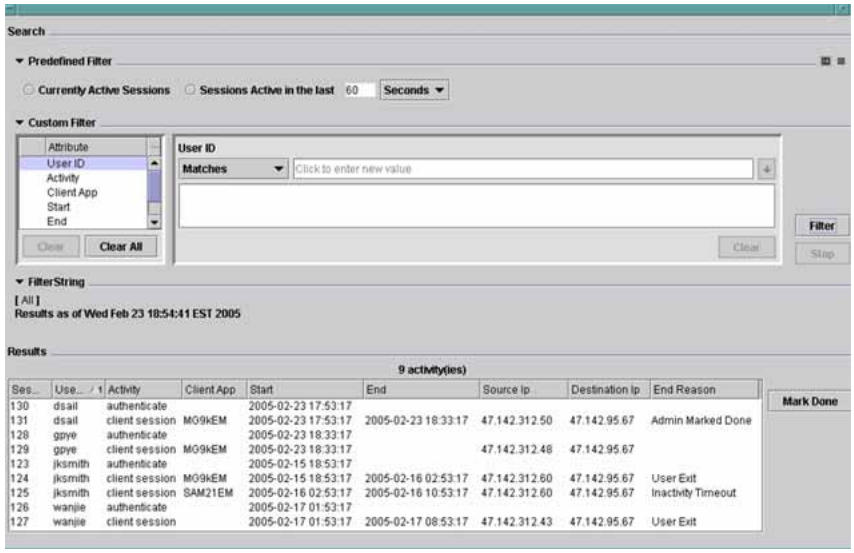
- you must have the IEMS Central SS software installed
- you must be a root user to configure the CSMonitor Audit using command line interface (CLI)

Action

Perform the following steps to complete this procedure.

Configuring the display criteria for a CSM report

Step	Action
	At your workstation using the CSM GUI client
1	Decide how you want to customize the default filter criteria and then perform some or all of the following steps. The default filter criteria displays results for all currently active application sessions. It also displays historical data about the owner of each of the active application sessions. The displayed data refreshes every 60 seconds. *A window similar to the following figure is displayed on your desktop after having launched CSM. The window displays all current application sessions monitored by CSM.*



2 Deselect Currently Active Sessions which is the default setting.

3 Select the attributes you want to use as the filter criteria from the Customer Filter scroll box.

The Custom Filter scroll box allows you to build customized criteria from the list of available attributes.

For those fields that are strings, such as UserID, Activity, ClientApp, SourceIp, and DestinationIp, the criteria used to match are selected from the drop-down menu to the right of the Customer Filter scroll box. The options in this menu are Matches, Does not match, Contains, Does not contain, and Starts with. Enter the information you want to use as a criteria in the field next to the option you have selected.

For fields that are dates, such as Start Activity and End Activity, the matching criteria are Matches, Does not match, Before, Between. The date requires the format of YYYY-MM-DD HH:MM:SS. The exceptions are the term Current and Null.

4 Replace the default setting of 60 seconds in the Sessions Active in the last field by selecting another time period (either Seconds, Minutes, Hours, or Days) from the drop-down menu.

5 Click Filter to update the report once you have finished modifying the filter criteria.

A customized CSM report displays in the Results section of the window using your customized filter criteria.

—End—

Configuring the CSMonitor Audit using CLI

Step	Action

At your workstation

1 Log in to IEMS security server by typing

```
> telnet <IEMS security server>
```

and pressing the Enter key.

where

IEMS security server is the IP address or host name of the IEMS security server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Configure the Client Session Monitor Audit (CSMonitor Audit) using CLI by following these steps.

6 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

7 Enter the number that corresponds to the Configuration option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - DCE Configuration
  4 - OAMP Configuration
  5 - CORBA Configuration
```

```
  6 - IP Configuration
  7 - DNS Configuration
  8 - Syslog Configuration
  9 - Database Configuration
  10 - NFS Configuration
  11 - Bootp Configuration
  12 - Restricted Shell Configuration
  13 - Security Services Configuration
  14 - Login Session
  15 - Location Configuration
  16 - Cluster Configuration
  17 - Succession Element Configuration
  18 - snmp_poller (SNMP Poller Configuration)
  19 - backup_config (Backup Configuration)
  x - exit
select -
```

8 Enter the number next to the Succession Element Configuration option in the menu.

Example response

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - PSE Application Configuration
  6 - SAM21EM Application Configuration
  7 - DDMSProxy Application Configuration
  8 - OMPUSH Application Configuration
  9 - RESMON Application Configuration
  x - exit
select -
```

9 Enter the number next to the CSMCLEANUP Application Configuration option in the menu.

Example response

```
CSMCLEANUP Application Configuration
  1 - setCleanupTime (How often cleanup DB)
  2 - setCleanupCriteria (Criteria used to
delete from DB)
x - exit
select -
```

10 Enter the number next to the setCleanupTime option in the menu.

All CSM sessions, even after they are closed, are recorded in the CSM database of logins and logouts. The CSMonitor Audit functionality prevents the session database from growing too large by cleaning up unwanted records of sessions. The selected time

determines when polling of the database for the clean up of sessions occurs. Sessions are removed from the audit when CSMonitor Audit re-activates following the selected time period. For example, if 24 hours is the selected time, the CSMonitor Audit reactivates 24 hours after the audit begins and queries the database for sessions needing to be removed.

The selection of sessions is based strictly on start time and may delete sessions that have not ended. Therefore, care must be taken to specify criteria so as not to delete any active sessions.

Example response

```
===Executing "setCleanupTime"
Current value for removing sessions from CSMonitor is:
400
Enter the CSMonitor Audit cleanup time in hours
(1->720):24
Modifying CSMonitor Audit cleanup time.
Done.
==="setCleanupTime" completed successfully
```

11 Enter the number next to the setCleanupCriteria option in the menu.

Max sessions per user criteria keeps the sessions based on start time for each user id. Time based criteria keeps sessions based on start time. For example, you can change the cleanup criteria from max sessions per user to deletion after 500 hours.

Example response

```
===Executing "setCleanupCriteria"
Current value for criteria for removing sessions from
CSMonitor Audit is:
CSM_CRITERIA=1
Enter 1 to set criteria for deletion based on max
sessions per user:
Enter 2 to set criteria for deletion based on time:2
Enter the number of hours to keep sessions (1->720):500
Modifying CSMonitor Audit cleanup time.  Done.
==="setCleanupCriteria" completed successfully
```

12 Exit each menu level of the command line interface to eventually exit the command line interface by typing

```
select - x
```

13 Restart CSMonitor_Audit in order to apply the new configuration by typing

```
servrestart CSMonitor_Audit
```

You have completed this procedure.

—End—

Configuring SPFS console access

Purpose

Use this procedure when you are performing a procedure that requires a direct connection to the Sun Server console port, as opposed to telnet/ssh access.

Application

The following procedures require console access:

- Fresh SPFS installations
- Upgrades and fallbacks
- Performing a full system restore on an SPFS-based server
- Network IP changes
- Cloning the image of one server in a cluster to the other server
- Shutting down an SPFS-based server
- Initiating a manual failover on a Sun Netra 240 server pair
- Replacing one or more failed disk drives on an SPFS-based server
- Changing an expired root password on an SPFS-based server

Console access can be achieved in two distinct methods:

- locally
- remotely

Prerequisites

This procedure describes how to configure both methods of console access. Additional information about setting up console access can be found in the *Sun Netra 240 Server Installation Guide*:

http://docs.sun.com/app/docs

You will not be able to make use of the serial console if the Sun server was booted with the keyboard/mouse plugged in. In order to make use of the serial console, you will need to disconnect the keyboard/mouse and reboot the Sun server.

Procedures

RS-232 device connection and configuration

There are two steps as follows:

- Physically connecting the desired RS-232 device to the serial management (Serial MGT) port.
- Configuring the RS-232 device with adequate RS-232 protocol settings.

Configuring and connecting the RS-232 device

Step	Action

At your workstation

1 Physical connection is established by using the correct cable to interconnect the RS-232 device to the serial management RJ-45 console port. This port is located on the back of the Sun T1400/N240 and is labeled "Serial MGT".

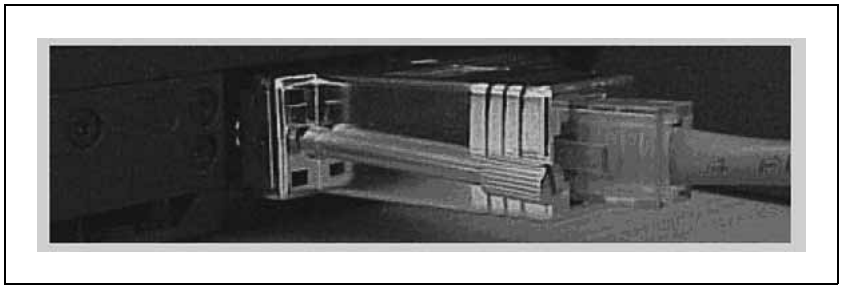
2 Connection to the Sun T1400/N240 can be established using a RJ-45 cable and a RJ-45-DB9 adaptor. Connect one end of the RJ-45 cable to the N240 Serial MGT port (located on the rear of the Netra). Connect the other end to the RJ-45-DB9 adaptor and then to the client PC/laptop as shown in the figure below. The Sun part number for the RJ-45-DB9 adaptor is Sun Part #530-2103.

> ***Note:*** A crossover or rollover cable connecting the RS-232 device and the console port might be required, so that each pin of the Netra 240 matches that of the terminal server's serial port.

More information about pinout configurations can be found in the *Sun Netra 240 Server Service Manual*:

http://www.sun.com/products-n-solutions/hardware/docs/html/817-2699-13/

Sun 240 DB9 connector on COM1 port of a laptop



3 By default, the console port requires the connecting RS-232 device to be configured as follows:

- Bits per second: 9600

- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: Xon/Xoff

4 You have completed this procedure.

—End—

Configuring local console access

To gain local console access to the T1400/N240, use a co-resident vt-100 terminal or laptop with vt-100 terminal emulation software (such as the Microsoft Windows Hyperterm application) as the RS-232 device. Use the device configuration parameters in "RS-232 device connection and configuration" (page 179).

Configuring local console access

Step Action

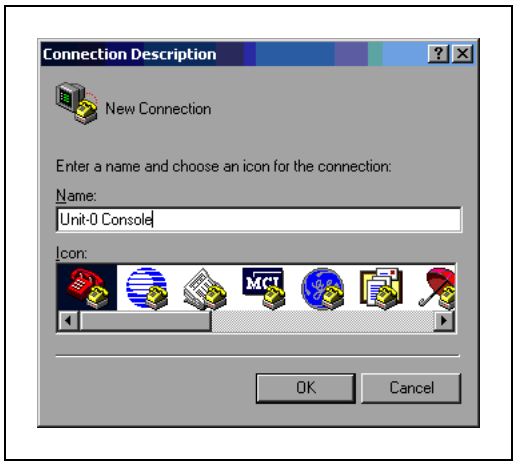
At your workstation

1 You can use HyperTerminal.

Click Start -> Programs/Accessories/Communications/HyperTerminal

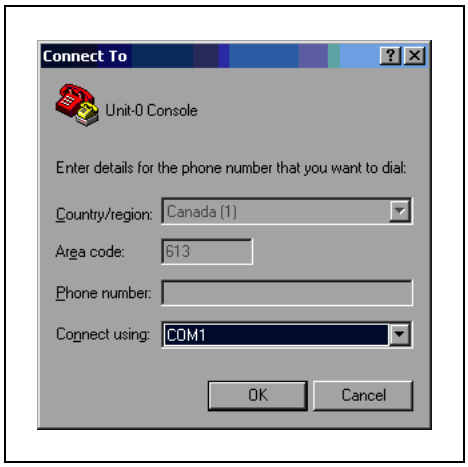
2 Give the session a name, such as "unit0 Console".

New connection dialog



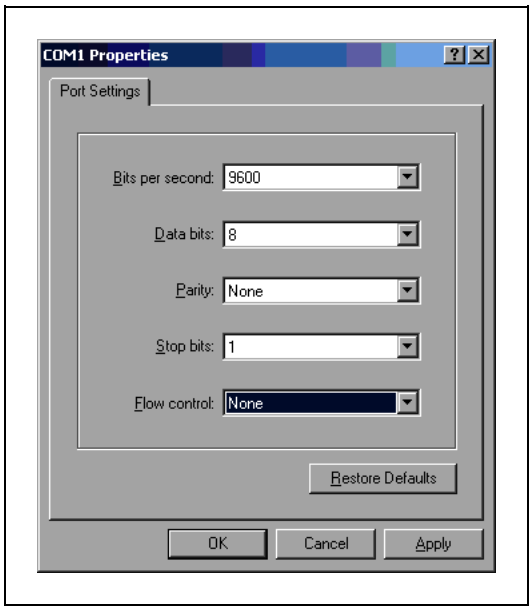
3 Configure the correct COM port setting, depending on the port to which you connected the serial adaptor. The default should usually be COM1.

Connection details



4 Configure the port settings as described above in "RS-232 device connection and configuration" (page 179).

Port settings



5 Once connected, press Enter and you should see a response from the machine, such as a session login prompt or the Open Firmware OK prompt. You now have console access.

6 You have completed this procedure.

—End—

Configuring remote console access

While terminal server and modems are supported for remote access, Nortel recommends using a terminal server as it is more secure, and console access for both units is readily available and remotely accessible. Nortel does not recommend modems as they are inherently insecure when connected to the PSTN. The customer's security policy must be followed regardless of Nortel recommendations.

To gain remote console access to the T1400/N240, use a terminal server as the RS-232 device. The terminal server allows seamless connections from its LAN connection (TCP/IP protocol), to multiple serial ports (RS-232 protocol) of the console port. Typically, each physical RJ-45 port on the terminal server is assigned to a virtual telnet port. Once configured, establish a telnet session to the terminal server with a specific telnet port.

Note: Supplying and configuring a terminal server or modems is the customer's responsibility.

Configuring remote console access

Step	Action

From your workstation

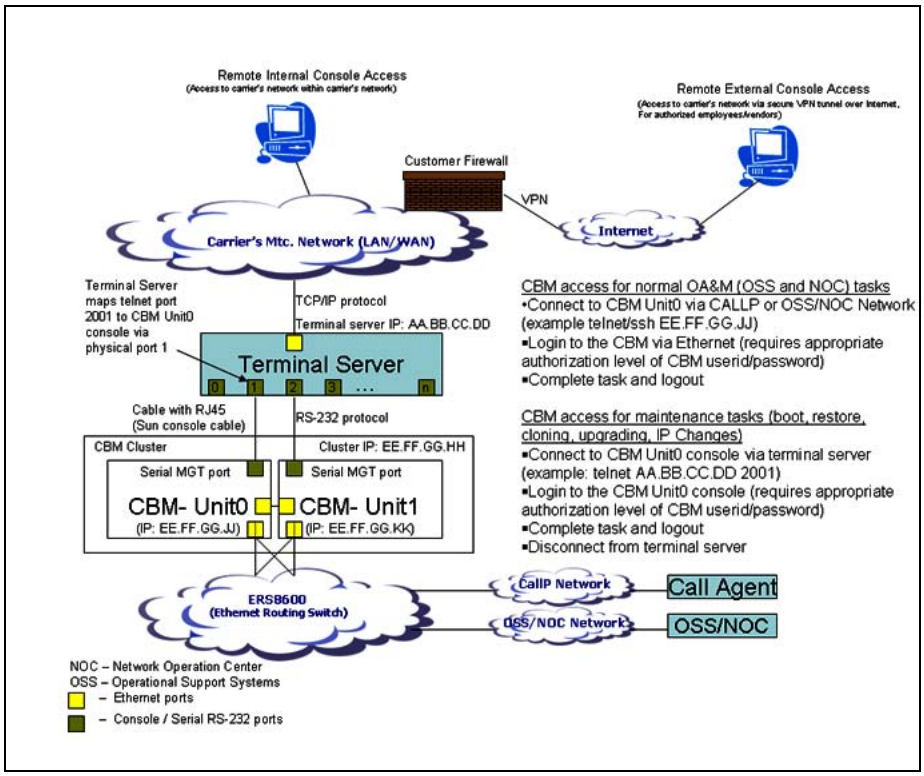
1 Connect the unit0 Serial MGT port to the physical RS-232 port 1 of the terminal server, and the unit1 Serial MGT port to the physical RS-232 port 2 of the terminal server.

2 If the IP address of the terminal server is AA.BB.CC.DD, and terminal server physical ports 1 and 2 have been configured to telnet ports 2001 and 2002 respectively, then the unit console ports can be accessed directly using telnet.

unit0: telnet AA.BB.CC.DD 2001

unit1: telnet AA.BB.CC.DD 2002

Remote terminal server console access - example network configuration



3 Once connected, press Enter and you should see a response from the machine, such as a session login prompt or the Open Firmware OK prompt. You now have console access.

4 You have completed this procedure.

—End—

Configuring a Timing Provider on an SPFS-Based Server

Application

Use this procedure to configure a timing provider for a Server Platform Foundation Software (SPFS) based server. The timing provider is a Network Timing Protocol (NTP) server supplied by the customer. Perform the steps under "Configure a timing provider on an SPFS server" (page 184).

For a cluster (two-server configuration), the Active server can serve as the master time provider for the Inactive server in the event that an NTP server is not provisioned. Perform the steps under "Configure the active server in a cluster as the timing provider" (page 186).

CAUTION
To avoid server configuration being overwritten, do not use this procedure to configure a timing provider for a CO-based MDM on an SPFS server. Instead, follow the Configuring Solaris NTP software sections in *MSS 15000, MG 15000 & MDM Configuration Attribute Summary* (NN10225-512).

Prerequisites

You must have the IP address of the customer-supplied NTP server.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you want to configure an NTP server
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su -`

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number that corresponds to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the number next to the "NTP Configuration" option in the menu.

Example response

```
NTP Configuration
1 - ntp_conf (Configure the NTP daemon)
2 - ntp_unconf (Unconfigure the NTP daemon)
3 - ntp_remove (Remove an NTP server)
```

```
4 - ntp_view (View NTP configuration information.)
X - exit
select -
```

8 Enter the number next to the "ntp_conf" option in the menu.

9 When prompted, enter IP address of the time server.

The system attempts to verify the IP address. If the IP address verification fails, check the IP address and try again.

You can specify up to three NTP servers.

10 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

select - x

and pressing the Enter key.

You have completed this procedure.

—End—

Configure the active server in a cluster as the timing provider

Step	Action

At your workstation

1 Log in to the Active server by typing

> telnet <server>

and pressing the Enter key.

where

server is the physical IP address of the Active server in the cluster

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

$ su -

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify the time is correct on the Active server by typing

 # date

and pressing the Enter key.

If the time	Do
is not correct	step 6
is correct	step 7

6 Adjust the time on the Active server using the "date" command. If required, refer to the man pages on the "date" command to adjust the time.

7 Synchronize the time on the Active server with the time on the Inactive server by typing

```
# synctime
```

and pressing the Enter key.

You have completed this procedure.

—End—

Adding IP Addresses for FTP Proxy and Restricted Shell Access

Application

Use this procedure to setup a list of IP addresses for FTP proxy and restricted shell access on an SPFS-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing **`> telnet <server>`** and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you are setting up FTP proxy and restricted shell access
2	When prompted, enter your user ID and password.
3	Change to the root user by typing **`$ su -`** and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Response
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	`X - exit`

```
select -
```

6 Enter the number that corresponds to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number that corresponds to the "Restricted Shell Configuration" option in the menu.

Example response

```
Restricted Shell Configuration
1 - valid_ip_add (Add Entries To The Restricted
Shell Usage List)
2 - valid_ip_remove (Remove Entries To The
Restricted Shell Usage List)
3 - valid_ip_list (List Entries On The
Restricted Shell Usage List)
X - exit
select -
```

8 Enter the number that corresponds to the "valid_ip_add" option in the menu.

9 When prompted, enter the IP address you want to add.

10 When prompted, enter the group name to use for the IP address.

Example response:

```
==="valid_ip_add" completed successfully
```

11 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

—End—

Configuring the Time Zone on an SPFS-Based Server

Application

Use this procedure to configure the time zone on a Server Platform Foundation Software (SPFS) based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server on which you want to configure the time zone

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "Location Configuration" option in the menu.

Example response

```
Location Configuration
1 - Chg_tz (Change Timezone
2 - sys_loc (System Location)
X - exit
select -
```

8 Enter the number next to the "chg_tz" option in the menu.

Example response

```
=== Executing "chg_tz"
WARNING: Changing the timezone will require a reboot
Current setting:
Timezone:       US/Eastern
Enter the timezone for this host <default:  US/Easter
n>:
```

9 When prompted, enter the correct time zone and press the Enter key.

Example response

```
New setting:
Timezone:       US/Eastern
Enter "ok" to commit changes
```

```
Enter "quit" to exit
Enter anything else to re-enter settings
```

10 When prompted, confirm the change by typing

`ok`

and pressing the Enter key.

11 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

12 You have completed this procedure.

—End—

Configuring Domain Name Service on an SPFS-Based Server

Application

Use this procedure to configure Domain Name Service (DNS) on a Server Platform Foundation Software (SPFS) based server.

ATTENTION

Do not configure an SPFS-based server that is hosting the Core and Billing Manager (CBM) as a DNS client. The CBM must never be configured to act as a DNS client.

A HTTPS certificate must be installed and DNS must be enabled on the following SPFS platforms:

- IEMS
- CS 2000 Management Tools
- MG 9000 Element Manager

This procedure provides the instructions for the following tasks:

- "Configure DNS on a master server" (page 195)

ATTENTION

A Call Server LAN (CS LAN) only uses one DNS master server. Configure other hosts in the CS LAN that use DNS to use the DNS master server.

- "Add (remove) a host entry in the DNS database" (page 198)
- "Configure server as a DNS client" (page 200)
- "Turn off DNS capability on the server" (page 203)

ATTENTION

Perform the steps under "Turn off DNS capability on the server" (page 203) when the DNS master server function is no longer required, or if the DNS master server function is moving to a different server. If needed the server can then be configured as a DNS client using the steps under "Configure server as a DNS client" (page 200).

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password for the server
- you need the office CLLI to complete the steps under "Configure DNS on a master server" (page 195)

- you need to complete the steps under "Configure DNS on a master server" (page 195) prior to performing the steps under "Add (remove) a host entry in the DNS database" (page 198)
- you need familiarity with the "vi" editor to perform the steps under "Add (remove) a host entry in the DNS database" (page 198)

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d. When prompted, enter the root password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

ATTENTION

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

4 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

5 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
```

```
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

6 Enter the number next to the "DNS Configuration" option in the menu.

Example response

```
DNS Configuration
1 - turn_dns_on (Configure as DNS client)
2 - turn_dns_off (Turn off a system's DNS capability)
3 - enable_dnssvr (Configure as DNS server)
X - exit
select -
```

7 Enter the number next to the "enable_dnssvr" option in the menu.

Example response

```
===Executing "enable_dnssvr"
Enter domain name for the office:
```

8 When prompted, enter the domain name for the office.

This procedure configures a DNS master server that is not connected to any other DNS zones outside of the CS LAN. To allow possible future connections of CS LAN DNS zones, it is recommended that the domain name for each CS LAN be the office CLLI.

9 If prompted, indicate whether you want to overwrite the existing DNS configuration.

Example response

```
Configuring with:
hostname:  <hostname>
DNS domain:  <office clli>
server IP: <IP address>
Starting DNSSVR through servstart
DNSSVR Started
==="enable_dnssvr" completed successfully
```

10 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

11 Verify that DNS is working by typing

`# nslookup <hostname>`

and pressing the Enter key.

Example response

```
Server:  <hostname>.<domain name>
Address:  <IP address>
Name:  <hostname>.<domain name>
Address:  <IP address>
```

You have completed this procedure.

—End—

Add (remove) a host entry in the DNS database

Step	Action

At your workstation

1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d. When prompted, enter the root password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

> ssh -l root <server>

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

4 Add or remove host entries in the DNS database, which entails editing two files; the "forward" (hosts) zone file, which translates domain names to IP addresses, and the "reverse" (hosts.rev) zone file, which translates IP addresses to domain names.

Increment the "serial" number at the beginning of each zone file every time you update the file.

The zone files will only be present if a DNS master server was configured. If required, refer to the steps under "Configure DNS on a master server" (page 195).

Following is an example of adding a host named "annex" with an IP address of "45.136.123.46. The serial number for the file is also incremented to 2. In the example, the domain name (or office CLLI if used as domain name) is "loco".

 # vi /data/dns/named/hosts

Example response:

```
$TTL  3h
  ; SOA
  loco.  IN SOA apex.loco. root.apex.loco (
                           2   ; Serial
                           3h  ; Refresh
                           15  ; Retry
                           1W  ; Expire
                           3h ); Minimum
  ; name servers
  loco.  IN   NS   apex.loco
  ; addresses
  apex   IN   A    45.136.123.70
  annex  IN   A    45.136.123.46
```

 # vi /data/dns/named/hosts.rev

Example response:

```
$TTL  3h
  ; SOA
  123.136.45.in-addr.arpa.  IN SOA apex.loco.
  root.apex.loco (
                            2    ; Serial
                            3h   ; Refresh
                            15   ; Retry
                            1W   ; Expire
                            3h ); Minimum
  ; name servers
  123.136.45.in-addr.arpa.  IN   NS   apex.loco
  ; addresses
  70.123.136.45.in-addr.arpa  IN   PTR apex.loco
  46.123.136.45.in-addr.arpa. IN   PTR annex.loco
```

5 Restart the DNS service by typing

`# servrestart DNSSVR`

and pressing the Enter key

Example response

```
Stopping DNSSVR
Starting DNSSVR
DNSSVR re-started successfully
```

You have completed this procedure.

—End—

ATTENTION

Do not execute the procedure that follows on an SPFS-based server that is hosting the Core and Billing Manager (CBM). The CBM must never be configured to act as a DNS client.

Configure server as a DNS client

Step Action

At your workstation

1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

> telnet <server>

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

$ su - root

and pressing the Enter key.

d. When prompted, enter the root password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

> ssh -l root <server>

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

4 Access the command line interface by typing

 # cli

and pressing the Enter key.

Example response

```
Command Line Interface
   1 - View
2 - Configuration
3 - Other
X - exit
```

```
select -
```

5 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -
```

6 Enter the number next to the "DNS Configuration" option in the menu.

Example response

```
DNS Configuration
   1 - turn_dns_on (Configure as DNS client)
 2 - turn_dns_off (Turn off a system's DNS
       capability)
   3 - enable_dnssvr (Configure as DNS server)
X - exit
select -
```

7 Enter the number next to the "turn_dns_on" option in the menu.

8 When prompted, confirm the command by typing

`yes`

and pressing the Enter key.

9 When prompted, enter the DNS domain.

Example
us.nortel.com

10 When prompted, enter the IP address of a DNS server.

11 When prompted, enter the IP address of a second DNS server.

12 When prompted, enter the IP address of another DNS server. If there are no other DNS server addresses to enter, press the Enter key.

13 When prompted, enter the name of a search domain.

Example
us.nortel.com

14 When prompted, enter the name of another search domain. If there are no other search domains, press the Enter key.

15 Accept the DNS configuration that is displayed by typing

```
ok
```

and pressing the Enter key.

16 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Turn off DNS capability on the server

Step Action

At your workstation

1 Establish a login session to the server using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

b. When prompted, enter your user ID and password.

c. Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

d. When prompted, enter the root password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that you want to configure as a DNS master server

In a two-server configuration, enter the cluster IP address, which automatically defaults to the Active node in the cluster.

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter the root password.

4 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

5 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - DCE Configuration
  4 - OAMP Application Configuration
  5 - CORBA Configuration
  6 - IP Configuration
  7 - DNS Configuration
  8 - Syslog Configuration
  9 - Remote Backup Configuration
 10 - Database Configuration
 11 - NFS Configuration
 12 - Bootp Configuration
 13 - Restricted Shell Configuration
 14 - Security Services Configuration
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

6 Enter the number next to the "DNS Configuration" option in the menu.

Example response

```
DNS Configuration
1 - turn_dns_on (Configure as DNS client)
2 - turn_dns_off (Turn off a system's DNS capability)
3 - enable_dnssvr (Configure as DNS server)
X - exit
select -
```

7 Enter the number next to the "turn_dns_off" option in the menu.

Example response

```
===Executing "turn_off_dns"
Do you really want to turn off DNS? (default:  No):
```

8 When prompted, confirm you want to turn off DNS capability by typing

`yes`

and pressing the Enter key.

Example response

```
Group registered
Stopping group using servstop
DNSSVR Stopped
DNS successfully turned off
```

```
==="turn_dns_off" completed successfully
```

9 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

—End—

Unconfiguring Domain Name Service on a Sun Server

Application

Use this procedure to turn off Domain Name Service (DNS) capability on a Sun server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the server on which you want to disable DNS

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number that corresponds to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number that corresponds to the "DNS Configuration" option in the menu.

Example response

```
DNS Configuration
  1 - turn_dns_on <Turn on a system's DNS
      capability>
2 - turn_dns_off <Turn off a system's DNS
       capability>
X - exit
select -
```

8 Enter the number that corresponds to the "turn_dns_off" option in the menu.

9 When prompted, confirm the command by typing

yes

and pressing the Enter key.

10 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

11 You have completed this procedure.

—End—

Configuring Client/Server Ports on an SPFS-Based Server for Secure Firewall Communications

Application

Use this procedure to configure the client-side and server-side ports on a Server Platform Foundation Software (SPFS) based server to facilitate secure firewall communication between client and server applications. You can also use this procedure to list the ports that are currently configured.

ATTENTION

The server-side port has a default value of 10080, and the client-side port has a default value of 10090. If the default value is acceptable, it is not necessary to configure the ports.

Prerequisites

The server-side port must have the same value across all offices in the network. If the ports do not have the same value, the client application GUIs will fail to launch.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation:

1 Telnet to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "Security Services Configuration" option in the menu.

Example response:

```
Security Services Configuration
1 - Socks Configuration
2 - IEMS Server Location Configuration
3 - PAM Configuration
X - exit
select -
```

8 Enter the number next to the "Socks Configuration" option in the menu.

Example response:

```
Socks Configuration
1 - config_socks (Modify Socks Security Service)
2 - list_socks (List Socks Security Service)
X - exit
select -
```

9 Enter the number next to the "list_socks" option in the menu to display the server-side and client-side Socks Proxy ports that are currently configured.

Example response:

```
The ports configured for use by socks are:
The Client side SOCKS Proxy will listen on port 10090
The Server side SOCKS Proxy will listen on port 10080
==="list_socks" completed successfully
```

10 Use the following table to determine how to proceed.

If you	Do
want to change the ports	Step 11
do not want to change the ports	you have completed this procedure

11 Enter the number next to the "config_socks" option in the menu.

Example response:

```
The changes of the server side port is a disruptive
action.  If the server side port is changed, the
SOCKS server and all dependent applications must be
restarted.
SOCKS ports in all offices must be configured to the
same port.  Misconfiguration will cause EMS clients to
not function.
Proceed with caution.
Enter the port the Server side SOCKS Proxy will listen
on.  Value must be within [1025 - 655351].  current
Value - 10080 [?, q]
```

12

ATTENTION

Changing the Socks server-side port requires a restart of the SOCKS server and all dependent applications.

Enter the server-side port, or press Enter to leave at the default value (10080).

Example response:

```
Leaving SERVER port at 10080
```

```
Enter the port the Client side SOCKS Proxy will listen
on.  Value must be within [1025 - 655351].  Current
value - 10090 [?, q]
```

13

ATTENTION
Changing the Socks client-side port requires that all client workstations already running the application GUIs, be restarted to use the new port.

Enter the client-side port, or press Enter to leave at default the value (10090).

Example response:

```
Leaving CLIENT port at 10090
Leaving both ports at configured values:
           Server side SOCKS Proxy port: 10080
           Client side SOCKS Proxy port: 10090
==="Config_socks" completed successfully
```

14 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

`select - x`

and pressing the Enter key.

15 Use the following table to determine how to proceed.

If you	Do
changed one or both ports	Step 16
did not change the port values	you have completed this procedure

16 Perform one or both of the following substeps depending on whether you changed the server-side or client-side port, or both.

a. After changing the server-side port, restart the Socks server and all dependent server applications (SESM, SAM21EM, and MG9KEM)

Refer to the*ATM/IP Solution-level Security and Administration* , NN10402-600 for the Socks server, SESM and SAM21 server applications. Refer to the *MG 9000 Security and Administration*, NN10162-611 for the MG 9000 Manager serer application. Refer to*Packet MSC Administration and Security* , NN20000-216, for the Socks and dependent server applications.

b. After changing the client-side port, restart any client workstations already running the application GUIs.

—End—

Configuring a Virtual IP Address on an SPFS-Based Server

Application

Use this procedure to configure a virtual IP address on a Server Platform Foundation Software (SPFS) based server. This procedure applies to simplex and high availability (HA) servers. An HA server refers to a Sun Netra 240 server pair.

A virtual IP address is required for the Audio Provisioning Server (APS), which resides on the same SPFS-based server as the CS 2000 Management Tools software (CS2M). A virtual IP address is also required for the Integrated Element Management System (IEMS) when the IEMS is on the same SPFS-based server as the CS 2000 Management Tools software (CS2M).

Prerequisites

You need the root user ID and password for the server on which you are configuring the virtual IP address.

Prerequisites for Core and Billing Manager 850

In order to perform this procedure, you must have the following authorization and access:

- You must be a user in a role group authorized to perform config-admin actions.
- You must obtain non-restricted shell access.

For more information about how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

Related procedures

Procedure	Document
Logging in to the CBM	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Requesting non-restricted shell access	*Core and Billing Manager 850 Security and Administration*, NN10358-611
Displaying actions a role group is authorized to perform	*Core and Billing Manager 850 Security and Administration*, NN10358-611

Action

Perform the following steps to complete this procedure.

ATTENTION
In a two-server configuration, perform the steps that follow on the Active server.

Step	Action

At your workstation

1 Log in to server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server on which you are configuring the virtual IP address

In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

2 When prompted, log in as root .

In a two-server configuration, ensure you are on the Active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

3 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
 1 - View
2 - Configuration
3 - Other
X - exit
select -
```

4 Enter the number that corresponds to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
```

```
  3- OAMP Application Configuration
  4- CORBA Configuration
  5- IP Configuration
  6- DNS Configuration
  7- Syslog Configuration
  8- Remote Backup Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

5 Enter the number that corresponds to the "IP Configuration" option in the menu.

Example response

```
IP Configuration
 1 - config_router (Configure Default
Router and Netmask)
 2 - config_data (Configure System Data IP Addresses)
 3 - ipsecike_config (Configure IPSec/IKE Rules)
 4 - Enable_2network (Enable Second Network
Interface)
 5 - Config_data_2network (Configure Second
Network IP Addresses
 6 - Disable_2network (Disable Second
Network     Interface)
X - exit
select -
```

6 Enter the number that corresponds to the "config_data" option in the menu.

Example response

```
===Executing "config_data"
WARNING: Changing the network settings will effect all
applications!  Improper network configuration will
result in loss of service!  Applications may require
restart or reconfiguration after network changes
CAUTION: You are not accessing this tool via the system
console.  Changing network configuration may disrupt
this session.
```

```
CAUTION: HTTPS Certificate is installed for web
services.  Changing the hostname or ip may require an
updated certificate.
hostname:          <hostname>
ip address:            <ip address>
Enter the hostname for this system [hostname]
```

7 When prompted, enter the hostname for this SPFS-based server, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter ip address for <hostname> [00.00.00.00]
```

8 When prompted, enter the IP address for this SPFS-based server, or press the Enter key to accept the default value if one is specified.

Example response

```
Configure additional ip address?  [yes]
```

9 When prompted, indicate whether you want to configure an additional IP address.

If you enter	Do
yes	step 12
no	step 15

10 When prompted, enter the virtual IP address you want to configure on this server, or press the Enter key to accept the default value if one is specified.

Example response

```
Enter application for ip address <ip address>
```

11 When prompted, enter the application name for the additional IP address you just specified, or press the Enter key to accept the default value if one is specified.

When configuring a virtual IP address for APS, the application name is APS. When configuring a virtual IP address for IEMS, the application name is IEMS.

The system allocates a hostname for each virtual IP address that is configured. The hostname is in the form of <spfs_primary_hostname-application>, for example, “wxe0s00j-iems” when the virtual IP address is set up for IEMS. Hostnames are stored in file” /etc/hosts” on the system.

Example response

```
Configure additional ip address?  [no]
```

12 Repeat step 11.

13 When prompted, confirm the settings by typing

```
ok
```

and pressing the Enter key.

*Example response on an **HA system***

```
The network changes have been made, however the cluster
requires a restart of both units.  The units must be
restarted in the below order.
1) Login as root on the console of the standby unit and
shut it down with the command: "shutdown -i 0 -y".
2)  After the standby unit has shutdown, restart the
active unit with the command: "shutdown -i 6 -y".
3) After the restart is complete, the new network
settings are in effect.
4) Boot the standby unit with the command "boot".
===="config_data" completed successfully
```

*Example response on a **simplex system***

```
The network changes have been made, however a restart
is required to use the new network settings.  Reboot to
ensure all applications are restarted.  Exit this "cli"
tool and reboot using the Solaris command "shutdown -i
6 -y".
===="config_data" completed successfully
```

14 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

If you have	Do
a simplex system	step 17 only
an HA system	step 18

15 Reboot the server by typing

```
# shutdown -i 6 -y
```

and pressing the Enter key.

You have completed this procedure.

At the console of the Inactive node

16 Log in to the inactive node through the console (port A) using the root user ID and password.

Ensure you are on the Inactive server by typing ubmstat. If *ClusterIndicatorACT* is displayed in the response, which indicates you are on the Active server, log out of that server and log in to the other server. The response must display *ClusterIndicatorSTBY*, which indicates you are on the Inactive server.

17 Shutdown the inactive node by typing

```
# shutdown -i 0 -y
```

and pressing the Enter key.

At the console of the active node

18 Log in to the active node through the console (port A) using the root user ID and password.

Ensure you are on the Active server by typing ubmstat. If *ClusterIndicatorSTBY* is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display *ClusterIndicatorACT*, which indicates you are on the Active server.

19 Restart the active node by typing

```
# shutdown -i 6 -y
```

and pressing the Enter key.

At the console of the Inactive node

20 Boot the inactive node by typing

```
# boot
```

and pressing the Enter key.

You have completed this procedure.

—End—

Setting the CS 2000 IP Address on an SPFS-Based Server

Application

Use this procedure to set the IP address of the Communication Server 2000 (CS 2000) on a Server Platform Foundation Software (SPFS) based server. You can also use this procedure to remove the IP address of the CS 2000 from the server.

Prerequisites

You must have the IP address for the CS 2000 that is associated with the SPFS-based server on which you are setting the IP address.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing **`> telnet <server>`** and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you are setting the CS 2000 IP address
2	When prompted, enter your user ID and password.
3	Change to the root user by typing **`$ su -`** and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Example response
	`Command Line Interface`
	`  1 - View`
	`2 - Configuration`

```
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "OAMP Application Configuration" option in the menu.

Example response

```
OAMP Application Configuration
   1 - sdm_conf (Configure SDM IP Address)
   2 - sdm_unconf (Unconfigure SDM IP Address)
   3 - sdmuser_conf (Configure SDM User)
   4 - sdmuser_unconf (Unconfigure SDM User)
   5 - cmClli_rediscovery (Re-discovery the
CM CLLI by SDM IP)
   6 - cmClli_conf (Configure CM_CLLI Address)
   7 - cmClli_unconf (Unconfigure CM_CLLI
IP         Address)
   8 - cm_conf (Configure CM IP Address)
   9 - cm_unconf (Unconfigure CM IP Address)
X - exit
select -
```

8 Use the following table to determine your next step.

If you are	Do
setting the CS 2000 IP address on the Sun server	step 9
removing the CS 2000 IP address from the Sun server	step 10

9 Set the CS 2000 IP address as follows:

a. Enter the number next to the "cm_conf" option in the menu.

Example response

```
===Executing "cm_conf"
CM IP:
Enter the CM IP Address (default:  ):
```

b. When prompted, enter the IP address for the CS 2000.

Example response

```
CM IP:      47.142.122.89
Enter "ok" to commit changes
  Enter "quit" to exit
  Enter anything else to re-enter settings
```

c. When prompted, commit the change by typing

ok

and pressing the Enter key.

Example response

```
==="cm_conf" completed successfully
```

d. Proceed to step 11.

10 Remove the CS 2000 IP address as follows:

a. Enter the number that corresponds to the "cm_unconf" option in the menu.

Example response

```
===Executing "cm_unconf"
CM IP: 47.142.122.89
CM IP address will be unconfigured
Enter "ok" to commit changes
 Enter "quit" to exit
 Enter anything else to re-enter settings
```

b. When prompted, commit the change by typing

ok

and pressing the Enter key.

Example response

```
==="cm_unconf" completed successfully
```

11 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

—End—

Creating or Modifying the Login Greeting Message on an SPFS-Based Server

Application

Use this procedure to create or modify the login greeting message on a Server Platform Foundation Software (SPFS) based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing **`> telnet <server>`** and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you want to modify the login greeting
2	When prompted, enter your user ID and password.
3	Change to the root user by typing **`$ su -`** and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Example response
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	`X - exit`
	`select -`

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
  Select -
```

7 Enter the number next to the "Login Session" option in the menu.

Example response

```
Login Session
1 - login_session_timeout (User Inactivity Timeout
Configuration)
2 - login_session_termination (User Termination Timeout
Configuration)
3 - login_session_reauthentication (User Reauthenticat
ion Disable Timeout Configuration)
4 - login_session_server (Login Session Master Server
Configuration)
5 - telnet_greeting (Telnet Login Greeting)
6 - login_retries (Login Retries Limit)
X - exit
select -
```

8 Enter the number next to the "telnet_greeting" option in the menu.

Example response

```
===Executing "telnet_greeting"
Telnet Login Greeting Message:
Authorized use only, activities logged.
Enter the Telnet Login Greeting Message.
```

```
Enter a blank line to end the message:
```

9 When prompted, enter the message. End the message with a blank line.

Example response

```
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

10 When prompted, commit the change by typing

`ok`

and pressing the Enter key.

Example response

```
==="telnet_greeting" completed successfully
```

11 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

—End—

Configuring the Apache Web Server for HTTPS Proxy

Application

Use this procedure to configure the Apache Web Server on a Server Platform Foundation Software (SPFS) based server for HTTPS proxy.

To perform this procedure for Session Server Lines, refer to the procedure *Linking the Provisioning and System Manager to SESM* in NN10437-111.

ATTENTION

The preferred location to configure the Apache Web Server for HTTPS proxy is on the SPFS-based server that hosts the Integrated Element Management System (IEMS). If the IEMS is not present in the network, configure the Apache Web Server for HTTPS proxy on the SPFS-based server that hosts the CS 2000 Management Tools.

You can provision a maximum of 100 IP addresses for use in HTTPS proxy.

Configuring the Apache Web Server for HTTPS proxy is applicable to the following components:

- Storage Management (STORM)
- Session Server Trunks
- Centrex IP Client Manager (CICM) and CICM Element Manager
- Session Server Lines

Prerequisites

This procedure has the following prerequisites:

- You need the root user ID and password for the SPFS-based server.
- If you are adding a component to the proxy, you need to know what entries are required for the component. If you do not know what entries are required, refer to the applicable Configuration document in the following list for specific instructions on how to add the component to the proxy:
  - *STORM Configuration Management*, NN10110-511
  - *Session Server Configuration Management*, NN10338-511
  - *CICM Configuration Management*, NN10240-511

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server on which you are configuring the proxy

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

6 Enter the number next to the "Configuration" option in the menu and press the enter key.

7 Enter the number next to the "Apache Proxy Configuration" option in the menu and press the enter key.

8 Use the following table to determine your next step:

If you want to	Do
add an entry in the proxy	step 9
delete an entry from the proxy	step 10
list the entries in the proxy	step 11
exit	step 12

9 Enter the number next to the "add_proxy_conf" option in the menu.

Follow the prompts to add the component to the proxy. If you do not know what entries are required, refer to the applicable Configuration document in the following list for specific instructions on how to add the component to the proxy:

ATTENTION
Using "x" and "X" for tagnames is not supported in SPFS.

- *STORM Configuration Management*, NN10110-511
- *Session Server Configuration Management*, NN10338-511
- *CICM Configuration Management*, NN10240-511

Return to step 8.

10 Enter the number next to the "del_proxy_conf" option in the menu, and follow the prompts to delete the component from the proxy.

Return to step 8.

11 Enter the number next to the "list_proxy_conf" option in the menu.

Return to step 8.

12 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Configuring Automated Data Backups on an SPFS-Based Server

Application

Use this procedure to view or change the configuration settings for an automated data backup on a Server Platform Foundation Software (SPFS) based server. The automated backup backs up Oracle and critical data.

ATTENTION

Log SSPFS320 is generated when an automated data backup fails. Refer to the *Carrier Voice over IP Fault Management Logs Reference document* (NN10275-909) for log details.

You can also schedule a full system backup that overwrites a previous one on a backup media or copy the last successful Oracle backup to DVD or tape when performing an automated data backup on an SPFS-based server. This functionality is designed for use in dark office' conditions where you need to copy backup data more than once before the backup media is ejected from the server. Refer to procedure "Configuring Dark Office Backups on an SPFS-Based Server" (page 409).

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you want to configure automated data backups
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su -`

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Response

```
Command Line Interface
 1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3- OAMP Application Configuration
  4- CORBA Configuration
  5- IP Configuration
  6- DNS Configuration
  7- Syslog Configuration
  8- Remote Backup Configuration
 9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "Database Configuration" option in the menu.

Example response

```
Database Configuration
 1 - change_db (Change Database Host)
 2 - change_orabackup (Configure database
      backup)
```

```
X - exit
select -
```

8 Enter the number next to the "change_orabackup" option in the menu.

Example response

```
===Executing "change_orabackup"
Current setting:
Automated Backup Enabled N
Backup Time      6:00 Hours
Enable Automated backup (default:  N):
```

9 When prompted, enter Y to enable automated backup or press the Enter key to accept the default value (N) to disable automated backup.

Example response

```
Set backup hour to:  (default:  22):
```

10 When prompted, enter the time you want the automated backup to occur, or press the Enter key to accept the default value.

Example response

```
New settings:
Automated Backup Enabled   Y
Backup Time               22:00 Hours
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

11 Commit the changes by typing

`ok`

and pressing the Enter key.

Example response

```
==="change_orabackup" completed successfully
```

ATTENTION

If enabled, automated backup will start within the first 45 seconds of the backup hour. If the backup hour is set to the current hour, automated backup will occur 24 hours from the current hour.

12 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

—End—

Setting the Threshold for File Systems on an SSPFS-Based Server

Application

Use this procedure to change the default threshold for a file system on a Succession Server Platform Foundation Software (SSPFS)-based server. The default threshold is 90%. An alarm is raised when the file system exceeds the specified threshold, and log SPFS350 is generated.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Telnet to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SSPFS-based server on which you are setting the file system threshold
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su - root` and pressing the Enter key.
4	When prompted, enter the root password.
5	Set the threshold by typing `# filesys update -m <mount_point> -a <threshold>` and pressing the Enter key. where **`mount_point`** is the directory of the file system you are setting the threshold for **`threshold`** is 0 to 99% (default is 90%)

Example
filesys update -m /data -a 80

The preceding example sets the threshold for the /data file system to 80%.

6 You have completed this procedure.

—End—

Configuring the destination for SNMP traps

Application

Use this procedure to configure the destination for SNMP traps on the Integrated Element Management System (IEMS) server and other Server Platform Foundation Software (SPFS) based servers that need to forward their SNMP traps to the Integrated Element Management System (IEMS) application.

Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password for the server on which you are configuring the destination for SNMP traps
- you need the IP address of the server where the Integrated Element Management System (IEMS) resides

  You can obtain the IEMS IP address to use as the destination for SNMP traps, by logging in to the IEMS server and executing the command "getpip.ksh IEMS".

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Log in to the SPFS-based server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

`IP address` is the IP address of the SPFS-based server on which you are configuring the destination for SNMP traps

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "Succession Element Configuration" option in the menu.

Example response:

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
```

```
  9 - OMPUSH Application Configuration
 10 - RESMON Application Configuration
X - exit
select -
```

8 Enter the number next to the "RESMON Application Configuration" option in the menu.

Example response

```
RESMON Application Configuration
   1 - settrapdest (Set location for IEMS traps)
   2 - queryFaults (Query all faults on the box)
   3 - enableLocalLogs (Enable Local Logging Of Faults)
   4 - disableLocalLogs (Disable Local
Logging Of Faults)
X - exit
select -
```

9 Enter the number next to the "settrapdest" option in the menu.

Example response

```
===Executing "settrapdest"
Enter the IEMS Server IP Address (default:  45.123.45
6.78):
```

10 When prompted, enter the IP address of the server where the IEMS resides, or press the Enter key to accept the default if one is specified.

You can obtain the IEMS IP address to use as the destination for SNMP traps, by logging in to the IEMS server and executing the command "getpip.ksh IEMS".

Example response

```
IEMS IP: 45.123.456.78
Enter "ok" to commit changes
Enter "quit" to exit
Enter anything else to re-enter settings
```

11 When prompted, confirm the IP address you entered by typing

`ok`

and pressing the Enter key.

Example response

```
==="settrapdest" completed successfully
RESMON Application Configuration
   1 - settrapdest (Set location for IEMS traps)
   2 - queryFaults (Query all faults on the box)
   3 - enableLocalLogs (Enable Local Logging Of Faults)
   4 - disableLocalLogs (Disable Local
Logging Of Faults)
```

```
X - exit
select -
```

12 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

`select - x`

and pressing the Enter key.

You have completed this procedure.

—End—

Configuring the SESM Server Application

Application

Use this procedure to configure the Succession Element and Sub-element Manager (SESM) server application.

ATTENTION
Only perform this procedure if you installed an HTTPS certificate after the CS2M software was installed or upgraded.

Prerequisites

Prior to performing this procedure, obtain the following information:

- the IP address of the CS 2000 Management Tools server
- the market for which you are configuring this application (North America or International)
- the CLLI name of the office (CM CLLI), and the IP address of the SDM (CS 2000 Core Manager)Packet SDMX (XA-Core manager) associated with the CLLI
- the IP address of the Media Gateway 9000 Manager if present in the network

ATTENTION
Only the root user can perform this procedure.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Telnet to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the CS 2000 Management Tools server
2	When prompted, enter your user ID and password.
3	Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Execute the configuration script by typing

```
# configure
```

and pressing the Enter key.

Example response

```
SESM_configuration
 1 - SESM common configuration (IP addresses,
market, CM CLLI
 2 - SESM database tools
 3 - SESM related applications configuration
 4 - SESM provisioning configuration
 5 - SESM logging  configuration (syslog,
sesm debug log)
 6 - view sesm configuration settings
 7 - SESM refresh properties
X - exit
select -
```

6 Enter the number next to the "SESM common configuration" option in the menu.

7 When prompted, enter the IP address of the CS 2000 Management Tools server, or press the Enter key to accept the default if one is specified.

8 When prompted, enter the number next to the market for which you are configuring the SESM server application.

9 When prompted, enter the CLLI name of the office (CM CLLI), or press the Enter key to accept the default if one is specified.

10 When prompted, enter the IP address of the SDM (CS 2000 Core Manager)Packet SDMX (XA-Core manager) associated with the CM CLLI, or press the Enter key to accept the default if one is specified.

The system displays the information you entered for confirmation.

11 When prompted, confirm the information by typing

```
y
```

and pressing the Enter key.

The system executes the command, and returns you to the SESM configuration main menu.

12 Exit "SESM configuration" by typing

```
select - x
```

and pressing the Enter key.

13 You have completed this procedure.

—End—

Setting up the PM Poller on an SPFS-Based Server

Application

Use this procedure setup the PM poller on a Server Platform Foundation Software (SPFS) based server. Setting up the PM poller on an SPFS-based server involves adding a device to a poller profile. Once complete, the PM poller will collect the performance information for the device you specified in this procedure.

The PM poller can gather performance information from the gateway controller (GWC), Universal Audio Server (UAS), SAM21 shelf controller, Media Server 2010 (MS 2010), and the SPFS.

For more details on the PM poller, refer to "PM poller" in *Basics (ATM Solution)* (NN10320-100) or *Basics (IP Solution)* (NN10300-100).

If you need to start the poller, refer to procedure "Starting the PM Poller" in *ATM/IP Security and Administration* (NN10402-600).

You can configure the SNMP defaults for a poller profile, which will be used by all devices associated with the profile, and you can set the polling interval. Refer to procedure "Configuring the SNMP Defaults for a Poller Profile and Setting the Polling Interval" (page 250) in this document.

Prerequisites

You must have a valid PM poller profile to which you can associate the device.

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Telnet to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you want to setup the PM poller
2	When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
  1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "snmp_poller" option in the menu.

The PM Poller Configuration Menu is displayed.

8 Add a device as follows:

a. Select "Add a device to a selected profile" using the up/down arrow key, and press the Enter key.

b. Enter the device name, and press the Enter key.

The Select Poller Profile Menu is displayed.

9 Select a profile as follows:

a. Select a profile using the up/down arrow key, and press the Enter key.

ATTENTION

The IPOA profile is for the SAM21 shelf controller OM configuration.

In order for data to be collected from the SAM21 shelf controller card, an ATM PCI card is required.

An X is placed next to the profile you selected.

b. Select "Accept this setting" using the up/down arrow key, and press the Enter key.

The Select Poller Device Type Menu is displayed.

10 Select the device type as follows:

a. Select the device type using the up/down arrow key, and press the Enter key.

An X is placed next to the device type you selected.

b. Select "Accept this setting" using the up/down arrow key, and press the Enter key.

The Add Device Menu is displayed.

11 Select the SNMP attributes as follows:

a. Select "Select SNMP Device Attributes" using the up/down arrow key, and press the Enter key.

The "Device Select SNMP Default Attributes Menu" is displayed.

b. Select the required or applicable attributes to include in the device configuration using the up/down arrow key, and press the Enter key after each. The table titled "Managed device SNMP

default attributes" (page 247), provides the default values for the SNMP attributes, and the device-specific SNMP attribute values.

Managed device SNMP default attributes

SNMP attribute [default]	SAM21SC	UAS	GWC	SPFS	MS 2010
AuthPass [none]	Not Required	Not Required	Not Applicable	Not Applicable	Not Applicable
AuthProto [MD5]	Not Applicable	Not Required	Not Applicable	Not Applicable	Not Applicable
Community (SNMP community name) [public]	private	Not Applicable	Contact Network Administrator	Contact Network Administrator	Contact Network Administrator
Context [none]	Not Applicable	Not Required	Not Applicable	Not Applicable	Not Applicable
ContexEngineId [SecEngineID]	Not Applicable	Not Required	Not Applicable	Not Applicable	Not Applicable
DestHost [none]	Physical IP address of unit 0 or 1 (configure a PM poller for each unit)	Physical IP address of domain 0 and domain 1	Physical IP address of unit 0 and unit 1	IP address of server where the CS 2000 Management Tools reside	IP address of MS 2010
PrivPass [none]	Not Applicable	Not Required	Not Applicable	Not Applicable	Not Applicable
PrivProto [DES]	Not Applicable	Not Required	Not Applicable	Not Applicable	Not Applicable
RemotePort [161]	161	161	161	1161	161
Retries [5]					
SecEngineId [none]	Not Applicable	Not Required	Not Applicable	Not Applicable	Not Applicable
SecLevel [noAuthNoPriv]	Not Applicable	noAuthNoPriv	Not Applicable	Not Applicable	Not Applicable
SecName [none]	Not Applicable	v3admin	Not Applicable	Not Applicable	Not Applicable
Timeout [1000000 micro seconds]					
UseNumeric [0]					
Version (SNMP version) [1]	2	3	2	1	2

An X is placed next to the attributes you selected.

c. Select "(Done with selections)" using the up/down arrow key, and press the Enter key.

The screen displays the attributes you selected and their default value if any.

d. Press any key to continue.

The Confirm Change Menu is displayed.

e. Confirm the action by pressing the Enter key.

f. Press any key to continue, which returns you to the Add Device Menu.

12 The SNMP attributes you specify for a device using this procedure will override the default SNMP attributes specified in the associated poller profile. Set the SNMP attributes as follows:

a. Select "Modify SNMP Device Attribute Value" using the up/down arrow key, and press the Enter key.

The SNMP Attribute Change Template is displayed.

b. Select the attribute you want to change using the up/down arrow key and change the value. When all values are correct, press the Enter key.

The screen displays the attributes and their value.

c. Press any key to continue.

The Confirm Change Menu is displayed.

d. Confirm the action by pressing the Enter key.

e. Press any key to continue, which returns you to the Add Device Menu.

f. Select "Done with configuration" using the up/down arrow key, and press the Enter key, which returns you to the PM Poller Configuration Menu.

If you	Do
want to add another device	step 8
do not want to add another device	step 13

13 Re-sync the poller as follows:

a. Select "Re-Sync the poller with new configuration" using the up/down key, and press the Enter key.

The Confirm Change Menu is displayed.

b. Confirm the action by pressing the Enter key.

c. Press any key to continue, which returns you to the PM Poller Configuration Menu

14 Exit the PM poller configuration and the command line interface as follows:

a. Select "Exit the Configuration Menu" using the up/down arrow key, and press the Enter key.

b. Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

At any time you can view the configuration data for a profile or a device. Refer to procedure "Viewing the Configuration Data for a Profile or Device" (page 255) in this document.

—End—

Configuring the SNMP Defaults for a Poller Profile and Setting the Polling Interval

Application

Use this procedure to configure the default SNMP attributes in a selected poller profile, and set the interval for the PM poller to collect data.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing **`> telnet <server>`** and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server that has the poller profile you want to configure
2	When prompted, enter your user ID and password.
3	Change to the root user by typing **`$ su - root`** and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Example response
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	`X - exit`
	`select -`

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "snmp_poller" option in the menu.

The PM Poller Configuration Menu is displayed.

8 Select "Configure SNMP defaults for a profile" using the up/down arrow key, and press the Enter key.

The Change Poller Profile Menu is displayed.

9 Select a profile using the up/down arrow key, and press the Enter key.

An X is placed next to the profile you selected.

10 Select "Accept this setting" using the up/down arrow key, and press the Enter key.

The Modify Profile Defaults Menu is displayed.

11 Select "Select SNMP attributes to include as default attributes" using the up/down arrow key, and press the Enter key.

The SNMP Profile Select SNMP Default Attributes Menu is displayed.

12 Select the attributes you want to include using the up/down arrow key. Press the Enter key after each selection.

Use the table provided in procedure " Setting up the PM Poller on an SPFS-Based Server" (page 244) as a reference to determine the required default SNMP attributes for the profile you are configuring.

An X is placed next to each attribute you select.

13 Select "Done with configuration" using the up/down arrow key, and press the Enter key.

The screen displays the attributes you selected and their default value if any.

14 Press any key to continue.

The Confirm Change Menu is displayed.

15 Confirm the action by pressing the Enter key.

16 Press any key to continue, which returns you to the Modify Profile Defaults Menu.

If you	Do
want to modify the default attribute values	step 17
do not want to modify the default attribute values	step 22

17 Select "Modify SNMP default attribute values" using the up/down arrow key, and press the Enter key.

The SNMP Attribute Change Template is displayed.

18 Select the attribute you want to change using the up/down arrow key and change the value. When all values are correct, press the Enter key.

The screen displays the attributes and their value.

19 Press any key to continue.

The Confirm Change Menu is displayed.

20 Confirm the action by pressing the Enter key.

21 Press any key to continue, which returns you to the Modify Profile Defaults Menu.

22 Use the following table to determine your next step.

If you	Do
want to modify the polling interval	step 23
do not want to modify the polling interval	step 27

23 Select "Modify polling interval" using the up/down arrow key, and press the Enter key.

The Change Polling Interval Menu is displayed.

24 When prompted, enter the polling interval time (default is 30 minutes), and press the Enter key.

ATTENTION
Setting the polling interval time to a value less than 15 for a profile with a large number of devices, will impact the required disk storage requirements for CSV output files.

The Confirm Change Menu is displayed.

25 Confirm the action by pressing the Enter key.

26 Press any key to continue, which returns you to the Modify Profile Defaults Menu.

27 Select "Done with configuration" using the up/down arrow key, and press the Enter key, which returns you to the PM Poller Configuration Menu.

28 Select "Re-sync the poller with new configuration" using the up/down arrow key, and press the Enter key.

29 When prompted, confirm you want to proceed with restarting the poller process by typing

```
y
```

and pressing the Enter key.

30 Select "Exit the Configuration Menu" using the up/down arrow key, and press the Enter key.

31 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Viewing the Configuration Data for a Profile or Device

Application

Use this procedure to view the configuration data for a specific PM poller profile or device.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the Sun server that has the PM poller profile you want to view

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the PM poller directory by typing

```
# cd /opt/nortel/snmp-poller/bin
```

and pressing the Enter key.

6 Use the following table to determine your next step.

If you want to view the configuration data for a	Do
profile	step 7
device	step 8

7 Display the configuration data for a profile by typing

```
# ./snmpp_ctl -qprofile <profile name>
```

and pressing the Enter key.

where

profile name is one of the following:
GWC
MIB-2
UAS
SPFS

8 Display the configuration data for a device by typing

```
# ./snmpp_ctl -qdevice <device name>
```

and pressing the Enter key.

where

device name is the name of the device

9 You have completed this procedure.

—End—

Deleting a Device from a PM Poller Profile

Application

Use this procedure to delete a device from a PM poller profile.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Telnet to the Sun server by typing **`> telnet <server>`** and pressing the Enter key. where **`server`** is the IP address or host name of the Sun server that has the PM poller profile from which you want to delete a device
2	When prompted, enter your user ID and password.
3	Change to the root user by typing **`$ su - root`** and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Example response
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	`X - exit`
	`select -`

6	Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "snmp_poller" option in the menu.

The PM Poller Configuration Menu is displayed.

8 Select "Delete a device from a selected profile" using the up/down arrow key, and press the Enter key.

9 Enter the device name, and press the Enter key.

The Delete Device Menu is displayed.

10 Select the device profile using the up/down arrow key, and press the Enter key.

An X is placed next to the device profile you selected.

11 Select "(Done with selections)" using the up/down arrow key, and press the Enter key.

12 Press any key to continue.

The Confirm Change Menu is displayed.

13 Confirm the action by pressing the Enter key.

14 Press any key to continue, which returns you to the PM Poller Configuration menu.

15 Select "Exit the Configuration Menu" using the up/down arrow key, and press the Enter key.

16 Exit each menu level of the command line interface to eventually exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

17 You have completed this procedure.

—End—

Creating an OMPUSH Session

Application

Use this procedure to create an OMPUSH session using one of the following two methods:

- "Create an OMPUSH session in menu mode" (page 260)
- "Create an OMPUSH session from the command line" (page 265)

You can create a maximum of six OMPUSH sessions.

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

OMPUSH Session Interval

OMC files are generated either in 5 and 30 minute, or 15 minute intervals, depending upon the configuration chosen. In order to send the right OMC files at the right time, configure the OMPUSH interval in sync with the OMC interval configuration. For example, if OMC is set to 5/30 and OMC is enabled at 5:00, configure OMPUSH interval to start at 5:05:22 so that the 5 minute file generated at 5:05 on the element manager is pushed immediately at 5:05:22 by OMPUSH.

Want to Delete (WTD)

A new variable - Want to Delete (WTD) - is introduced in (I)SN09U which is used to enable the Delete After Transfer functionality. If enabled, the files will be deleted from the MG9000 element manager. The default setting is to have this functionality disabled (no).

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Create an OMPUSH session in menu mode

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server on which you want to create the OMPUSH session

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
```

```
Select -
```

7 Enter the number next to the "Succession Element Configuration" option in the menu.

Example response:

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
  9 - OMPUSH Application Configuration
 10 - RESMON Application Configuration
  X - exit
select -
```

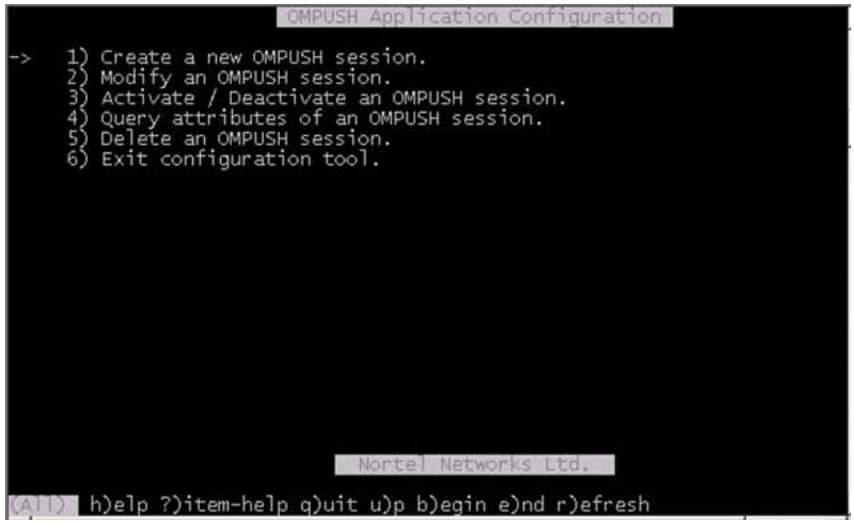
8 Enter the number next to the "OMPUSH Application Configuration" option in the menu.

Example response:

```
OMPUSH Application Configuration
1 - OMPUSH_cfg (OMPUSH configuration tool)
X - exit
select -
```

9 Enter the number next to the "OMPUSH_cfg" option in the menu.

Example response:



10 Type the number next to "Create a new OMPUSH session," or use the up/down arrow key, then press the Enter key.

Example response:

11 Type the number next to the desired source of OM files, or use the up/down key, then press the Enter key.

An X is placed next to the source you selected.

12 Type the number next to "Accept this setting", or use the up/down arrow key, then press the Enter key.

13 When prompted, enter the name of the session, and press the Enter key.

14 Use the following table to determine your next step.

If you	Do
want to modify the default transfer mode (FTP)	step 15
do not want to modify the transfer mode	step 16

15 Type the number next to "SSH File Transfer Protocol (SFTP)", or use the up/down arrow key, then press the Enter key.

An X is placed next to the transfer mode you selected.

16 Type the number next to "Accept this setting", or use the up/down arrow key, then press the Enter key.

Example response:

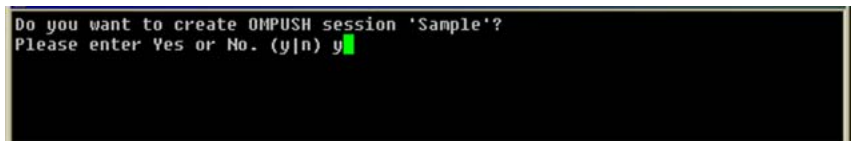
If the Delete After Transfer field is set to yes, the OM files from the MG9000 element manager will be deleted after transferring the files to the destination host. By default, Delete After Transfer is set to no.

17 Enter the session attributes as required, and press the Enter key when finished.

Changing the session name at this point is not supported. If you want to change the name, you need to delete this session and create a new one under the desired name.

If the password has expired on the destination host, the password needs to be updated in the OMPUSH session as well.

Example response:



18 Confirm you want to create this new session by typing

y

and pressing the Enter key.

If you	Do
want to create another session	step 10
do not want to create another session	step 19

19 Type the number next to "Exit configuration tool", or use the up/down arrow key, then press the Enter key.

You have completed this procedure.

—End—

Create an OMPUSH session from the command line

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server where you want to create the OMPUSH session

2 When prompted, enter your user ID and password.

3 Create a new session by typing

```
$ ompush_cfg -create <SessionName> <attribute=value>
```

and pressing the Enter key.

where

`SessionName` is the name of the session you want to create

`attribute=value` are the following attributes:
host=destination host (name or IP address)
user=FTP or SFTP user name
pwd=FTP or SFTP user password
src=source of OM files (MG9K or poller)
mode=transfer mode (FTP or SFTP)
port=FTP or SFTP service port (21 for FTP, or 22 for SFTP)
dir=upload directory for OM files on destination host (default is login directory for the user)
interval=session interval (in minutes)
start=session start day and time (mm/dd/yyyy hh:mm:ss)
wtd=user wants to delete the OM files immediately after FTP/SFTP (yes/no)

Example

```
ompush_cfg -create sample host=47.142.89.70
user=user1 pwd=user1psswd src=poller interval=20
wtd=no
```

—End—

Activating or Deactivating an OMPUSH Session

Application

Use this procedure to activate or deactivate an OMPUSH session using one of the following two methods:

- "Activate (deactivate) an OMPUSH session in menu mode" (page 266)
- "Activate (deactivate) an OMPUSH session from the command line" (page 270)

By default, an OMPUSH session is activated when it is created.

ATTENTION

When a session is deactivated, the session will not transfer any OM files to its destination host.

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Activate (deactivate) an OMPUSH session in menu mode

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that has the OMPUSH session you want to activate or deactivate

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the "Configuration" option number.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the "Succession Element Configuration" option number.

Example response:

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
```

```
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
  9 - OMPUSH Application Configuration
 10 - RESMON Application Configuration
X - exit
select -
```

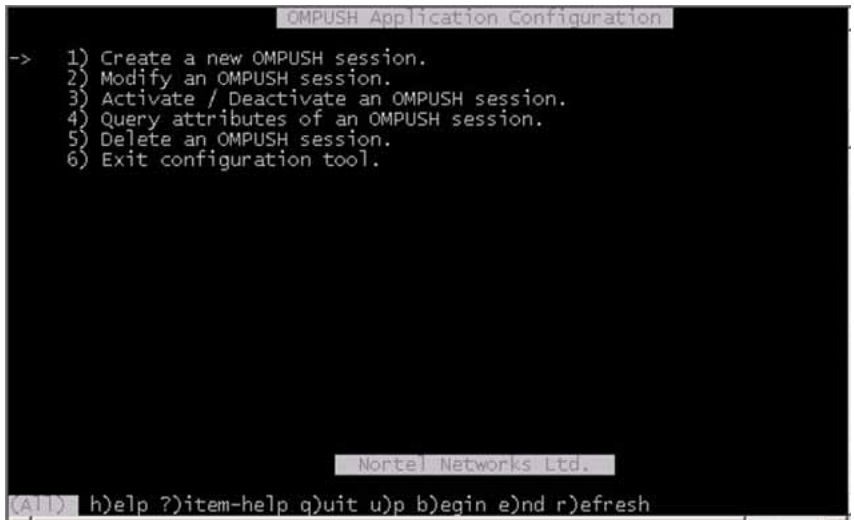
8 Enter the "OMPUSH Application Configuration" option number.

Example response:

```
OMPUSH Application Configuration
1 - OMPUSH_cfg (OMPUSH configuration tool)
X - exit
select -
```

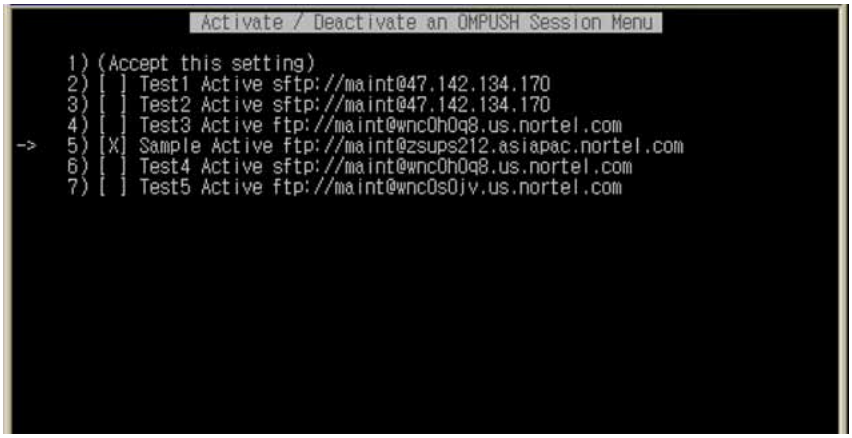
9 Enter the "OMPUSH_cfg" option number.

Example response:



10 Type the number next to "Activate/Deactivate an OMPUSH session", or use the up/down arrow key, then press the Enter key.

Example response:



All session items are shown in the following format:

<Session_Name> <Active/Inactive>
<TransMode>://<RemoteUser>@<Destination_Host>

11 Type the number next to the session you want to activate or deactivate, or use the up/down key, then press the Enter key.

An X is placed next to the session you selected.

12 Type the number next to "Accept this setting", or use the up/down arrow key, then press the Enter key.

13 Confirm you want to make the session Active or Inactive by typing

y

and pressing the Enter key.

14 Use the following table to determine your next step

If you	Do
want to activate or deactivate another session	step 10
do not want to activate or deactivate another session	step 15

15 Type the number next to "Exit configuration tool", or use the up/down arrow key, then press the Enter key.

You have completed this procedure.

—End—

Activate (deactivate) an OMPUSH session from the command line

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server that has the OMPUSH session you want to activate or deactivate

2 When prompted, enter your user ID and password.

3 Use the following table to determine your next step.

If you want to	Do
activate a session	step 4
deactivate a session	step 5

4 Activate a session by typing

```
$ ompush_cfg -activate <SessionName>
```

and pressing the Enter key.

where

`SessionName` is the name of the session you want to activate

5 Deactivate a session by typing

```
$ ompush_cfg -deactivate <SessionName>
```

and pressing the Enter key.

where

`SessionName` is the name of the session you want to deactivate

You have completed this procedure.

—End—

Modifying an OMPUSH Session

Application

Use this procedure to modify an OMPUSH session using one of the following two methods:

- "Modify an OMPUSH session in menu mode" (page 271)
- "Modify an OMPUSH session from the command line" (page 275)

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Modify an OMPUSH session in menu mode

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server that has the OMPUSH session you want to modify
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su -` and pressing the Enter key.
4	When prompted, enter the root password.
5	Access the command line interface by typing `# cli` and pressing the Enter key. *Example response*

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the "Configuration" option number.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the "Succession Element Configuration" option number.

Example response:

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
  9 - OMPUSH Application Configuration
 10 - RESMON Application Configuration
  X - exit
select -
```

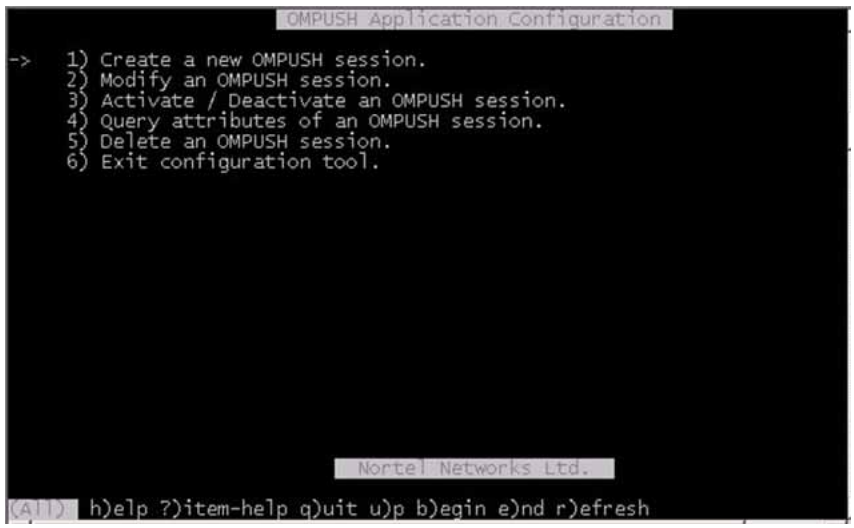
8 Enter the "OMPUSH Application Configuration" option number.

Example response:

```
OMPUSH Application Configuration
1 - OMPUSH_cfg (OMPUSH configuration tool)
X - exit
select -
```

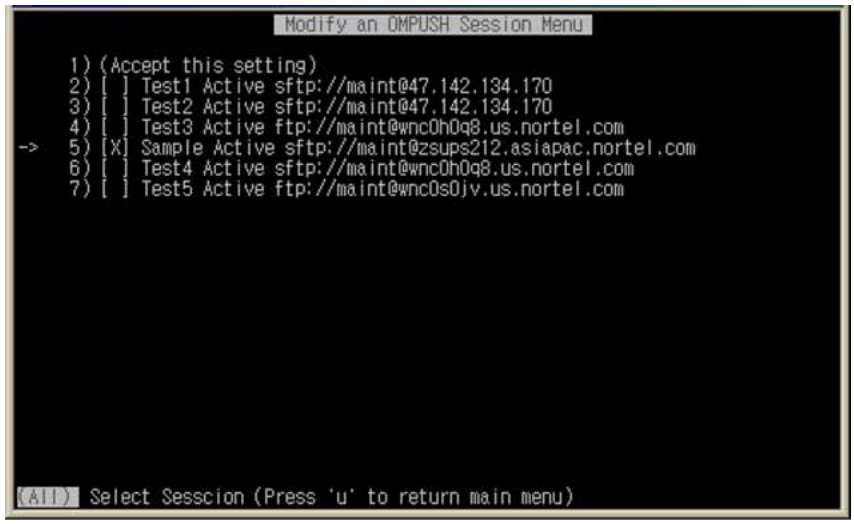
9 Enter the "OMPUSH_cfg" option number.

Example response:



10 Type the number next to "Modify an OMPUSH session", or use the up/down arrow key, then press the Enter key.

Example response:



All session items are shown in the following format:

```
<Session_Name> <Active/Inactive>
<TransMode>://<RemoteUser>@<Destination_Host>
```

11 Type the number next to the session you want to modify, or use the up/down key, then press the Enter key.

An X is placed next to the session you selected.

12 Type the number next to "Accept this setting", or use the up/down arrow key, then press the Enter key.

Example response:

13 Use the following table to determine your next step.

If you	Do
want to modify the transfer mode	step 14
do not want to modify the transfer mode	step 15

14 Type the number next to the transfer mode you want to use, or use the up/down key, then press the Enter key.

An X is placed next to the transfer mode you selected.

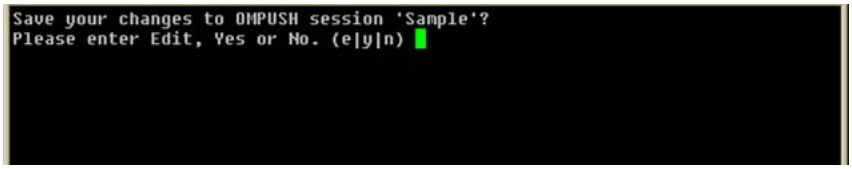
15 Type the number next to "Accept this setting", or use the up/down arrow key, then press the Enter key.

The OMPUSH session attributes are displayed.

16 Modify the session attributes as required, and press the Enter key when finished.

You can modify any of the attributes for a session except the session name.

Example response:



17 Save your modifications by typing

y

and pressing the Enter key.

If you	Do
want to modify another session	step 10
do not want to modify another session	step 18

18 Type the number next to "Exit configuration tool", or use the up/down arrow key, then press the Enter key.

You have completed this procedure.

—End—

Modify an OMPUSH session from the command line

Step Action

At your workstation

1 Log in to the server by typing

> telnet <server>

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that has the OMPUSH session you want to modify

2 When prompted, enter your user ID and password.

3 Modify a session by typing

$ ompush_cfg -modify <SessionName> <attribute=value>

and pressing the Enter key.

where

SessionName is the name of the session you want to modify
attribute=value is any of the following attributes:

- host=destination host (name or IP address)
- user=FTP or SFTP user name
- pwd=FTP or SFTP user password
- src=source of OM files (MG9K or poller)
- mode=transfer mode (FTP or SFTP)
- port=FTP or SFTP service port (21 for FTP, or 22 for SFTP)
- dir=upload directory for OM files on destination host (default is login directory for the user)
- interval=session interval
- wtd=user wants to delete the OM files immediately after FTP/SFTP (yes/no)

Example

```
ompush_cfg -modify sample mode=ftp port=21
interval=20 wtd=no
```

You have completed this procedure

—End—

Deleting an OMPUSH Session

Application

Use this procedure to delete an OMPUSH session using one of the following two methods:

- "Delete an OMPUSH session in menu mode" (page 277)
- "Delete an OMPUSH session from the command line" (page 280)

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Delete an OMPUSH session in menu mode

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server that has the OMPUSH session you want to delete
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su -` and pressing the Enter key.
4	When prompted, enter the root password.
5	Access the command line interface by typing `# cli` and pressing the Enter key. *Example response*

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the "Configuration" option number.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the "Succession Element Configuration" option number.

Example response:

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
  9 - OMPUSH Application Configuration
 10 - RESMON Application Configuration
  X - exit
select -
```

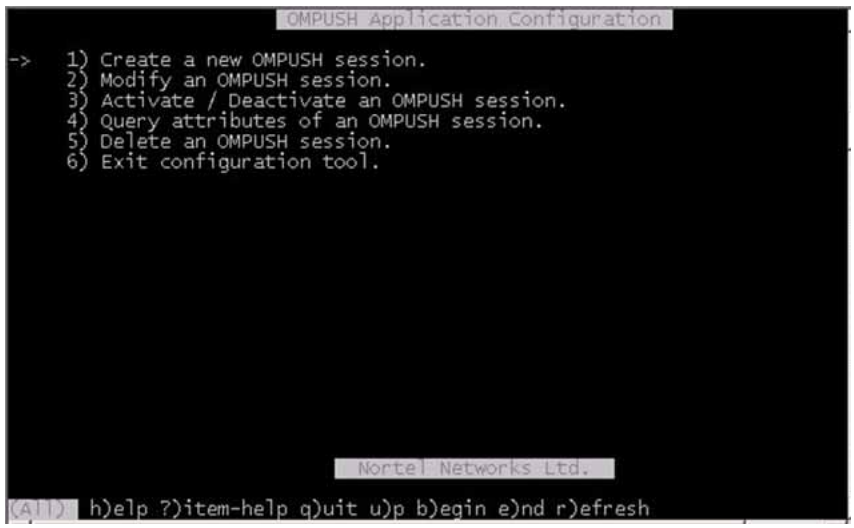
8 Enter the "OMPUSH Application Configuration" option number.

Example response:

```
OMPUSH Application Configuration
1 - OMPUSH_cfg (OMPUSH configuration tool)
X - exit
select -
```

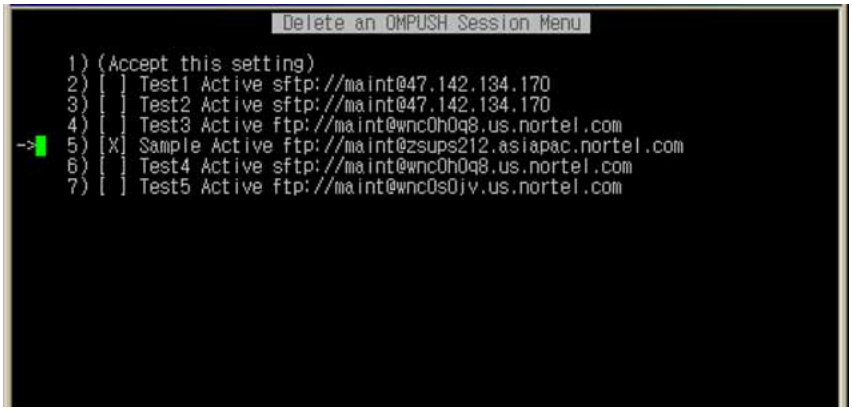
9 Enter the "OMPUSH_cfg" option number.

Example response:



10 Type the number next to "Delete an OMPUSH session", or use the up/down arrow key, then press the Enter key.

Example response:



All session items are shown in the following format:

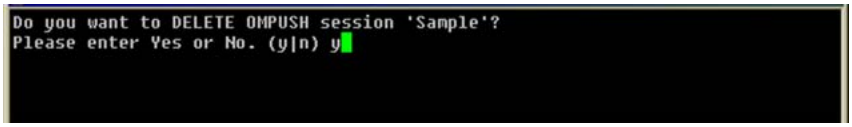
<Session_Name> <Active/Inactive>
<TransMode>://<RemoteUser>@<Destination_Host>

11 Type the number next to the session you want to delete, or use the up/down key, then press the Enter key.

An X is placed next to the session you selected.

12 Type the number next to "Accept this setting", or use the up/down arrow key, then press the Enter key.

Example response:



13 Confirm you want to delete the session by typing

```
y
```

and pressing the Enter key.

ATTENTION
If the session is running, the system will not allow you to delete it.

14 Use the following table to determine your next step

If you	Do
want to delete another session	step 10
do not want to delete another session	step 15

15 Type the number next to "Exit configuration tool", or use the up/down arrow key, then press the Enter key.

You have completed this procedure.

—End—

Delete an OMPUSH session from the command line

Step	Action

At your workstation

1 Telnet to the Sun server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the Sun server that has the OMPUSH session you want to delete

2 When prompted, enter your user ID and password.

3 Delete a session by typing

```
$ ompush_cfg -delete <SessionName>
```

and pressing the Enter key.

where

SessionName is the name of the session you want to delete

You have completed this procedure.

—End—

Querying OMPUSH Session Attributes

Application

Use this procedure to query the attributes of an OMPUSH session using one of the following two methods:

- "Query OMPUSH session attributes in menu mode" (page 282)
- "Query OMPUSH session attributes from the command line" (page 285)

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

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Query OMPUSH session attributes in menu mode

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server that has the OMPUSH sessions you want to query
2	When prompted, enter your user ID and password.
3	Change to the root user by typing `$ su -` and pressing the Enter key.
4	When prompted, enter the root password.
5	Access the command line interface by typing `# cli` and pressing the Enter key. *Example response*

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the number next to the "Succession Element Configuration" option in the menu.

Example response:

```
Succession Element Configuration
  1 - RADSVR Application Configuration
  2 - S1IS Application Configuration
  3 - CSMCLEANUP Application Configuration
  4 - NPM Application Configuration
  5 - SESM Application Configuration
  6 - SAM21EM Application Configuration
  7 - PSE Application Configuration
  8 - DDMSProxy Application Configuration
  9 - OMPUSH Application Configuration
 10 - RESMON Application Configuration
  X - exit
select -
```

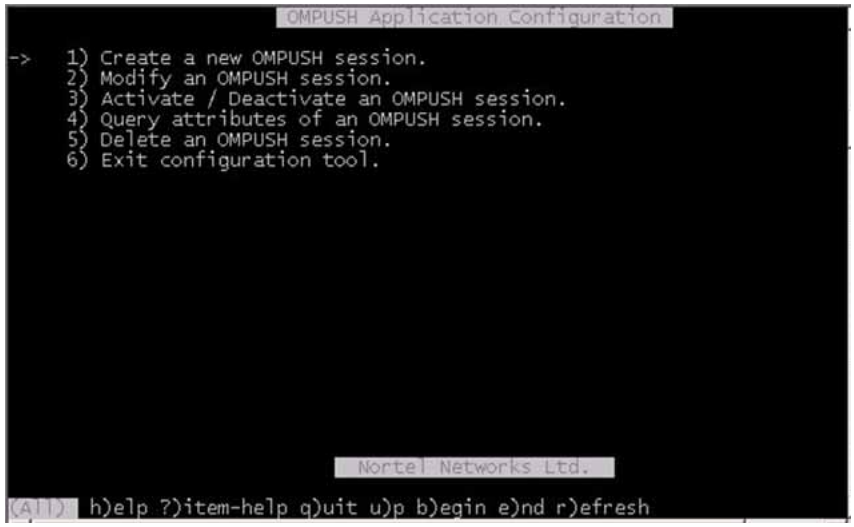
8 Enter the number next to the "OMPUSH Application Configuration" option in the menu.

Example response:

```
OMPUSH Application Configuration
1 - OMPUSH_cfg (OMPUSH configuration tool)
X - exit
select -
```

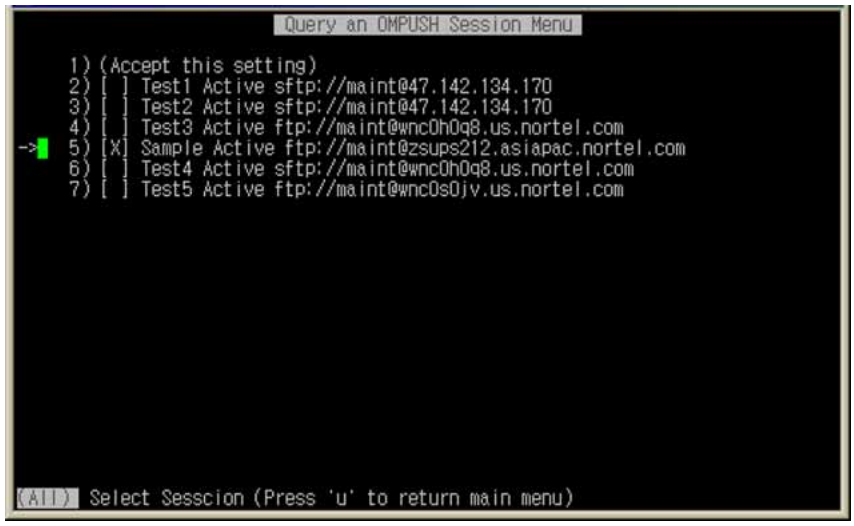
9 Enter the number next to the "OMPUSH_cfg" option in the menu.

Example response:



10 Type the number next to "Query attributes of an OMPUSH session", or use the up/down arrow key, then press the Enter key.

Example response:



All session items are shown in the following format:

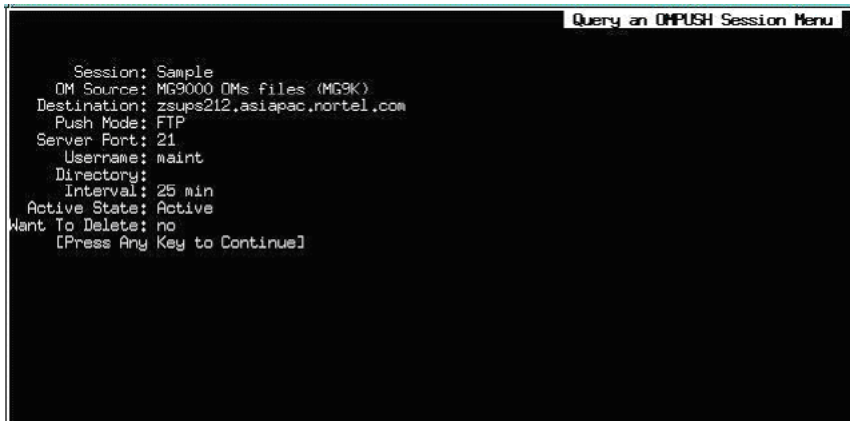
```
<Session_Name> <Active/Inactive>
<TransMode>://<RemoteUser>@<Destination_Host>
```

11 Type the number next to the session you want to query, or use the up/down key, then press the Enter key.

An X is placed next to the session you selected.

12 Type the number next to "Accept this setting", or use the up/down arrow key, then press the Enter key.

Example response:



13 Press any key to return to the main menu.

If you	Do
want to query another session's attributes	step 10
do not want to query another session's attributes	step 14

14 Type the number next to "Exit configuration tool", or use the up/down arrow key, then press the Enter key.

You have completed this procedure.

—End—

Query OMPUSH session attributes from the command line

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server that has the OMPUSH sessions you want to query

2 When prompted, enter your user ID and password.

3 Query an OMPUSH session by typing

```
$ ompush_cfg -query <SessionName>
```

and pressing the Enter key.

where

SessionName is the name of the session you want to query

If you do not specify the session name, the system will display the details for all existing sessions.

You have completed this procedure.

—End—

Setting the CM CLLI on the TMM

Application

Use this procedure to set the CLLI of the Communication Server 2000 on the Trunk Maintenance Manager (TMM) by setting the IP address of the XA-Core manager (SDM/CBM), which automatically retrieves the associated CM CLLI. If there are no communication problems with the Communication Server 2000, the IP address of the XA-Core manager (SDM/CBM) and the associated CM CLLI are automatically set during the TMM GUI startup.

Prerequisites

You need the IP address of the XA-Core manager (SDM/CBM).

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the TMM GUI. Refer to procedure "Launching CS 2000 Management Tools and NPM Client Applications" (page 292) in this document, if required.
	At the TMM GUI
2	Click the **CM Clli** link on the left side of the page.

3 Enter the IP address for the XA-Core manager (SDM/CBM), and click **Ok**.

ATTENTION

The CM CLLI associated with the IP address of the XA-Core manager (SDM/CBM) is automatically retrieved.

You have completed this procedure.

—End—

Setting the TMM Auto-Refresh Value

Application

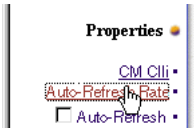
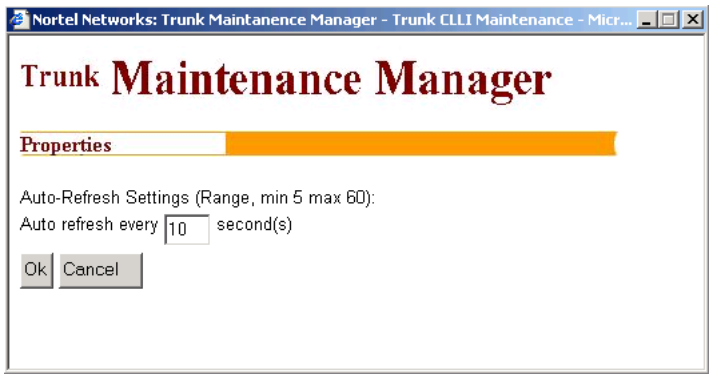
Use this procedure to set the value for the auto refresh rate.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the TMM GUI. If required, refer to procedure "Launching CS 2000 Management Tools and NPM Client Applications" (page 292).
	At the TMM GUI
2	Click the **Auto-Refresh Rate** link on the left side of the window. 
3	Enter a new value and click **Ok**.  You have completed this procedure.

—End—

Turning TMM Auto-Refresh On or Off

Application

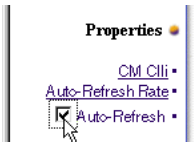
Use this procedure to toggle auto-refresh.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the TMM GUI. If required, refer to procedure "Launching CS 2000 Management Tools and NPM Client Applications" (page 292).
	At the TMM GUI
2	Select the **Auto-Refresh** check box on the left side of the page. 
	You have completed this procedure.

—End—

Setting the TMM Confirmation for the Busy Command

Application

Use this procedure to turn confirmation for the busy command on or off. When turned on, the user will be prompted to confirm the busy command when attempting to busy an entire posted set of trunks.

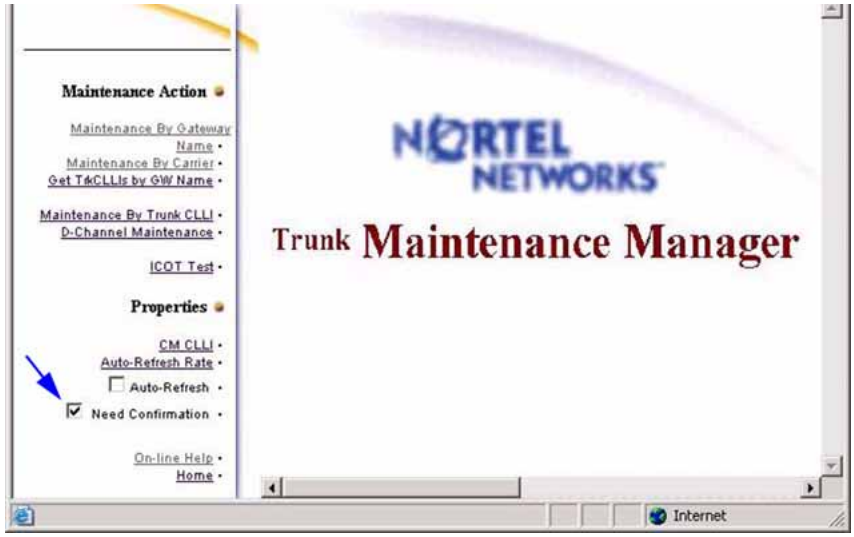
Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Access the TMM GUI. If required, refer to procedure "Launching CS 2000 Management Tools and NPM Client Applications" (page 292).
	At the TMM GUI
2	Check the **Need Confirmation** checkbox.



You have completed this procedure.

—End—

Launching CS 2000 Management Tools and NPM Client Applications

Application

Use this procedure to launch any one of the following client applications:

- Trunk Maintenance Manager (TMM)
- CS2000 Management Tools (CMT)
- Line Maintenance Manager (LMM)
- SAM21 Element Manager (SAM21 EM)
- Batch Configuration Monitor (BCM)
- Network Patch Manager (NPM)

ATTENTION

This only applies when the NPM is installed and enabled on the same SPFS-based server as CS 2000 Management Tools.

The NPM also has its own command line user interface (CLUI). Refer to procedure "Accessing the network patch manager CLUI" (page 303).

This procedure provides the following four methods to launch a CS 2000 Management Tools client application:

1. "Launch applications from a web browser" (page 294).

ATTENTION

You must use method one to launch an application for the first time.

You cannot use launch methods two through four to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

2. "Launch applications from the JWS Application Manager" (page 296).
3. "Launch applications from a desktop icon or Start menu (Windows only)" (page 298)
4. "Launch specific applications using a URL" (page 300).

You can also launch applications from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to document *IEMS Basics* (NN10329-111).

Prerequisites

- Ensure the client workstation meets the minimum requirements. Refer to section "Client workstation requirements" under "CS 2000 Management Tools" in the Basics document for your solution.
-
- Make sure the client workstation meets the minimum requirements.

CAUTION

If you have an ATI Radeon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you can experience the "blue screen of death" in your Windows environment. You can obtain information on this issue at the following website:

http://developer.java.sun.com/developer/bugParade/bugs/4713003.html

A workaround for this issue is to download the latest ATI graphics driver from the following web site:

http://mirror.ati.com/support/driver.html

Contact your IT support team if you need assistance.

You need the IP address or host name of the SPFS-based server where the CS 2000 Management Tools are installed, and a valid user name and password to launch an application.

ATTENTION

Users of the CS 2000 Management Tools client applications must belong to the primary user group "succssn" for login access, and to one or more secondary user groups, which specify the operations a user is authorized to perform. If required, refer to procedure "Setting up local user accounts on an SPFS-based server" in *ATM/IP Security and Administration* (NN10402-600)

You must have JavaTM 2 Runtime Environment (JRE) version 1.4.2_08 and JavaTM Web Start (JWS) version 1.4.2_08 installed to launch the following applications:

- CS 2000 Management Tools
- Line Maintenance Manager
- CS 2000 SAM21 Manager
- Network Patch Manager

Action

Launch applications from a web browser

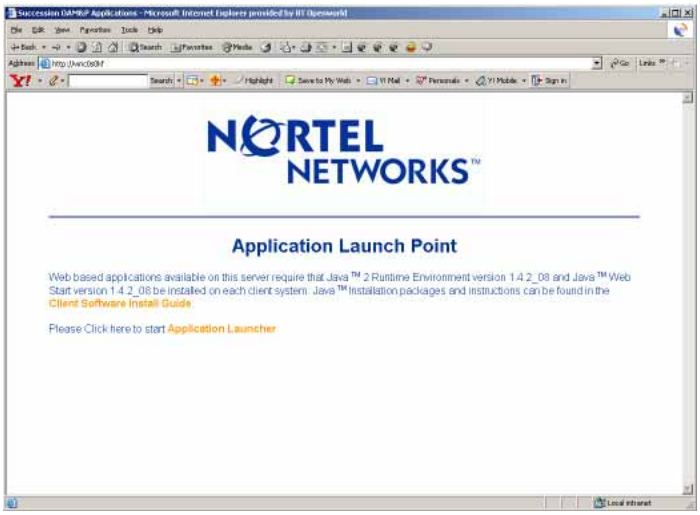
Step	Action

At your workstation

1 Launch your web browser.

2 In the Address field, enter the name or IP address of the SPFS-based server where the CS 2000 Management Tools are installed.

The Application Launch Point page appears.



3 Use the following table to determine your next step.

If	Do
you have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 9
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 4
you do not know which version of JRE and JWS you have	step 4

4 Click **Client Software Install Guide** and follow the instructions under How to check version to verify your client setup.

If	Do
you have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 8
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed	step 5

5 Click **Java 2 Runtime Environment Install Guide** under Microsoft Windows or Sun Solaris for system requirements and installation instructions.

6 Once you have read through the Java 2 Runtime Environment Install Guide, click **Back** to return to the Client Software Installation page.

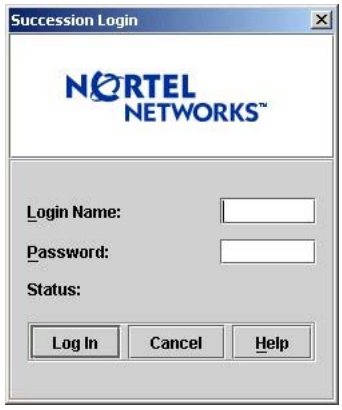
7 Click **Java 2 Runtime Environment Software Download** under Microsoft Windows or Sun Solaris to download and install the software.

ATTENTION
You must have administrative privileges to install the software on the workstation.

8 Click **Back** to return to the Application Launch Point.

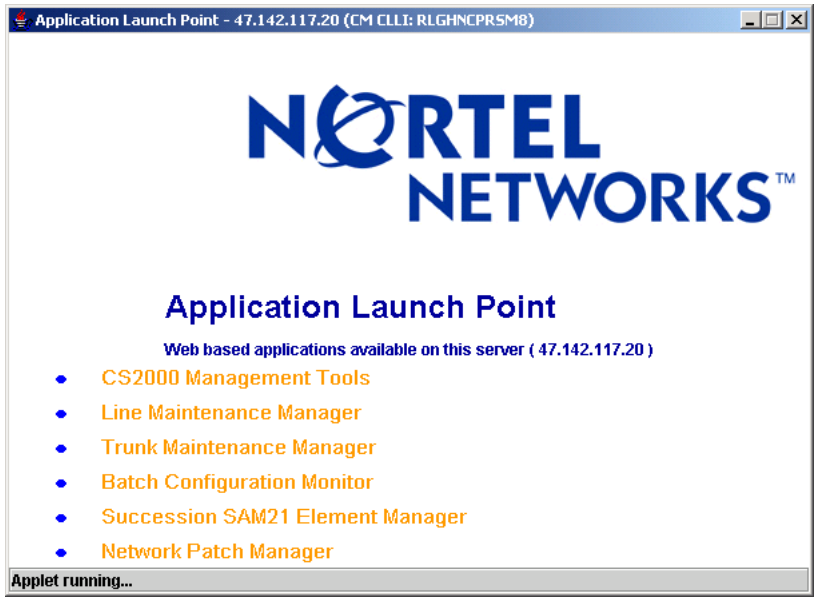
9 Click **Application Launcher**.

The Login window appears.



10 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.



11 Click the link for the application you want to launch.

If you delay clicking an application link by 5 minutes or more after you log in, the login window will appear requiring you to log in again.

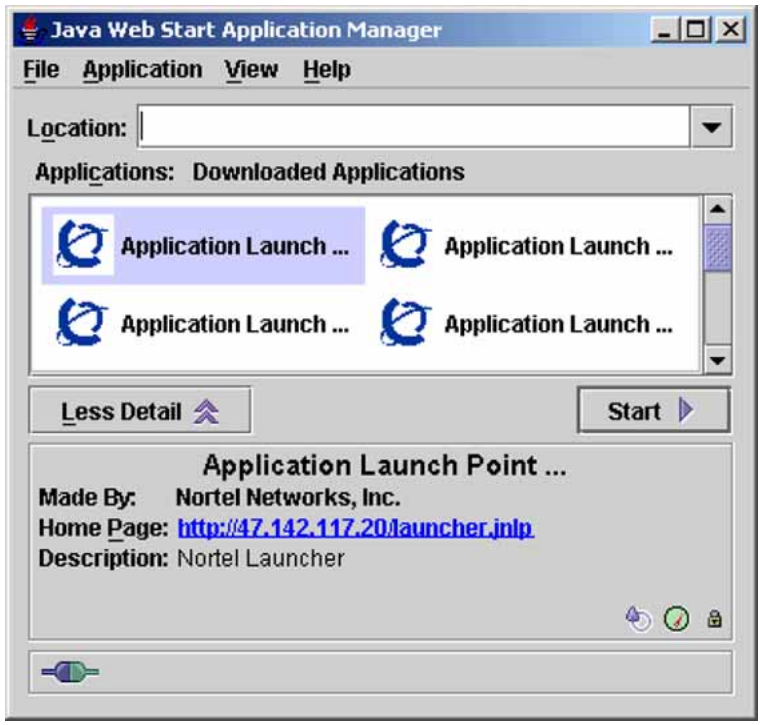
The interface for the application you launched, is displayed.

12 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Launch applications from the JWS Application Manager

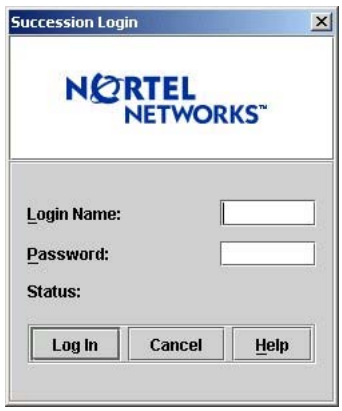
Step	Action
	At your workstation
1	Launch the Java Web Start Application Manager.



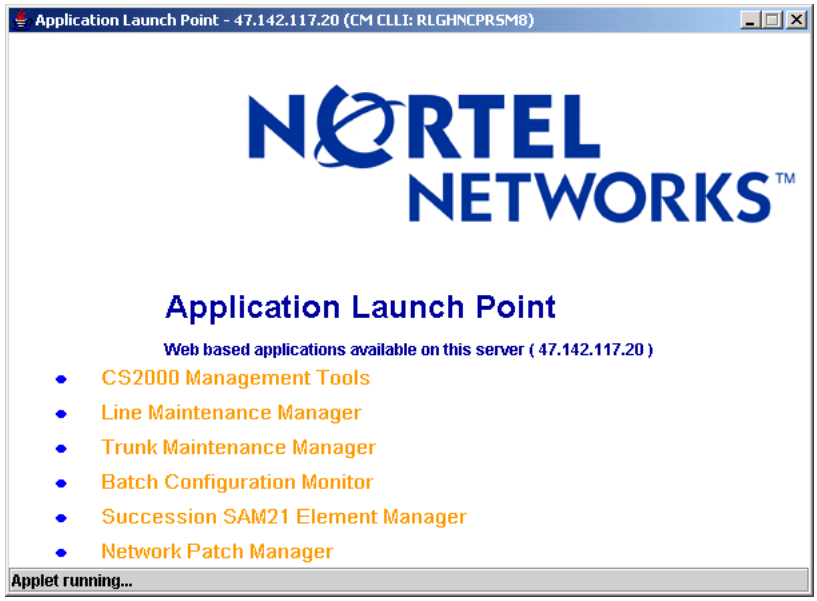
2 If you do not see the downloaded applications as shown in the previous figure, then on the View menu click **Downloaded Applications**. Otherwise, skip to the next step.

3 Double-click the Application Launch Point you want to access, or select the Application Launch Point and click Start.

The Login window appears.



4 Enter your user name and password, then click Log In. The Application Launch Point, similar to following, appears.



5 Click the link for the application you want to launch.

The interface for the application you launched, is displayed.

6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

—End—

Launch applications from a desktop icon or Start menu (Windows only)

Step	Action

At your workstation

1 Use the following table to determine your next step.

If you want to launch an application from …	Do
… a desktop icon	step 2
… the Start menu	step 4

2 To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double-click it to start the application.

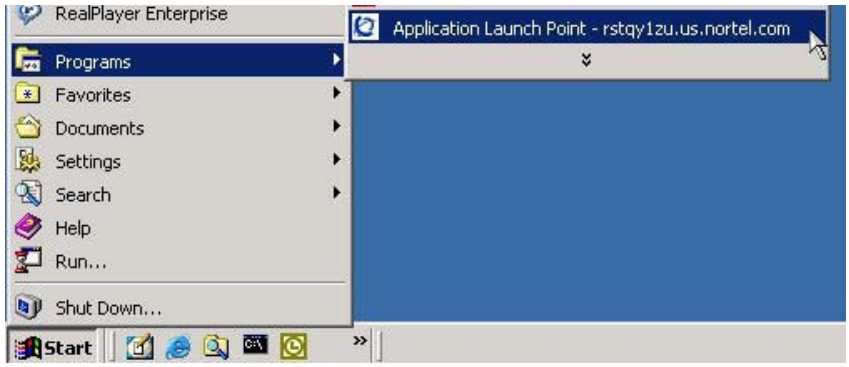
ATTENTION

For short-cut icons to be present on your desktop, you must have the correct settings under the Shortcut Options tab. Access the Shortcut Options tab through File->Preferences in the JWS Application Manager.

The Login window appears.

3 Proceed to step 5.

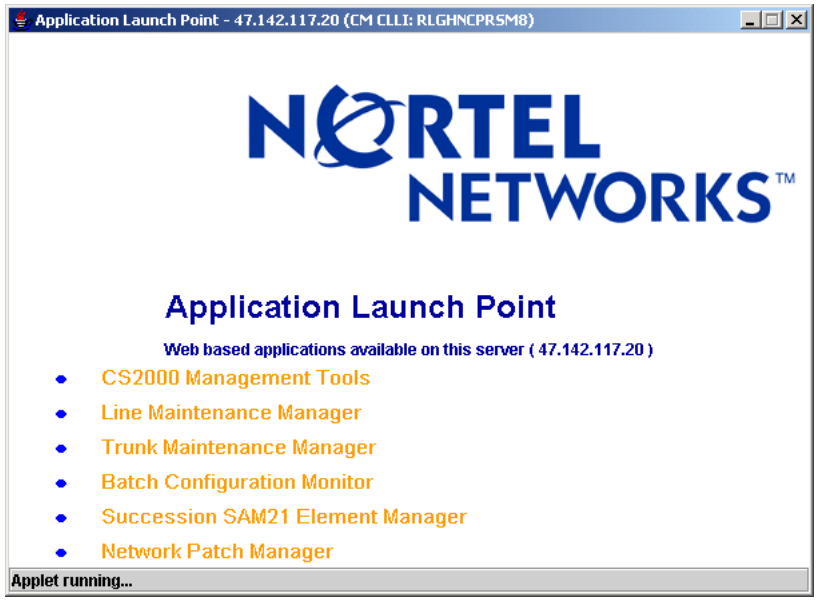
4 To launch a CS 2000 Management Tools client application from the Start menu, click Start->Programs, then click the CS 2000 Management Tools client application you want to launch.



The Login window appears.

5 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.



6 Click the link for the application you want to launch.

The interface for the application you launched, is displayed.

7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

ATTENTION

You can use this method to launch the CS2000 Management Tools, Line Maintenance Manager (LMM), Network Patch Manager (NPM), and CS2000 SAM21 Manager client applications, but not the Trunk Maintenance Manager (TMM) or Batch Configuration Monitor.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.2_08 and Java™ Web Start (JWS) version 1.4.2_08 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in the "Launch applications from a web browser" (page 294) procedure.

—End—

Launch specific applications using a URL

Step	Action

At your workstation

1 Launch your web browser.

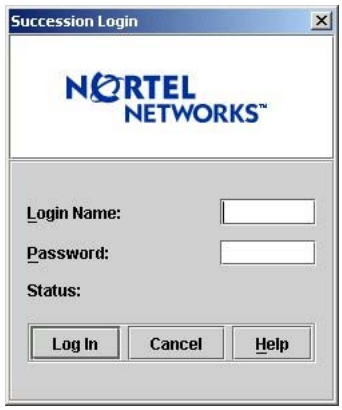
2 In the Address field, enter one of the following URLs for the application you want to launch:

Application	URL
CS2000 Management Tools	http://<host>:8080/launch/servlet/Launch?app=sesm
Line Maintenance Manager	http://<host>:8080/launch/servlet/Launch?app=lmm
CS2000 SAM21 Manager	http://<host>:8080/launch/servlet/Launch?app=sam21em
Network Patch Manager	http://<host>:8080/launch/servlet/Launch?app=npm

where

host is the host name or IP address of the SPFS-based server where the application resides

The Login window appears.



3 Enter your user name and password, then click **Log In**.

The interface for the application you launched, is displayed.

4 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and SAM21 Manager) connect to their corresponding server-side application through a Socks proxy.

The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

When you launch a client application that connects through a Socks proxy, you can receive an error message indicating that the Socks connection to the server has failed, the server is down and needs to be rebooted. Once the server has rebooted, you can relaunch the client application.

Accessing the network patch manager CLUI

Application

Use this procedure to access the Network Patch Manager (NPM) command line user interface (CLUI).

You can also access the NPM CLUI from the Integrated Element Management System (IEMS) when the IEMS is present in the office. Refer to *IEMS Basics*, NN10329-111.

The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure" Launching CS 2000 Management Tools and NPM Client Applications" (page 292) .

Prerequisites

You must have a valid user ID and password to access the NPM interface. In addition, you must be assigned to user group emsadm to perform patching activities using the NPM. If required, refer to procedure “Setting up local user accounts on an SPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.

Action

Perform the following steps to complete this procedure.

Step	Action

At your workstation

1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step 2
ssh (secure)	step 3

2 Log in to the server using telnet (unsecure) as follows:

a. Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

`server` is the IP address or host name of the SPFS-based server

b. When prompted, enter your user ID and password.

Proceed to step 4.

3 Log in using ssh (secure) as follows:

a. Log in to the server by typing

```
> ssh -l <userID> <server>
```

and pressing the Enter key.

where

server is the IP address or host name of the SPFS-based server

If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter **yes** at the prompt.

b. When prompted, enter your password.

4 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

5 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode:  Enter npm' commands, help or quit
to exit.
npm>
```

6 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

—End—

Clearing the JWS Cache on a Client Workstation

Application

Use this procedure to clear the Java™ Web Start (JWS) cache on a client workstation.

The JWS cache on a client workstation needs to be cleared after an HTTPS certificate is installed on an existing Sun server that was not previously using a certificate. Clearing the cache allows you to properly launch the CS 2000 Management Tools client applications from your workstation.

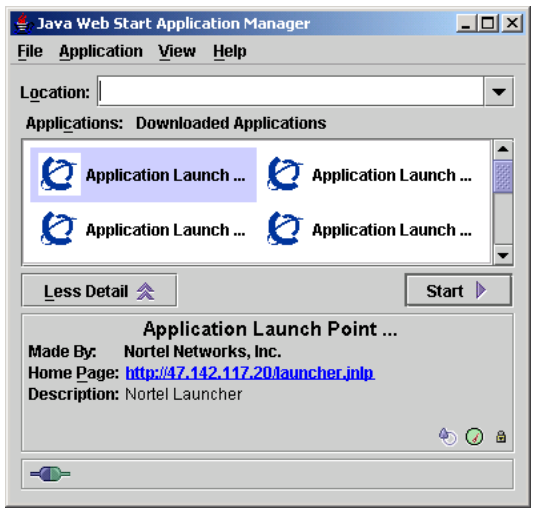
Prerequisites

None

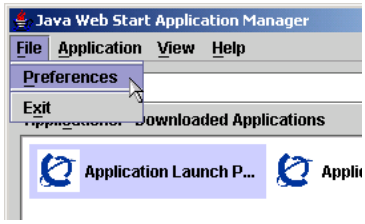
Action

Perform the following steps to complete this procedure.

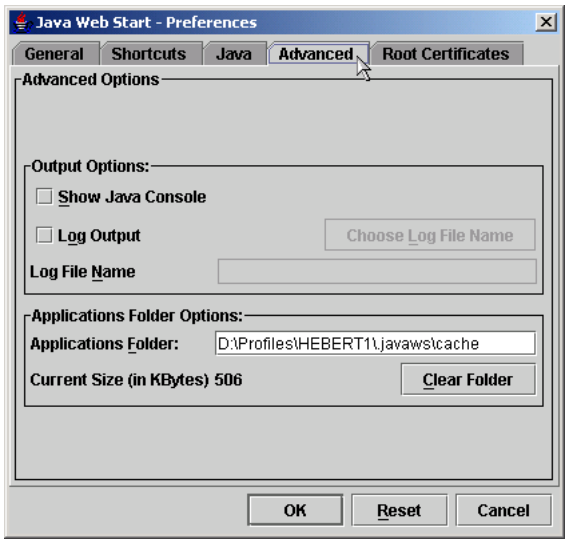
Step	Action
	At your workstation
1	Access the Java Web Start Application Manager.



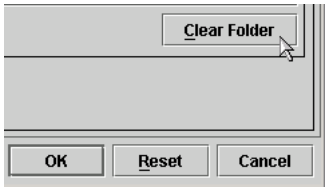
2	Click **File->Preferences** to access the Preferences window.



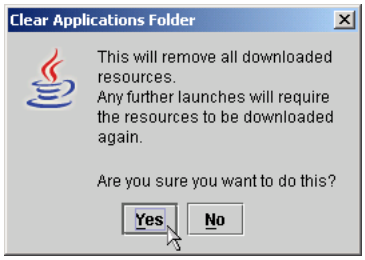
3 Click the **Advanced** tab to access the Advanced window.



4 Click **Clear Folder** to clear the cache.



5 Click **Yes** to confirm you want to clear the cache (remove all downloaded resources).



6 Click **OK** to close the Preferences window.

7 Exit the Java Web Start Application Manager.

You have completed this procedure.

—End—

ATM/IP Solutions Client Configuration

This document describes the requirements for the Client PC that must be met to correctly run the client applications for ATM and IP solutions. It also provides procedures for installing, configuring, and validating the applications.

Client PC requirements

This section lists the platform and browser requirements for client workstations.

Note: Nortel recommends the use of Nortel-verified browser and operating system combinations. Use of other versions are not supported. Any compatibility issues will not be resolved using standard Nortel support processes.

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

Note: PCs configured with dual Network Interface Cards (NICs) are not supported. The client may be configured only with a single NIC.

Platform

Table "Client workstation platforms" (page 309) lists the workstation platform and operating system for each client application.

Client workstation platforms

Application	Invocation	Platform	Operating System
IEMS (JWS mode)	Browser (JWS)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
IEMS (HTTP mode)	Browser (HTML)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
CS 2000 Core Mgr Clients • ATA • ETA • SFT	Desktop	Sun	Solaris 2.7, 2.8, 2.9 to current
CS 2000 Core Mgr/ CBM Clients • Telnet • SSH	Telnet/SSH	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
CS 2000 SAM21 Mgr	Browser (JWS)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
CS 2000 Mgmt Tools	Browser (HTML)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
CS 2000 GWC Mgr	Browser (JWS)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
UAS Mgr	Browser (JWS)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
LMM	Browser (JWS)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current

Application	Invocation	Platform	Operating System
Nodes Provisioning	Browser (JWS)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
NPM	Browser (JWS)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
NPM CLUI	Telnet/SSH login	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
MG 9000 Mgr	• Browser (JWS) install • Desktop runtime	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
MG 9000 LCI	Browser	PC	Windows 2000, XP, 2003 to current
Trunk Provisioning	Telnet/SSH Login	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
Line Provisioning	Telnet/SSH Login	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
Nodes Provisioning	Telnet/SSH Login	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
USP Mgr (clients outside CO)	Desktop (Citrix Metaframe 1.8)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
APS Mgr	Browser	PC	Windows 2000, XP, 2003 to current
STORM Mgr	Browser (Proxy)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
Call Agent Mgr	Telnet (Proxy)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
MDM/MDP (supported)	Desktop (X.11)	Sun	Solaris 2.7, 2.8, 2.9 to current
MDM/MDP (unsupported)	Desktop (Exceed)	PC	Windows 2000, XP, 2003 to current

Application	Invocation	Platform	Operating System
Device Manager	Desktop (Java)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current

Web browser

Table "Web browser" (page 311) lists required web browser for each client application that uses a browser.

Web browser

Application	Invocation	Browser
CS 2000 Mgmt Tools	Browser (HTML)	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
CS 2000 GWC Mgr	Browser (JWS)	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
UAS Mgr	Browser (JWS)	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
LMM	Browser (JWS)	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
Nodes Provisioning	Browser (JWS)	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
NPM	Browser (JWS)	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
NPM CLUI	Telnet/SSH login	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
MG 9000 LCI	Browser	Netscape 4.7 only
APS Mgr	Browser	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
STORM Mgr	Browser (Proxy)	Microsoft Internet Explorer 6 SP1 to current
		Netscape 6.2 to current
Note: Nortel supports all versions of browser software officially supported by the browser vendor. Microsoft does not support Internet Explorer on a Solaris client.		

Client applicability

The following table shows which clients apply to each NA solution.

Client to solution mapping for NA solutions

Client	IAC/W	PT-AAL1	PT-IP	UA-AAL1	UA-IP
CS 2000 Management Tools	X		X	X	X
CS 2000 GWC Manager	X		X	X	X
UAS Manager	X		X	X	X
CS 2000 SAM21 Manager	X		X	X	X
Line Maintenance Manager (LMM)	X				X
Trunk Maintenance Manager (TMM)	X		X		X
Network Patch Manager (NPM)	X		X	X	X
Media Gateway 9000 Manager				X	X
Universal Signaling Point Manager	X		X	X	X
Nortel Networks Device Manager	X	X	X	X	X
MDM	X	X	X	X	X

The following table shows which clients apply to each Intl solution.

Client to solution mapping for Intl solutions

Client	Intl IAC	Intl IAW	Intl PT-IP/PTAAL2	Intl UA-IP
CS 2000 Management Tools	X	X	X	X
CS 2000 GWC Manager	X	X	X	X
UAS Manager	X	X	X	X
CS 2000 SAM21 Manager	X	X	X	X
Line Maintenance Manager (LMM)	X	X	X	X

Client	Intl IAC	Intl IAW	Intl PT-IP/PTAAL2	Intl UA-IP
Trunk Maintenance Manager (TMM)	X	X	X	X
Network Patch Manager (NPM)	X	X	X	X
Media Gateway 9000 Manager				X
Universal Signaling Point Manager	X	X	X	X
Nortel Networks Device Manager	X	X	X	X
MDM	X	X	X	X

Client procedures

This section provides an overview of configuration information for all of the clients of the managers provided for the ATM/IP solutions. This information relates to installing and validating that the client installation was successful. The following procedures are provided:

Note: CS 2000 Management Tools includes the CS 2000 GWC Manager and the UAS Manager.

Client procedures

Component	Procedure (s)
INSTALLATION	
CS 2000 Management Tools	""Installing Java Web Start" (page 315)"
CS 2000 SAM21 Manager	""Installing Java Web Start" (page 315)"
Line Maintenance Manager	""Installing Java Web Start" (page 315)"
Trunk Maintenance Manager	""Installing Java Web Start" (page 315)"
Network Patch Manager	""Installing Java Web Start" (page 315)"
Media Gateway 9000 Manager	""Installing Java Web Start" (page 315)"
Universal Signaling Point Manager	"Installing the USP Manager" (page 319)

Component	Procedure (s)
Nortel Networks Device Manager	"Installing the Device Manager software" (page 321)
CONFIGURATION	
Universal Signaling Point Manager	"Configuring the USP Manager" (page 323)
Nortel Networks Device Manager	"Configuring the Passport 8600Ethernet Routing Switch 8600 Device Manager" (page 325)
All components	"Organizing the Clients on Multiple Switches" (page 329)
VALIDATION	
CS 2000 Management Tools	"Validating an Installation of the CS 2000 Management Tools" (page 337)
CS 2000 SAM21 Manager	"Validating an Installation of the CS 2000 SAM21 Manager" (page 345)
Line Maintenance Manager	"Validating an installation of the LMM" (page 378)
Trunk Maintenance Manager	"Validating an Installation of the TMM" (page 403)
Network Patch Manager	"Validating an Installation of the Network Patch Manager" (page 350)
Media Gateway 9000 Manager	"Validating an installation of the MG 9000 Manager" (page 356)
Universal Signaling Point Manager	"Validating an Installation of the Universal Signaling Point Manager" (page 361)
Nortel Networks Device Manager	"Validating an Installation of the Device Manager" (page 372)

Installing Java Web Start

Application

The following applications require Java 2 Runtime Environment (version 1.4.2_08) and Java Web Start (version 1.4.2_08) for their web based applications:

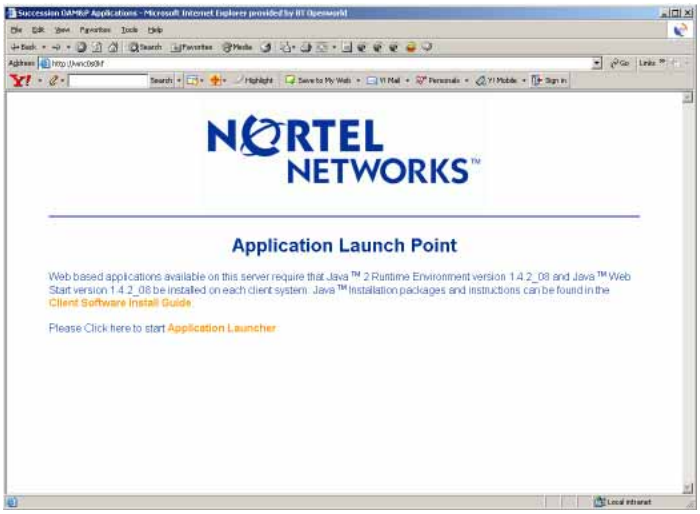
- CS 2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Batch Configuration Monitor
- MG 9000 Manager

Prerequisites

- Ensure the client workstation meets the minimum requirements. Refer to section "Client workstation requirements" in *IP Solutions Basics* (NN10300-100) for more information.
- You need the IP address or host name of the server where the CS 2000 Management Tools or MG 9000 Manager software is installed.
- You must have administrative privileges to install the software on the workstation.

Action

Step	Action
	At your workstation
1	Launch your web browser.
2	Access the server where the CS 2000 Management Tools or the MG 9000 Manager software is installed by typing **`>http:// <host>`** where **`<host>`** is the name or IP address of the server where the CS 2000 Management Tools software is installed The "Application Launch Point" page appears.



3 Click **Client Software Install Guide**, and read the instructions under "How to Check Version".

If	Do
you have JRE 1.4.2_08 and JWS 1.4.2_08 installed	you have completed this procedure
you do not have JRE 1.4.2_08 and JWS 1.4.2_08 installed	Step 4

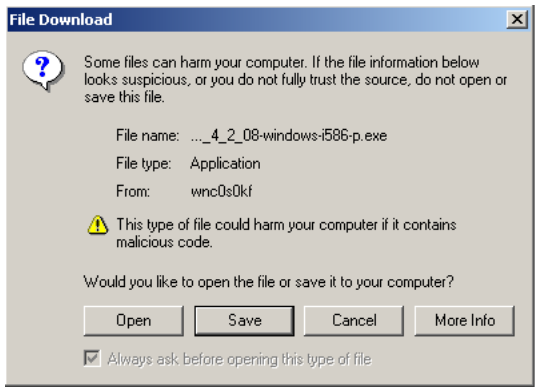
4 Click **Java 2 Runtime Environment Install Guide** under "Microsoft Windows" or "Sun Solaris" for system requirements and installation instructions.

5 Once you have read through the "Java 2 Runtime Environment Install Guide", click the **Back** button to return to the "Client Software Installation" page.

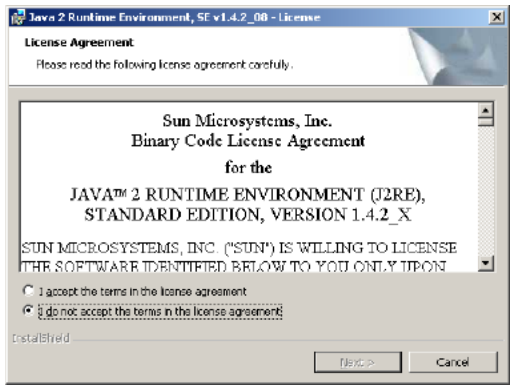
6 Click **Java 2 Runtime Environment Software Download** under "Microsoft Windows" or "Sun Solaris" to download and install the software.

ATTENTION
You must have administrative privileges to install the software on the workstation.

7 Either save the executable file to your computer and run it, or run it from its current location.



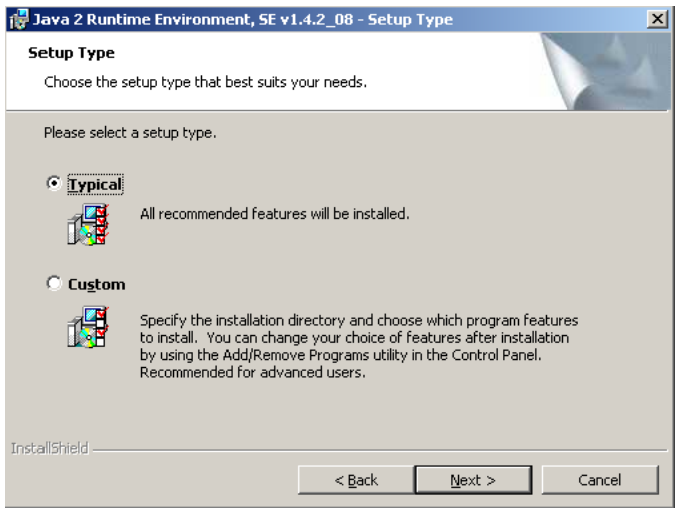
8 Read the terms of the license agreement. If you agree to terms, click **Yes**.



ATTENTION

You must click **Yes** to complete the installation.

9 Select a Setup Type for the installation, then click **Next** to complete the installation.



10 You have completed this procedure.

—End—

Installing the USP Manager

You must install Windows client software on each remote Windows workstation before you can use the remote reach-through feature. For details refer to the Administrator's Guide, Citrix ICA Win32 Client, Version 4.21 or Administrator's Guide, Citrix ICA Win16 Client, Version 4.21.

Application

NTST30CA servers support five terminal server licenses for remote Windows workstations.

NTST30DA servers support five terminal server licenses for remote Windows workstations and five Citrix licenses for remote Windows or UNIX workstations. Nortel recommends using the terminal server licenses for remote Windows workstations, reserving the Citrix licenses for remote UNIX workstations. If you need more than five terminal server licenses for remote Windows workstations, use the Citrix licenses.

Prerequisites

- None

Action

Installing the USP Manager client

Step	Action
	At the OAMP Workstation
1	Insert Diskette 1 from the set of Windows client software diskettes into the disk drive of your remote Windows workstation.
2	Run the setup.exe file on the diskette.
3	Follow the on-screen instructions to install the Windows client software.
4	You have completed this procedure.

—End—

Installing the Passport 8600 Device Manager

Application

The Device Manager software is provided on the Passport 8000 Switch Series Software Release 3.3 CD as a self-extracting executable file. This section provides instructions to install the Device Manager software in a Windows™ or UNIX™ environment.

ATTENTION

If you have other Passport 8000 Series devices in your network and are running earlier versions of Device Manager software, you must install Device Manager version 5.8.2.1 in order to access Passport 8000 Series switches running switch software version 3.7.2.2 .

Prerequisites

The minimum system requirements for installing Device Manager on a Windows™ workstation are:

- 400 MHz or higher Pentium Processor
- 128 MB DRAM
- 100 MB space on hard drive

The minimum system requirements for installing Device Manager on a UNIX platform are:

- SPARC workstation running the Sun OS 5.6/Solaris 2.6 (or higher) Operating System with 128 MB DRAM (preferred 256 MB DRAM) and 100 MB available on the hard disk

  or

- HP workstation running the HP/UX 11.0 (or higher) Operating System with 256 MB DRAM and 100 MB available on the hard disk

  or

- AIX workstation running the AIX 4.3.3.10 (or higher) Operating System with 256 MB DRAM and 100 MB available on the hard disk

Before you install the Device Manager software, you must have the Java Runtime Environment (JRE) version 1.4.2_08 or higher installed. After the JRE is installed, you can upgrade your system to later versions of Device Manager without installing the JRE again.

Action

Install the Device Manager software

Step	Action

At the Workstation

1 Insert the Passport 8000 Software CD into your CD-ROM drive.

2 From the Windows Start menu, choose Run.

The Run dialog box opens.

3 Use Browse to navigate to the drive where the CD-ROM is located.

4 On the CD-ROM drive, locate the \Windows\Device Manager subdirectory.

5 Determine if you need to install the JRE.

If you have …	Do
… already performed the "Installing Java Web Start" (page 315) procedure	step 7
… not performed the "Installing Java Web Start" (page 315) procedure	step 6

6 Install the JRE by performing the following steps:

ATTENTION

If you have already performed the "Installing Java Web Start" (page 315) procedure, skip this step.

a. Double-click the current JRE installation file.

b. Follow the instructions appearing on the screen to complete the JRE installation.

7

CAUTION

To ensure that the you have the newest shortcuts, properly uninstall your previous software version before installing the newest software. Ensure that the shortcut to the previous version has been removed. Accessing Device Manager with an old shortcut results in a loss of software functionality.

Prior to upgrading Device Manager, either uninstall your previous version of the Device Manager software, or install the new software to a different directory. (You can have multiple versions of Device Manager stored on your PC provided they are stored in separate directories.)

If you uninstall your previous version of Device Manager, but want to retain your list of IP addresses (Device > OpenLast), save the dm.ini file to a different location prior to uninstalling Device Manager. Once you have installed the new version of Device Manager, copy the saved dm.ini file into the directory.

8 Install Device Manager by performing the following steps:

a. Double-click the jdm_5xxx.exe file.

ATTENTION

To install Device Manager for Windows, you must specify the destination directory folder as jdm on a drive. For example, if you specify d:\jdm, jdm is a directory folder on the D drive, and the software will be installed in the directory folder jdm. The d: drive is used as an example. Change the drive ID as needed.

b. Follow the instructions appearing on the screen to complete the installation.

9 You have completed this procedure.

—End—

Configuring the USP Manager

Application

This procedure demonstrates how to configurethe USP Manager after you have installed it. You must perform this procedure before launching the USP Manager.

Prerequisites

- None

Action

Configuring the USP Manager client

Step	Action
	At the client workstation
1	

If you are connecting to an	Do
NTST30CA server	step 2
NTST30DA server	step 10

2	After the client software has been installed on your remote workstation you need to configure the workstation. Start the Client Connection Manager (Start->Programs->Terminal Service Client->Client Connection Manager). Select File-> New Connection.
3	Enter a name for your connection.
4	Enter the name or IP address of your alternate boot server.
5	Configure your remote workstation for Automatic Logon if you want this feature.
6	Select the screen options for your remote workstation from the Screen Option dialog box.
7	Accept all system default values by clicking Next, until the configuration procedure in completed.
8	Launch the session by selecting Start on your workstation. From there, select Programs -> Terminal Services Client -> new connection name.

Note: Select the new connection name of the ICA client that you re-named prior to this procedure.

9 Go to step 14.

10 After you install the client software you will see a Citrix Program Neighborhood icon on your desktop. Double click the icon. Select Add ICA Connection.

11 After you have created a connection you will see an icon for the new connection in Citrix Program Neighborhood - ICA Connections.

12 After you have finished configuring the new connection icon, double click on it to connect your remote Windows workstation to your alternate boot server and run the selected application.

13 Go to step 14.

14 You have completed this procedure.

—End—

Configuring the Passport 8600 Device Manager

Application

The Device Manager uses the Simple Network Management Protocol (SNMP) to configure and manage 8000 Series switches. You can use the Device Manager Properties dialog box to configure important communication parameters such as the polling interval, timeout, and retry count. You can set these parameters at any time before or after you open a device.

Prerequisites

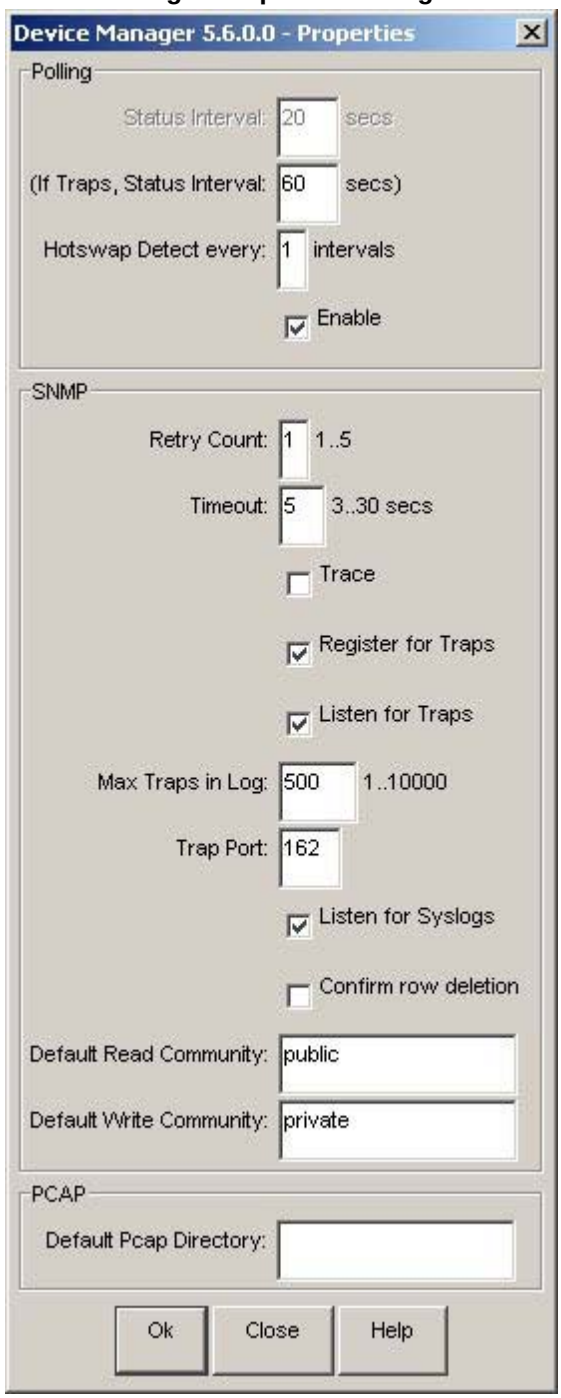
- None

Action

Setup the Device Manager properties

Step	Action
	At the Device Manager client GUI
1	From the abbreviated Device Manager window menu bar, chose Device>Properties. The Device Manager Properties dialog box opens.

Device Manager Properties dialog box



2 Select the properties you want to change and set their values. The following table describes the properties.

Properties dialog box fields

Field	Description
Status interval	Interval at which statistics and status information are gathered (default is 20 seconds)
(IfTraps, Status Interval)	If the Register for Traps box is check, interval, in seconds, at which statistics and status information are gathered.
Hotswap Detect every	Enter a number for the number of intervals at which Device Manager will check for module hot swaps
Enable	If checked, Device Manager will poll the switch according to the settings listed above the Enable box.
Retry Count	If Device Manager cannot transmit polling information at startup, the number of times Device Manager retransmits polling information.
Timeout	Length of each retry of each polling waiting period. When accessing the device through a slow link, you may want to increase the timeout interval and then change the Retransmission Strategy to superlinear.
Trace	If checked, you have the ability to perform trace routes.
Register for Traps	If checked, Device Manager will register a trap.
Listen for Traps	If checked, Device Manager will listen for a trap.
Max Traps in Log	The specified number of traps that may exist in the trap log. The default is 500.
Trap Port	The number of the port that trap messages will be captured on. The default is 162.
Listen for Syslogs	If checked, Device Manager will listen for syslogs.
Confirm row deletion	If checked, Device Manager will send a message when a system table row was deleted.

Field	Description
Default Read Community	Displays the default Read Community type.
Default Write Community	Displays the default Write Community type.

3 Click OK to accept the changes.

4 You have completed this procedure.

—End—

Organizing the Clients on Multiple Switches

Application

Often multiple switches are used for the element management servers. Thus, the launch points for the different managers are in different locations. The procedure that follows demonstrates the recommended method for organizing the clients in this situation.

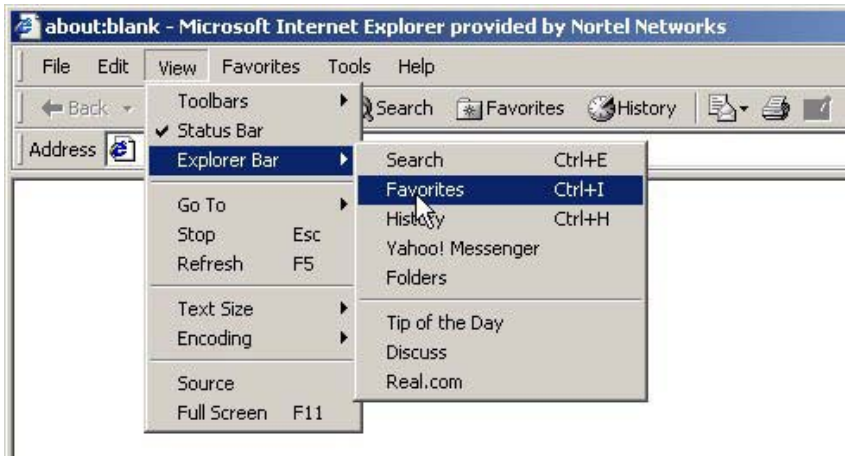
ATTENTION

This procedure is written for use with Internet Explorer. Performing the procedure with Netscape Navigator would entail similar, but slightly different steps.

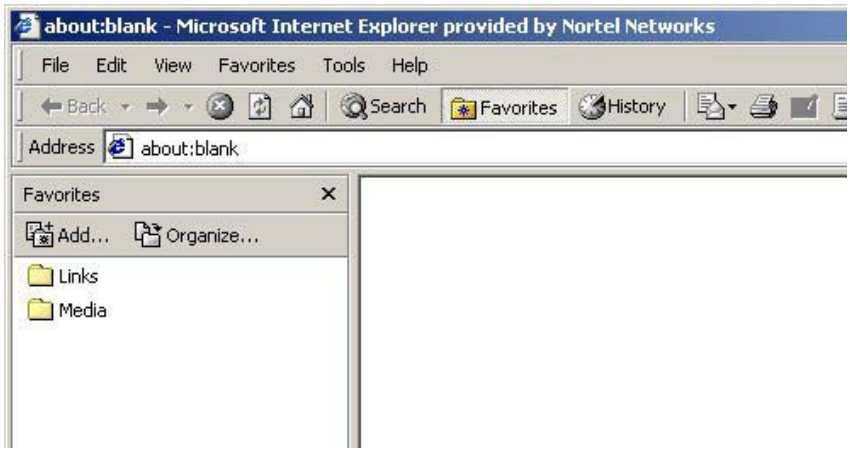
Prerequisites

Action

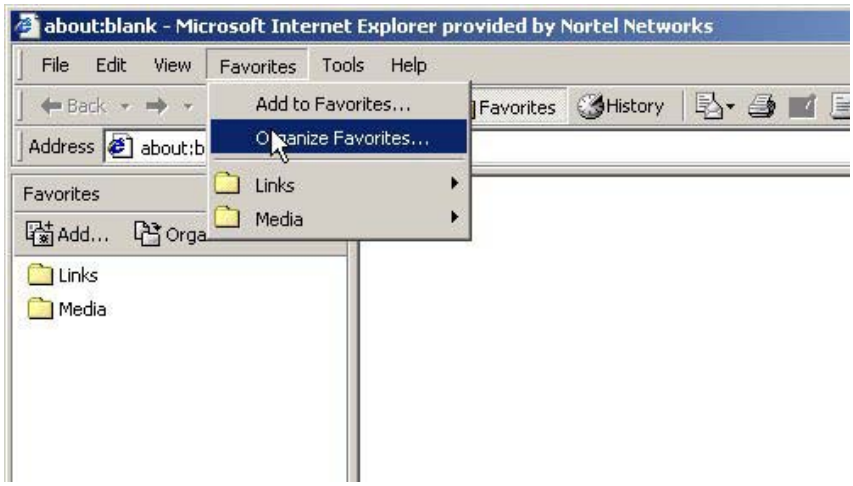
Step	Action
	At your workstation
1	Launch Internet Explorer.
2	From the **View** menu, click **Explorer Bar** then **Favorites**.



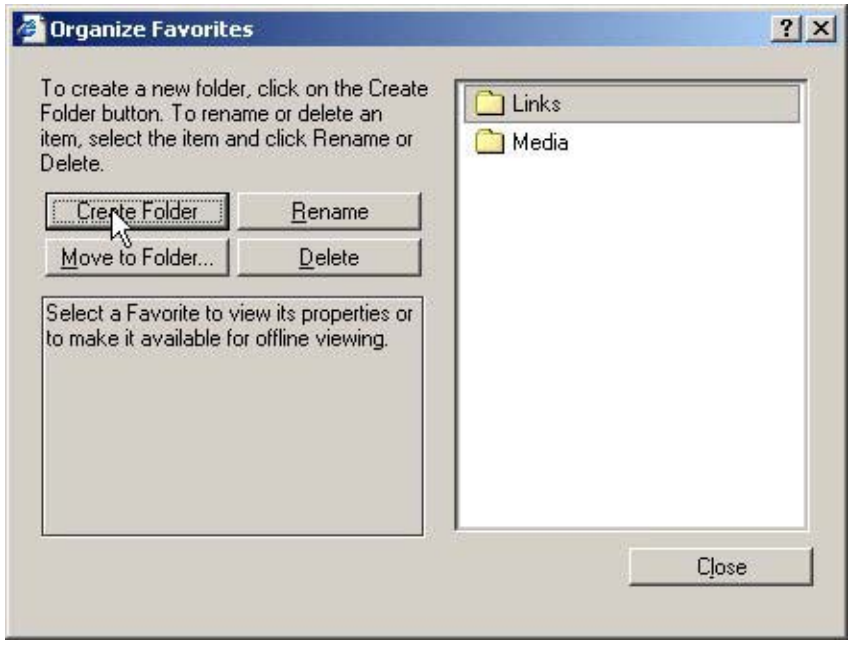
The favorites for the browser should appear in the left side of the browser window.



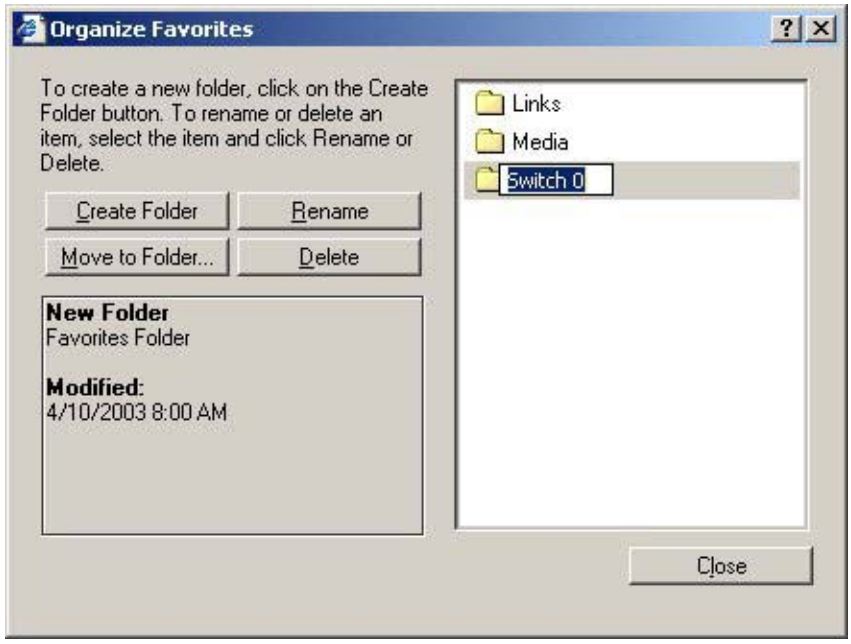
3 From the **Favorites** menu, click **Organize Favorites**....



4 Click **Create Folder**.



5 Enter the name of the switch for the new folder name, and click **Close**.



6 Create a link to the CS 2000 Management Toolsand MG 9000 Manager client applications as follows:

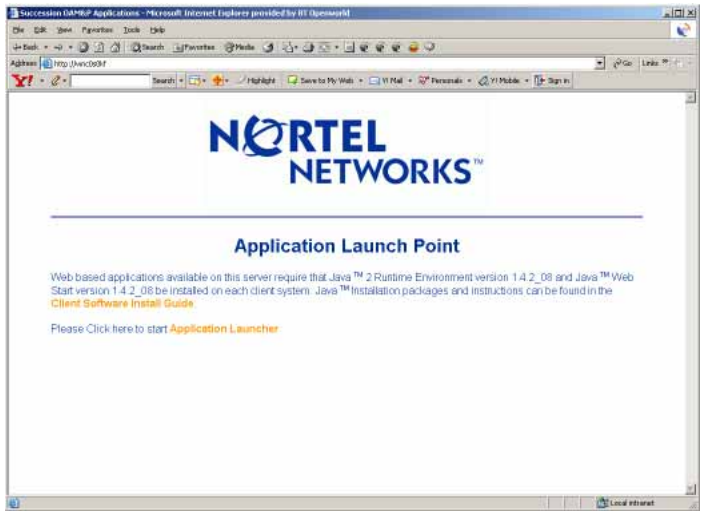
a. Access the server where the CS 2000 Management Toolsor the MG 9000 Manager software is installed by typing

http:// <host>

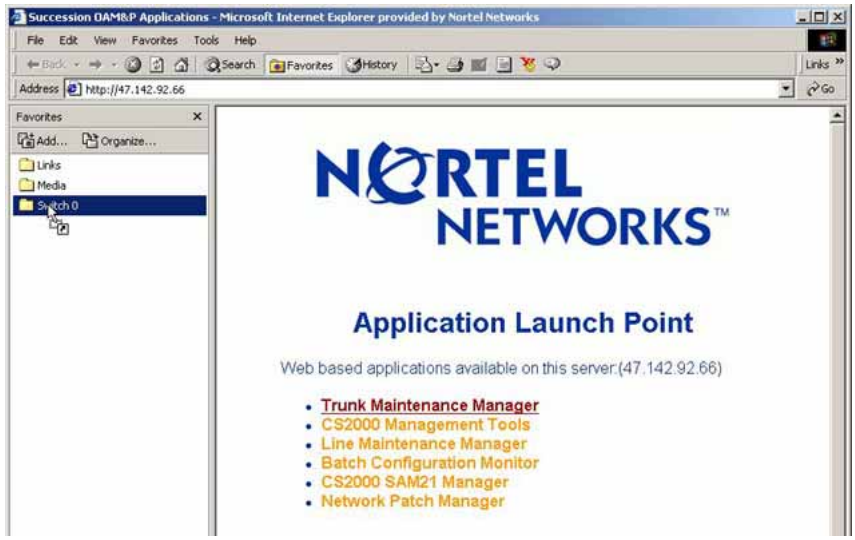
where

<host> is the name or IP address of the server where the CS 2000 Management Toolsor MG 9000 Managersoftware is installed

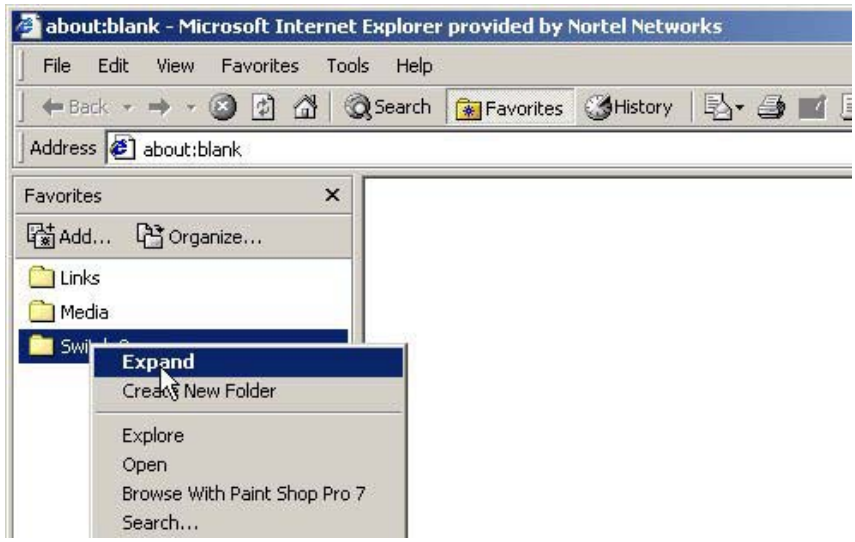
The "Application Launch Point" page appears.



b. Without letting go of the left mouse button, left click on **Application Launcher** and drag it over to the folder you created in step 4. When the cursor is over the folder name, let go of the left mouse button.



c. In the Favorites pane on the browser, right click on the folder you created in step 4 and click **Expand**. The Application Launcher link should now appear under the folder name.

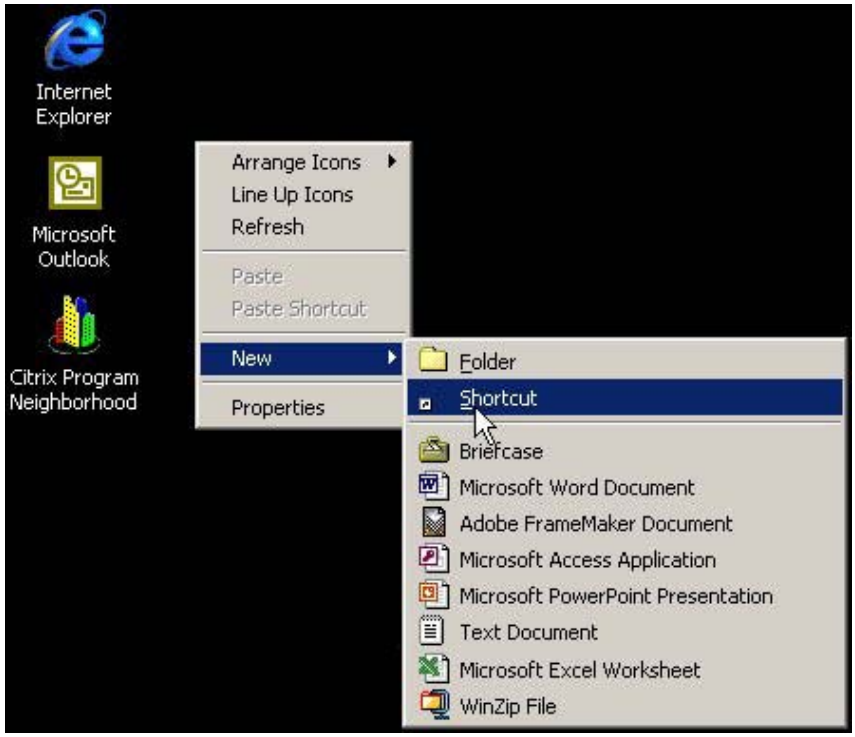


d. In the Favorites pane on the browser, right-click on the Application Launcher link that is in the folder, and click **Rename**.

e. Enter a distinguishable name for this Application Launcher, for example "CS2K Mgmt Tools" or "MG9K Manager".

7 Create a link to the core as follows:

a. Right-click on your desktop, click **New**, then click **Shortcut**.



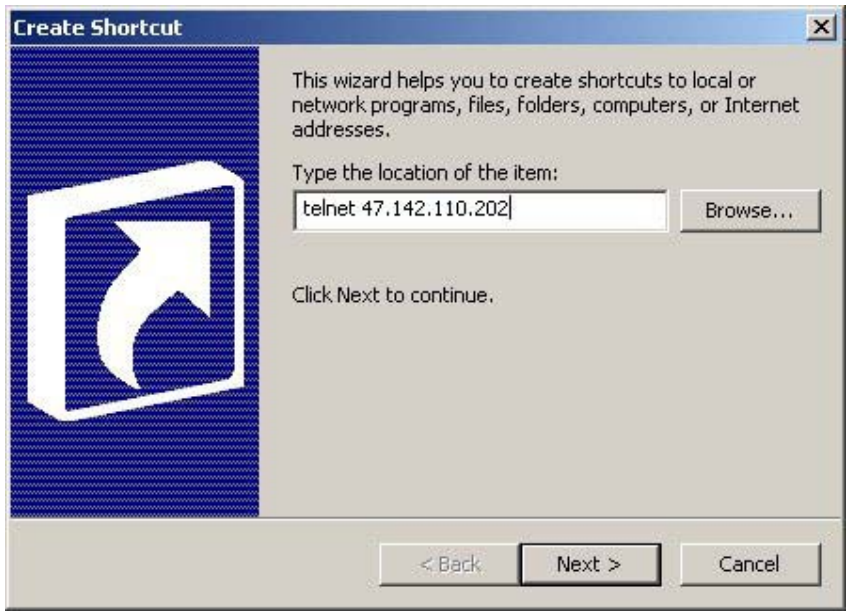
b. When prompted for the location of the item, enter "telnet <core_ip>", then click **Next**.

   where

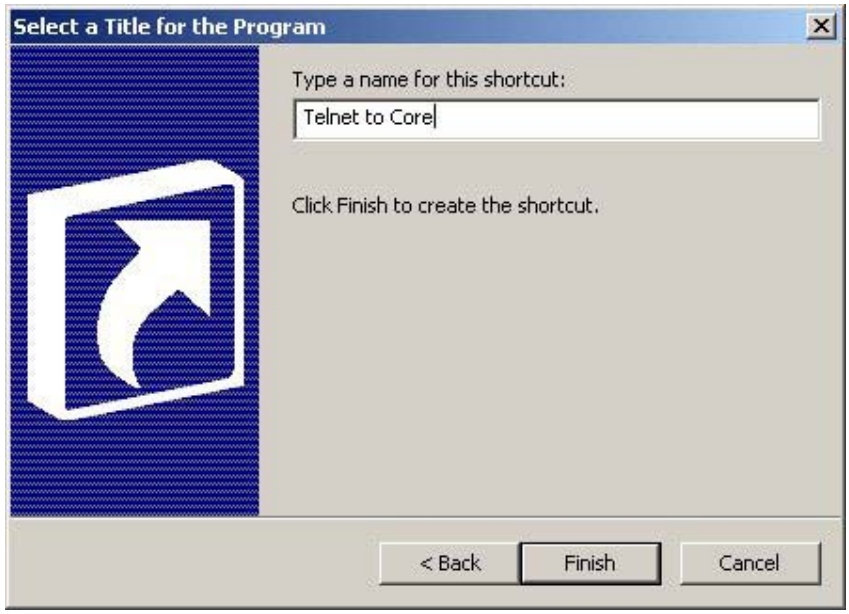
   `core_ip` is the Core IP address

   Example

   telnet 47.142.110.202



c. When prompted for the name of the shortcut, enter "Telnet to Core", then click **Finish**.



d. Once the new shortcut appears on the desktop, drag it over to the folder you created in step 4 using the same method described in step b.

8 Create a link to the Device Manager as follows:

a. Right-click on your desktop, click **New**, then click **Shortcut**.

b. When prompted for the location of the item, enter "<dm_location> <passport_address>", then click **Next**.

where

`dm_location` is the directory where the Device Manager is located

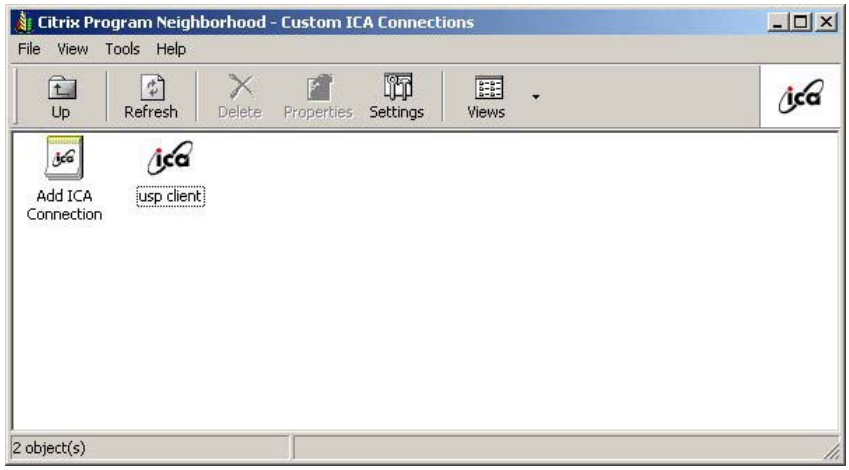
`passport_address` is the IP address for the Passport server

c. When prompted for the name of the shortcut, enter "PP8600 Client", and click **Finish**.

d. Once the new shortcut appears on the desktop, drag it over to the folder you created in step 4 using the same method described in step b.

9 Create a link to the USP client as follows:

a. Open the Citrix Program Neighborhood by clicking on the desktop icon.



b. Drag the USP client icon to the folder you created in step 4 using the same method described in step b.

—End—

At this point, all the clients applicable to the switch are under a single folder and can be accessed with a single click. Repeat this procedure as desired for other switches on the network.

Validating an Installation of the CS 2000 Management Tools

Application

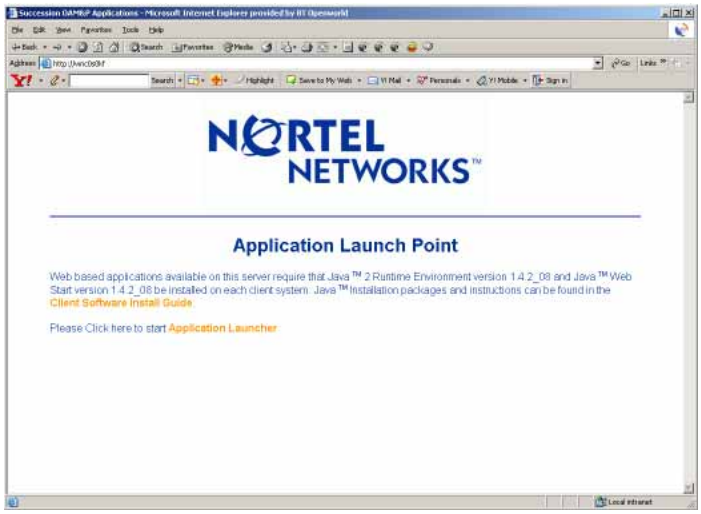
Use this procedure to validate the installation of the CS 2000 Management Tools, which involves launching the CS 2000 Management Tools application GUI and verifying the CS 2000 GWC Manager and UAS Manager are displaying correctly.

Prerequisites

You need the IP address or host name of the server where CS 2000 Management Tools reside, and a valid user name and password to launch the application.

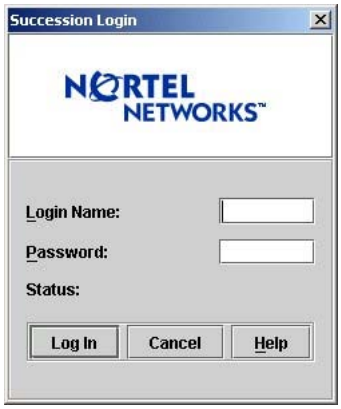
Action

Step	Action
	At your workstation
1	Launch your web browser.
2	Access the server where the CS 2000 Management Tools reside by typing `>http://<host>` where **`<host>`** is the name or IP address of the server where the CS 2000 Management Tools software resides The "Application Launch Point" page appears.



3 Click **Application Launcher**.

The Login window appears.

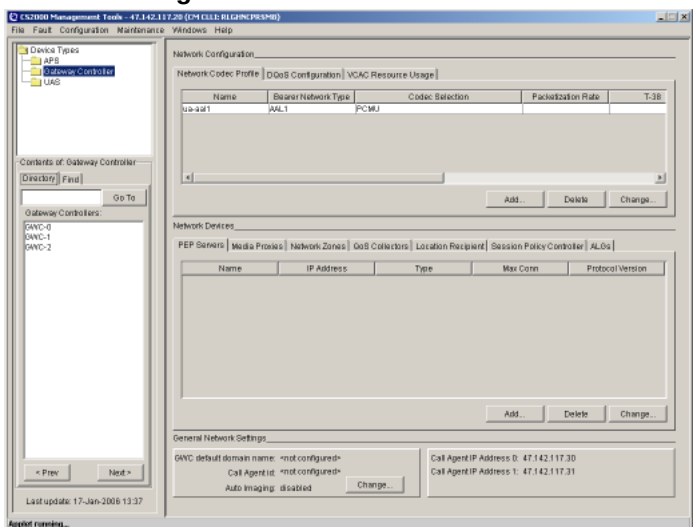


4 Enter your user name and password, then click Log In. The Application Launch Point, similar to following, appears.

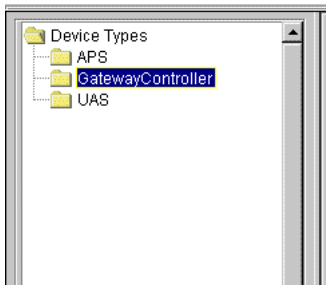
5 Click **CS2000 Management Tools**.

The CS2000 Management Tools GUI, similar to following, appears.

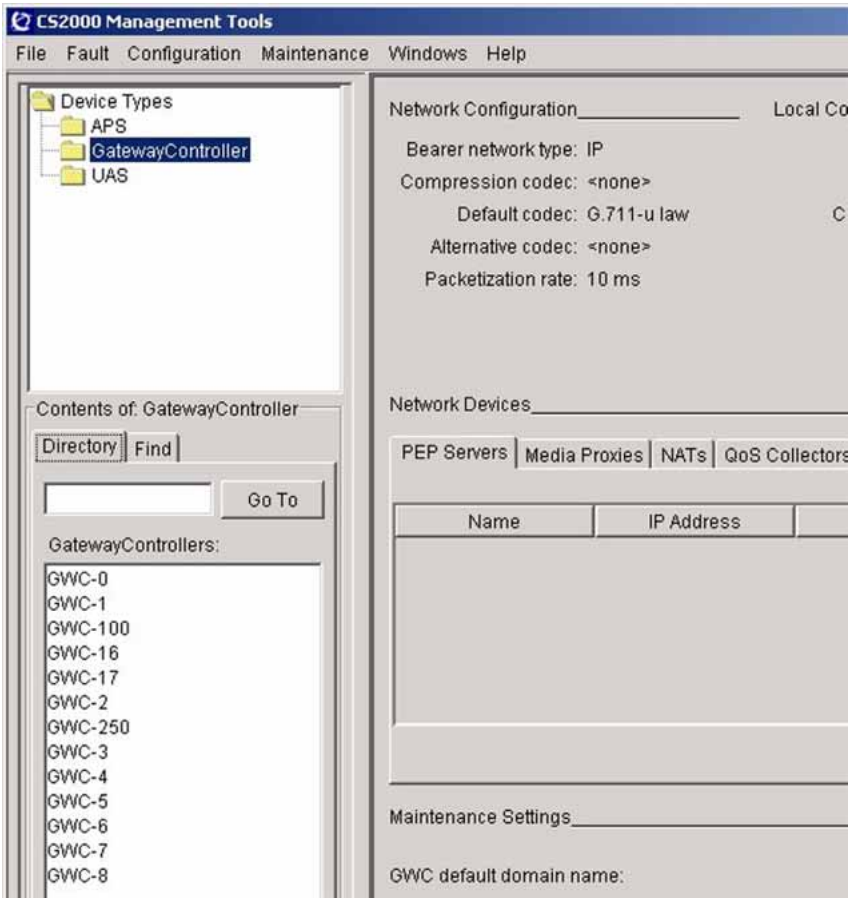
CS2000 Management Tools GUI



6 From the Device Types window, click Gateway Controller.



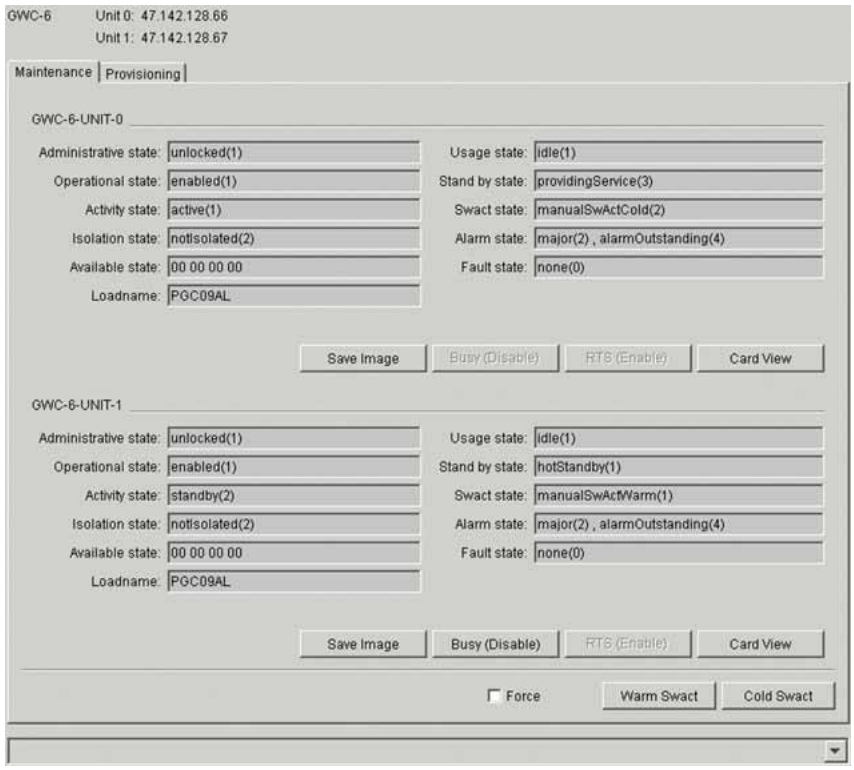
The Network View of the CS 2000 GWC Manager appears in the main window. A list of GWC devices appear in the Contents window.



7 Access the Node View of the CS 2000 GWC Manager by clicking on one of the GWC devices.

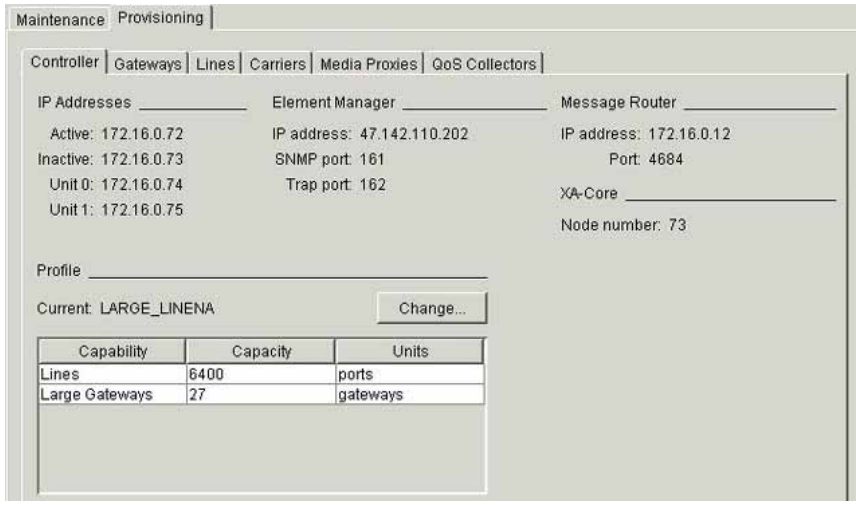
The Node View of the CS 2000 GWC Manager will appear in the main window.

CS 2000 GWC Manager



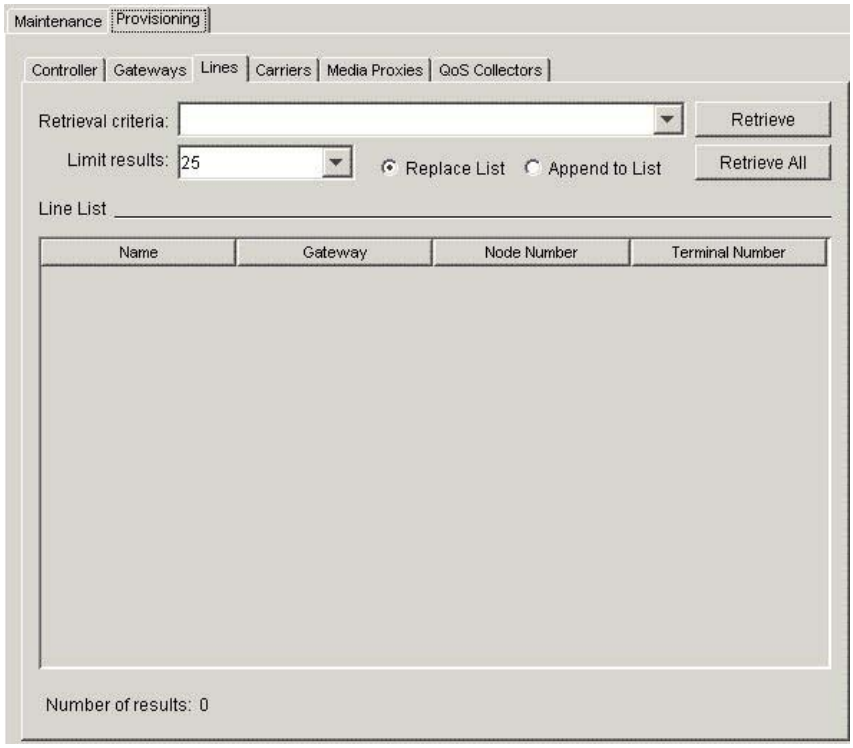
8 Click on the Provisioning tab to bring up the Provisioning view.

Provisioning tab



9 Click on the Lines tab to bring up the Lines view

Lines tab



10 To validate the CS 2000 GWC Manager, click on the Retrieve All button to verify that the manager communicates with the GWC.

Line List

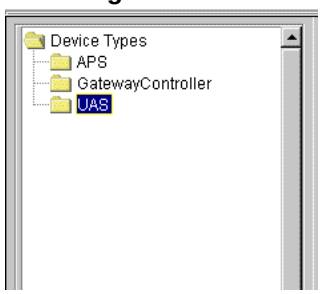
If the CS 2000 GWC Manager is …	Do
… able to retrieve the lines	step 11
… not able to retrieve the lines	Contact your next level of support

11 From the Device Types window, click **UAS**.

ATTENTION

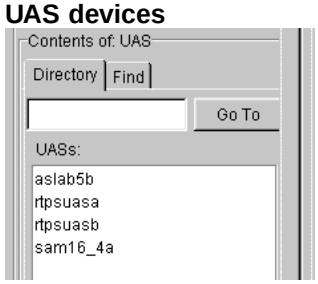
Nortel only supports the Universal Audio Server in MTX14 for existing MTX13 Packet MSC customers that already use this server and upgrade to MTX14.

Selecting UAS



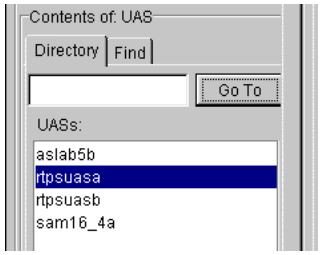
A list of UAS devices will appear in the Contents window.

UAS devices



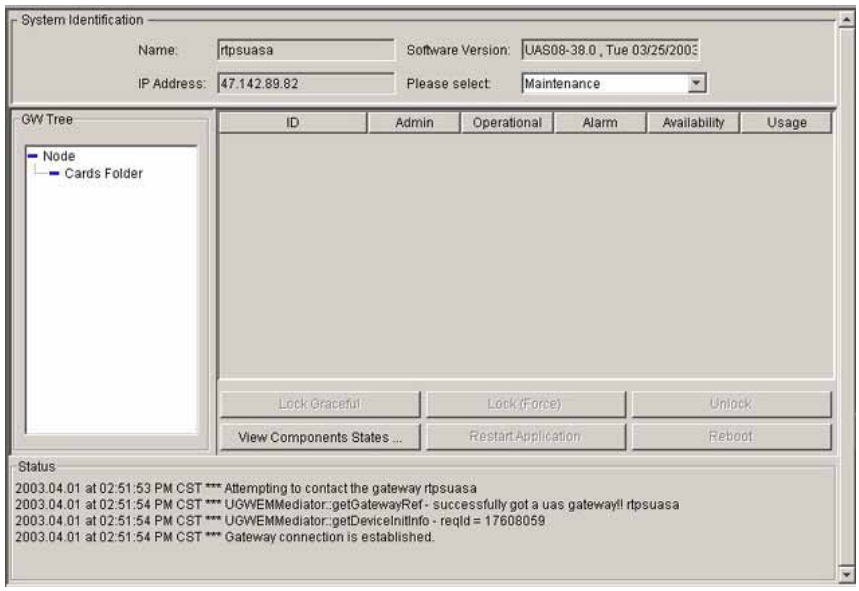
12 Access the UAS Manager by clicking on one of the UAS devices.

Accessing the UAS Manager



The UAS Manager will appear in the main window.

UAS Manager



13 Check the Status bar at the bottom of the manager to make sure the UAS Manager is able to communicate with the UAS device.

Connection status

If the connection was	Do
established	you have completed this procedure
not established	contact your next level of support

14 You have completed this procedure.

—End—

Validating an Installation of the CS 2000 SAM21 Manager

Application

Use this procedure to validate the installation of the CS 2000 SAM21 Manager, which involves launching the CS 2000 SAM21 Manager application GUI and verifying the network elements appear, and verifying any alarms on the elements also appear in the Alarm Manager.

Prerequisites

You need the IP address or host name of the server where CS 2000 SAM21 Manager resides, and a valid user name and password to launch the application.

Action

Step	Action

At your workstation

1 Launch your web browser.

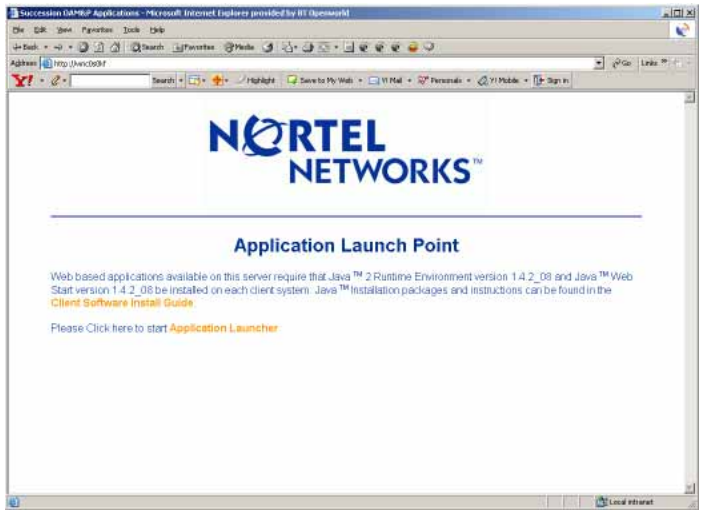
2 Access the server where the CS 2000 SAM21 Manager resides by typing

`>http:// <host>`

where

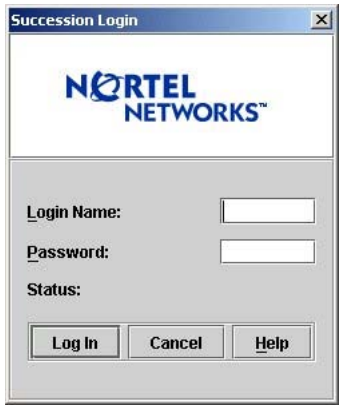
`<host>` is the name or IP address of the server where the CS 2000 SAM21 Manager resides

The "Application Launch Point" page appears.



3 Click **Application Launcher**.

The Login window appears.



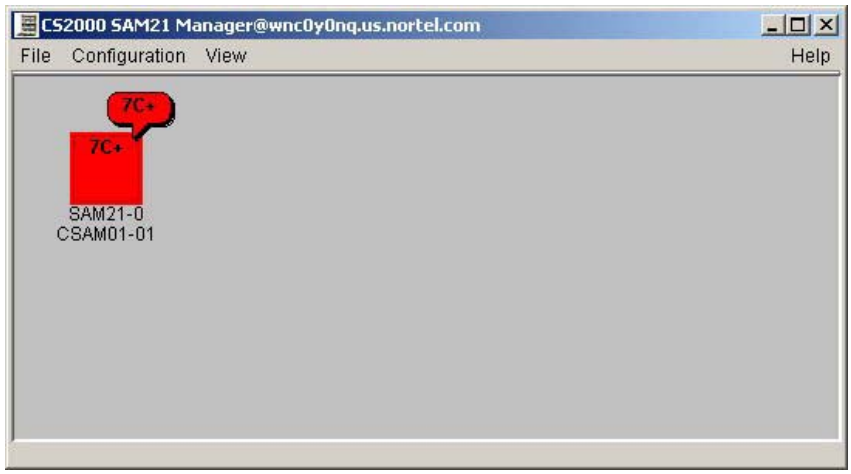
4 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.

5 Click CS2000 **SAM21 Manager**.

The Subnet View, similar to the following, appears.

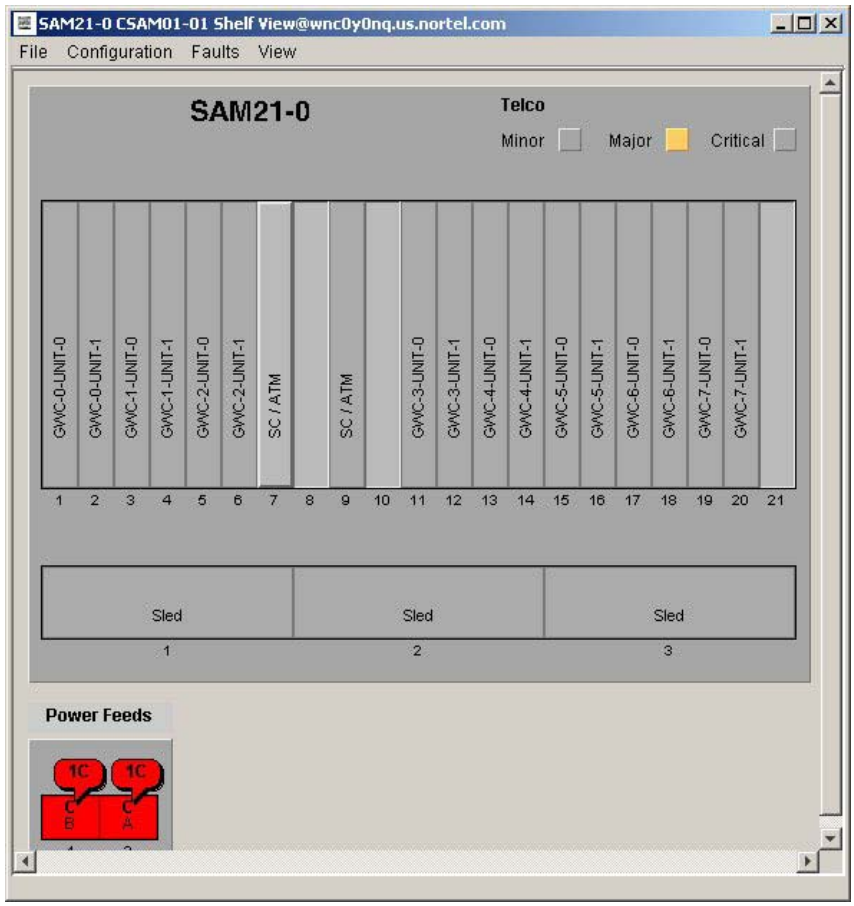
Subnet View



the Subnet View	Do
appeared	step 6
did not appear	contact your next level of support

6 Double click on an network element to verify that the Shelf View appears.

CS 2000 SAM21 Shelf View

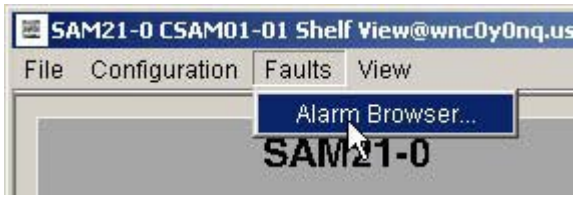


If the Shelf View	Do
appeared	step 7
did not appear	contact your next level of support

7 Use the following table to determine your next step.

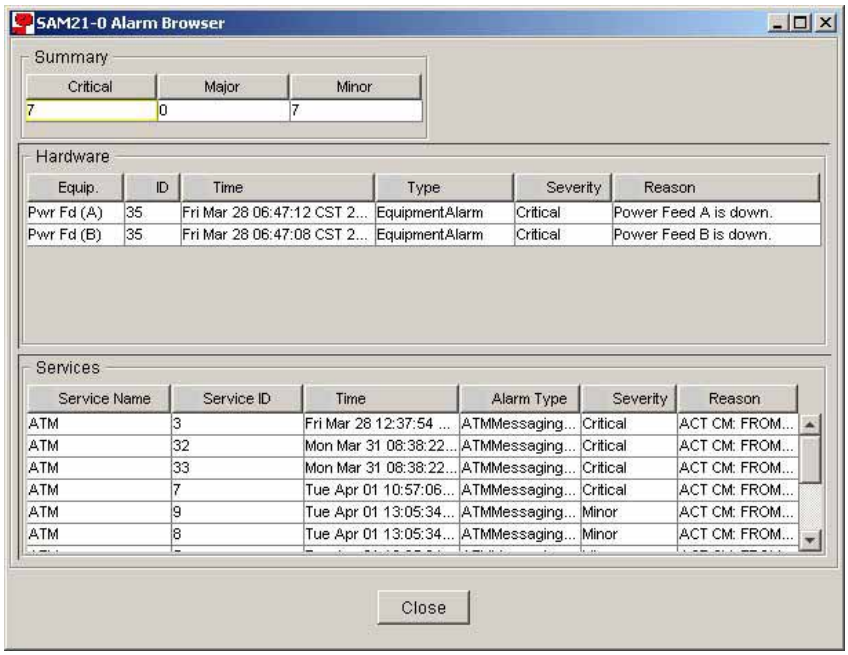
If there are	Do
no alarms present on the Shelf View	you have completed this procedure
alarms present on the Shelf View	step 8

8 On the **Faults** menu, click **Alarm Browser...**.



9 Verify that alarms appear in the Alarm Browser.

Alarm Browser



If the alarms	Do
appear on the Alarm Browser	you have completed this procedure
do not appear on the Alarm Browser	contact your next level of support

10 You have completed this procedure.

—End—

Validating an Installation of the Network Patch Manager

Application

Use this procedure to validate the installation of the Network Patch Manager (NPM), which involves launching the NPM GUI and generating a report to verify communication between the client and server.

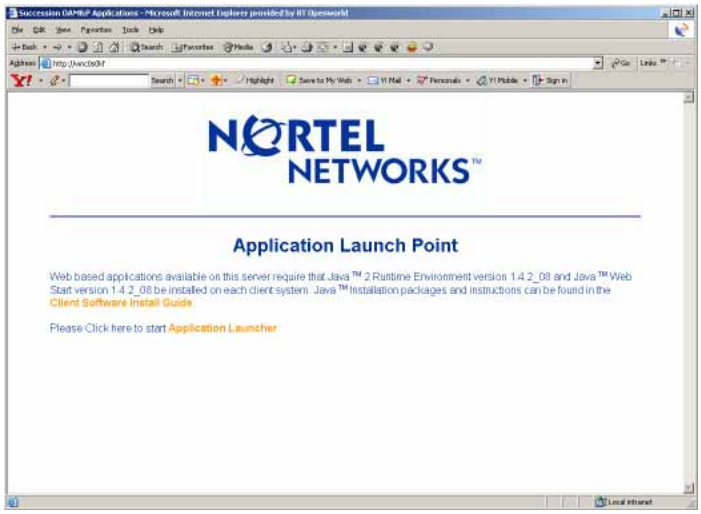
The report generated in the procedure is only an example. The report could be any valid report.

Prerequisites

You need the IP address or host name of the server where the NPM software resides, and a valid user name and password to launch the application.

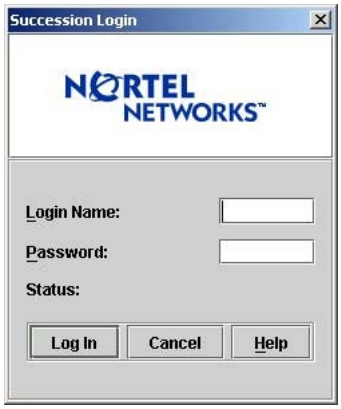
Action

Step	Action
	At your workstation
1	Launch your web browser.
2	Access the server where the NPM software resides by typing **`>http:// <host>`** where **`<host>`** is the name or IP address of the server where the NPM software resides The "Application Launch Point" page appears.



3 Click **Application Launcher**.

The Login window appears.



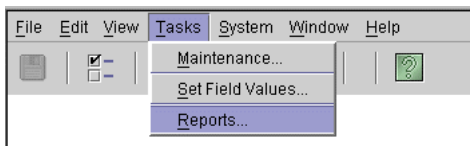
4 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.

5 Click **Network Patch Manager**.

The NPM GUI appears.

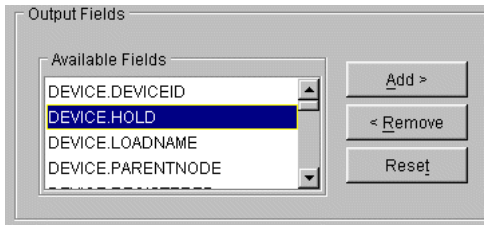
6 On the **Tasks** menu, click **Reports....**



7 Select the fields to be included in the report by performing the following steps:

a. Select the field from the Available Fields list.

Selecting the field to include



b. Press the Add button to add the selected field to the Selected Fields list.

c. Repeat Steps 7a and 7b for each field.

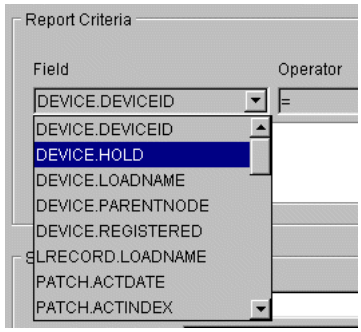
8 Enter the search criteria for the report.

If you want to enter the search criteria	Do
using the combo boxes	step 9
manually	step 10

9 Specify the search criteria in the Report Criteria panel by performing the following steps:

a. Select the field from the Field Combo Box.

Selecting the field

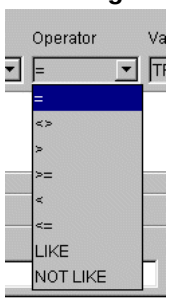


b. Select the operator from the Operator Combo box. The following table lists the supported operators and their meaning.

Supported operators

Operator	Meaning
=	Equal
<>	Not equal
>	Greater than
>=	Greater than or equal
<	Less than
<=	Less than or equal
LIKE	Matches string with wildcard (%)
NOT LIKE	Does not match string with wildcard (%)

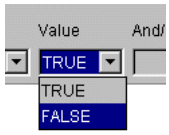
Selecting the operator



c. In the Value Combo Box, select the value or enter the value manually.

The Value Combo Box data type will change depending on the data type of the field. For alphanumeric data, enter the value manually. For boolean data, select the value.

Selecting the value



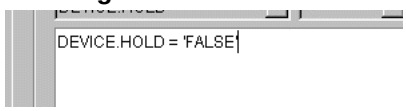
d. To combine multiple criteria statements, select the AND or the OR options from the And/Or combo box.

e. Go to step 11.

10 Enter the search criteria in the text area following the combo boxes.

Parenthesis "()" may be inserted to define precedence for multiple criteria statements.

Entering search criteria manually

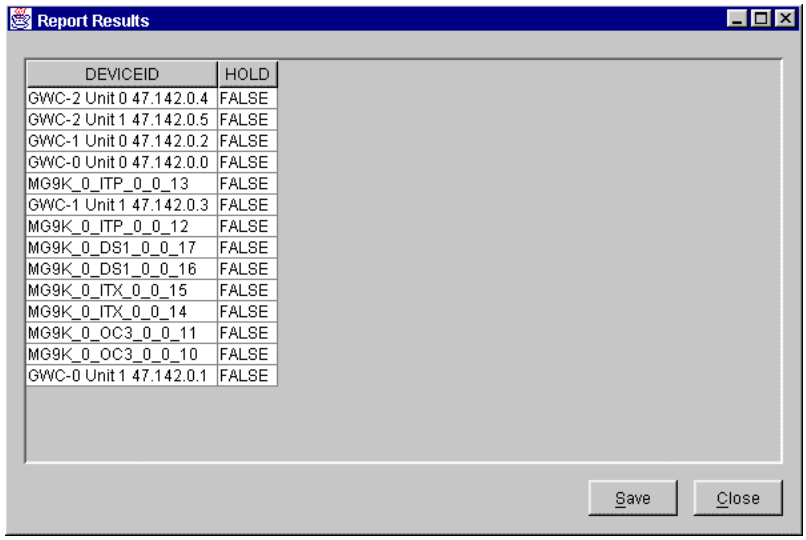


11 Execute the report by pressing the Execute button.

12 After the report data has been received, the Report Results window will be displayed.

The time required to generate the report depends on the number of patches and devices in the database and the complexity of the search criteria.

Report Results window



13

If the report ran	Do
as expected	you have completed this procedure
with errors	contact your next level of support

14 You have completed this procedure.

—End—

Validating an installation of the MG 9000 Manager

Validating the MG 9000 Manager installation involves logging into the MG 9000 Manager, verifying the shelves appear, and verifying any alarms on the shelves also appear in the Alarm Manager.

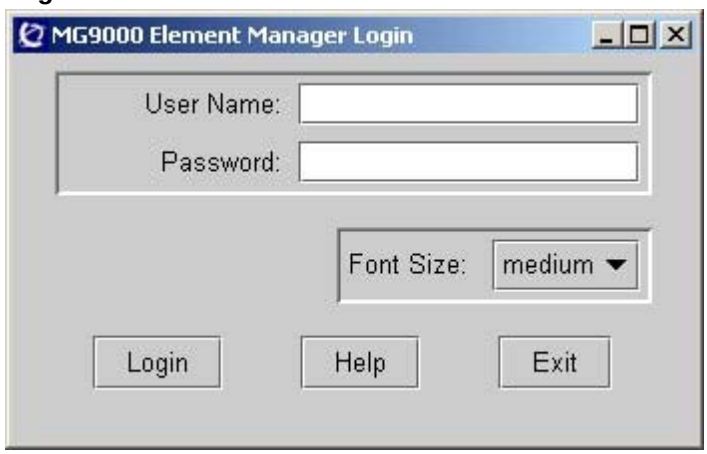
Validating the MG 9000 Manager installation

Step	Action
	At a web browser
1	Access the Application Launch Point on the server on which you installed the MG 9000 Manager.

MG 9000 Application Launch Point

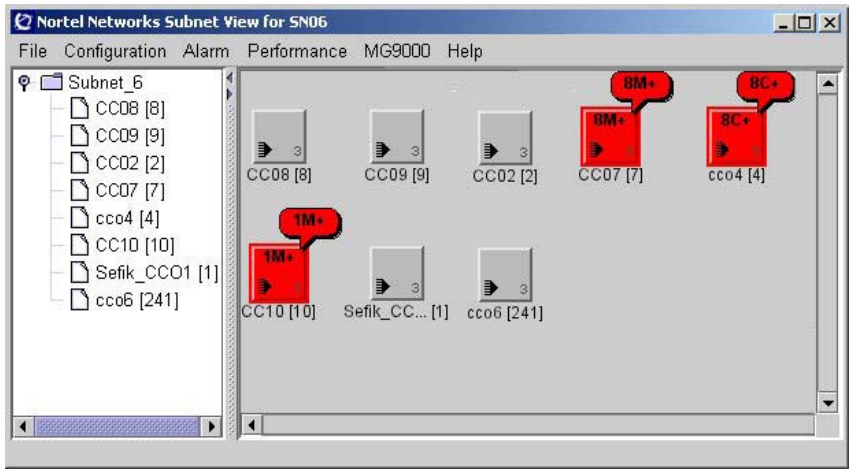
2	Click on the link for the MG 9000 Element Manager. Once the application loads, you will be asked to for a User Name and Password to access the manager.

Login screen



3 Verify that the Subnet View appears.

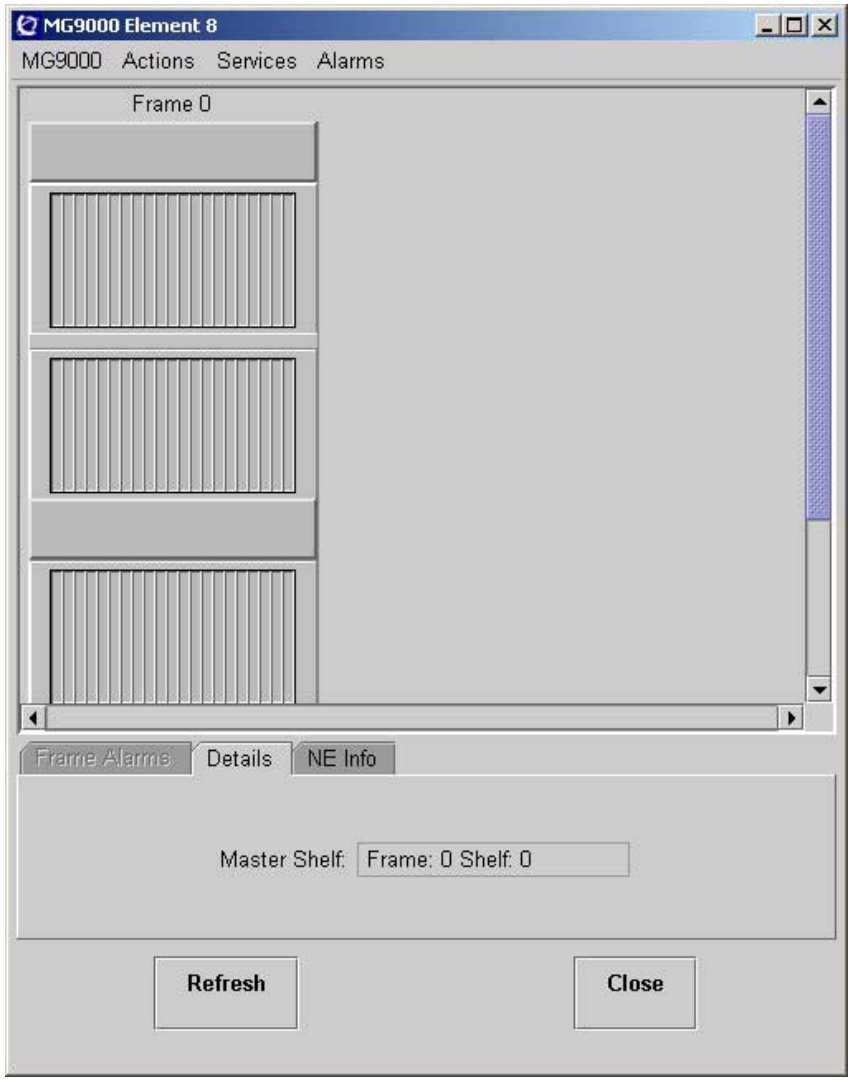
Subnet View for (I)SN06



If the Subnet View	Do
appeared	step 4
did not appear	step 9

4 Double click on an element to verify that the element view appears.

MG 9000 Element



If the Element view	Do
appeared	step 5
did not appear	step 9

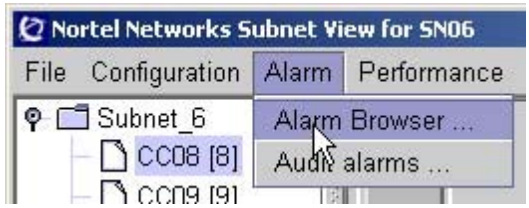
5 Close the Element view and return to the Subnet View.

6

If there are	Do
no alarms present on the subnet view	step 10
alarms present on the subnet view	step 7

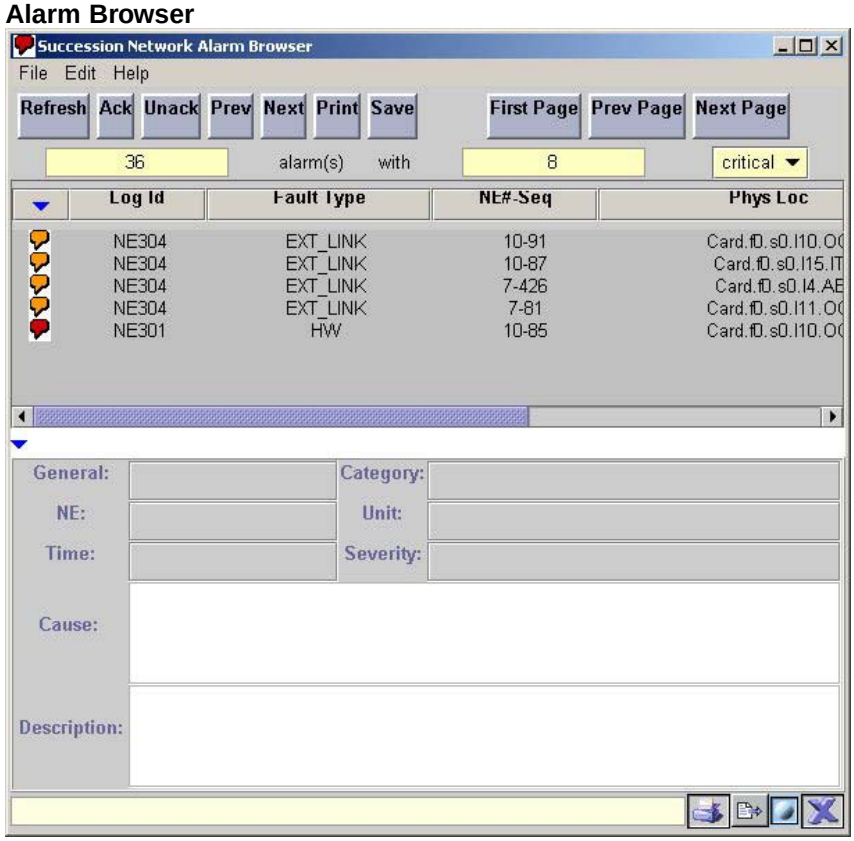
7 Access the Alarm Browser by clicking on the Alarm Browser item in the Alarm menu.

Accessing the Alarm Browser



8 Verify that alarms appear in the Alarm Browser.

Alarm Browser



If the alarms	Do
appear on the Alarm Browser	step 10
do not appear on the Alarm Browser	step 9

9 Contact your next level of support.

10 You have completed this procedure.

—End—

Validating an Installation of the Universal Signaling Point Manager

Validating the Universal Signaling Point (USP) Manager installation involves logging into the USP manager, connecting to the shelves, and verifying the alarm data.

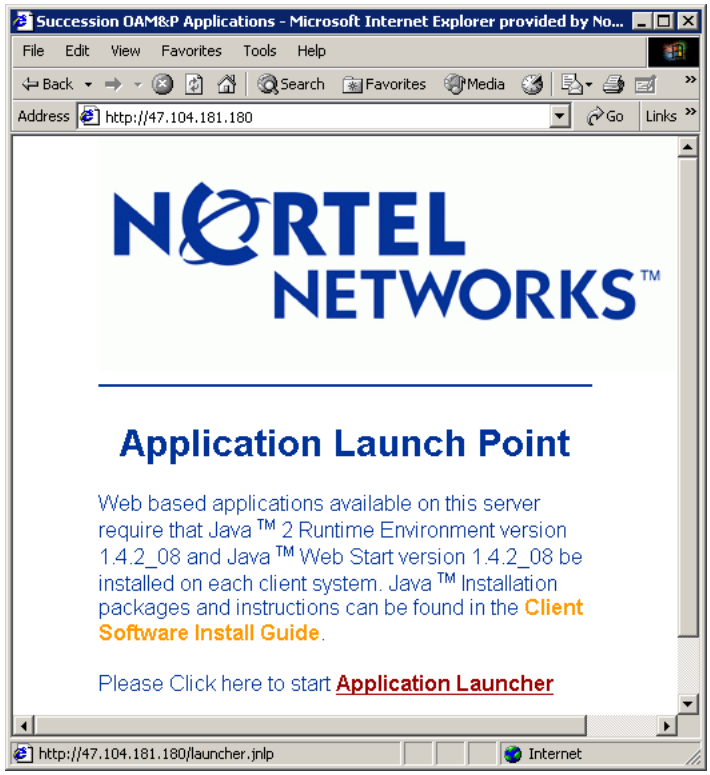
Validating the USP Manager installation

Step	Action

At the client workstation:

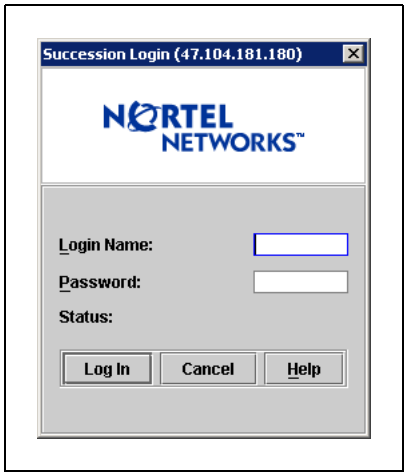
1 Using the web address valid for your site, launch the CS 2000 Management Tools application

The CMT application launch point appears:



2 Click on Application Launcher

The CMT Login screen appears

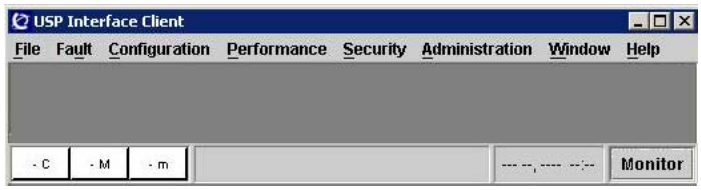


3 Enter your **Login Name** and **Password** information then select Login

The list of supported web-based applications appears:

4 Select the Universal Signaling Point Interface Client

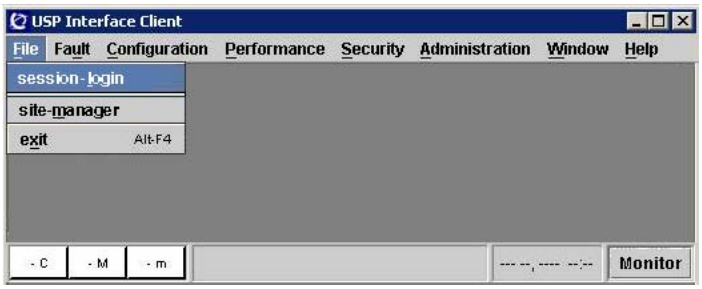
The USP Interface Client GUI appears:



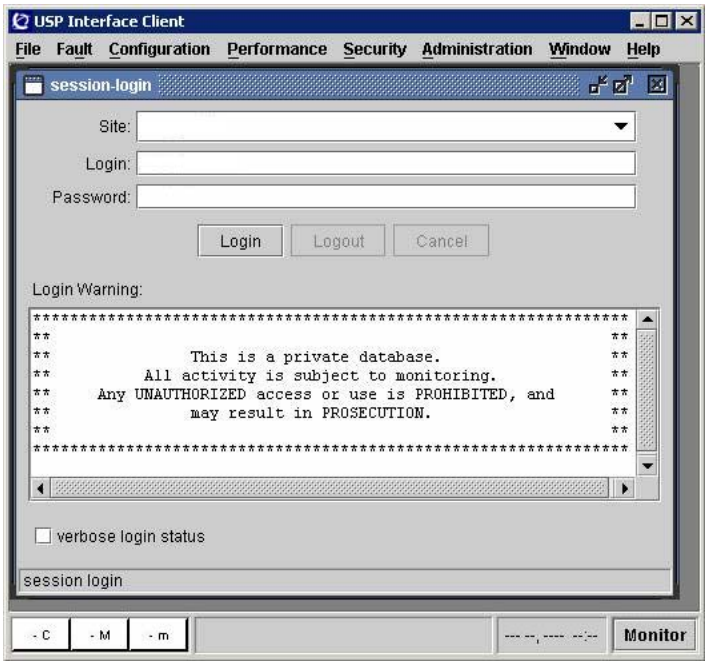
ATTENTION

The view provided in this sample system response shows an empty window. The USP Interface Client GUI window can open with an empty window or with either the **session-login** or **site-manager** pane appearing.

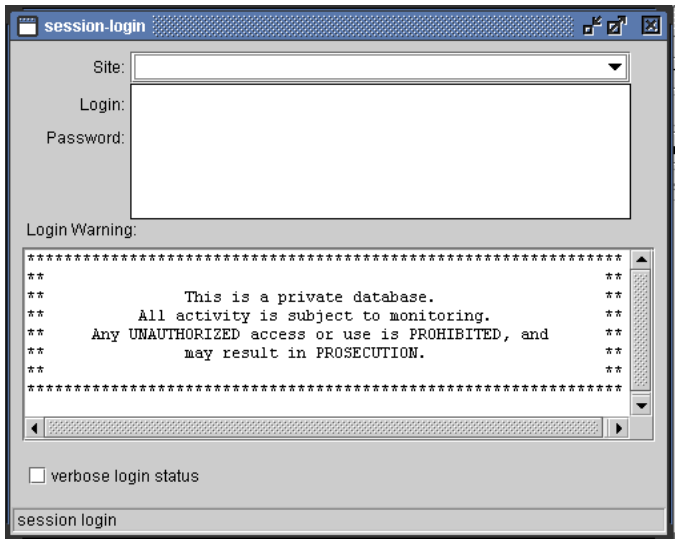
5 Select **session-login** from the **File** menu.



The USP Manager login screen appears:



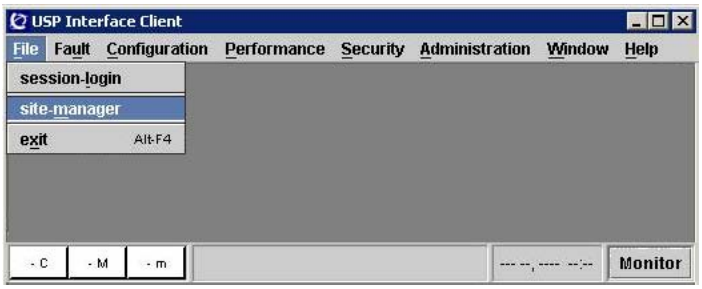
6 Click on the **Site** drop-down list.



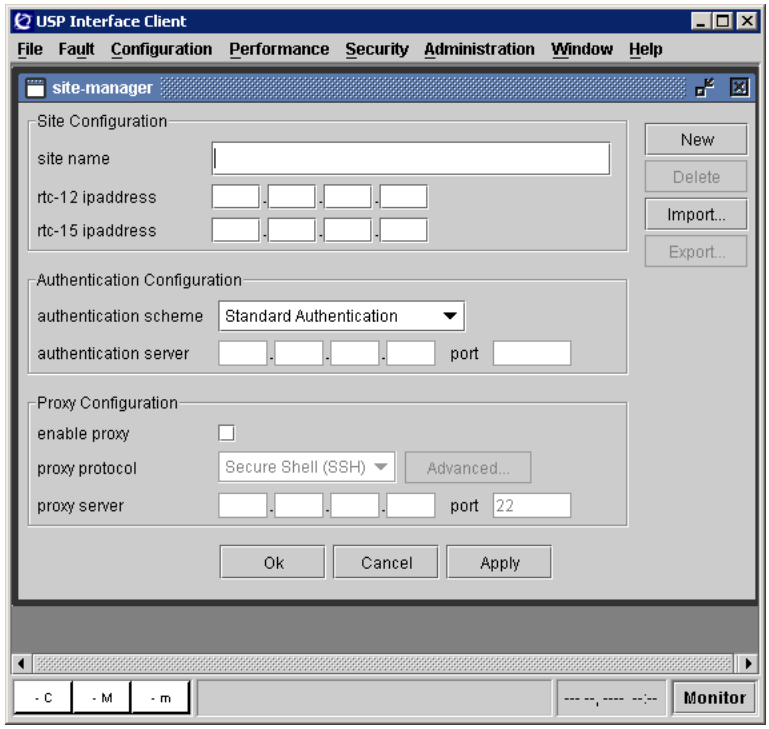
7 Select the next step as follows:

If the Site drop-down list …	Do
… is empty	Step 8
… does not contain the desired site	Step 8
… contains the desired site	Step 13

8 Select **site-manager** from the **File** menu.



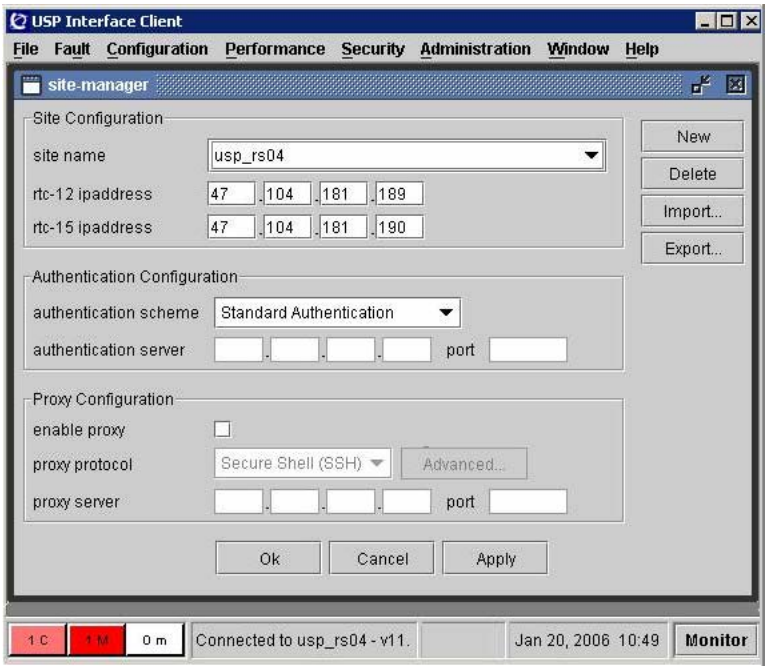
The site-manager window opens.



9 Select **New** to begin entering the required site information.

10 Enter the required **Site Configuration** information and select the appropriate **Authentication Configuration** information for the related drop-down menu.

The site information illustrated in the following serves as an example only.



Click on **Apply**.

ATTENTION

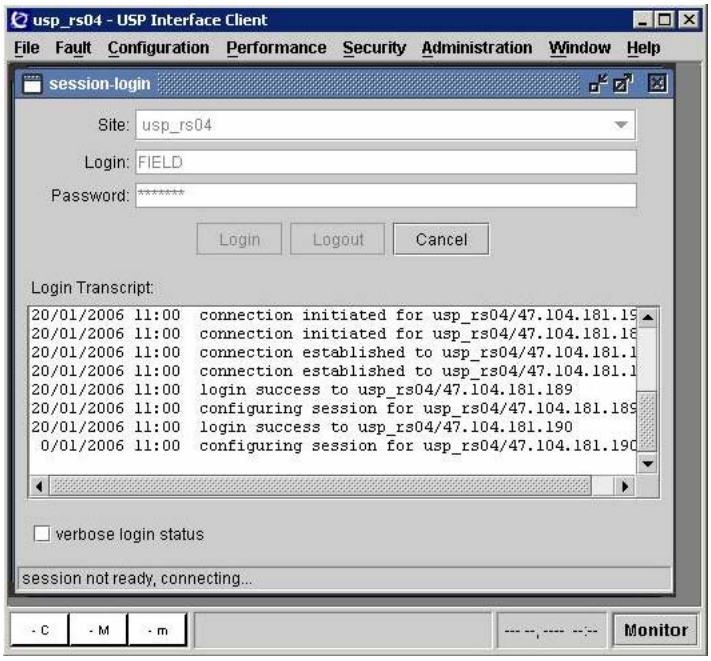
If necessary repeat this step to enter information for additional sites (pressing **Apply** to enter the information for each new site) until all required site information is entered.

11 Press **OK** to complete entering the required site information.

12 Go to Step 5

13 Select the desired **Site** from the drop-down menu, enter your **Login** and **Password** information, then click the **Login** button.

Observe the Login Transcript window below the Login screen. A sample of a login transcript appears in the following:

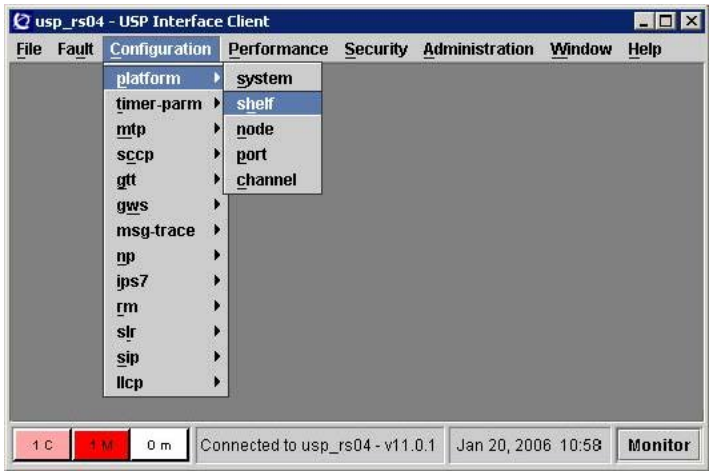


Following a successful login, an active session of the USP Interface Client appears. The task bar shows the alarm and connection status as well as the current time for the session.

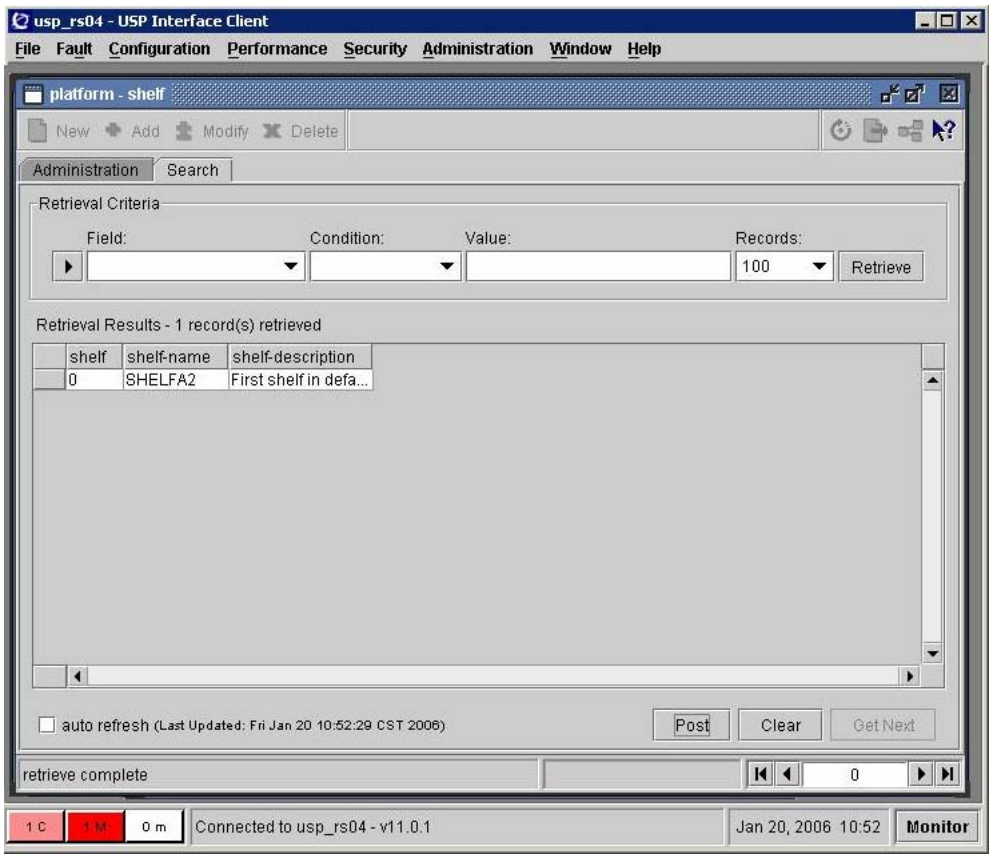
14 Select your next step as follows:

If your attempt to login to the USP manager …	Do
… completes successfully	Step 15
… fails	contact your next level of support

15 At the USP Client Interface GUI, select **Configuration >> platform >> shelf**



The platform-shelf window appears



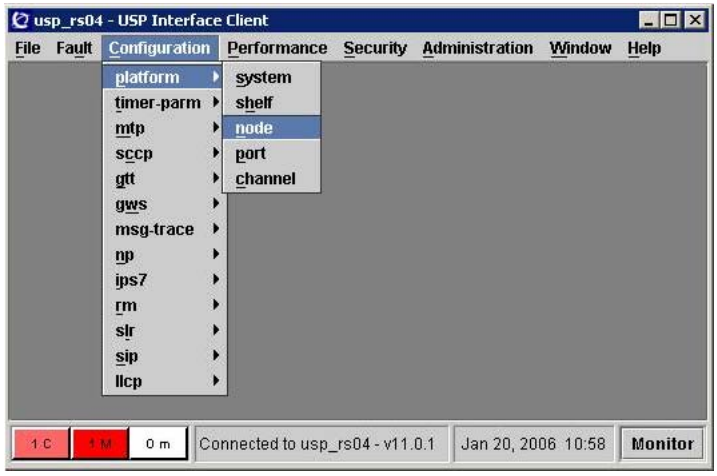
16 Check the **Retrieval Results** field.

ATTENTION

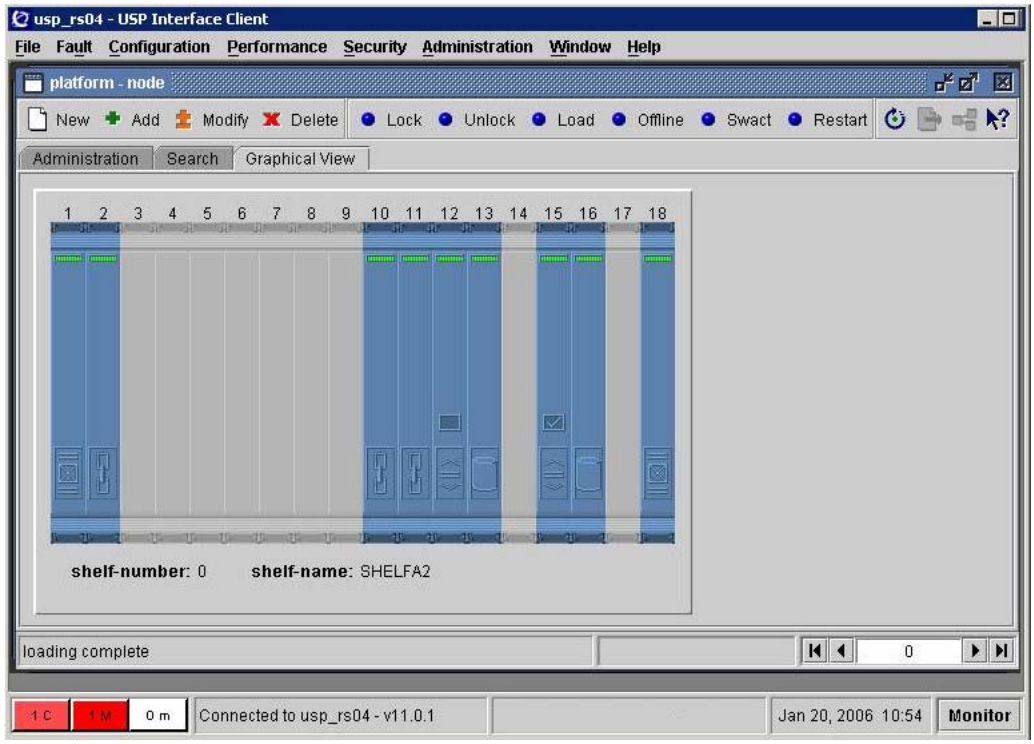
If the USP Interface Client is operating correctly, the **Retrieval Results** field lists one or more shelves.

If an error message appears, contact your next level of support.

17 At the USP Client Interface GUI, select **Configuration >> platform >> node**



The **platform-node** *window appears*



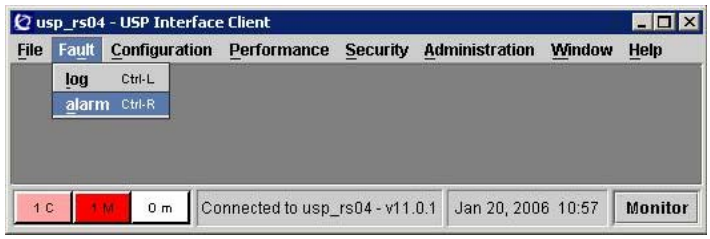
18 Select the **Graphical View** tab to display the blades inserted in a USP shelf.

ATTENTION

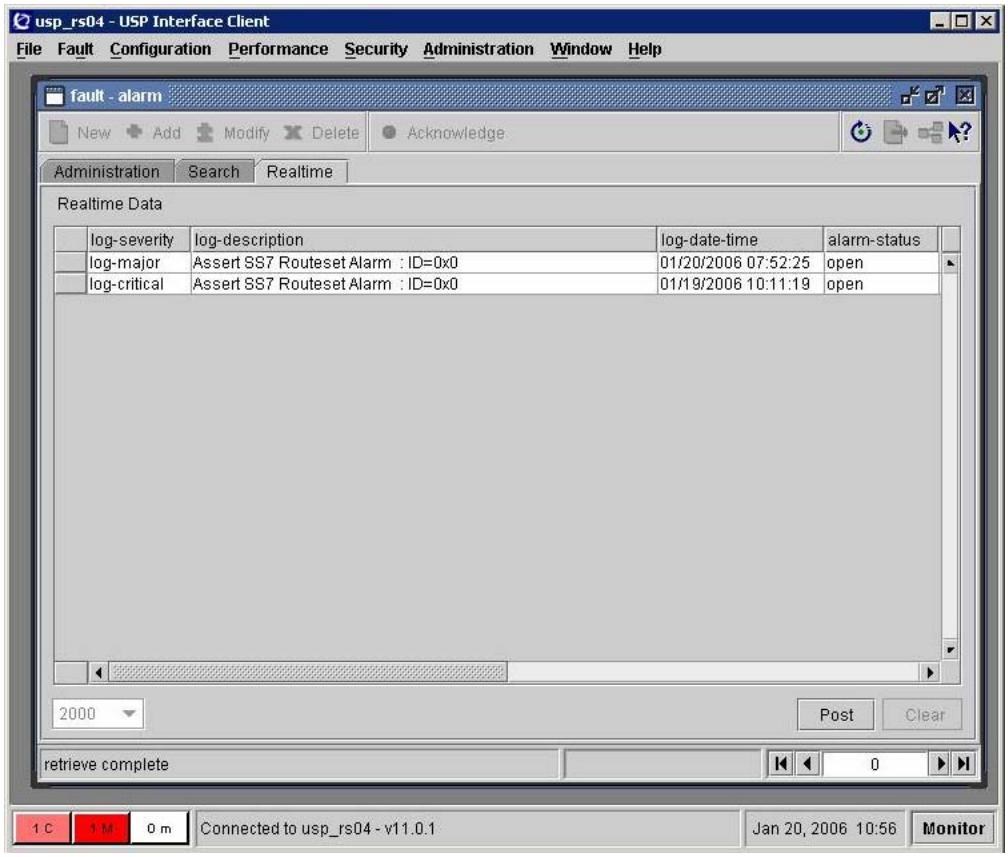
If the USP Interface Client is operating correctly, the **Graphical View** pane displays the blades inserted in a USP shelf.

If an error message appears, contact your next level of support.

19 At the USP Client Interface GUI, select **Fault >> alarm**



The **fault-alarm** *pane appears.*



20 When the **fault-alarm** pane appears, select the **Realtime** tab and check the **Realtime Data** list.

ATTENTION

The detailed information that appears in the **Realtime Data** list must agree with the alarm summary that appears at the left hand side of the task bar.

If the listed information does not agree with the task bar summary, or you receive an error report, contact your next level of support.

—End—

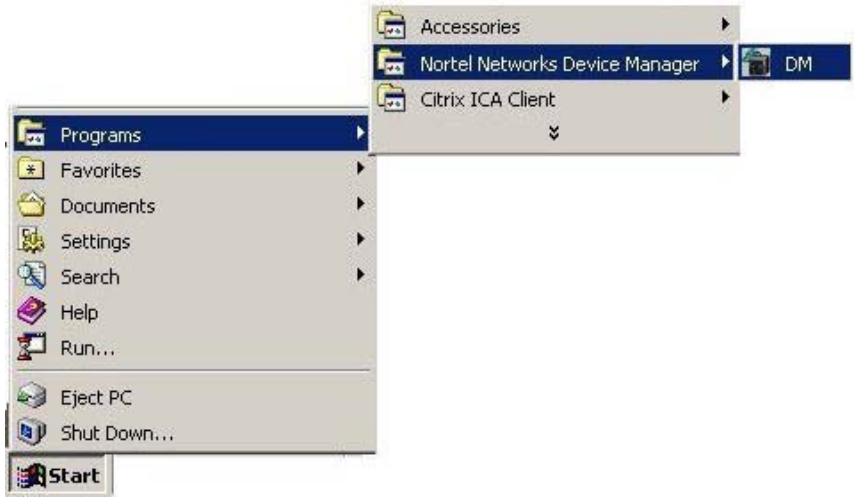
Validating an Installation of the Device Manager

Validating the Device Manager installation involves logging into the Device Manager client and running diagnostics to verify connection between the client and server.

Validate the Device Manager installation

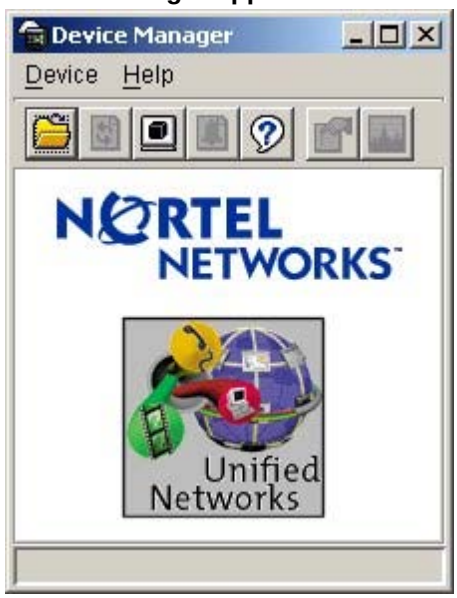
Step	Action
	At a Windows PC
1	Using the Windows Start menu, access the Device Manager by selecting the DM item from the Nortel Device Manager menu.

Accessing the Device Manager Application



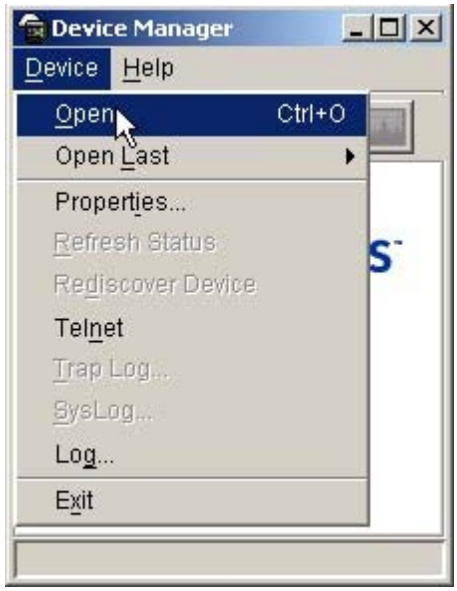
2	The Device Manager application client window will appear.

Device Manager application client



3 Select the Open item from the Device menu.

Selecting the Open item

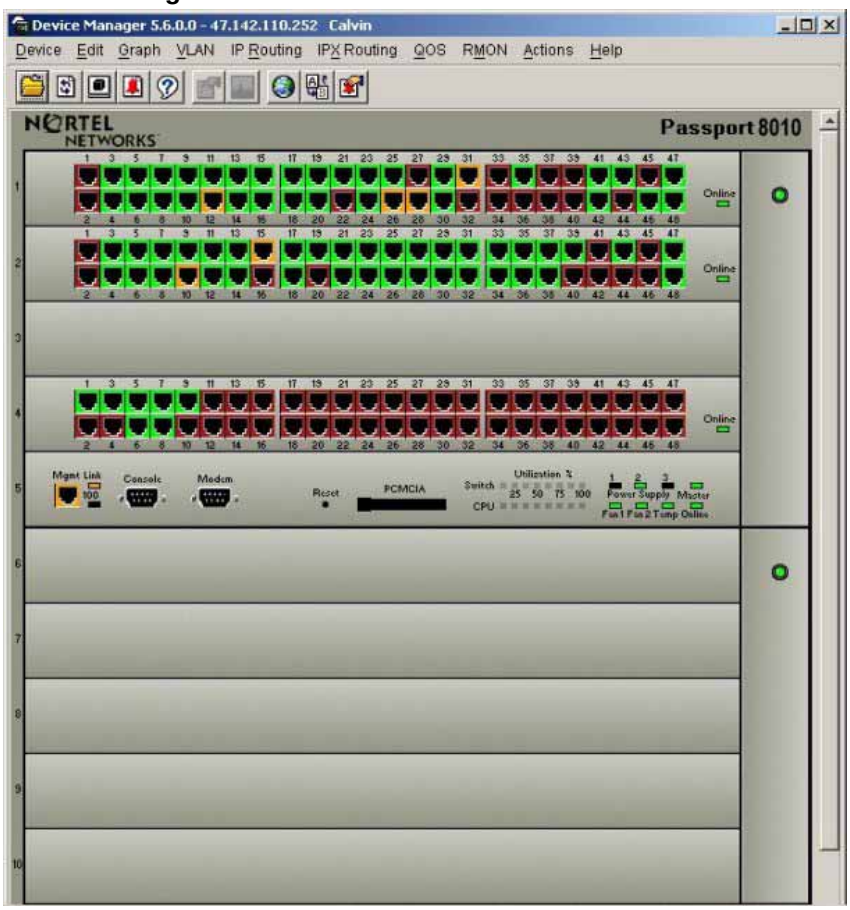


4 In the Open Device window, enter the IP address of the Device to which you wish to connect and click the Open button.

Open Device window

5 The Device Manager GUI will appear.

Device Manager GUI



6 Verify that the client GUI appears.

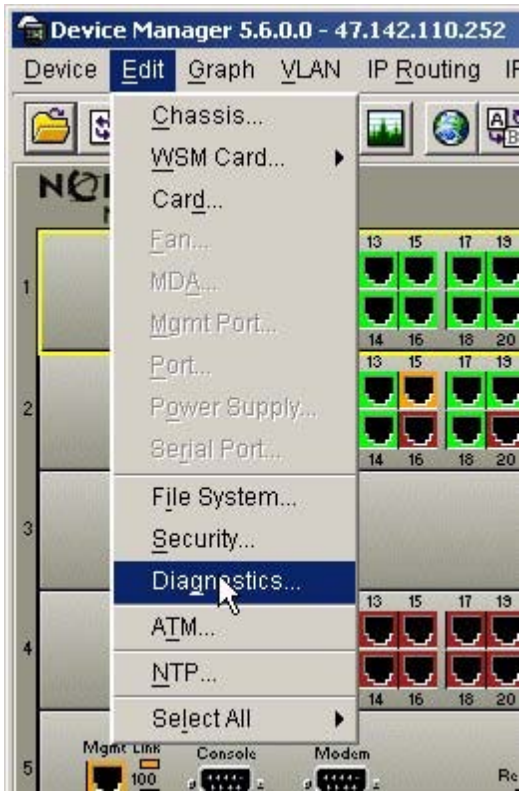
If the Device Manager client	Do
appears	step 7
does not appear	step 11

7 Select one of the ports by clicking on it with the left mouse button.

Selecting a port

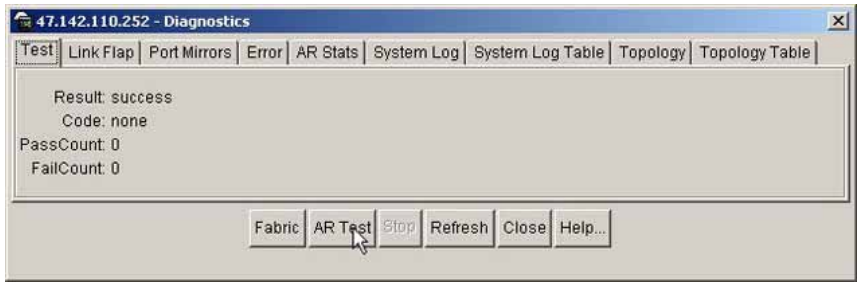
8 Select the Diagnostics item from the Edit menu.

Selecting Diagnostics



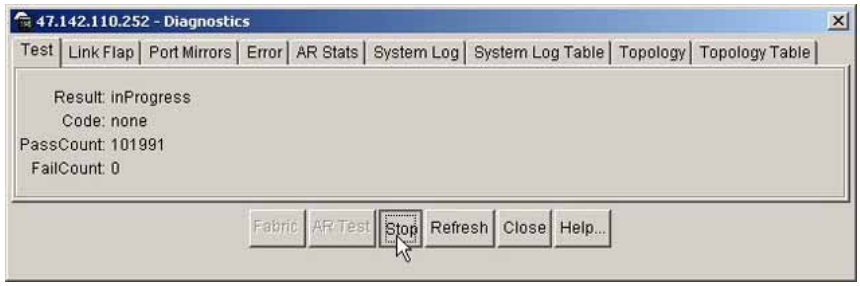
9 Start an AR test by clicking on the AR Test button.

Starting the AR test



10 Allow about a minute for the test to run. The PassCount should increase as the window is automatically refreshed. After the PassCount has increased, you can stop the test by pressing the Stop button.

Stopping the test



If the diagnostics ran	Do
with no errors	step 12
with errors	step 11

11 Contact your next level of support.

12 You have completed this procedure.

—End—

Validating an installation of the LMM

Validating the LMM installation involves logging into the LMM and checking the connection between the client and server.

Validating the LMM installation

Step	Action

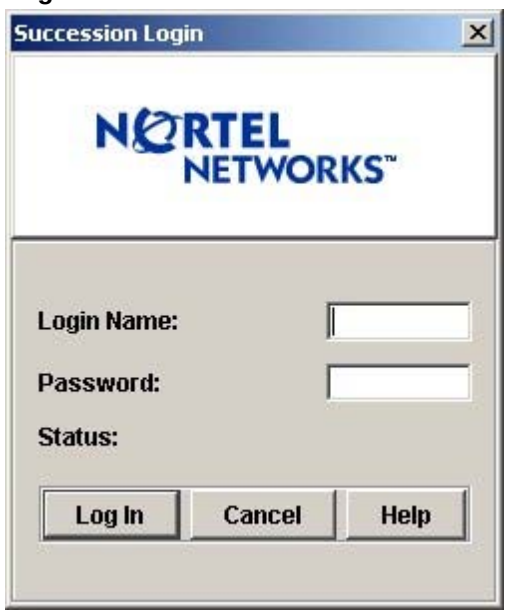
At a web browser

1 Access the Application Launch Point on the server on which you installed the LMM.

LMM Application Launch Point

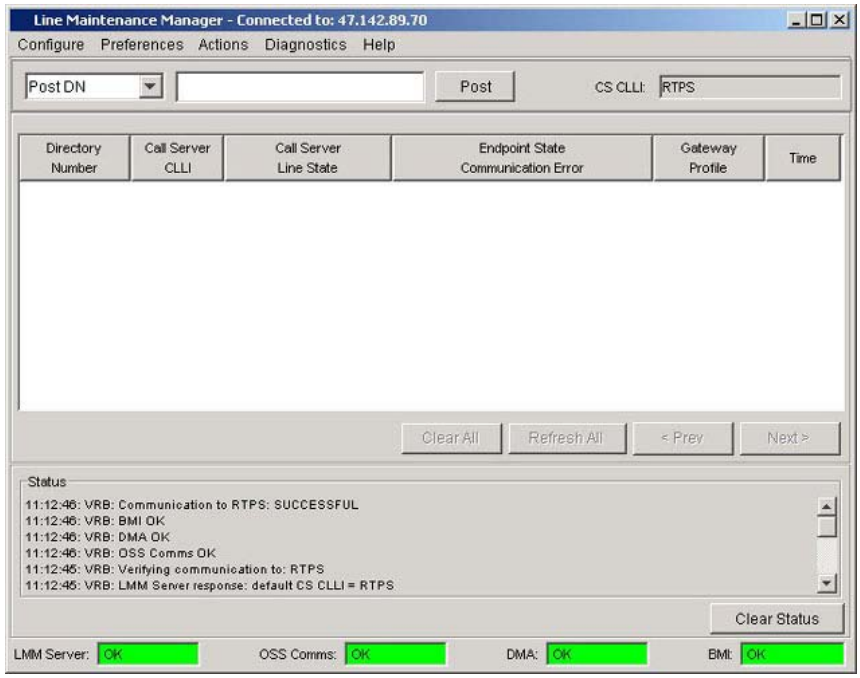
2 Click on the link for the Line Maintenance Manager. Once the application loads, you will be asked to for a User Name and Password to access the manager.

Login screen



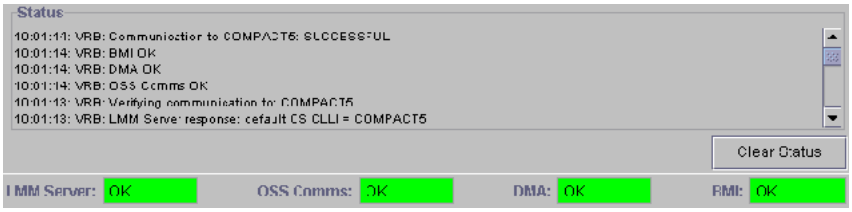
3 The LMM GUI will appear.

LMM GUI



4 Upon successful connection to the LMM server, the Status area should contain similar output to that found in the following example.

LMM Status area



If the LMM status area reports	Do
no errors	step 6
any errors	step 5

5 Contact your next level of support.

6 You have completed this procedure.

—End—

Setting up local user accounts on an SPFS-Based Server

Application

Use this procedure to add local user accounts on a Server Platform Foundation Software (SPFS)-based server and assign them to user groups. Also use this procedure to assign existing user accounts to user groups. For information on user groups, see "Additional information" (page 383).

If you choose to centrally manage your user accounts, refer to procedure "Adding new users" in *IEMS Security and Administration* (NN10336-611).

If you want to launch the ping and traceroute operations that are performed remotely on SPFS-based platforms from a centralized GUI on Integrated Element Management System (IEMS), refer to procedures "Running a ping test on the GWC network element or SPFS platform" and "Running a traceroute test on the GWC network element or SPFS platform" in *IEMS Basics* (NN10329-111).

ATTENTION

User accounts and passwords are automatically propagated from the active server to the inactive server in a high-availability (two-server) configuration to allow users to log in to either server. However, user files are not propagated to the other server.

Prerequisites

To perform this procedure, you need to have the root user ID and password to log in to the server.

Action

Perform the following steps to complete this procedure.

ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

Step	Action
	At your workstation
1	Log in to the server by typing `> telnet <server>` and pressing the Enter key. where

server is the IP address or host name of the SSFPS-based server

In a two-server configuration, log in to the active server using its physical IP address.

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Use the following table to determine your next step.

If you are	Do
adding a new user	step 6
assigning an existing user to secondary user groups	step 11

6 Add the user to the primary user group *succssn* by typing

```
useradd -d /export/home/<userid> -g succssn -G
<any additional groups> -m <userid>
```

and press the Enter key.

where

userid is a variable for the user name

7 Create a password for the user you just added by typing

```
# passwd -r files <userid>
```

and press the Enter key.

where

userid is the user name you added in the previous step

8 When prompted, enter a password of at least three characters.

It is not recommended to set a password with an empty value. Use a minimum of three characters.

9 When prompted, enter the password again for verification.

10 Proceed to step 13.

11 Determine which groups the user currently belongs to by typing

```
# groups <userid>
```

and pressing the Enter key.

where

userid is a variable for the user name

12 Note the user groups the user currently belongs to.

13 Assign the user to one or more secondary user groups by typing

```
# usermod -g succssn -G <groupA,groupB,...>
<userid>
```

and pressing the Enter key.

where

groupA, groupB,... are the secondary user groups (see table "Secondary user groups" (page 383)) and any other user groups you noted in step 12 to which the user already belonged Include a comma between groups, but no space.
userid is a variable for the user name

Example input for a user who can perform line and trunk maintenance operations

```
# usermod -g succssn -G lnmtc,trkmtc johndoe
```

The usermod command overwrites any previous user groups. Therefore, anytime you enter this command, specify all the user groups for the user.

You have completed this procedure.

—End—

Additional information

Users of the Nortel OAM&P client applications must belong to the primary user group succssn for login access. Users must also belong to one or more secondary user groups listed in the following table, which specify the operations a user is authorized to perform.

Secondary user groups

trkadm	lnadm	mgcadm	mgadm	emsadm	secadm
trkrw	lnrw	mgcrw	mgrw	emsrw	secrw
trksprov	lnsprov	mgcsprov	mgsprov	emssprov	secmtc
trkmtc	lnmtc	mgcmtc	mgmtc	emsmtc	secro
trkro	lnro	mgcro	mgro	emsro	

A secondary user group consists of

- a user group domain
- a user group operation

User group domain

A user group domain defines the range of applications to which a user group applies. The user group domains are listed in the following table:

Domain	Application mapping
trk	trunks, trunk-based services, small trunking gateways (port level), carrier-based services
ln	line services, line cards, small line gateways (port level)
mgc	CS2K, CS3K, USP, GWC, SAM21, IMS, 3PC, Storm, CS 2000 SAM21 Manager, CS 2000 GWC Manager
mg	small and large gateways such as UAS, line gateways, trunk gateways
ems	SDM, MDM, MDP, KDC, device manager, NPM

User group operation

A user group operation dictates the operations a user can perform using the Nortel OAM&P client applications. The user group operations are listed in the following table:

Operation	User role mapping
adm (administration)	Can reconfigure, access all functions, setup fundamental configuration, commission (add, delete, rehome), base frames and systems (SAM21 frames, call servers, large gateways), and run service-impacting diagnostics. The adm user can also do rw, sprov, mtc, and ro user operations.
rw (read/write)	Can view and change configuration and status, commission and reconfigure elements (GWCs, cards, shelves). The rw user can also do sprov, mtc, and ro user operations.
mtc (maintenance)	Can view status and configuration, make changes to status, and run service-impacting diagnostics. The mtc user can also do sprov and ro user operations.
sprov (subscriber provisioning)	Can view status and configuration and change provisioning data, but cannot change maintenance state or do base component configuration. The sprov user can also do ro user operations.
ro (read-only)	Can view status and configuration, but cannot make changes.

When assigning users to secondary user groups, use the tables that follow, which provide a mapping between commands and secondary user groups. The list of the available tables is as follow:

The mappings of commands to secondary user groups in the tables in this section do not apply to Multiservice Data Manager (MDM) when installed on a SPFS-based server.

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
View alarms, cards, subnet, shelf, mate shelf, mate card					x
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			
Perform a swact			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Add carrier		x			
Delete carrier		x			
Get endpoint					x
Get carrier					x
Get carrier by filter					x

Alarm operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
View/filter alarms					x

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro

Add, delete, change SPC	x				
Query SPCs					x
Set network VCAC	x				
Add, delete, change a network zone	x				
Query one or all network zones					x
addMPGroup	x	x			
changeMPGroup	x	x			
queryMPGroup	x	x	x	x	x
deleteMPGroup	x	x			
addVPN	x	x			
deleteVPN	x	x			
queryVPN	x	x	x	x	x

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Get tuple					x
Get tuple range					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro

Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
Post by gateway					x
Maintenance by gateway			x		
Post by carrier					x
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x
D-channel maintenance by trunk CLLI			x		
ICOT			x		
Set Auto Refresh					x

ADSL provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Get subscriber					x
Add subscriber				x	
Add cross connection				x	
Modify subscriber				x	
Modify cross connection				x	

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Delete subscriber				x	
Delete cross connection				x	

Line provisioning operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
ECHO, QX75, QBB, QBERT, QCM, QCOUNTS, QCPUGNO, QDCH, QDN, QDNA, QGRP, QHLR, QIT, QLEN, QLRN, QLT, QMODEL, QMSB, QPHF, QPRIO, QSCONN, QSCUGNO, QSIMR, QSL, QTOPSPOS, QTP, QWUCR					x
QCUST, QDNSU, QDNWRK, QHA, QHASU, QHU, QLENWRK, QLOAD, QMADN, QNCOS, QPDN	x				
All other supported commands for line provisioning				x	

Line maintenance operations

Command	User group				
	lnadm	lnrw	lnmtc	lnsprov	lnro
Validate line using DN CLLI					x
Validate line using TID CLLI					x
Get line post info					x
Busy line			x		
Return line to service			x		
Force release line			x		
Installation busy line			x		
Cancel deload			x		
Get CM CLLI					x
Get endpoint state					x
GetGwlp					x
run all TL1 line test commands			x		

V5.2 provisioning operations

Com-mand	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
Add, delete, modify V5.2 interface		x					x			

Com-mand	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
View all V5.2 interfaces					x					x
View signalling channel information entry, update list (V5 Prov)					x					x
Add, modify, delete signalling channel information entry (V5Prov)		x					x			
View ringing cadence mapping, update list (V5 Ring)					x					x
Add, modify, delete ringing cadence mapping (V5 Ring)		x					x			

Com-mand	User group									
	trkadm	trkrw	trkmtc	trksprov	trkro	lnadm	lnrw	lnmtc	lnsprov	lnro
View signalling characteristic profile, update list (V5 Sig)					x					x
Add, delete, modify signalling characteristic profile (V5Sig)		x					x			
View carrier-to-interface and interface-to-carrier mappings					x					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
apply, remove, activate, deactivate, auditd, restart, and	x				

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
smartimage from the NPM GUI or CLUI					
Software image from MG 9000 Manager GUI		x			

Automated upgrade operations

Com-mand	User group									
	emsadm	emsrw	emsmtc	emsprov	emkro	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Access and run the GWC upgrade CLUI			x					x		
Access and run the SC upgrade CLUI			x					x		

Ping and traceroute operations

Command	User group		
	emsadm	emsrw	emsmtc
Launch remote ping	x	x	x
Launch remote traceroute	x	x	x
These operations are for remote operations performed on SPFS platforms but launched from a centralized GUI on IEMS.			

- "Node provisioning operations" (page 396)

Node provisioning operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Disassociate a media gateway (MG) from a gateway controller (GWC)		x			
Associate an MG with a GWC		x			
Change the provisioning data for an MG		x			
Query site info					x
Query a GWC					x
Query an MG					x
change MG GWCEM data		x			
Get policy enforcement point (PEP) server data					x
Query a GWC PEP connection					x
Get dynamic quality of service (DQoS) policies data					x

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add or change a network address translations (NAT) device		x			
Query a NATdevice					x
Add, change, delete a media proxy (MP)		x			
Add, change, delete resource usage (RU)		x			
Query RU					x
Add, change, delete limited bandwidth links (LBL)		x			
Query LBL					x
Display call agent identification (ID)					x
Set or change call agent ID		x			
Change root middleboxes		x			
Add, modify, or decommission a SAM21 network element		x			
Reprovision a SAM21 node		x			
Configure IPoA services, ATM PMC addresses		x			
View alarms, cards, subnet, shelf, mate shelf, mate card					x

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Lock/unlock a card			x		
Perform diagnostics			x		
Modify provisioning		x			
Perform a swact (refer to the notes that follow this table)			x		
Firmware flash			x		
Assign/unassign services		x			

Audit operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Configure audit	x				
Run audit	x				
Get audit description					x
Get audit configuration					x
Get list of registered audits					x

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Retrieve audit report					x
Take action on problem	x				

Carrier provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Add carrier		x			
Delete carrier		x			
Get endpoint					x
Get carrier					x
Get carrier by filter					x

Alarm operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
View/filter alarms					x

Internet transparency operations

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, delete, change SPC	x				
Query SPCs					x
Set network VCAC	x				

Command	User group				
	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro
Add, delete, change a network zone	x				
Query one or all network zones					x

Trunk provisioning operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Get tuple					x
Get tuple range					x
Add tuple		x			
Replace tuple		x			
Delete tuple		x			

Trunk maintenance operations

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
Post by trunk CLLI					x
Maintenance by trunk CLLI			x		
Post by gateway					x
Maintenance by gateway			x		
Post by carrier					x
Maintenance by carrier			x		
D-channel Post by trunk CLLI					x

Command	User group				
	trkadm	trkrw	trkmtc	trksprov	trkro
D-channel maintenance by trunk CLLI			x		
ICOT			x		
Set Auto Refresh					x

Patching operations

Command	User group				
	emsadm	emsrw	emsmtc	emssprov	emsro
apply, remove, activate, deactivate, auditd, restart, and smartimage from the NPM GUI or CLUI	x				
Software image from MG 15000 Manager GUI		x			

Automated upgrade operations

Com-mand	User group									
	emsadm	emsrw	emsmtc	emssprov	emkro	mgcadm	mgcrw	mgcmtc	mgcsprov	mgcro

Access and run the GWC upgrade CLUI			x					x		
Access and run the SC upgrade CLUI			x					x		

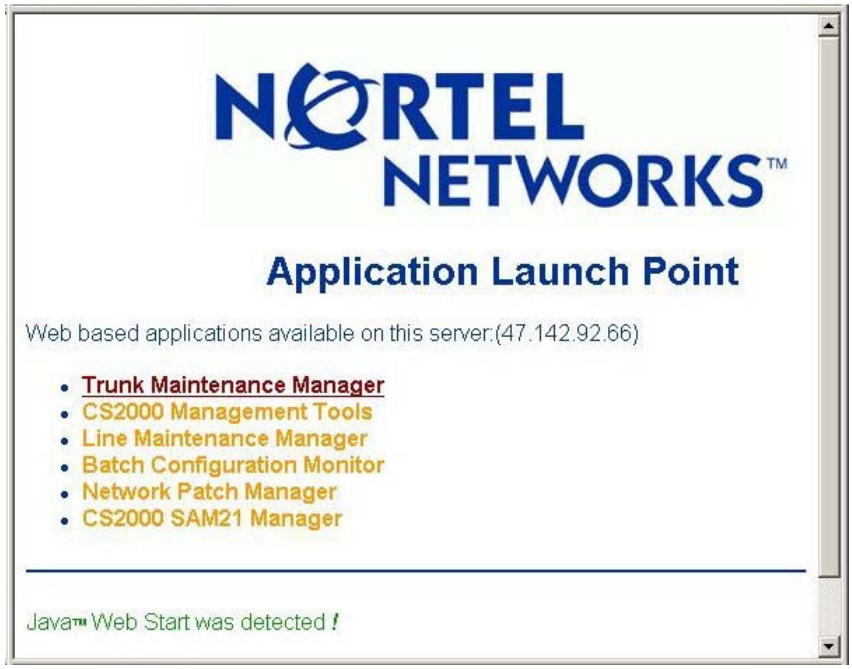
Validating an Installation of the TMM

Validating the TMM installation involves logging into the TMM client and verifying that the links in the client window work properly.

Validate the TMM installation

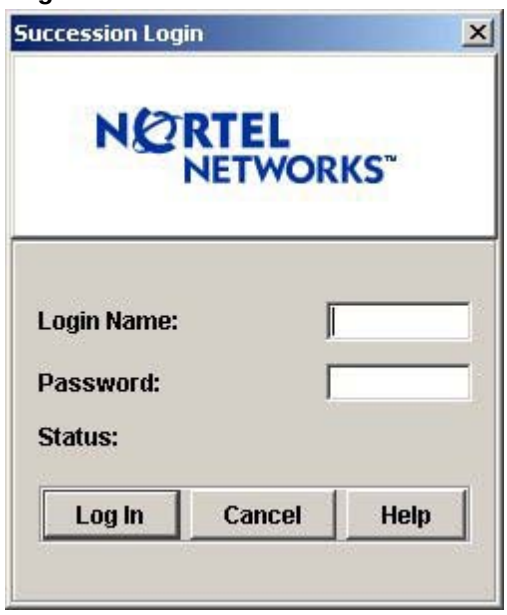
Step	Action
	At a web browser
1	Access the Application Launch Point on the server on which you installed the TMM.

TMM Application Launch Point



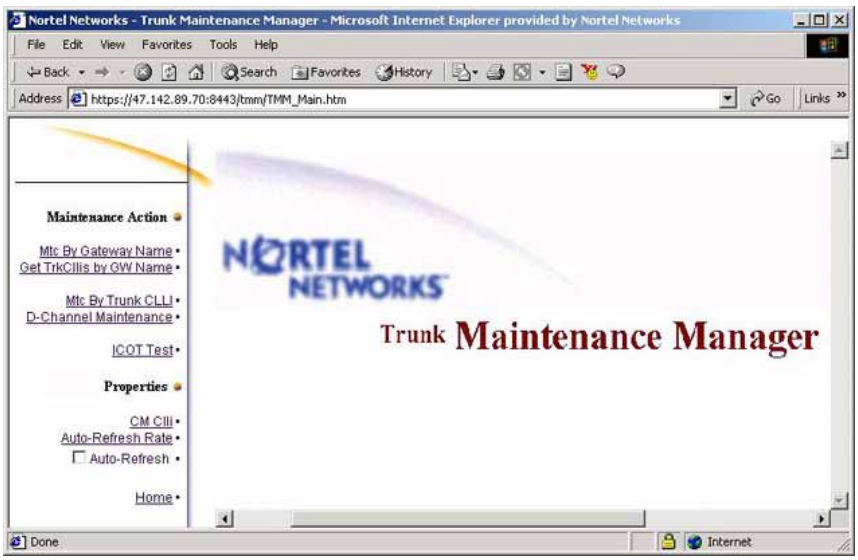
2	Click on the link for the Trunk Maintenance Manager. Once the application loads, you will be asked to for a User Name and Password to access the manager.

Login screen



3 The TMM GUI will appear.

TMM GUI



4 Verify that clicking on each of the links on the GUI takes you to the appropriate action or property page.

If the links are	Do
working properly	step 6
not working properly	step 5

5 Contact your next level of support.

6 You have completed this procedure.

—End—

Setting a limit for login retries on an SPFS-based server

Application

Use this procedure to set a limit on the number of login retries on a Server Platform Foundation Software (SPFS)-based server. When a user exceeds the number of login retries specified, the user loses connection to the host.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Step	Action
	At your workstation
1	Log in to the server by typing **`> telnet <server>`** and pressing the Enter key. where **`server`** is the IP address or host name of the SPFS-based server on which you want to modify the login greeting
2	When prompted, enter your user ID and password.
3	Change to the root user by typing **`$ su -`** and pressing the Enter key.
4	When prompted, enter the root password.

5	Access the command line interface by typing
	`# cli`
	and pressing the Enter key.
	Example response
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	`X - exit`

```
select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
  1 - NTP Configuration
  2 - Apache Proxy Configuration
  3 - OAMP Application Configuration
  4 - CORBA Configuration
  5 - IP Configuration
  6 - DNS Configuration
  7 - Syslog Configuration
  8 - Remote Backup Configuration
  9 - Database Configuration
 10 - NFS Configuration
 11 - Bootp Configuration
 12 - Restricted Shell Configuration
 13 - Security Services Configuration
 14 - Disk Drive Upgrade
 15 - Login Session
 16 - Location Configuration
 17 - Cluster Configuration
 18 - Succession Element Configuration
 19 - snmp_poller (SNMP Poller Configuration)
 20 - backup_config (Backup Configuration)
  X - exit
Select -
```

7 Enter the number next to the "Login Session" option in the menu.

Example response

```
Login Session
1 - login_session_timeout (User Inactivity Timeout
Configuration)
2 - login_session_termination (User Termination Timeout
Configuration)
3 - login_session_reauthentication (User Reauthenticat
ion Disable Timeout Configuration)
4 - login_session_server (Login Session Master Server
Configuration)
5 - telnet_greeting (Telnet Login Greeting)
6 - login_retries (Login Retries Limit)
X - exit
select -
```

8 Enter the number next to the "login_retries" option in the menu.

Example response

```
===Executing "login_retries"
Current value for Login Retries is:
```

```
RETRIES=3
Enter the Login Retries Limit Value (1->15):
```

9 When prompted, enter the limit value for login retries.

Example response

```
==="login_retries" completed successfully
```

Exceeding the range of the login retries limit value generates the error message "ERROR - Login Retries Limit Value Out Of Range", at which point you are prompted to enter a value between 1 and 15.

10 Exit each menu level of the command line interface to eventually return to the command prompt, by typing

```
select - x
```

and pressing the Enter key.

You have completed this procedure.

—End—

Configuring Dark Office Backups on an SPFS-Based Server

Application

This procedure is designed for use in dark office conditions where the customer needs to copy backup data to a DVD or tape more than once before the DVD or tape is ejected from the server. Instead of ejecting the DVD or tape after every backup, this procedure allows a second backup to be written over the previous one.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

ATTENTION

Nortel recommends that provisioning activities be put on hold during the time of the data backup.

Prerequisites

This procedure has the following prerequisites:

- You must be running SPFS (I)SN06.2 or greater
- You must have performed a successful backup of Oracle data prior to performing Step 14. Refer to procedure Performing a backup of oracle data on an SSPFS-based server to complete this task.

  ATTENTION

  The data backup is not required prior to this procedure for the Core and Billing Manager (CBM) product family.

- For Sun Netra 240, use one or more blank DVD-R or DVD-RW disks to store the data

ATTENTION

The backup utility limits the storage to 4 GB on a DVD-R and DVD-RW.

If you are using a new DVD-RW, or want to reuse a used DVD-RW and need to erase the contents, complete procedure "Preparing a CD-RW or DVD-RW for use" in *ATM/IP Security and Administration* (NN10402-600).

Action

Perform the following steps to complete this procedure.

ATTENTION

If the data being backup is larger than 4 gigabytes (GB), an alarm is raised and the automated data backup aborted.

Step	Action

At your workstation

1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

<server> is the IP address or host name of the SPFS-based server on which you want to configure automated data backups

2 When prompted, enter your user ID and password.

3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

4 When prompted, enter the root password.

5 Access the command line interface by typing

```
# cli
```

and pressing the Enter key.

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
Select -
```

6 Enter the number next to the "Configuration" option in the menu.

Example response

```
Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Remote Backup Configuration
10 - Database Configuration
11 - NFS Configuration
12 - Bootp Configuration
13 - Restricted Shell Configuration
14 - Security Services Configuration
15 - Login Session
16 - Location Configuration
17 - Cluster Configuration
18 - Succession Element Configuration
19 - snmp_poller (SNMP Poller Configuration)
20 - backup_config (Backup Configuration)
X - exit
Select -
```

7 Enter the number next to the "backup_config (Backup Configuration)" option in the menu.

Example response

```
=== Executing "backup_config"
Automated Backup Menu
 1 - Configure backup settings
 2 - Schedule full system backup
 3 - View backup settings
 4 - Copy last Oracle backup to DVD or tape
X - exit
Select - [x, 1-4]
```

8 Select next step as follows:

To …	Do
… configure the backup settings	Step 9
… schedule a full system backup	Step 11
… view the backup settings	Step 13
… copy the last Oracle backup to DVD or tape	Step 14

9 Enter the number next to the "Configure backup settings" option in the menu.

Example response

```
Backup Settings Configuration
When a backup occurs, the following 3 modes will define
if the DVD needs to be ejected or not after a backup is
complete.  If using the automated full system backup,
its recommended that option 3 is chosen so that the
data can be overwritten after every auto scheduled
backup, provided all data can fit on single DVD-RW.
1 - When performing backup, eject DVD tray when done.
2 - When performing backup, do not eject DVD tray.
3 - When performing backup, do not eject DVD tray,
subsequent backups will overwrite previous data.
X - exit
Current setting => 1 select - [x, 1-3]
```

10 At the prompt, enter the number next to the backup option you want in the "Backup Settings Configuration" menu. Option 1 is the default.

Following the completion of the backup and restore operation, you will be able to physically eject the DVD using either the eject button or by typing eject in the command line interface.

11 Enter the number next to the "Schedule full system backup" option in the menu in step step 7.

Example response

```
Automated Full System Backup Configuration
WARNING: The full system backup backs up everything
except your oracle data. You will need to run the
Automated Synchronous Backup Restore Manager from an
IEMS Server to schedule a synchronized oracle backup.
Current Configuration Settings
Backup Enabled                : N
Backup Day                    : SUNDAY
Backup Hour                   : 1:00 Hours
Enable Automated Full System Backup (Default => N):
```

12 Enter the information required to configure the automated full system backup in the "Automated Full System Backup Configuration" menu.

Selecting no at the prompt results in menus being displayed that allow you to configure the day of the week and time for an automated full system backup. Set a day for the backup to run by selecting a number between 0 and 6 (0 for Sunday, 1 for Monday, 2 for Tuesday, 3 for Wednesday, 4 for Thursday, 5 for Friday, and 6 for Saturday). Set a time for the backup to run by entering a number from 1 to 24 that represents the matching hour in a 24 hour day.

13 Enter the number next to the "View backup settings" option in the menu in step step 7.

Example response

```
Automated Full System Backup
Configuration Settings
Backup Enabled                : N
Backup Day                    : SUNDAY
Backup Hour                      : 1:00 Hours
```

Selecting this option results in the display of the current configuration backup settings. The backup settings can not be configured using this menu.

14 Enter the number next to the "Copy last Oracle backup to DVD or tape" option in the menu in step step 7.

ATTENTION

The Synchronized Backup Manager needs to be configured and at least one scheduled backup must have been successfully performed before attempting to copy the last Oracle backup to the /data/bkresmgr/backup directory.

A system response displays whether the attempt to copy the last Oracle backup to the /data/bkresmgr/backup directory succeeded or failed. If the attempt to copy the backup fails, a reason for the failure is provided in the system response.

—End—

Carrier VoIP

Nortel ATM/IP Solution-level Configuration

Publication: NN10409-500
Document status: Standard
Document version: 04.03
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

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