ATM/IP Solution-level Configuration Management

What's new

The following table highlights the (I)SN07 features that affect configuration management.

Note: The terms Passport and PVG have been re-branded in conjunction with the new Nortel Networks brand simplified naming format. Passport is now referred to as the Nortel Networks Multiservice Switch, and PVG is now Media Gateway 7480/15000.

(I)SN07 ATM/IP features (Sheet 1 of 3)

Feature descriptions
CS 2000 features **A00003454 --Secure and firewall compatible Call Server 2000 Manager and UE9000 manager client GUI communication (PT-IP, UA-AAL1, UA-IP, IAC, Intl IAW, Intl IAC, Intl PT-IP, Intl UA-IP)** This feature facilitates firewall protection for traffic for the Succession OAM&P GUI Client/Server communication. The Succession GUIs will work even with the addition of a firewall in the customer network. The data sent through a firewall will also be encrypted. **A00003630 -- TGCP for the cable market (IAC)** This feature makes changes on the Core, GWC, and Call Server 2000 Manager (CS2M) to support ISUP IT, ISUP ATC, MF OP, and MF ES trunk signaling and associated services on a trunking gateway control protocol (TGCP) MG.

(I)SN07 ATM/IP features (Sheet 2 of 3)

Feature descriptions
A00001743 - Syslog consolidation for Succession (all solutions) This activity improves the Log Delivery application to: • provide a single consolidated northbound log feed for all the components in a Succession node • implement the initial phase of Lost Log detection for non-CM logs • enhance the Log Delivery applications capacity to handle traffic bursts • enhance the Logroute tool interfaces and to remove redundant processing **A00002741 - ECAN for trimodal, 9000-IP-IPW to legacy (UA-AAL1, UA-IP)** This feature enables SBA base RTB to be able to auto recover from downstream and network connectivity problems once the issues are resolved. **CICM features** **A00005986 -- CICM Manager integration with PAM+ proxy (Intl IAW)** This feature allows user authentication on the CICM Manager to be provided by the Pluggable Authentication Module (PAM+) proxy located on the SSPFS platform.
A00005987 -- CICM Provisioning, Backup and Restore (Intl IAW) This feature changes the provisioning process for the CICM, the CICM gateway, and the CICM Manager. The feature provides: • extension of the CICM Manager interface to provide an extensive provisioning interface to allow automatic CICM configuration once the CICM is physically installed and imaged • enhancements to the backup and restore process to provide a consistent recovery procedure that interfaces with the new provisioning method
Traffic Office Position System (TOPS) feature **A00005160 -- OSSAIN XA-CORE data messages capability enhancements (All solutions)** This feature enables OSSAIN data messaging to use XA-Core Ethernet interfaces such as the HIOP and the new HCMIC card. Prior to this activity, all OSSAIN messaging used the EIU (Ethernet Interface Unit).

(I)SN07 ATM/IP features (Sheet 3 of 3)

Feature descriptions

GWC/CCM feature

A00003459 -- SSC re-architecture (UA-AAL1, UA-IP, IAC, IAW, int'l IAW, int'l IAC, int'l UA-IP)

This feature covers a part of the SSC re-architecture. The feature provides four main enhancements:

- Adds a new alarm for Succession SYSB line. The class of the alarm (Major, Minor, or Critical) is displayed in the system status display under the Lns header of the MAPCI display.
- Generates a new log when the new Succession SYSB alarm is raised or cleared. The LINE 811 log is generated when a SYSB line alarm is either raised or cleared.
- Adds a new PM sub-level for LGRP. The user can post LGRP under the PM maintenance level on the MAPCI.
- Raises an alarm when there are LGRPs in the SYSB state.

From (I)SN07 onwards, the S-type LGRPs are set to OFFL state when they are initially provisioned in the XA-Core. (Prior to (I)SN07 the LGRPs were set to INSV when initially provisioned).

To enable the lines in the LGRP to be in service, the following states must be set from the XA-Core (MAPCI):

- After the virtual media gateway is added in MG9000, the LGRPs should be BSYed
- After the virtual media gateway is added in XA-Core, and the LGRP is MB in the XA-Core, the LGRPs should be RTSed

Overview

ATTENTION

This document addresses all Nortel Networks Succession solutions. Some statements may not apply to your solution. The North American IAW solution is not included in the (I)SN07 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)	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)

Note: Collectively, these two Succession solutions are referred to as ATM solutions.

Nortel Networks performs initial installation and commissioning of the 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 Networks delivers Succession 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 Networks 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 Networks, 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 Networks 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
  - Preside Multiservice Data Manager (Preside MDM) - provides FCAPS tasks for the Multiservice Switch 15000 and Media Gateway 7400/15000
  - Device Manager for Passport 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
  - Integrated EMS - 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, Passport 8600 commissioning for initial install via Command Line Interface (CLI) and respective element managers
- Media Gateway 7400/15000 provisioning via Preside Multi-Service Data Manager (Preside 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
- Integrated EMS addition of network elements, EMSs, EMS platforms, or EMS applications via the Integrated EMS wizard
- Nortel Media Server 2000 (MS 2000) configuration via MS 2000 Series Configuration Tool
- Auto hardware discovery of UAS to the UAS Manager
- Passport 8600 configuration via Passport 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 SSPFS
- 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 Passport 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 CDs 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 Succession Server Platform Foundation Software (SSPFS) 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 (Integrated EMS) is an application which ties all the OAM&P managers into a single integrated desktop environment. Integrated EMS 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

- Integrated EMS Configuration Management, NN10330-511
- MG9000 Configuration Management, NN10096-511
- MS 2000 Series Configuration Management, NN10340-511
- Mediant 2000 Gateway User Manual, LTRT00727
- Mediant 2000 Gateway Installation Guide, LTRT00904
- Nortel Networks Multiservice Switch 15000/20000 Hardware Description, NN10600-120
- Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade, NN10600-130
- SAM21 Manager Configuration Management, NN10111-511
- Session Server Configuration Management, NN10338-511
- 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 Succession 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
- CS 2000 Communication Server LAN (Passport 8600 and Device Manager)
- Universal Signalling Point and Universal Signalling Point Manager
- Media Gateway and Preside MDM
- CS 2000 Service Application Module 21 (SAM21) Manager
- CS 2000 Gateway Controller Manager
- Universal Audio Server Manager
- Service Application Module 21 (SAM21)
- Gateway 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 point codes 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 Succession 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 Succession 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 Succession component network configuration tasks in the following order:

- Communication Server 2000 (CS 2000) and the CS 2000 Core Manager
- CS 2000 Communication Server LAN (Passport 8600 and Device Manager)
- Universal Signalling Point and Universal Signalling Point Manager
- ATM core network and element management (Media Gateway 7480/15000 and Preside Multiservice Data Manager)
- 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

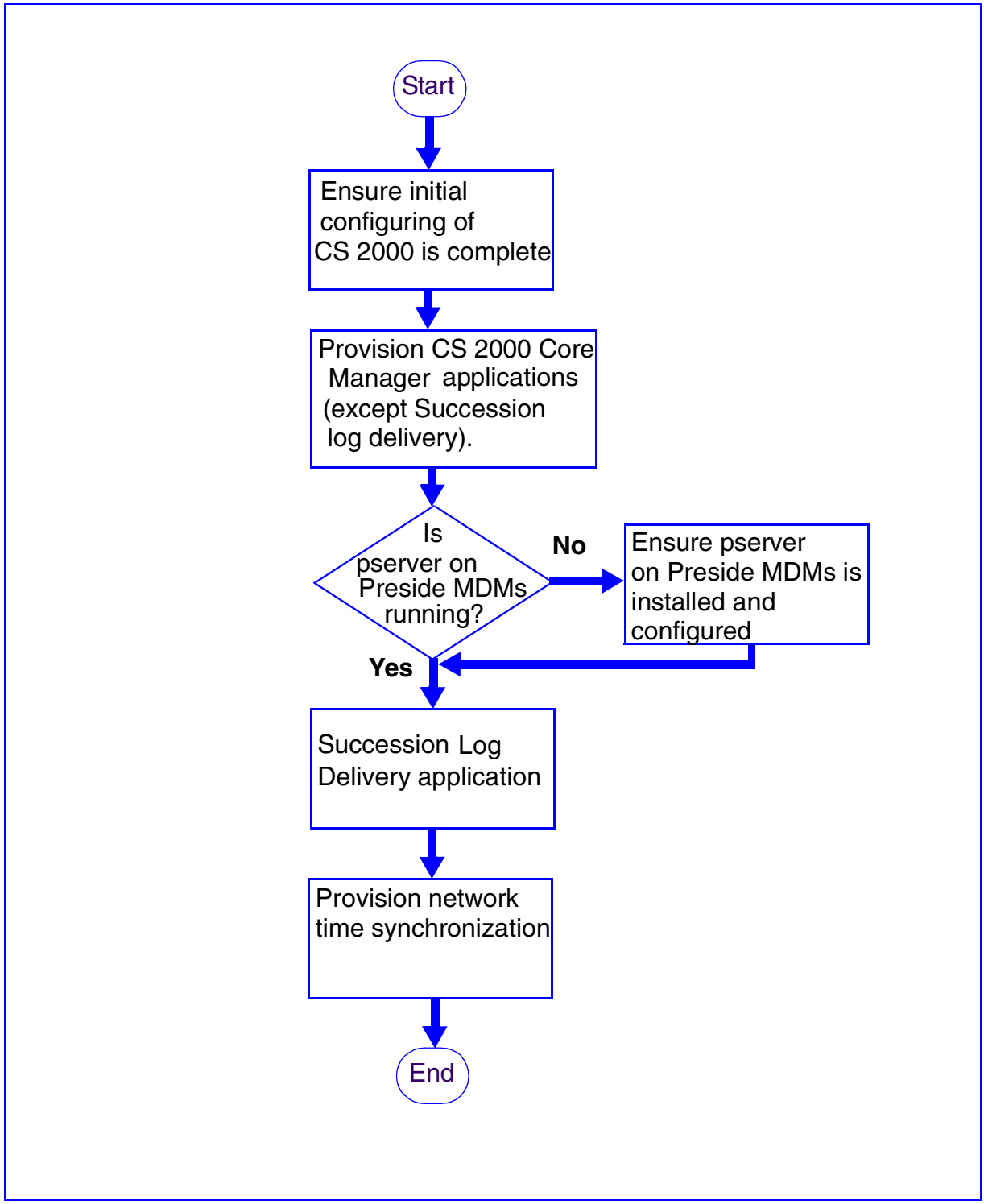
This section presents configuration task flows for the following ATM-based network elements:

Universal Access AAL1

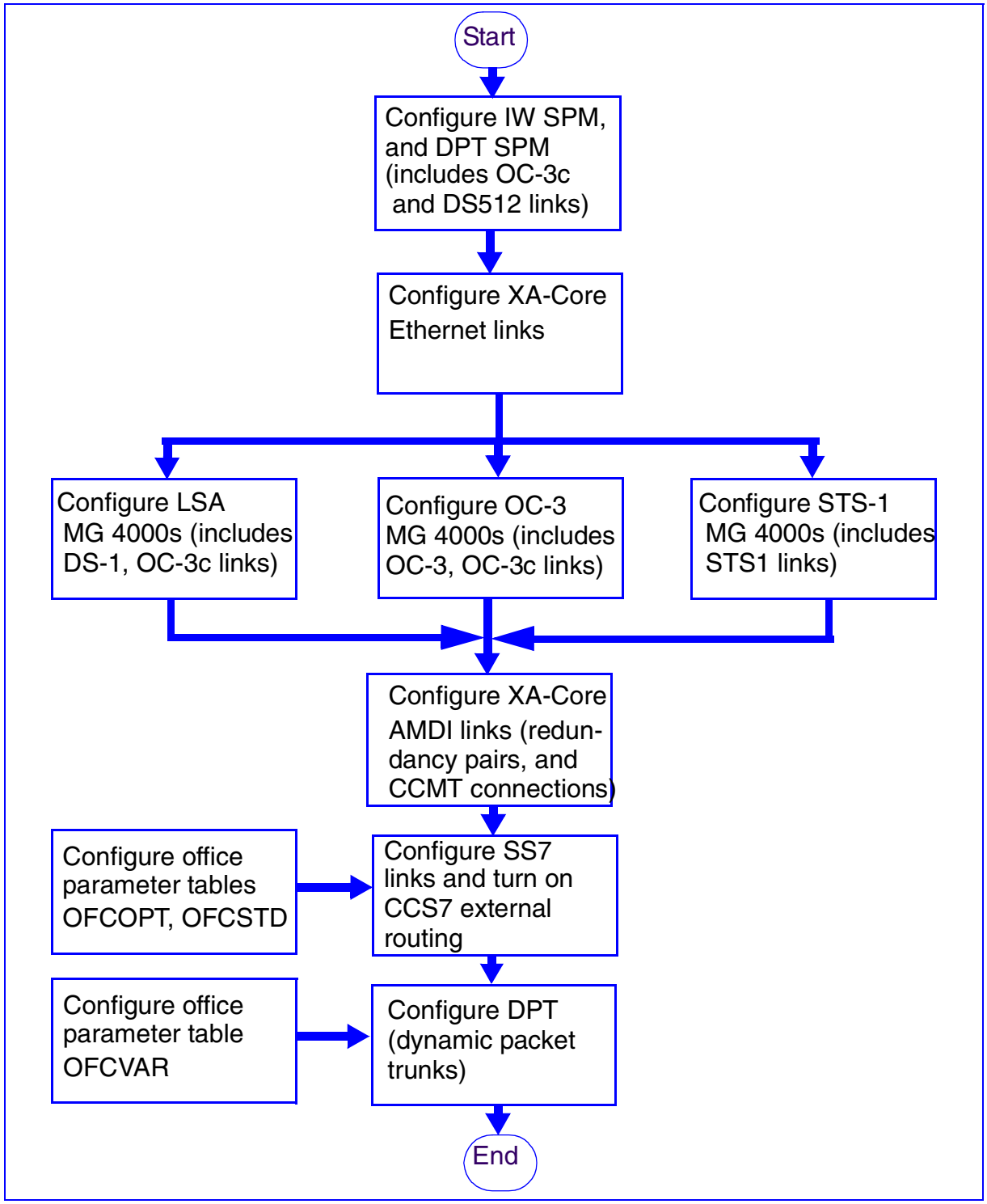
- Configuration tasks for CS 2000 Core Manager on page 16
- Configuration tasks for CS 2000, IW SPM, DPT SPM, and MG 4000 on page 17
- Configuration tasks for Media Gateway 7400/15000 and Preside MDM on page 18

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.

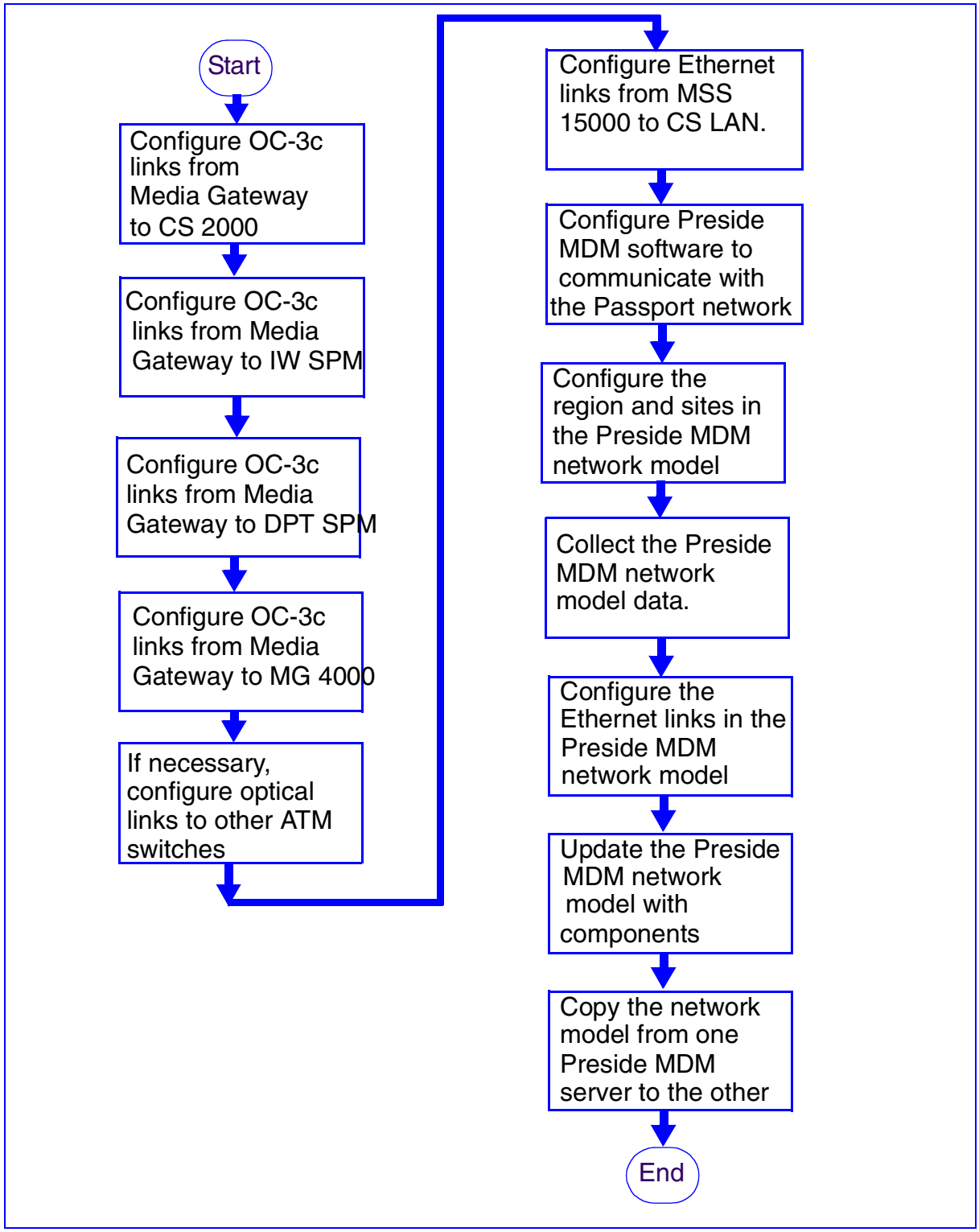
Configuration tasks for CS 2000 Core Manager



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



Configuration tasks for Media Gateway 7400/15000 and Preside MDM



Detailed configuration procedures

Network element	Configuration procedure location
NETWORK INTELLIGENCE	
CS 2000	Communication Server 2000 Configuration Management, NN10201-511
CS 2000 Communication Server LAN/Passport 8600	Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using the Command Line Interface Release 3.2, 313191A Configuring Switching and Routing Operations for the Passport 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
Universal Signalling Point	USP Configuration Management, NN10093-511
Universal Signalling Point Compact	USPc (compact) Configuration Management, NN10094-511
Real-time Transport Protocol (RTP) Media Portal	RTP Media Portal Basics, NN10367-111
CICM	CICM Configuration Management, NN10240-511
Session Server	Session Server Configuration Management, NN10338-511
CORE NETWORK	

Detailed configuration procedures

Network element	Configuration procedure location
Multiservice Switch 15000, Media Gateway 15000	Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP, NN10114-511
GATEWAYS	
MG 9000	MG 9000 Configuration Management, NN10096-511
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	Integrated EMS Configuration Management, NN10330-511
Preside Multiservice Data Manager	Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and Preside MDM in Succession Networks Configuration Overview PT-AAL1/UA-AAL1/UA-IP, NN10114-511

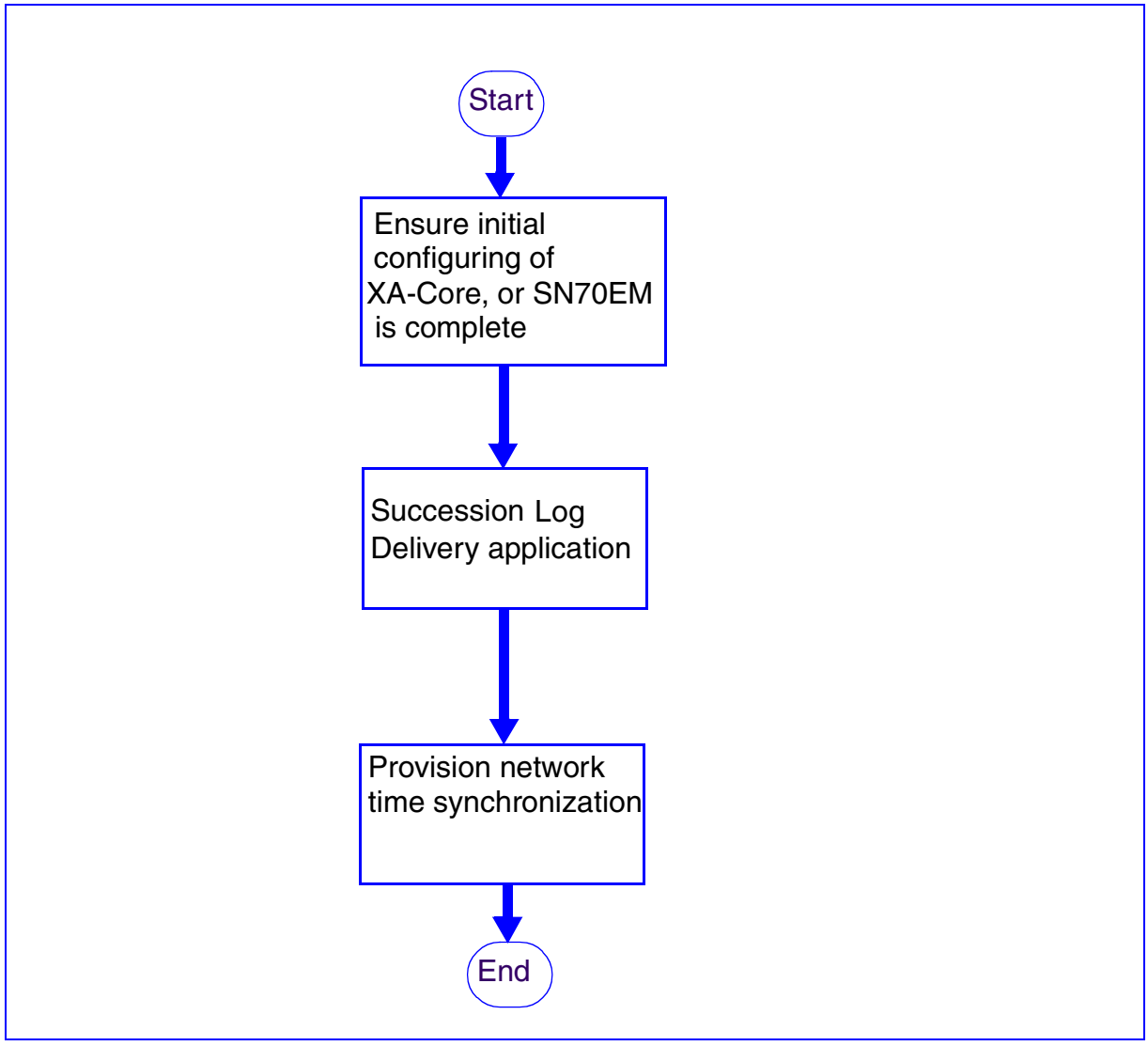
Detailed configuration procedures

Network element	Configuration procedure location
MG 9000 Manager	MG 9000 Configuration Management, NN10096-511
Passport 8600 Device Manager	Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using the Command Line Interface Release 3.2, 313191A Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using Device Manager Release5.5.x, 313193A

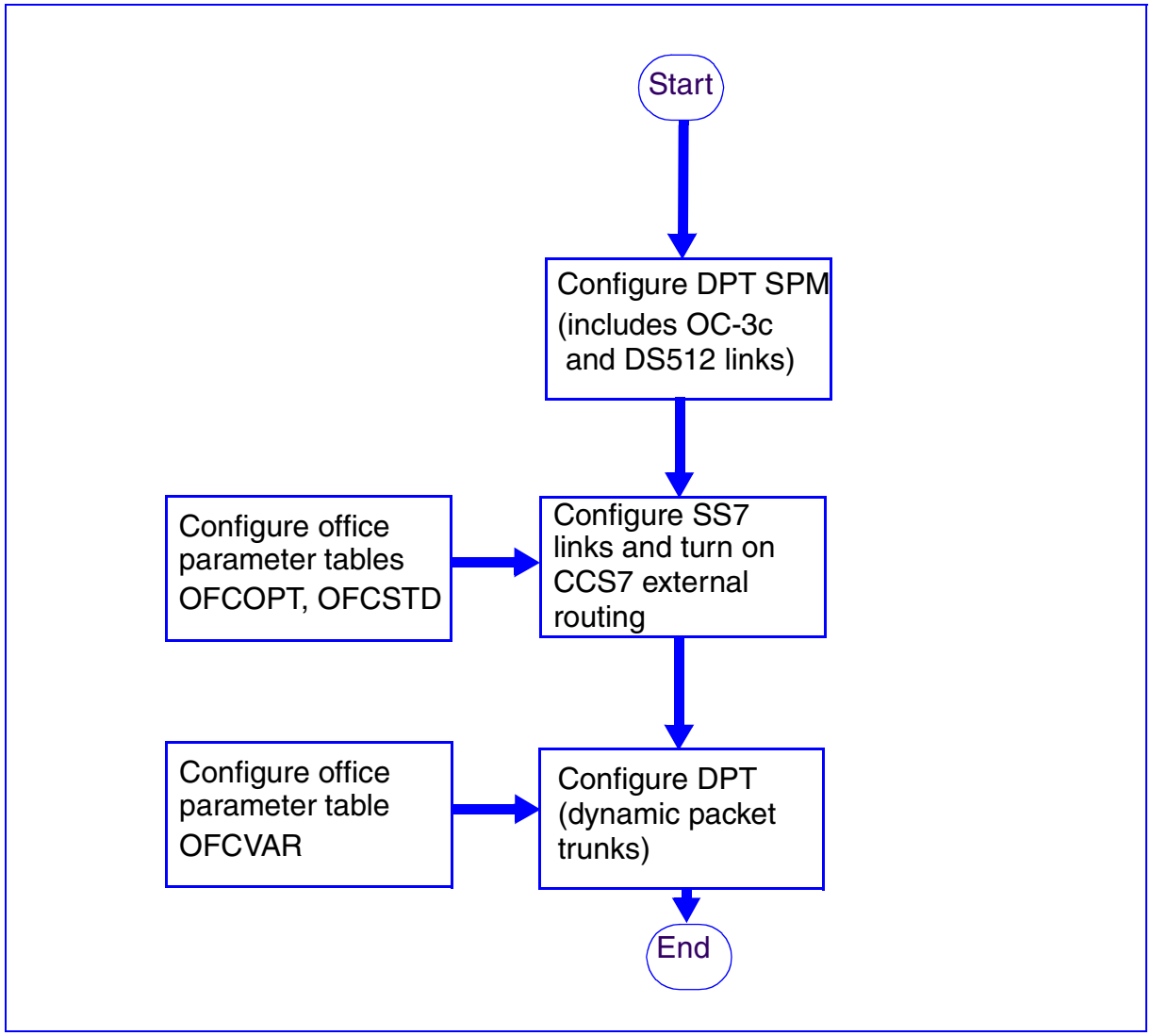
Packet Trunking XA Core or Packet Trunking SN70

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 Succession solutions varies by access type, either by trunk or line.

Trunk provisioning

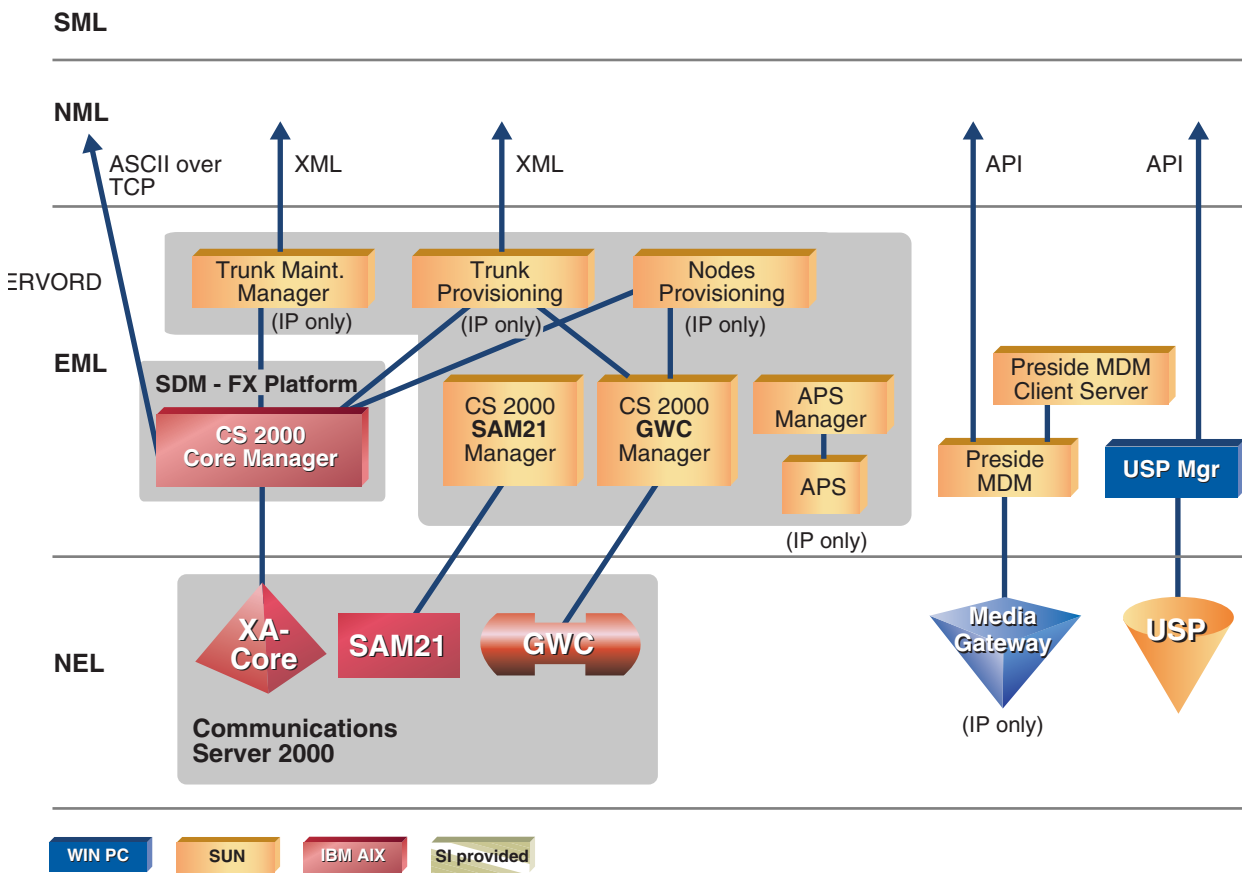
Trunk provisioning or trunk service activation involves creation, change, or deletion of trunk groups or individual trunks. This is required for the trunks of every solution. The steps required will be different for different solutions however.

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 (I)SN07 configuration management architecture for trunking solutions for the CS 2000 network.

(I)SN07 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.

1. Add the GWC to CS 2000 using the CS 2000 GWC Manager.

   Note: This step is performed by the Nortel Networks 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).

Deleting a trunk

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 Preside MDM.

Changing trunk group data

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

  Note: 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 to take advantage of the SN05 ‘post by gateway’ feature.

Note: 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 Networks Multiservice Switch 7400/15000/20000 Components Reference, NN10600-060
- Nortel Networks Multiservice Switch 15000/20000 Hardware Description, NN10600-120
- Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade, NN10600-130
- Getting Started with the Passport 8600 Management Software Part #209663-C
- Reference for the Passport 8600 Series Management Software Routing Operations 207415-C
- XML Schema for Carrier Provisioning (OSSGate User Guide)

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 co-ordinated: 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 Succession 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 Succession 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.

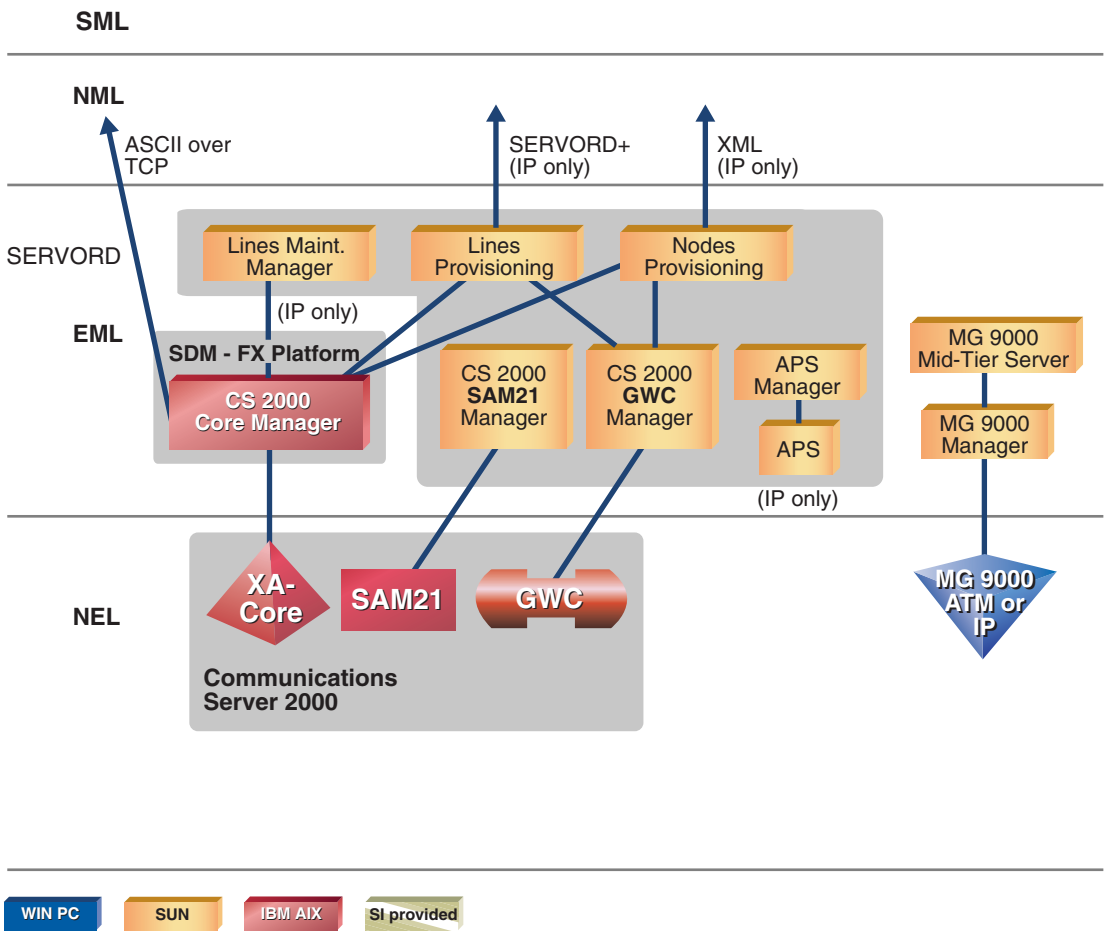
Note: In a CS 2000 lines solution, in common with many DMS/XPM-based line access solutions, a moment of ringback may be heard prior to an announcement being played. This is designed to fill in quiet periods of audio while the connected equipment prepares and connects the announcement resources to the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

Note: Steps 1 and 2 must be completed in the specified order, however, steps 3 through 5 can be completed in any order.

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.

Deleting a line

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

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.

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.
- Changing the number of endpoints requires deleting and re-adding the GW in (I)SN04

Routing and translations

For details on configuring routing or for adjusting and changing routing, refer to Translations and Routing.

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.

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 SN05.

Provisioning rules

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.

Provisioning the QoS collector application

In (I)SN07, 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

Succession user authentication services can use a single centralized third party server which provides authentication services to Succession management systems via a pluggable authentication module (PAM) on the Integrated EMS platform.

In (I)SN07, the CICM element manager is integrated into the Succession centralized user authentication strategy. The CICM element manager interfaces to PAM via the HTTPS PAM+ proxy on Integrated EMS.

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. For (I)SN07, the user name and password can be configured to be a global Succession account managed on a centralized authentication database which interfaces to Succession management tools via the PAM+ proxy located on the Integrated EMS.

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 Succession deployments, a method of local user authentication is also provided for use when connectivity is lost to the Integrated EMS 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.

Configuration management tools and utilities

This section lists tools and utilities used for operational configuration of Succession 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	Preside MDM
Communication Server LAN	Device Manager for Passport 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	
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

PT-IP configuration tools and utilities

Component	Tools and utilities
APS	SNMP configure_agent tool
USP	USP Mgr GUI
Media Gateway	Preside MDM API/EPI
Passport 8600	Passport 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 Networks 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 GRPCTRI level of the MAPCI is used for TDM (time division multiplex) trunks as well as DPT trunks (see GRPCTRL level of the MAPCI). 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 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.

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 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.

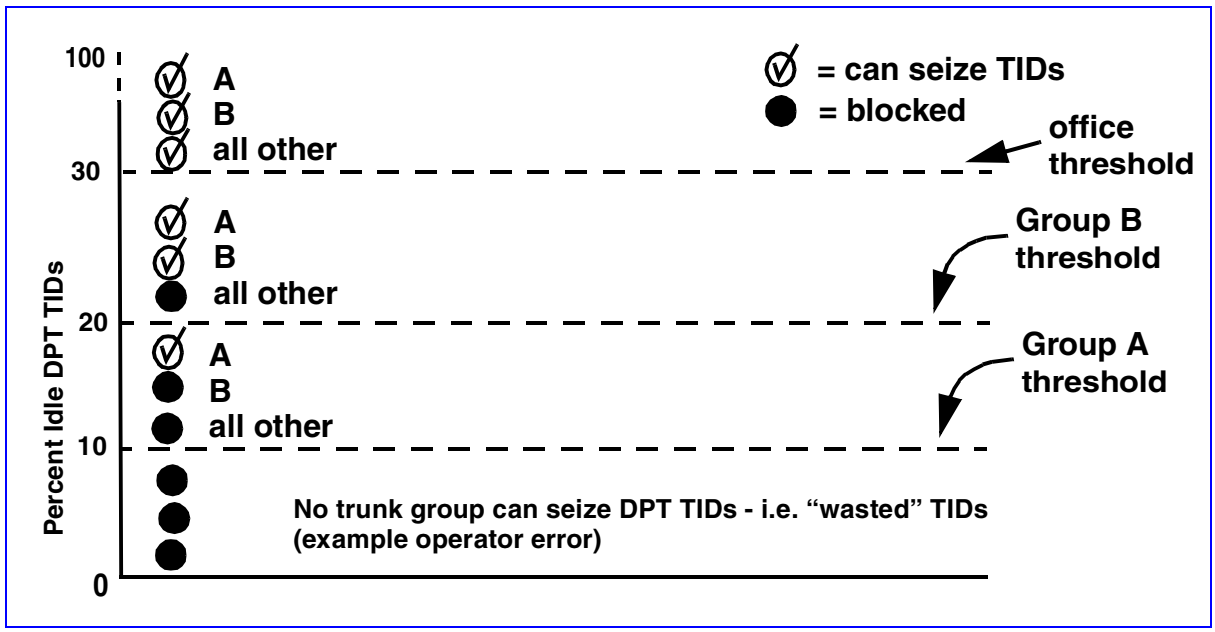
Note 3: For information on the order of precedence for DPT Priority and DPT Reservation, see Order of precedence for DPT Reservation and DPT Priority.

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.

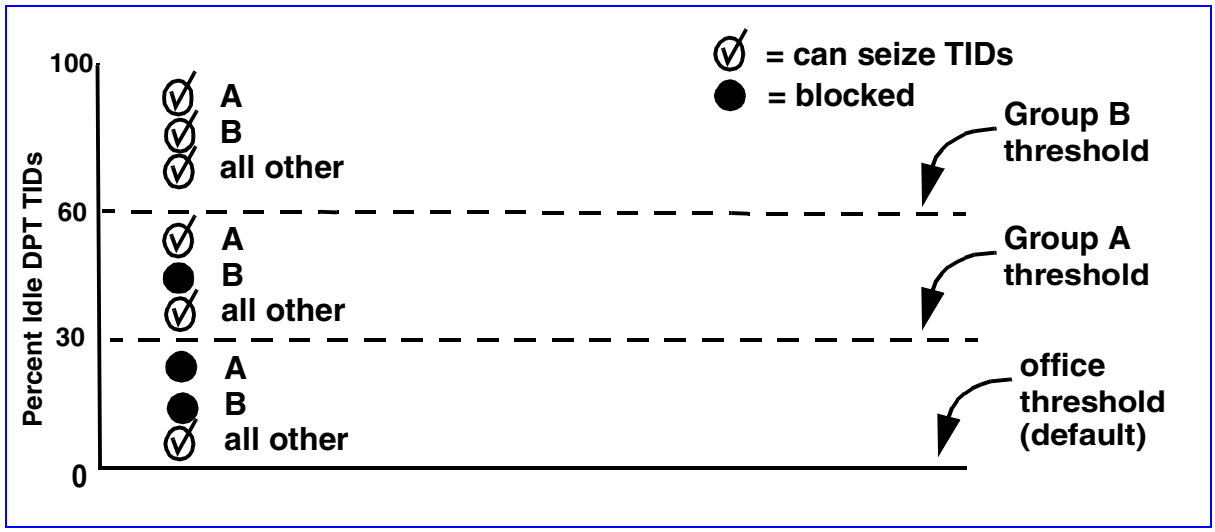
If in example 1, trunk group A can only support 6% of the total DPT capacity due to insufficient CICs or incoming traffic, then 14% of the

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



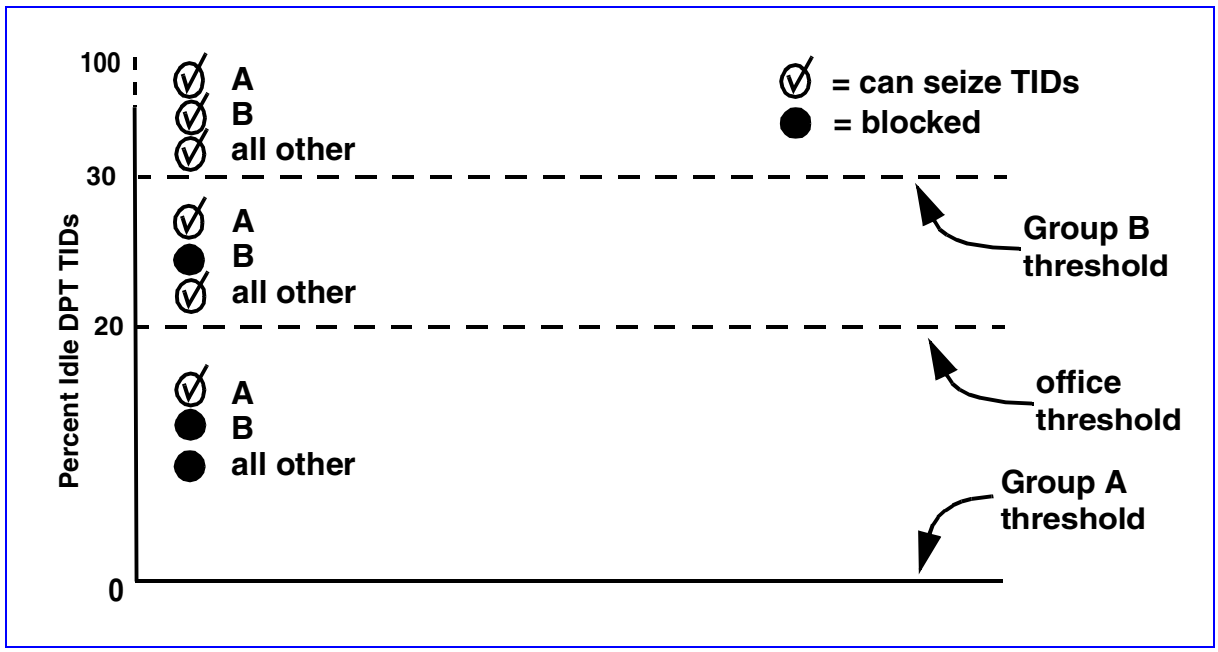
In example 2, if the idle TIDs stay between 30% and 60% for several minutes or more, then, all traffic through trunk group B has been “squeezed out” in favor of DPT traffic through trunk group A and all other trunk groups.

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)

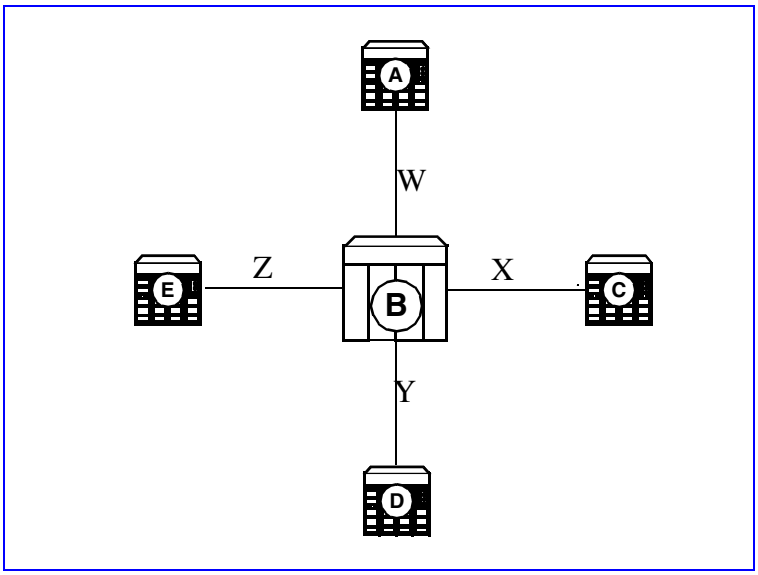
Enhanced Cancel To control for DPTs

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).

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:

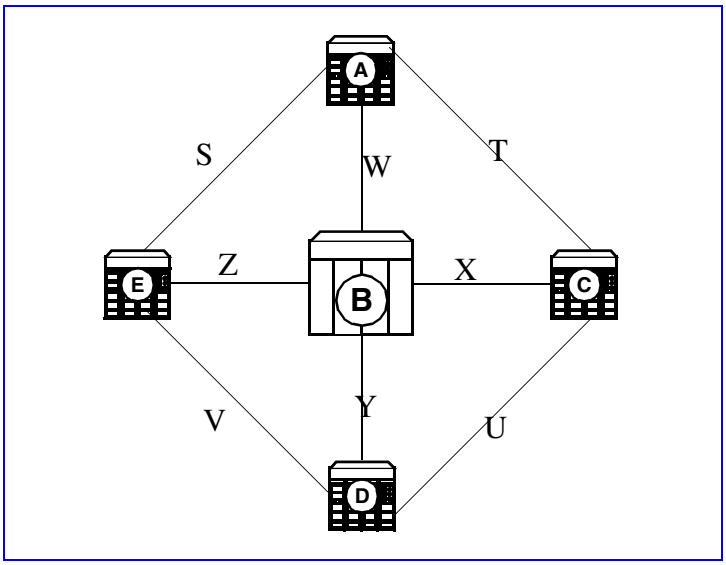
- The first trunk group (the in-chain route) is the trunk group to which the FRR control is applied. This trunk group is also referred to as the controlled trunk group.
- The second trunk group (the VIA route) is a standard route (standard digit manipulation). Calls that cannot be carried over the controlled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

- 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.)

APPLY command with DPT Priority control

Command, control and variables	
APPLY DPTP ppct otheppct	
where	
<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 (Sheet 1 of 2)

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.
<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 In—Chain 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.

APPLY command with enhanced FRR control (Sheet 2 of 2)

Command, control and variables	
<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):

- 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 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 CS 2000[1] 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

[1] For PT-XA Core or PT SN70 solutions, substitute PT XA Core or SN70 for references to CS 2000 in this section--could be done with conditional text.

bandwidth required by DPT trunks does not exceed the ATM bandwidth provided by the ATM links that connect the 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 CS 2000 and represents the total number of DPT terminals in-service on the CS 2000 at any point in time.
- DPT TID Limit—is 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_MAXTIDS, 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.

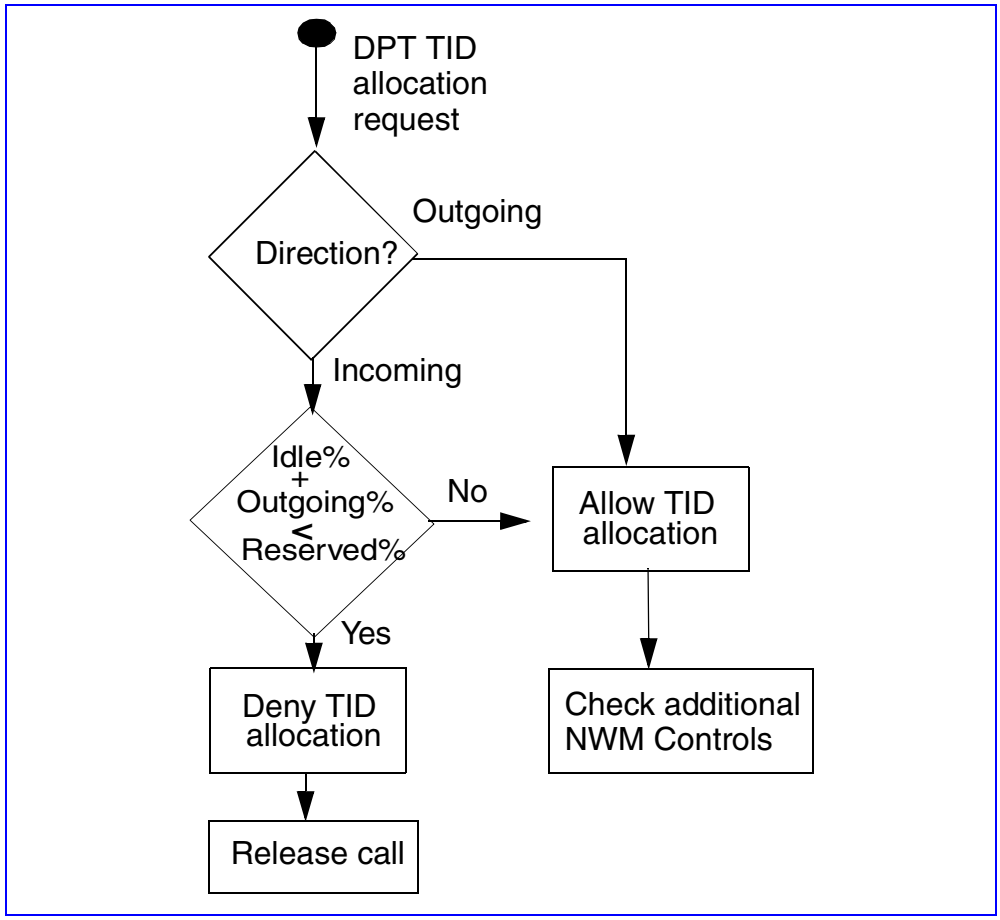
To determine whether or not to block, the CS 2000 software uses three percentages:

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

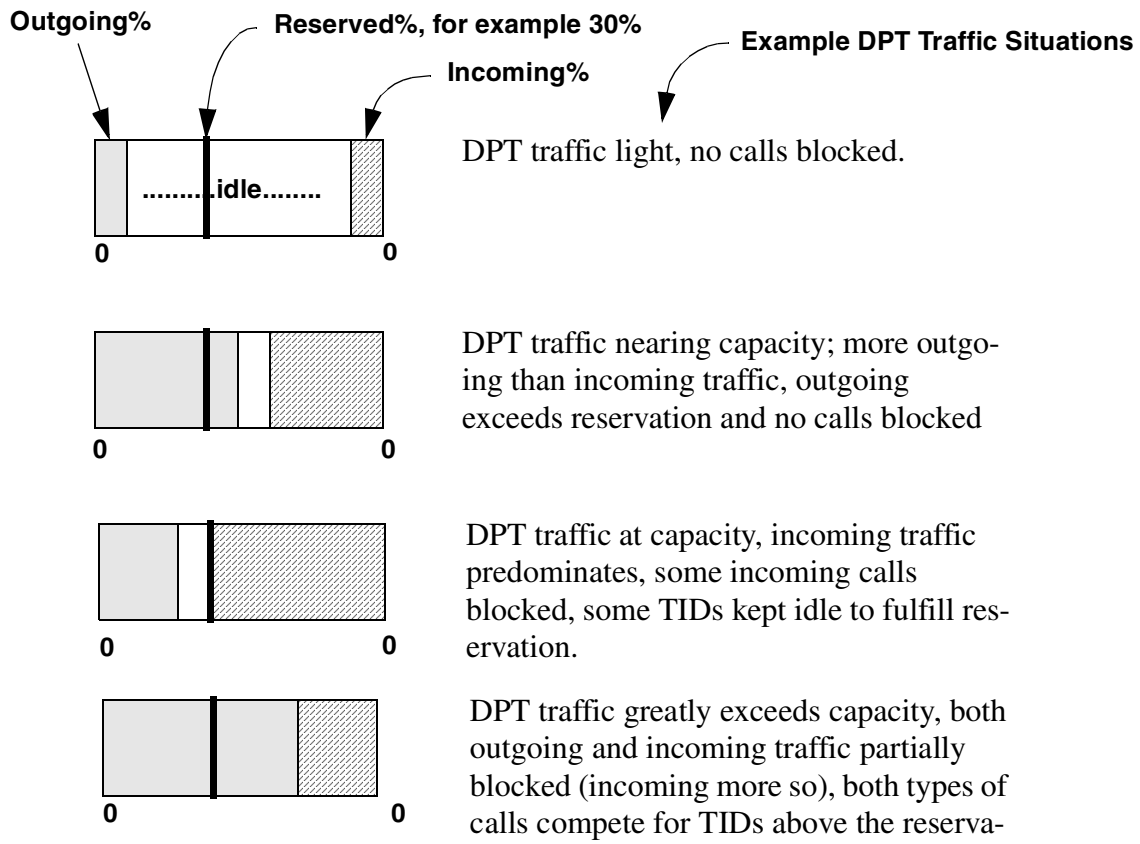
indicate that completing the call would violate the reservation. As a result, the CS 2000 clears the call by sending a release message to the originating CS 2000 and pegs OM register DPTR (in OM Group OFZ2). The operation of the DPT Reservation control is illustrated in DPT Reservation operation.

DPT Reservation operation



The consequence of this TID allocation policy is illustrated by a Effect of DPT Reservation on TID distribution 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 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):

- 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.

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.

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 Networks MAPCI for applying, removing and establishing settings for the Bandwidth Directionalization sub features. EADAS is based on Telecordia standard TR-746. Nortel Networks 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 Networks network management features

For more information on the use of EADAS and Netminder with DPT network management control see the following Nortel Networks 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 Networks 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 Networks 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 table below lists the configuration procedures available for the system audit.

System audit procedures

QoS Collector Application (QCA)

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

QCA procedures

Line Maintenance Manager (LMM)

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

LMM procedures

Network Patch Manager (NPM)

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

NPM procedures

Succession Server Platform Foundation Software (SSPFS)

The table below lists the configuration procedures available for the SSPFS.

SSPFS procedures

SSPFS procedures

Activity	Page
Configuring automated data backups on an SSPFS-based server	161
Setting the threshold for file systems on an SSPFS-based server	165
Configuring DCE on an SSPFS-based server	167
Unconfiguring DCE on an SSPFS-based server	174
Configuring the destination for SNMP traps	178

Succession Element and Sub-network Manager (SESM)

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

SESM procedures

Procedure	Page
Configuring the SESM server application	182

PM Poller

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

PM poller procedures

Procedure	Page
Setting up the PM poller on an SSPFS-based server	185
Configuring the SNMP defaults for a poller profile and setting the polling interval	192
Viewing the configuration data for a profile or device	197
Deleting a device from a PM poller profile	199

OMPUSH

The table below lists the configuration procedures available for OMPUSH.

OMPUSH procedures

Procedure	Page
Creating an OMPUSH session	202
Activating or deactivating an OMPUSH session	209
Modifying an OMPUSH session	217
Deleting an OMPUSH session	225
Querying OMPUSH session attributes	232

Trunk Maintenance Manager (TMM)

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

TMM procedures

Procedure	Page
Setting the TMM CLLI name	239
Setting the TMM Auto Refresh value	241
Turning TMM Auto-Refresh on or off	242
Setting the TMM confirmation for the busy command	243

Configuring an audit schedule

Application

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

- CS2K data audit
- Line audit
- Trunk audit
- V5.2 audit (only available in the international version of the software and not in the North American)

Note 1: It is recommended to run only one audit at a time. Therefore, schedule 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).

Note 2: It is recommended to not have any one of the audits run at the same time as the patching autoapply task when the patching autoapply task is enabled.

ATTENTION
Please keep in mind when scheduling audits, that when a nodes audit is running, the system is locked and no provisioning changes are allowed.

To perform an audit, refer to procedure “Performing an audit” in the ATM/IP Solution-level Fault Management document, NN10408-900.

Prerequisites

You must be logged in to the CS2000 Management Tools application GUI. Refer to procedure “Launching the CS2000 Management Tools client application” in the ATM/IP Security and Administration document, NN10402-600, if required.

You must be assigned to user group “mgcadm” to configure an audit schedule. Refer to procedure “Setting up users on a Sun server” in the ATM/IP Security and Administration document, NN10402-600, if required.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Launch the CS2000 Management Tools GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in the ATM/IP Security and Administration document, NN10402-600, if required.

At the CS2000 Management Tools GUI

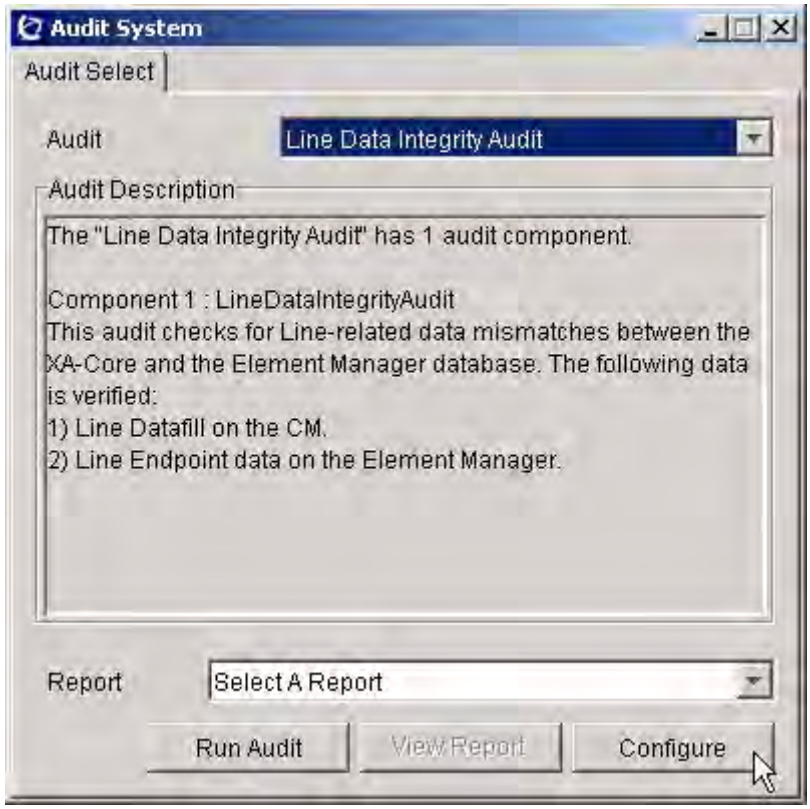
1 On the **Maintenance** menu, click **Audit System**.

The Audit System window opens.

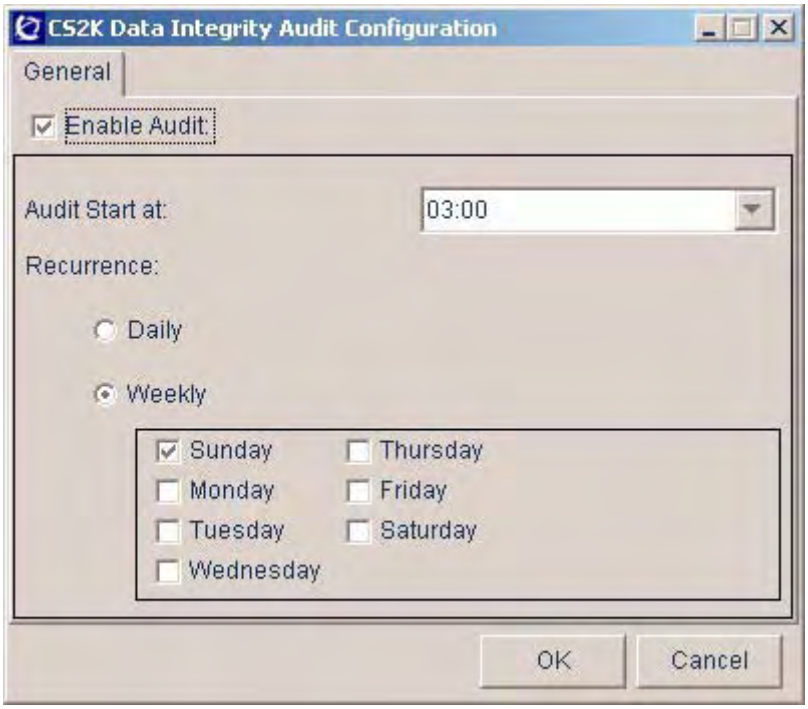
2 In the **Audit** list, select the audit type of your choice.

Note: The V5.2 audit is only available in the international version of the software and not in the North American.

3 Click **Configure**.



The Audit Configuration window opens.



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

5 Click **OK**.

6 You have completed this procedure.

Modifying the QoS Collector Application

Application

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

Note: QCA is not applicable to AAL2 solutions.

Prerequisites

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

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 where the QCA software 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 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
```

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

Name	Description	Range	Default
Port number (see Note 1)	The port number the QCA accepts connections on.	20000 to 20004	20000
MaxFileSize	The maximum size an output file can be before it is closed. ***Note:*** 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. ***Note:*** 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 (see Note 2)	The file should be compressed when closed and moved to today.	true or false	true
OldFileCompression (see Note 2 and Note 3)	The files should be compressed at the first directory recycle.	true or false	true

Note 1: 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.

Note 2: File compression may be required as there is limited disk space to store QCA IPDRs.

Note 3: If *ClosedFileCompression* is true, the value of the *OldFileCompression* is negated as the files will have already been compressed.

7 Exit the edit session and save the changes by typing

zz

and pressing the Enter key.

8 Stop and restart the QCA for the changes in the QCA properties file to take place. Refer to procedure “Starting and stopping the QoS Collector Application” in the ATM/IP Security and Administration document, NN10402-600, if required.

9 You have completed this procedure.

Setting the LMM CLLI name

Application

If there are no communication problems with the CM, the default CLLI should automatically be set during the LMM GUI startup. If the CLLI is not already set during initialization, use this procedure to set the LMM CLLI name.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

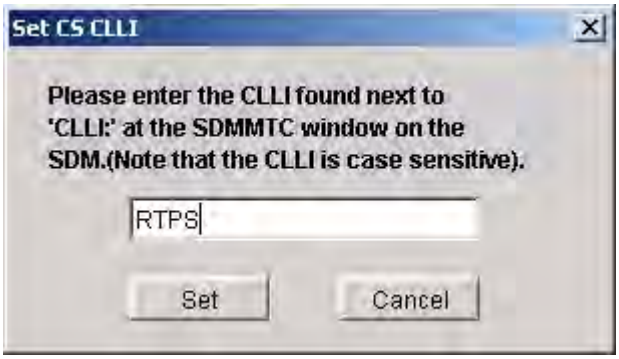
1 Access the LMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

At the LMM GUI

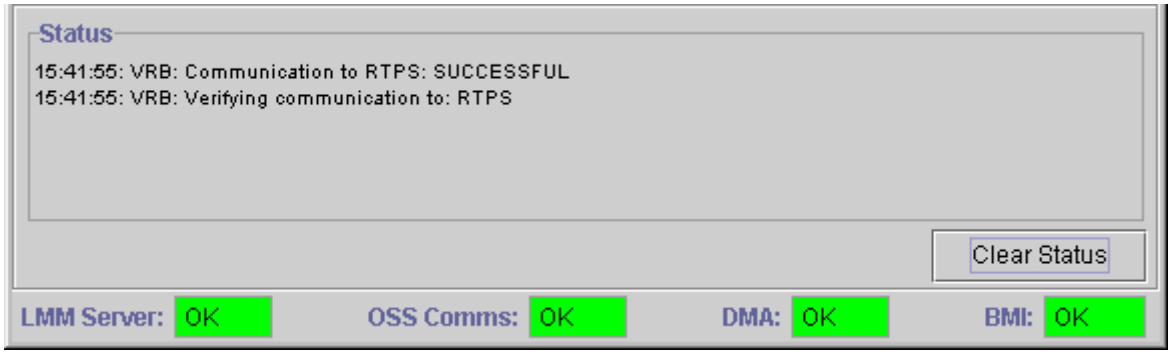
2 On the **Configure** menu, click **Set CS CLLI**.

The CS CLLI window opens.

3 Enter the CLLI name for the Communication Server, and click **Set**.



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



Note: If the connection fails, a Set CS CLLI failed window indicates the error.

5 You have completed this procedure.

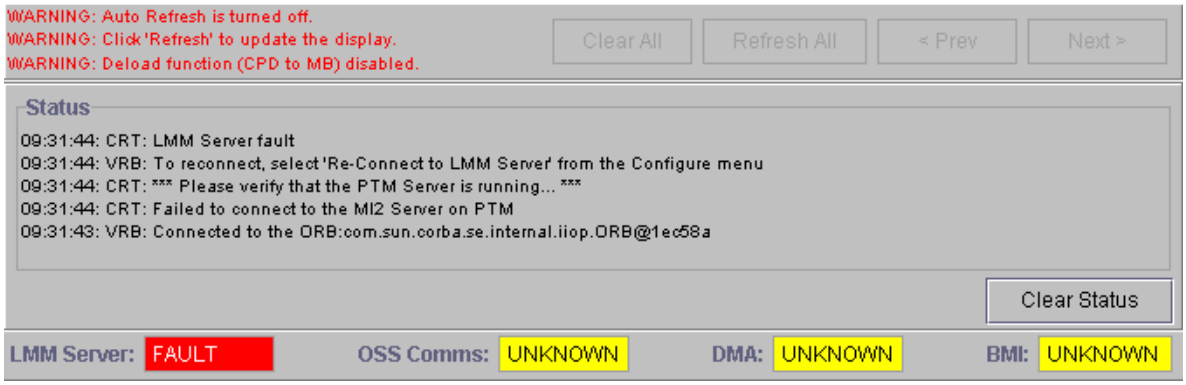
Reconnecting to LMM server

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.

At your workstation

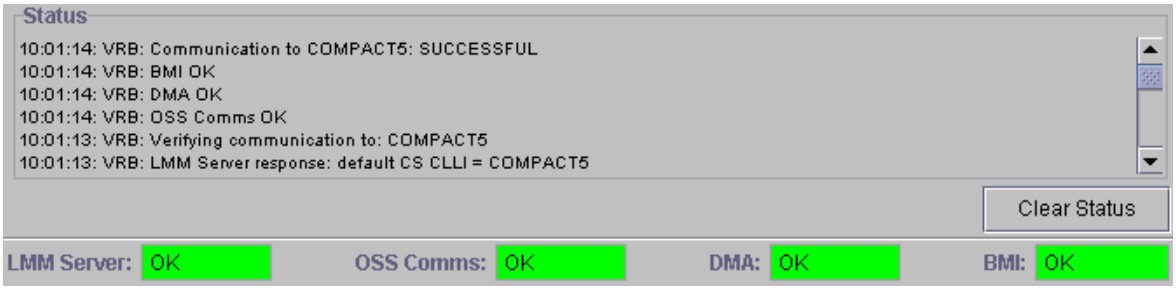
1 Access the LMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

At the LMM GUI

2 On the **Configure** menu, click **Re-Connect to LMM Server** to establish a connection with the LMM server again.

Note: 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.

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

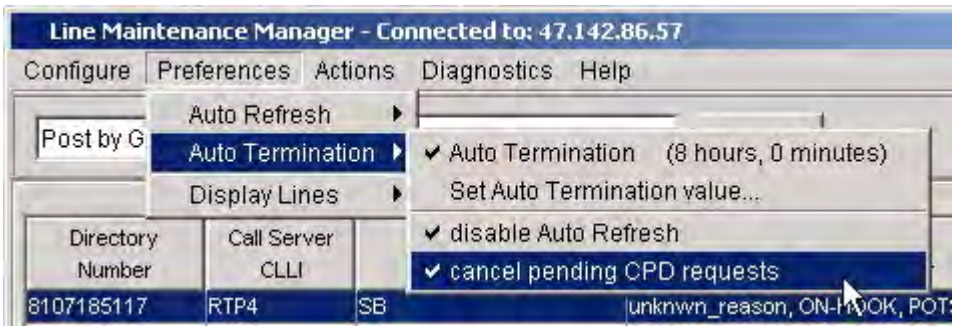
Perform the following steps to complete this procedure.

At your workstation

1 Access the LMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications. 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.

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.

At your workstation

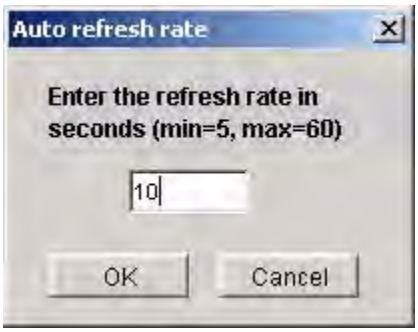
1 Access the LMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

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**.

Note: The minimum is 5 seconds, and the maximum is 60 seconds.



4 You have completed this procedure.

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.

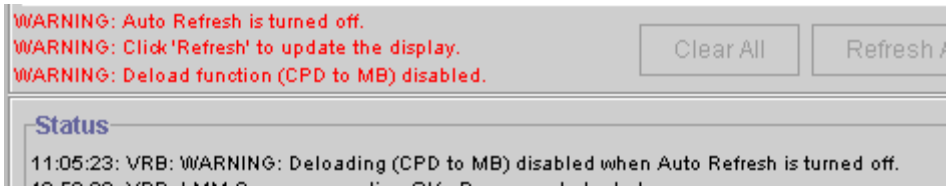
At your workstation

1 Access the LMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 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.

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.

At your workstation

1 Access the LMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

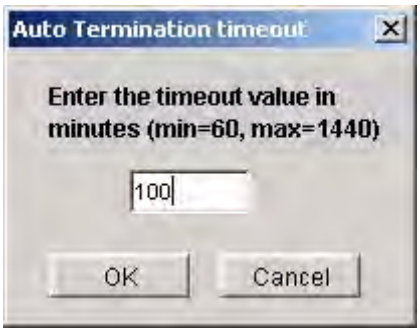
At the LMM GUI

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**.

Note: The minimum is 60 minutes, and the maximum is 1440 minutes.



4 You have completed this procedure.

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.

At your workstation

1 Access the LMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 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.

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.

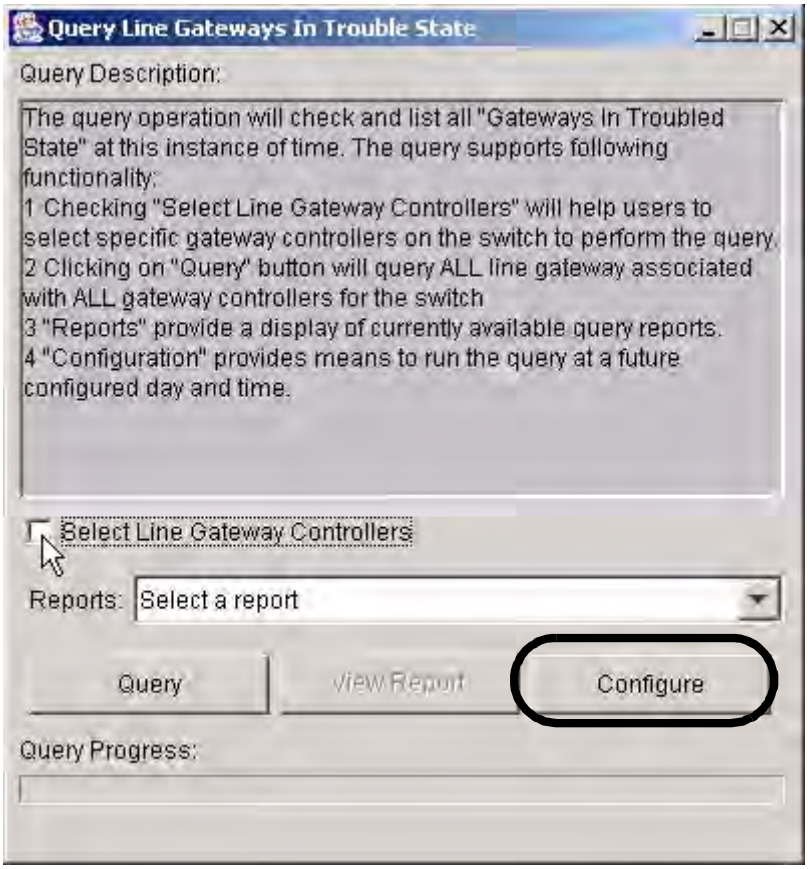
At your workstation

1 Access the LMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

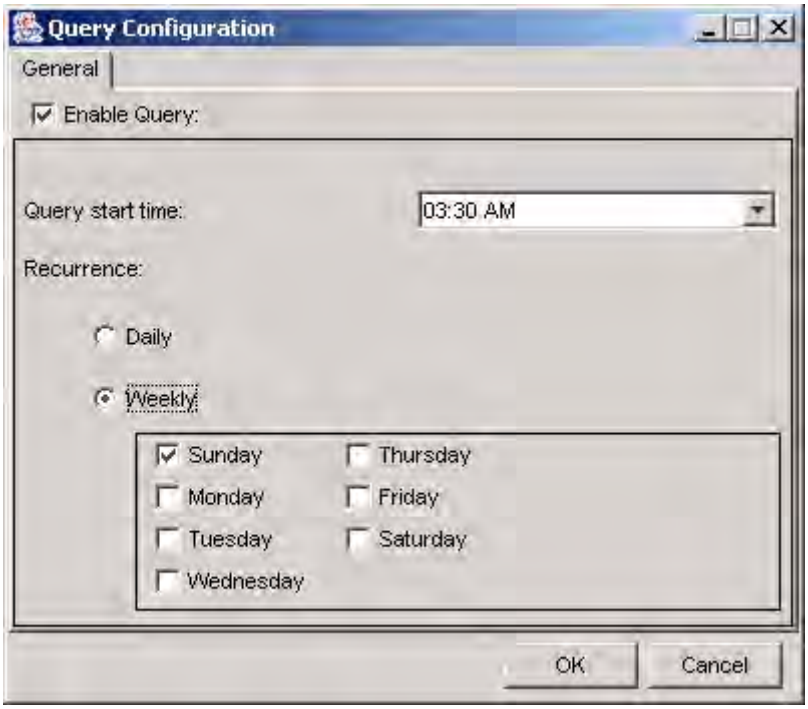
At the LMM GUI

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.

Configuring the Patching Server Element on an SSPFS-based server

Application

Use this procedure to configure the Patching Server Element (PSE) on a Succession Server Platform Foundation Software (SSPFS)-based server.

Prerequisites

The SSPFS upgrade is complete.

Action

Perform the following steps to complete this procedure.

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 configuring PSE

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

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

Example response:

```
Succession Element Configuration
 1 - NPM Application Configuration
 2 - SESM Application Configuration
 3 - SAM21EM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH 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...)


 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 SSPFS-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 SSPFS-based server where the NPM resides.

Note: 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 exit the command line interface, by typing

`select - x`

and pressing the Enter key.

13 You have completed this procedure.

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 enabling the Patch File Receipt System (PFRS). When the PFRS is enabled, patches are automatically delivered to the NPM database and retrieved for processing on a daily basis.

Options are provided to disable the PFRS, retrieve patches and generate reports on demand, and view the settings of the PFRS when it is already enabled.

Prerequisites

To enable the PFRS, you need the following information:

- the CLLI ID of the Communication Server 2000 associated with the office - You can obtain the CLLI ID from table OFCENG on the Communication Server 2000. Use the POS (position) command to locate the OFFICE_CLLI_NAME tuple. The value of this tuple, is the CLLI ID.
- 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.

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 where the NPM software 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 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 - 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)

 X - exit

Select -
```

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

Example response:

```
Succession Element Configuration
 1 - NPM Application Configuration
 2 - SESM Application Configuration
 3 - SAM21EM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

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

Example response:

```
NPM Application Configuration
  1 - PFRS (Patch File Receipt System
      Configuration (PFRS))
  2 - CreateDB (Initialize or re-initialize the
      NPM database)
  3 - ConfigureNpm (Configure the Network Patch
      Manager)

  X - exit

select -
```

9 Enter the number next to the “PFRS” option in the menu.

Example response:

```
===Executing “PFRS”

PFRS Configuration
1 - View
2 - Enable/Reconfigure
3 - Disable
4 - Patch retrieval (Now)
5 - Generate Report (Now)
```

10 Enter the number next to the “Enable/Reconfigure” option in the menu.

11 When prompted, enter the CLLI ID of the Communication Server 2000 associated with the office (see Prerequisites on page 105 at the beginning of this procedure).

12 When prompted, enter the host name or IP address of the drop-off server where patch files are to be delivered.

13 When prompted, enter the user ID that will be used to connect to the drop-off server.

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

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

15 When prompted, enter the time at which patch files are to be retrieved from the drop-off server.

Note: You can retrieve patches at any time using option 4, "Patch retrieval (Now)", in the PFRS Configuration menu.

16 When prompted, enter the time at which you would like reports to be generated and put on the drop-off server.

Note: You can generate reports at any time using option 5, "Generate Report (Now)", in the PFRS Configuration menu.

PFRS is now enabled. You can view the settings of PFRS at any time using option 1, "View", in the PFRS Configuration menu.

17 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.

18 You have completed this procedure.

Setting the CS 2000 CLLI on an SSPFS-based server

Application

Use this procedure to set the CLLI of the Communication Server 2000 (CS 2000) on a Succession Server Platform Foundation Software (SSPFS)-based server. You can also use this procedure to remove the CS 2000 CLLI from the server.

ATTENTION

Ensure your system is patch-current before performing this procedure. If the system is not patch-current, changing or unconfiguring the CM CLLI may cause loss of configuration data on the system. If you are unsure whether the patch that corrects this issue has been applied, contact your next level of support before proceeding.

Prerequisites

You must have the CLLI for the CS 2000 that is associated with the SSPFS-based server on which you are setting the CLLI. The CS 2000 CLLI is listed in table OFCENG.

Action

Perform the following steps to complete this procedure.

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 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 - DCE Configuration
 4 - OAMP Application 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)

 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 and
     User)
 2 - sdm_unconf (Unconfigure SDM IP Address and
     User)
 3 - cmClli_conf (Configure CM_CLLI Address)
 4 - cmClli_unconf (Unconfigure CM_CLLI IP
     Address)
 5 - cm_conf (Configure CM IP Address)
 6 - 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 CLLI on the Sun server	step 9
removing the CS 2000 CLLI from the Sun server	step 10

9 Set the CS 2000 CLLI as follows:

a Enter the number next to the “cmClli_conf” option in the menu.

Example response

```
===Executing “cmClli_conf”

Enter CM_CLLI:
```

b When prompted, enter the CLLI for the CS 2000.

Example response

```
CM CLLI:       CLLITEST

Enter “ok” to accept current settings
```

c When prompted, confirm the setting by typing

ok

and pressing the Enter key.

Example response

```
Processing values...

CM_CLLI Configured
Please perform a logout and login so your
shell will reflect CLLI environment settings

===”cmClli_conf” completed successfully
```

d Proceed to step 11.

10 Remove the CS 2000 CLLI as follows:

a Enter the number that corresponds to the “cmClli_unconf” option in the menu.

Example response

```
===Executing “cmClli_unconf”

Please perform a logout and login so your
shell will no longer contain the CLLI
environment settings

===”cmClli_unconf” completed successfully
```

b When prompted, enter the CLLI for the CS 2000.

Example response

```
CM CLLI:      CLLITEST

Enter “ok” to accept current settings
```

c When prompted, confirm the setting by typing

ok

and pressing the Enter key.

Example response

```
CM CLLI:      CLLITEST

Enter “ok” to accept current settings
```

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 Log out and log back in to the Sun server to reflect the CLLI environment changes.

13 You have completed this procedure.

Configuring a timing provider on an SSPFS-based server

Application

Use this procedure to configure a timing provider for a Succession Server Platform Foundation Software (SSPFS)-based server. The timing provider is a Network Timing Protocol (NTP) server supplied by the customer. Perform the steps under Configuring an NTP server as the timing provider on page 114.

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 Configuring the Active server in a cluster as the timing provider on page 116.

Prerequisites

You must have the IP address of the customer-supplied NTP server.

Action

Perform the following steps to complete this procedure.

Configuring an NTP server as the timing provider

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 want to configure an NTP 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.

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 - DCE Configuration
 4 - OAMP Application 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)

 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_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.

Note: You can specify up to three NTP servers.

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.

Configuring the Active server in a cluster as the timing provider

At your workstation

1 Telnet 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 - root
```

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.

8 You have completed this procedure.

Adding IP addresses for FTP proxy and restricted shell access

Application

Use this procedure to set up a list of IP addresses for FTP proxy and restricted shell access on a Sun server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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 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 - 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 that corresponds 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 - 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)

 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 exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

12 You have completed this procedure.

Configuring the time zone on an SSPFS-based server

Application

Use this procedure to configure the time zone on a Succession Server Platform Foundation Software (SSPFS)-based server.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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 want to configure the time zone

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 - DCE Configuration
 4 - OAMP Application 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)

 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/Eastern>:
```

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.

Configuring Domain Name Service on an SSPFS-based server

Application

Use this procedure to configure Domain Name Service (DNS) on a Succession Server Platform Foundation Software (SSPFS)-based server. This procedure provides the instructions for the following tasks:

- Configure server as a DNS master server on page 125

  Note: Only one DNS master server is used for one Communication Server (CS) LAN. Other hosts in the CS LAN that use DNS, should be configured to use the DNS master server.

- Add or remove a host entry in the DNS database on page 128
- Configure server as a DNS client on page 130
- Turn off DNS capability on the server on page 133

  Note: Perform the steps under Turn off DNS capability on the server 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 on page 130.

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 server as a DNS master server
- you need to complete the steps under Configure server as a DNS master server prior to performing the steps under Add or remove a host entry in the DNS database
- you need familiarity with the “vi” editor to perform the steps under Add or remove a host entry in the DNS database

Action

Configure server as a DNS master server

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 server you want to configure as the DNS master 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.

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 - 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)

 X - exit


Select -
```

7 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 -
```

8 Enter the number next to the “enable_dnssrv” option in the menu.

Example response

```
===Executing “enable_dnssvr”
Enter domain name for the office:
```

9 When prompted, enter the domain name for the office.

Note: 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.

10 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
DSNSVR Started

===”enable_dnssvr” completed successfully
```

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 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>
```

Note:

13 You have completed this procedure.

Add or remove a host entry in the DNS database

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 DNS master 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 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.

Note 1: Increment the “serial” number at the beginning of each zone file every time you update the file.

Note 2: The zone files will only be present if a DNS master server was configured. If required, refer to the steps under Configure server as a DNS master server on page 125.

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
```

6 Restart the DNS service by typing

```
# servrestart DNSSVR
```

and pressing the Enter key

Example response

```
Stopping DNSSVR
Starting DNSSVR
DNSSVR re-started successfully
```

7 You have completed this procedure.

Configure server as a DNS client

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 server you want to configure as a DNS client

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

7 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 -
```

8 Enter the number next to the “turn_dns_on” option in the menu.

9 When prompted, confirm the command by typing

yes

and pressing the Enter key.

10 When prompted, enter the DNS domain.

Example
us.nortel.com

11 When prompted, enter the IP address of a DNS server.

12 When prompted, enter the IP address of a second DNS server.

13 When prompted, enter the IP address of another DNS server. If there are no other DNS server addresses to enter, press the Enter key.

14 When prompted, enter the name of a search domain.

Example
us.nortel.com

15 When prompted, enter the name of another search domain. If there are no other search domains, press the Enter key.

16 Accept the DNS configuration that is displayed by typing

ok

and pressing the Enter key.

17 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.

18 You have completed this procedure.

Turn off DNS capability on the server

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 server on which you want to turn off DNS capability

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit


Select -
```

7 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 -
```

8 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):
```

9 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
```

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.

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.

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 - DCE Configuration
 4 - OAMP Application 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)

 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.

Configuring client/server ports on an SSPFS-based server for secure firewall communications

Application

Use this procedure to configure the client-side and server-side ports on a Succession Server Platform Foundation Software (SSPFS)-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.

Note: 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.

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

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 - DCE Configuration
 4 - OAMP Application 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)

 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 document, NN10402-600, for the Socks server, SESM and SAM21 server applications. Refer to the MG 9000 Security and Administration document, NN10162-611, for the MG 9000 Manager server application.

b After changing the client-side port, restart any client workstations already running the application GUIs.

17 You have completed this procedure.

Configuring virtual IP addresses on an SSPFS-based server

Application

Use this procedure to configure virtual IP addresses on a Succession Server Platform Foundation Software (SSPFS)-based server. This procedure applies to simplex and high availability (HA) systems. An HA system refers to a Sun Netra 240 server pair.

Note: A virtual IP address is required for the Integrated Element Management System (EMS) when the Integrated EMS is on the same 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 a virtual IP address.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the active node of the server pair by typing

```
> telnet <server>
```

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server on which you are configuring additional IP addresses

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit


Select -
```

7 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)

 X - exit

select -
```

8 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]
```

9 When prompted, enter the hostname for the system 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]
```

10 When prompted, enter the IP address for <hostname> or press the Enter key to accept the default value if one is specified.

Example response

```
Configure additional ip address? [yes]
```

11 When prompted, indicate whether you want to configure an additional IP address.

If you enter	Do
yes	step 12
no	step 15

12 When prompted, enter the additional IP address for <hostname> or press the Enter key to accept the default value if one is specified.

Example response

```
Enter application for ip address <ip address>
```

13 When prompted, enter the application name for <ip address> or press the Enter key to accept the default value if one is specified.

Note 1: When configuring an additional IP address for IEMS, the application name is IEMS.

Note 2: The system allocates a hostname for each virtual IP address that is configured. The hostname is in the form of <sspfs_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]
```

14 Repeat step 11.

15 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
```

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.

If you have	Do
a simplex system	step 17 only
an HA system	step 18

17 Reboot the system by typing

`# shutdown -i 6 -y`

and pressing the Enter key.

At the console of the Inactive node

18 Log in to the inactive node through the console (port A) using the root user ID and password.

19 Shutdown the inactive node by typing

```
# shutdown -i 0 -y
```

and pressing the Enter key.

At the console of the active node

20 Log in to the active node through the console (port A) using the root user ID and password.

21 Restart the active node by typing

```
# shutdown -i 6 -y
```

and pressing the Enter key.

At the console of the Inactive node

22 Boot the inactive node by typing

```
# boot
```

and pressing the Enter key.

23 You have completed this procedure.

Setting the CS 2000 IP address on an SSPFS-based server

Application

Use this procedure to set the IP address of the Communication Server 2000 (CS 2000) on a Succession Server Platform Foundation Software (SSPFS)-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 SSPFS-based server on which you are setting the IP address.

Action

Perform the following steps to complete this procedure.

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 CS 2000 IP address

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 - DCE Configuration
 4 - OAMP Application 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)

 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 and
     User)
 2 - sdm_unconf (Unconfigure SDM IP Address and
     User)
 3 - cmClli_conf (Configure CM_CLLI Address)
 4 - cmClli_unconf (Unconfigure CM_CLLI IP
     Address)
 5 - cm_conf (Configure CM IP Address)
 6 - 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 exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

12 You have completed this procedure.

Creating or modifying the login greeting message on an SSPFS-based server

Application

Use this procedure to create or modify the login greeting message on a Succession Server Platform Foundation Software (SSPFS)-based server. This message is presented to the user who logs in to the server through Telnet.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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 want to modify the login greeting

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

7 Enter the number next to the “Login Session” option in the menu.

Example response

```
OAMP Application Configuration
 1 - login_session_timeout (Login Session
     Timeout Configuration)
 2 - login_session_server (Login Session Master
     Server Configuration)
 3 - telnet_greeting (Telnet Login Greeting)

 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 exit the command line interface, by typing

`select - x`

and pressing the Enter key.

12 You have completed this procedure.

Configuring the Apache Web Server for HTTPS proxy

Application

Use this procedure to configure the Apache Web Server for HTTPS proxy.

Note: You can provision a maximum of 6 IP addresses for use in HTTPS proxy.

ATTENTION
Only perform this procedure if STORage Management (STORM) units are configured in your network. If Session Server units are configured in your network, refer to the Session Server Security and Administration document, NN10346-611 for a detailed procedure on configuring a web proxy.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At the server console

1 Log in to the server through the console (port A) using the root user ID and password.

2 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 -
```

3 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 - 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)

 X - exit


Select -
```

4 Enter the number next to the “Apache Proxy Configuration” option in the menu.

Example response

```
Apache Proxy Configuration
 1 - add_proxy_conf (Add an IP to the Apache
     Proxy Module configuration)
 2 - del_proxy_conf (Delete an IP from the
     Apache Proxy Module configuration)
 3 - list_proxy_conf (List the Apache Proxy
     Module configuration)

 X - exit

select -
```

5 Enter the number next to the “add_proxy_conf” option in the menu.

6 When prompted, enter the proxy IP address.

7 When prompted, enter the hostname associated with the IP address you just entered

8 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.

9 You have completed this procedure.

Configuring automated data backups on an SSPFS-based server

Application

Use this procedure to view or change the configuration settings for an automated data backup on a Succession Server Platform Foundation Software (SSPFS)-based server. The automated backup backs up Oracle and critical data.

Note: Log SPFS320 is generated when an automated data backup fails, and when the backup failure is cleared and the backup completes successfully. Refer to the Succession Fault Management Logs Reference document, NN10275-909 for log details.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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 want to configure automated data backups

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 - DCE Configuration
 4 - OAMP Application 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)

 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
```

Note: 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 exit the command line interface, by typing

`select - x`

and pressing the Enter key.

13 You have completed this procedure.

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.

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 example above sets the threshold for the /data file system to 80%.

6 You have completed this procedure.

Configuring DCE on an SSPFS-based server

Application

Use this procedure to configure the Distributed Computing Environment (DCE) on a Succession Server Platform Foundation Software (SSPFS)-based server following an SSPFS upgrade. Only perform this procedure if DCE is used as an authentication mechanism.

As of (I)SN05, DCE is not required for all systems, therefore, if your system does not have DCE, you do not need to perform this procedure.

Prerequisites

This procedure has the following prerequisites:

- unconfigure DCE if DCE was configured prior to upgrading the SSPFS - refer to procedure Unconfiguring DCE on an SSPFS-based server on page 174 in this document, if required
- obtain the following information
  - the DCE cell name for your customer-provided DCE cell

    Note: This should be the same DCE cell that contains the core manager.

  - the host name or IP address of the DCE Master Security Server (MSS)
  - the host name or IP address of the DCE Cell Directory Server (CDS)
  - the DCE cell administrator password.
  - the host name or IP address of the DCE Time Server (DTS)

Action

Perform the following steps to complete this procedure.

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 that uses DCE as an authentication method

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit


Select -
```

7 Enter the number next to the “DCE Configuration” option in the menu.

Example response

```
DCE Configuration
 1 - dce_conf <Configure the DCE Client>
 2 - dce_unconf <Unconfigure the DCE Client>


 X - exit

select -
```

8 Enter the number next to the “dce-conf” option in the menu.

Example response

```
DCE Cell Name(default:)
```

9 Enter the DCE Cell Name.

Example response

```
Master Security Server Name(default:)
```

10 Enter the host name or IP address of the MSS.

Example response

```
Time Server Name(default:)
```

11 Enter the host name or IP address of the DTS.

Example response

```
CDS Server Name(default:)
```

12 Enter the host name or IP address of the CDS

Example response

```
You have selected to configure your DCE
environment as the following:
Host Name                          : znc0s0jx
DCE Cell Name                      :
rtpptm.sdm.nortel.com
Time Server Name                   : wnc0s0j8
Master Security Server Host Name : wnc0s0j8
CDS Server Host Name               : wnc0s0j8
Continue with configuration?(default:Y[Y/N]
```

13 Continue the configuration by typing

y

and pressing the Enter key.

Example response

```
Synchronizing time with wnc0s0j8......
Tue Apr 16 15:00:47 2002
done synchronizing time with wnc0s0j8(0)
Configuring DCE.............................
Default DCE configuration timeout value
successfully changed.
Gathering current configuration information...
Enter password for principal cell_admin:
```

14 Enter the cell administrator password and press the Enter key.

Example response

```
Configuration of DCE Host, znc0s0jx, will now
begin.
Configuring RPC...
Starting RPC...
RPC was started successfully.
RPC configuration is complete.
Configuring the Security client...
Information from the /etc/krb5.conf.backup file
may need to be manually merged into the
/etc/krb5.conf file.
Starting the Security client...
The Security client was started successfully.
Security client configuration is complete.
Configuring the Directory client...
Starting the Directory client...
Waiting up to 10 minutes for the directory
server.
Contacted the directory server.
The Directory client was started successfully.
```

```
Waiting up to 10 minutes for DCED registration
to be functional.
Directory client configuration is complete.
Configuring the DTS client...
Starting the DTS client...
The DTS client was started successfully.
DTS client configuration is complete.
Gathering component state information...

Component Summary for Host: znc0s0jx
Component    Configuration State  Running State
Security client     Configured        Running
RPC                 Configured        Running
Directory client    Configured        Running
DTS client          Configured        Running

The component summary is complete.
Configuration of DCE Host, znc0s0jx, was
successful.
Configuration completed successfully.
done configuring DCE
Gathering current configuration information...
Configuration of DCE Host, znc0s0jx, will now
begin.
There are no components in the request that need
to be configured.
Gathering component state information...

Component Summary for Host: znc0s0jx
Component    Configuration State  Running State
Security client     Configured        Running
RPC                 Configured        Running
Directory client    Configured        Running
```

```
DTS client          Configured          Running


The component summary is complete.

Configuration of DCE Host, znc0s0jx, was
successful.

Configuration completed successfully.

=== "dce_conf" completed successfully
```

15 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.

16 You have completed this procedure.

Unconfiguring DCE on an SSPFS-based server

Application

Use this procedure to unconfigure the Distributed Computing Environment (DCE) on a Succession Server Platform Foundation Software (SSPFS)-based server following an SSPFS software upgrade. Only perform this procedure if DCE is used as an authentication mechanism. As of (I)SN05, DCE is not required for all systems, therefore, if your system does not have DCE, you do not need to perform this procedure.

Prerequisites

You need the DCE cell administrator password.

Action

Perform the following steps to complete this procedure.

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 that uses DCE as an authentication method

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

7 Enter the number next to the “DCE Configuration” option in the menu.

Example response

```
DCE Configuration
 1 - dce_conf <Configure the DCE Client>
 2 - dce_unconf <Unconfigure the DCE Client>

 X - exit

select -
```

8 Enter the number next to the “dce-unconf” option in the menu.

Example response

```
=== Executing "dce_unconf"
Gathering current configuration information...
Enter password for principal cell_admin:
```

9 Enter the cell administrator password and press the Enter key.

Example response

```
Start of DCE Host, znc0s0jy, will now begin.
RPC is already running.
The Security client is already running.
The Directory client is already running.


Unconfiguration of DCE Host, znc0s0jy, will now
begin.
Unconfiguring the DTS client...
Stopping the DTS client...
The DTS client was stopped successfully.
The DTS client will be completely unconfigured
when RPC is unconfigured.
Unconfiguration of this component has been
successful so far.
Unconfiguring the Directory client...
Stopping the Directory client...
The Directory client was stopped successfully.
```

```
The Directory client was unconfigured
successfully.

Unconfiguring the Security client...

Stopping the Security client...

The Security client was stopped successfully.

The Security client was unconfigured
successfully.

Unconfiguring RPC...

Stopping RPC...

RPC was stopped successfully.

RPC was unconfigured successfully.

Gathering component state information...


      Component Summary for Host: znc0s0jy
 Component   Configuration State   Running State

No DCE components are configured.

Unconfiguration of DCE Host, znc0s0jy, was
successful.

Unconfiguration completed successfully.

done unconfiguring DCE

=== "dce_unconf" 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 You have completed this procedure.

Configuring the destination for SNMP traps

Application

Use this procedure to configure the destination for SNMP traps on the Integrated Element Management System (EMS) server and other Succession Server Platform Foundation Software (SSPFS)-based servers that need to forward their SNMP traps to the Integrated Element Management System (EMS) 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 (EMS) resides

Note: You can obtain the Integrated EMS IP address to use as the destination for SNMP traps, by logging in to the Integrated EMS server and executing the command “getpip.ksh IEMS”.

Action

Perform the following steps to complete this procedure.

At your workstation

1 Telnet to the SSPFS-based server by typing

```
> telnet <IP address>
```

and pressing the Enter key.

where

IP address
is the IP address of the 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 - 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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

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

Example response:

```
Succession Element Configuration
 1 - SESM Application Configuration
 2 - SAM21EM Application Configuration
 3 - NPM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH 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:
45.123.456.78):
```

10 When prompted, enter the IP address of the server where the Integrated EMS resides, or press the Enter key to accept the default if one is specified.

Note: You can obtain the Integrated EMS IP address to use as the destination for SNMP traps, by logging in to the Integrated EMS 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 exit the command line interface, by typing

`select - x`

and pressing the Enter key.

13 You have completed this procedure.

Configuring the SESM server application

Application

Use this procedure to configure the 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) associated with the CLLI
- the IP address of the Media Gateway 9000 Manager if present in the network

Note: Only the root user can perform this procedure.

Action

Perform the following steps to complete this procedure.

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
     (MG9K, LMM, CICM)
 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) 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.

Setting up the PM poller on an SSPFS-based server

Application

Use this procedure set up the PM poller on a Succession Server Platform Foundation Software (SSPFS)-based server, which 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 Succession Server Platform Foundation Software (SSPFS).

For more details on the PM poller, refer to “PM poller” in the Basics document, NN10320-100 (ATM solution) or NN10300-100 (IP solution).

If you need to start the poller, refer to procedure “Starting the PM Poller” in the ATM/IP Security and Administration document, 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 on page 192 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.

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 want to set up the PM poller

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 - DCE Configuration
 4 - OAMP Application 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)

 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.

Note: The IPOA profile is for the SAM21 shelf controller OM configuration.

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 on page 188, 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	SSPFS	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

Managed device SNMP default attributes

SNMP attribute [default]	SAM21SC	UAS	GWC	SSPFS	MS 2010
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 Set the SNMP attributes as follows:

Note: The SNMP attributes you specify for a device using this procedure will override the default SNMP attributes specified in the associated poller profile.

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 exit the command line interface, by typing

```
select - x
```

and pressing the Enter key.

15 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 on page 197 in this document.

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.

The default SNMP attributes you specify for a poller profile, will be used by all devices associated with the profile. You can override the default SNMP attributes specified in a poller profile for a specific device.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

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 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 - DCE Configuration
 4 - OAMP Application 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)

 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.

Note: Use the table provided in procedure Setting up the PM poller on an SSPFS-based server on page 185 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.

Note: 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 “Exit the Configuration Menu” using the up/down arrow key, and press the Enter key.

29 Exit the command line interface by typing

```
select - x
```

and pressing the Enter key.

Note: Exit each menu level to eventually exit the command line interface.

30 You have completed this procedure.

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.

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
- SSPFS

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.

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.

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 - DCE Configuration
 4 - OAMP Application 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)

 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.

Creating an OMPUSH session

Application

Use this procedure to create an OMPUSH session using one of the following two methods:

- Creating an OMPUSH session in menu mode on page 202
- Creating an OMPUSH session from the command line on page 207

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.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

Creating an OMPUSH session in menu mode

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 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 - 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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

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

Example response:

```
Succession Element Configuration
 1 - SESM Application Configuration
 2 - SAM21EM Application Configuration
 3 - NPM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

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

Example response:

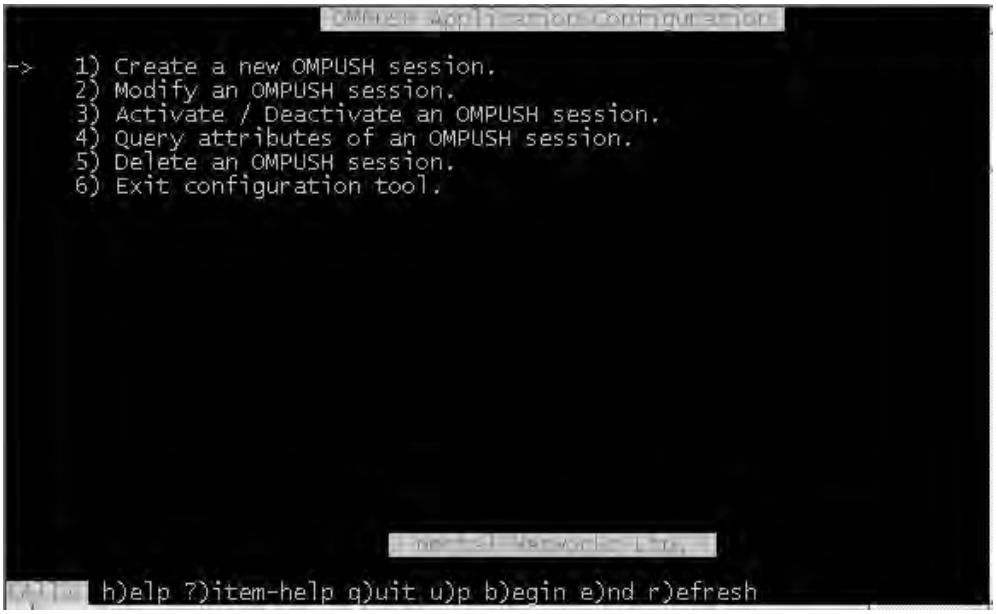
```
OMPUSH Application Configuration
 1 - OMPUSH_cfg (OMPUSH configuration tool)


 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.

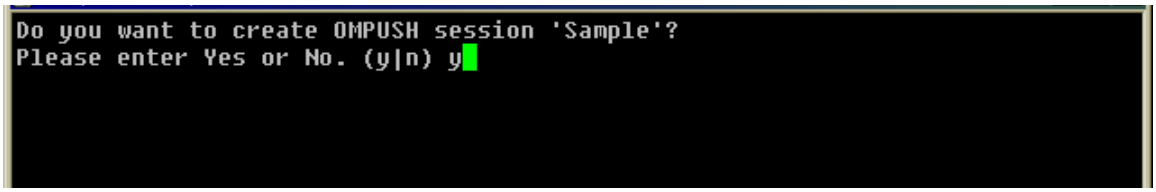
16 Type the number next to "Accept this setting", or use the up/down arrow key, then press the Enter key.

Example response:

17 Enter the session attributes as required, and press the Enter key when finished.

Note: 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.

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.

20 You have completed this procedure.

Creating an OMPUSH session from the command line

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 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 user's login directory)
- interval=session interval (in minutes)
- start=session start day and time (mm/dd/yyyy hh:mm:ss)

Example

```
ompush_cfg -create sample host=47.142.89.70
user=user1 pwd=user1psswd src=poller
interval=20
```

4 You have completed this procedure.

Activating or deactivating an OMPUSH session

Application

Use this procedure to activate or deactivate an OMPUSH session using one of the following two methods:

- Activating or deactivating an OMPUSH session in menu mode on page 209
- Activating or deactivating an OMPUSH session from the command line on page 215

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.

Activating or deactivating an OMPUSH session in menu mode

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 activate or deactivate

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

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

Example response:

```
Succession Element Configuration
 1 - SESM Application Configuration
 2 - SAM21EM Application Configuration
 3 - NPM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

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

Example response:

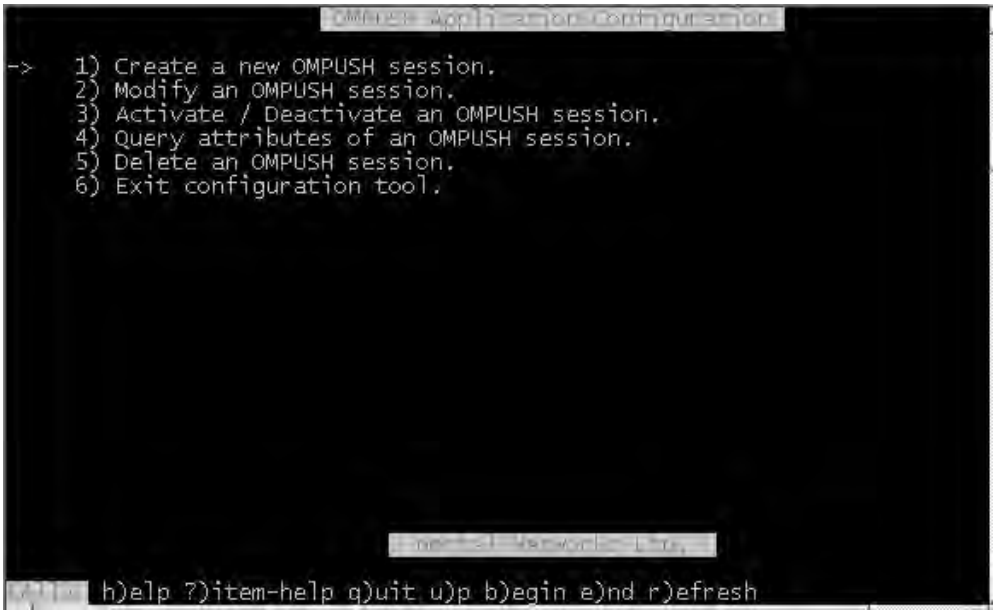
```
OMPUSH Application Configuration
 1 - OMPUSH_cfg (OMPUSH configuration tool)


 X - exit

select -
```

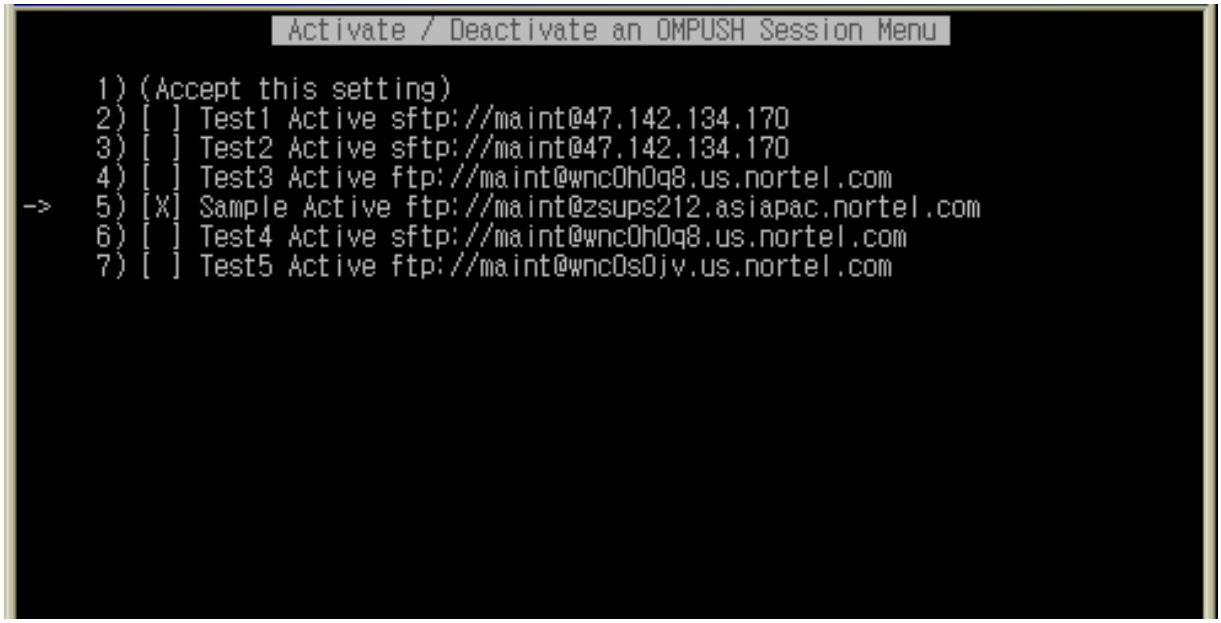
9 Enter the number next to the “OMPUSH_cfg” option in the menu.

Example response:



10 Type the number next to "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.

If you	Do
want to activate or deactivate another session	step 10
do not want to activate or deactivate another session	step 14

14 Type the number next to "Exit configuration tool", or use the up/down arrow key, then press the Enter key.

15 You have completed this procedure.

Activating or deactivating an OMPUSH session from the command line

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 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

6 You have completed this procedure.

Modifying an OMPUSH session

Application

Use this procedure to modify an OMPUSH session using one of the following two methods:

- Modifying an OMPUSH session in menu mode on page 217
- Modifying an OMPUSH session from the command line on page 223

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.

Modifying an OMPUSH session in menu mode

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 modify

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

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

Example response:

```
Succession Element Configuration
 1 - SESM Application Configuration
 2 - SAM21EM Application Configuration
 3 - NPM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

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

Example response:

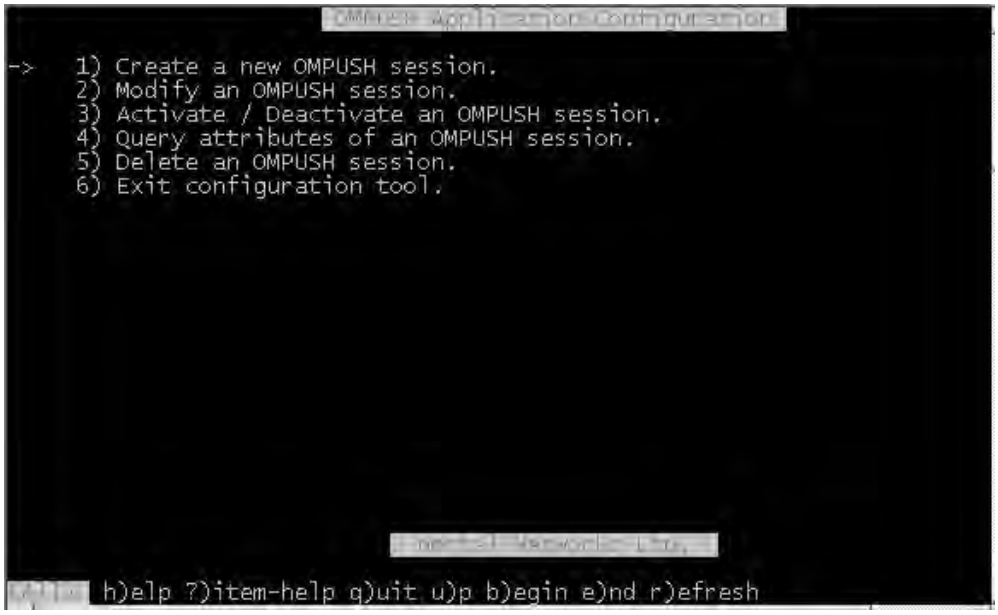
```
OMPUSH Application Configuration
 1 - OMPUSH_cfg (OMPUSH configuration tool)


 X - exit

select -
```

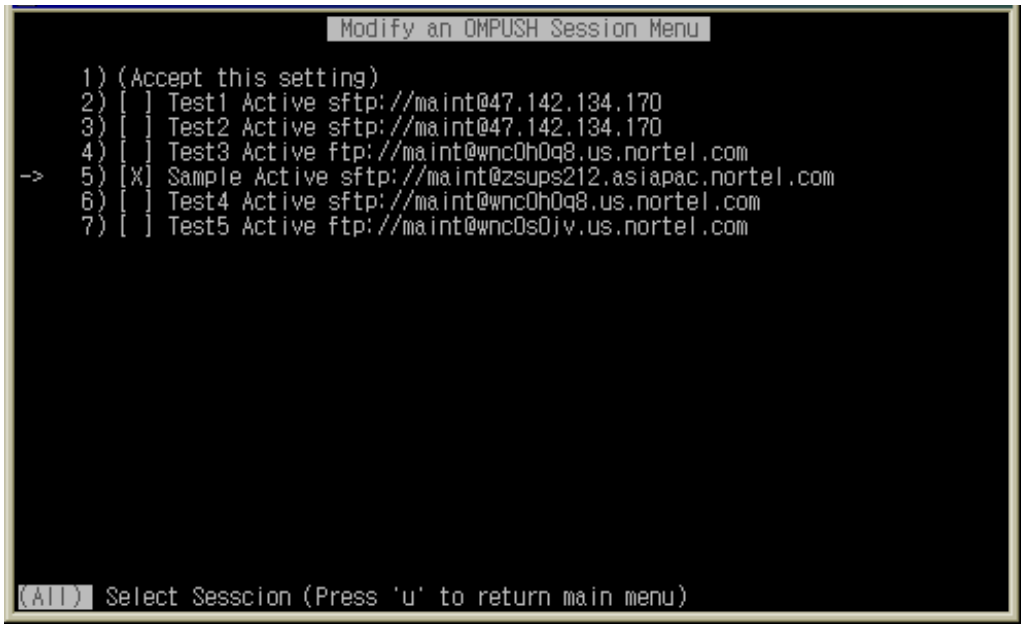
9 Enter the number next to the “OMPUSH_cfg” option in the menu.

Example response:



10 Type the number next to "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:

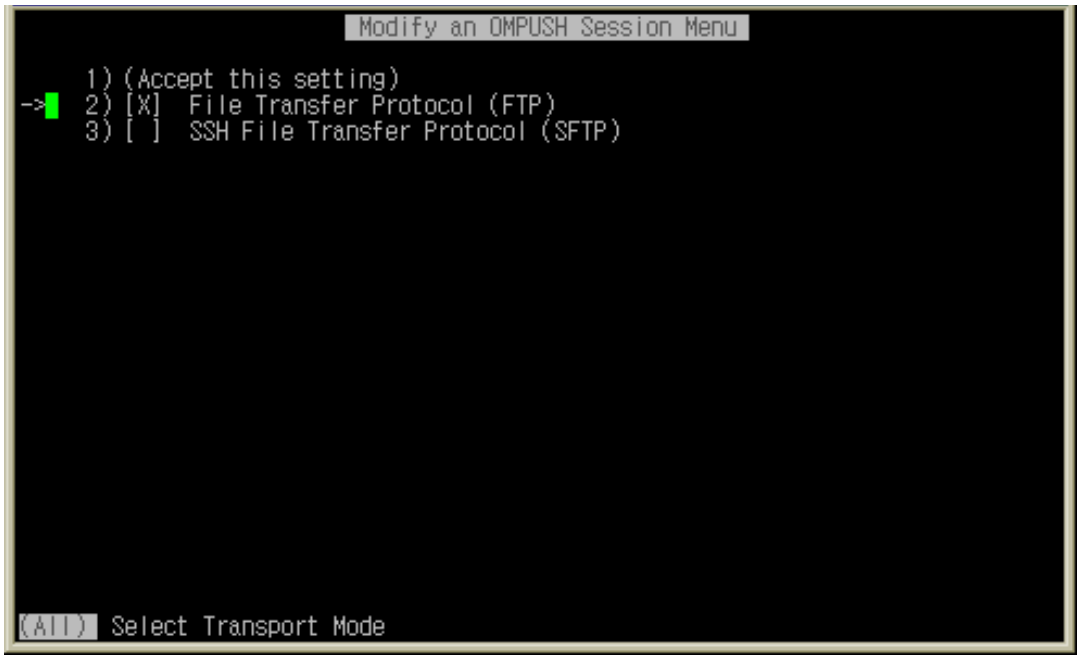
<Session_Name> <Active/Inactive>
<TransMode>://<RemoteUser>@<Destination_Host>

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.

Note: You can modify any of the attributes for a session except the session name.

Example response:

```
Save your changes to OMPUSH session 'Sample'?
Please enter Edit, Yes or No. (e|y|n)
```

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.

19 You have completed this procedure.

Modifying an OMPUSH session from the command line

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 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 user's login directory)
- interval=session interval

Example

```
ompush_cfg -modify sample mode=ftp port=21
interval=20
```

4 You have completed this procedure

Deleting an OMPUSH session

Application

Use this procedure to delete an OMPUSH session using one of the following two methods:

- Deleting an OMPUSH session in menu mode on page 225
- Deleting an OMPUSH session from the command line on page 231

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.

Deleting an OMPUSH session in menu mode

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 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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

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

Example response:

```
Succession Element Configuration
 1 - SESM Application Configuration
 2 - SAM21EM Application Configuration
 3 - NPM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

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

Example response:

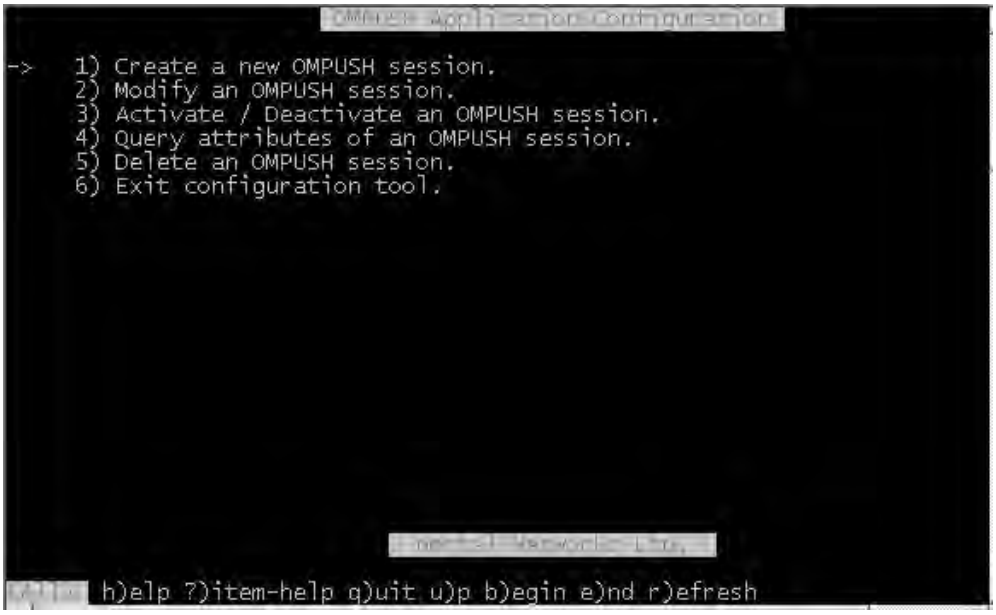
```
OMPUSH Application Configuration
 1 - OMPUSH_cfg (OMPUSH configuration tool)


 X - exit

select -
```

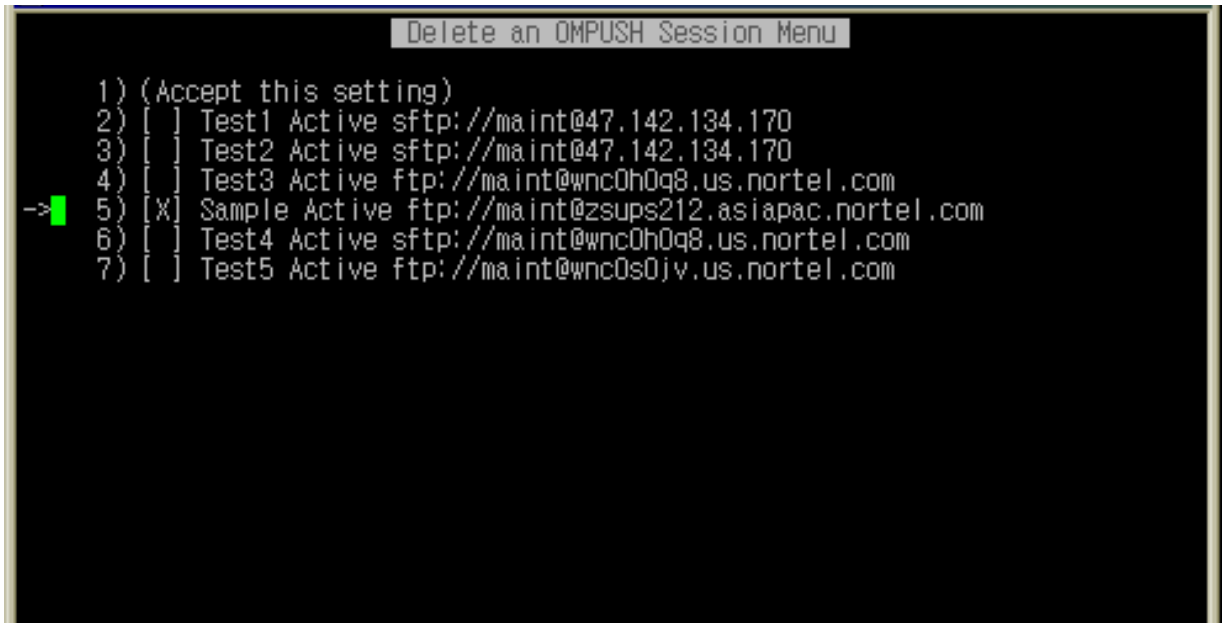
9 Enter the number next to the “OMPUSH_cfg” option in the menu.

Example response:



10 Type the number next to "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:

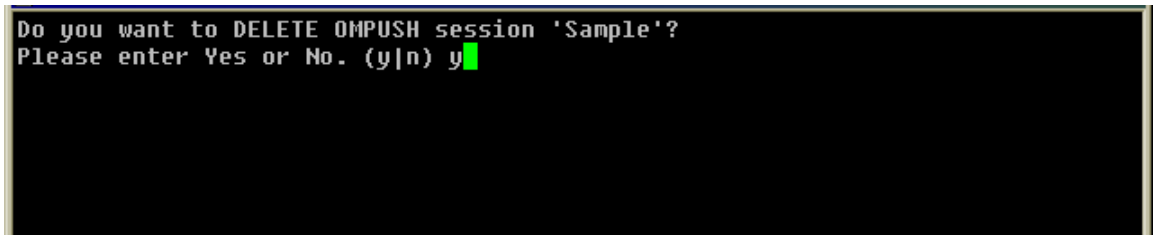
<Session_Name> <Active/Inactive> <TransMode>://<RemoteUser>@<Destination_Host>

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.

Note: If the session is running, the system will not allow you to delete it.

If you	Do
want to delete another session	step 10
do not want to delete another session	step 14

14 Type the number next to "Exit configuration tool", or use the up/down arrow key, then press the Enter key.

15 You have completed this procedure.

Deleting an OMPUSH session from the command line

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

4 You have completed this procedure.

Querying OMPUSH session attributes

Application

Use this procedure to query the attributes of an OMPUSH session using one of the following two methods:

- Querying OMPUSH session attributes in menu mode on page 232
- Querying OMPUSH session attributes from the command line on page 238

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.

Querying OMPUSH session attributes in menu mode

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 sessions you want to query

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 - DCE Configuration
 4 - OAMP Application 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)

 X - exit

Select -
```

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

Example response:

```
Succession Element Configuration
 1 - SESM Application Configuration
 2 - SAM21EM Application Configuration
 3 - NPM Application Configuration
 4 - PSE Application Configuration
 5 - RESMON Application Configuration
 6 - OMPUSH Application Configuration


 X - exit

select -
```

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

Example response:

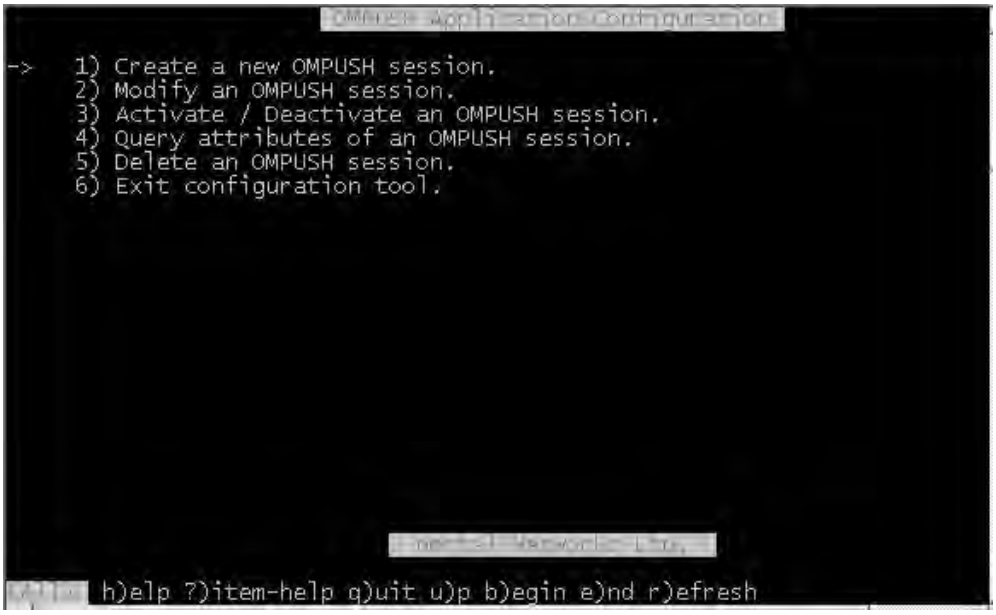
```
OMPUSH Application Configuration
 1 - OMPUSH_cfg (OMPUSH configuration tool)


 X - exit

select -
```

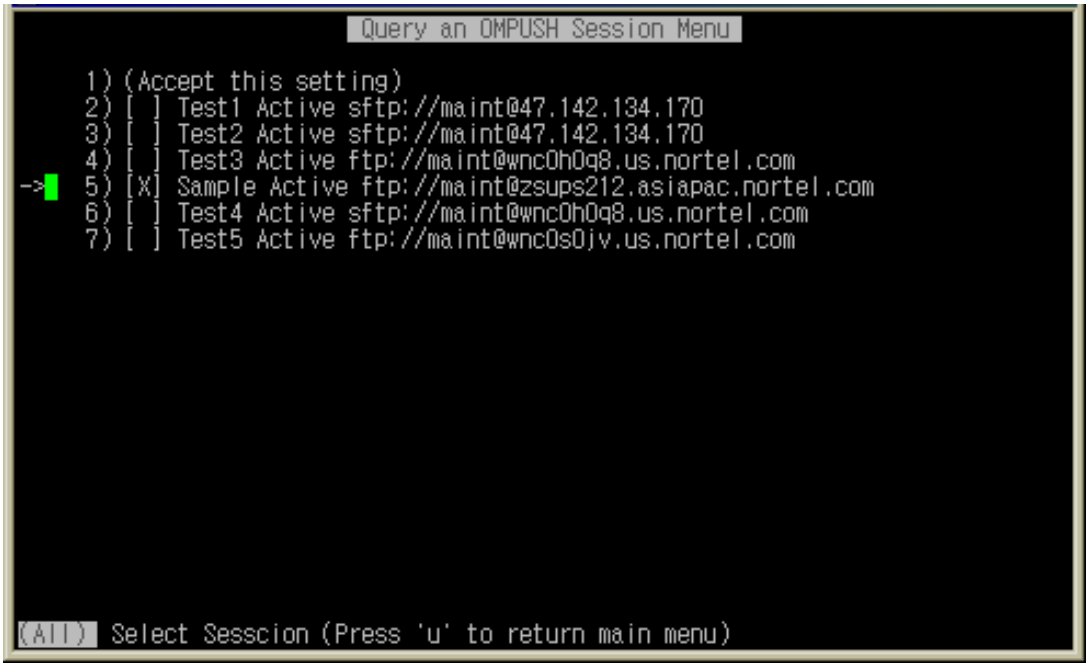
9 Enter the number next to the “OMPUSH_cfg” option in the menu.

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:

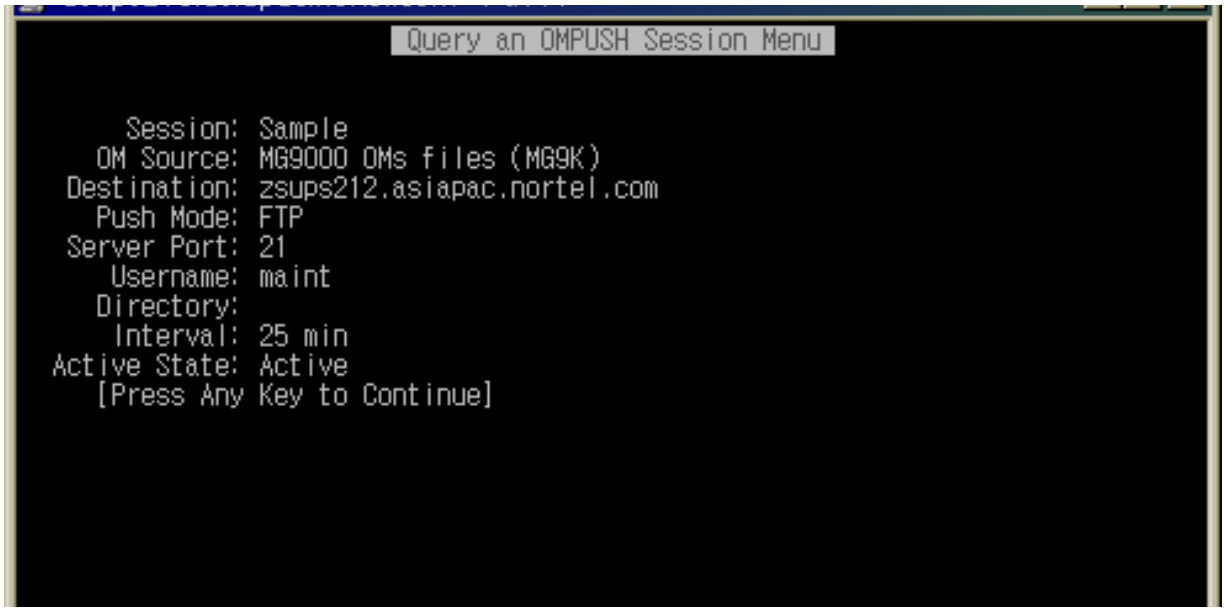
<Session_Name> <Active/Inactive> <TransMode>://<RemoteUser>@<Destination_Host>

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.

15 You have completed this procedure.

Querying OMPUSH session attributes from the command line

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 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

Note: If you do not specify the session name, the system will display the details for all existing sessions.

4 You have completed this procedure.

Setting the TMM CLLI name

Application

Use this procedure to set the TMM CLLI name.

Prerequisites

None

Action

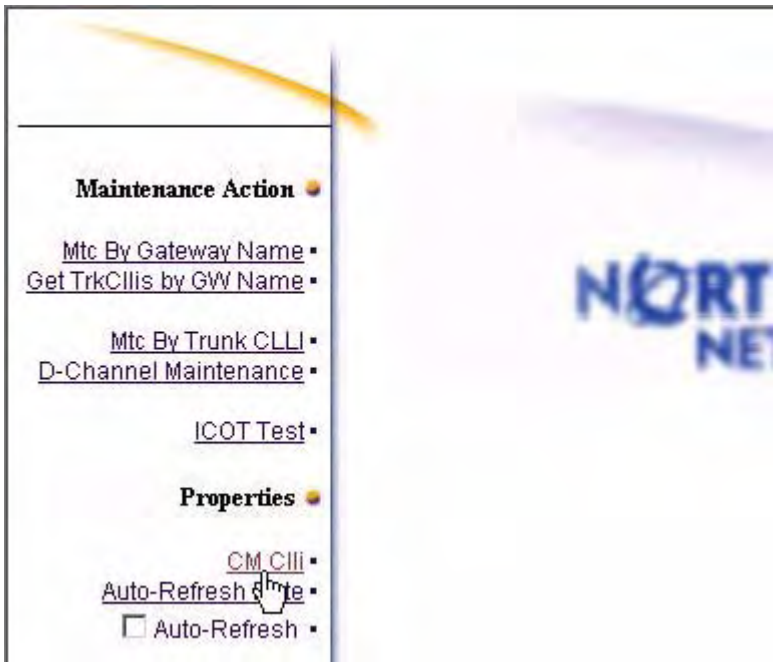
Perform the following steps to complete this procedure.

At your workstation

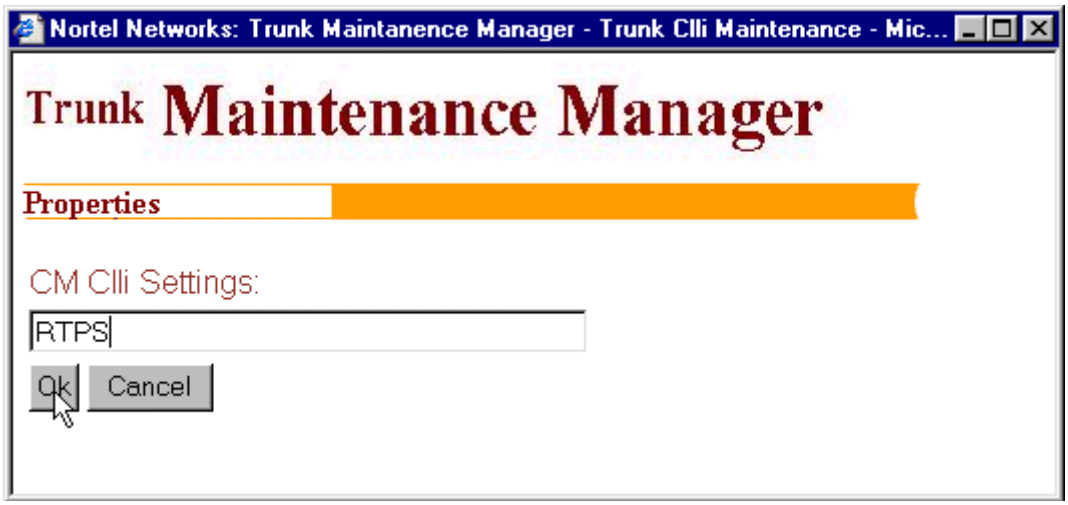
1 Access the TMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

At the TMM GUI

1 Click the **CM Clli** link on the left side of the page.



2 Enter the CLLI name for the Communication server 2000, and click **Ok**.



3 You have completed this procedure.

Setting the TMM Auto Refresh value

Application

Use this procedure to set the auto refresh value.

Prerequisites

None

Action

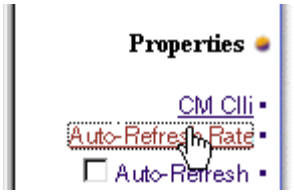
Perform the following steps to complete this procedure.

At your workstation

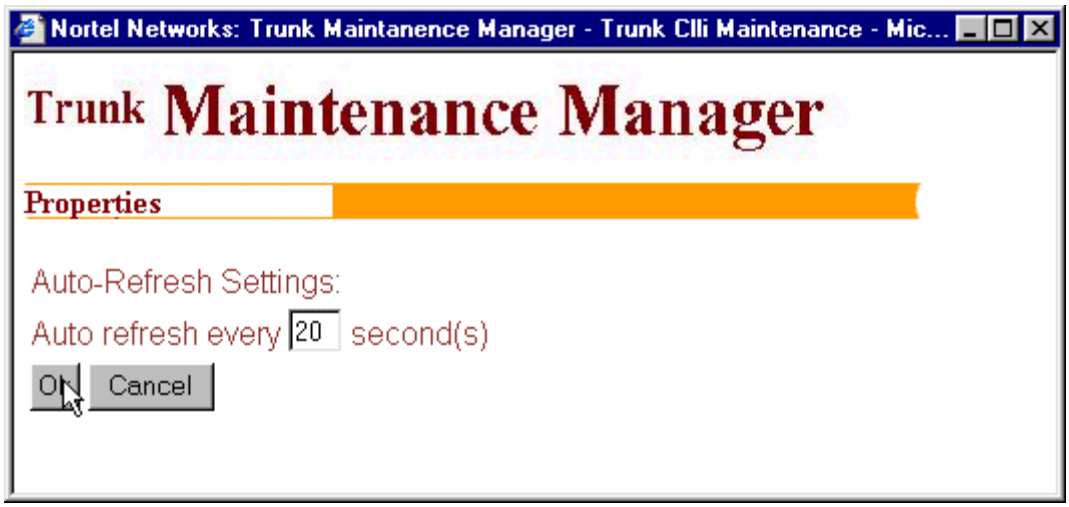
1 Access the TMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

At the TMM GUI

1 Click the **Auto-Refresh Rate** link on the left side of the window.



2 Enter a new value and click **Ok**.



3 You have completed this procedure.

Turning TMM Auto-Refresh on or off

Application

Use this procedure to toggle auto-fresh.

Prerequisites

None

Action

Perform the following steps to complete this procedure.

At your workstation

1 Access the TMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

At the TMM GUI

1 Select the **Auto-Refresh** check box on the left side of the page.

2 You have completed this procedure.

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

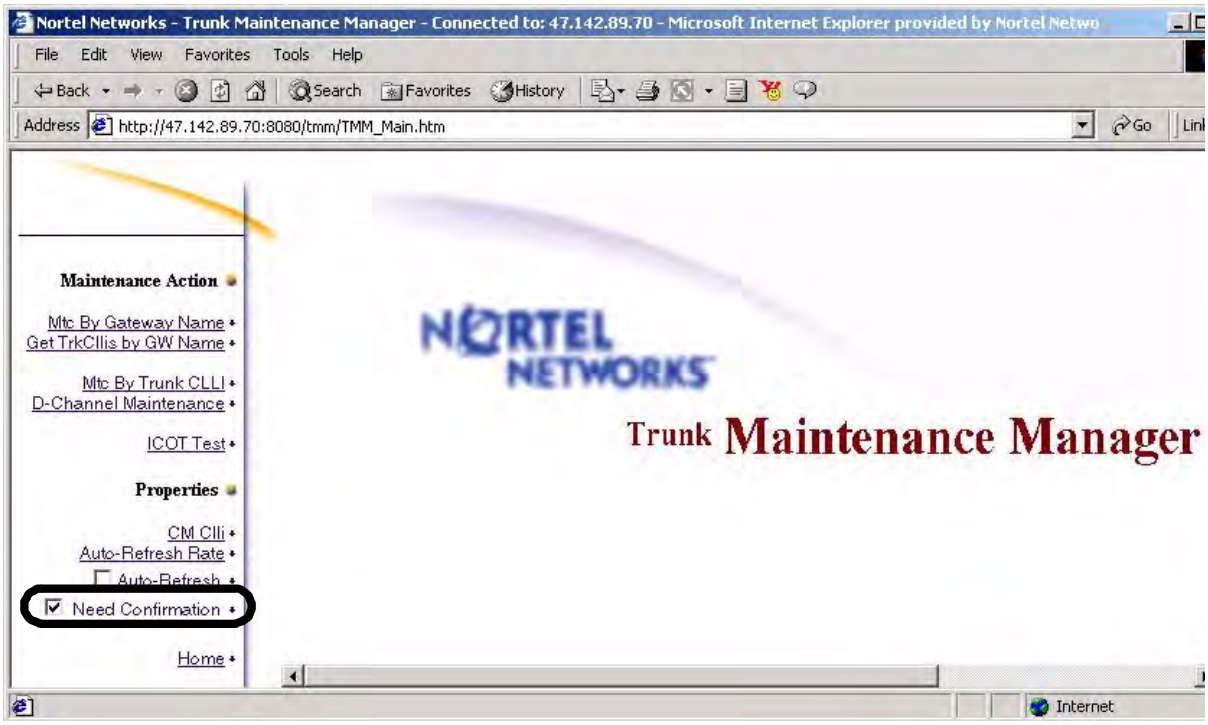
Perform the following steps to complete this procedure.

At your workstation

1 Access the TMM GUI. Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document, if required.

At the TMM GUI

1 Check the **Need Confirmation** checkbox.



2 You have completed this procedure.

Launching CS 2000 Management Tools client applications

Application

Use this procedure to launch any one of the following client applications:

- Trunk Maintenance Manager (TMM)
- CS2000 Management Tools
- Line Maintenance Manager (LMM)
- Succession SAM21 Element Manager
- Batch Configuration Monitor
- Network Patch Manager (NPM), when installed and enabled on the same server as the CS 2000 Management Tools

  Note: The NPM also has a command line user interface (CLUI). Refer to procedure Accessing the Network Patch Manager CLUI on page 257 in this document.

This procedure provides the following four methods to launch a CS 2000 Management Tools client application:

- Launching applications from a web browser on page 246. You must use this method when launching an application for the first time.
- Launching applications from the JWS Application Manager on page 249.

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching applications from a desktop icon or Start menu (Windows only) on page 252.

  Note: You cannot use this method to launch the Trunk Maintenance Manager (TMM) or the Batch Configuration Monitor.

- Launching specific applications using a URL on page 255.

Note: You can also launch applications from the Integrated Element Management System (EMS) when the Integrated EMS is present in the office. Refer to the Integrated EMS Basics document, 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, NN10320-100 (ATM solution) or NN10300-100 (IP solution).

ATTENTION

If you have an ATI Raedon 7000 series graphics card installed on your desktop computer, or an ATI Mobility graphics chip installed in your laptop computer, you may experience the “blue screen of death” in your Windows environment. You can obtain information on this issue at the following URL: 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 server where the CS 2000 Management Tools are installed, and a valid user name and password to launch an application.

Note: 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 a Sun server” in the ATM/IP Security and Administration document, NN10402-600.

You must have Java™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the following applications:

- CS2000 Management Tools
- Line Maintenance Manager
- CS2000 SAM21 Manager
- Network Patch Manager

Note: JWS 1.2.0_02 is included as part of JRE 1.4.1_02.

Action

Launching applications from a web browser

At your workstation

1 Launch your web browser.

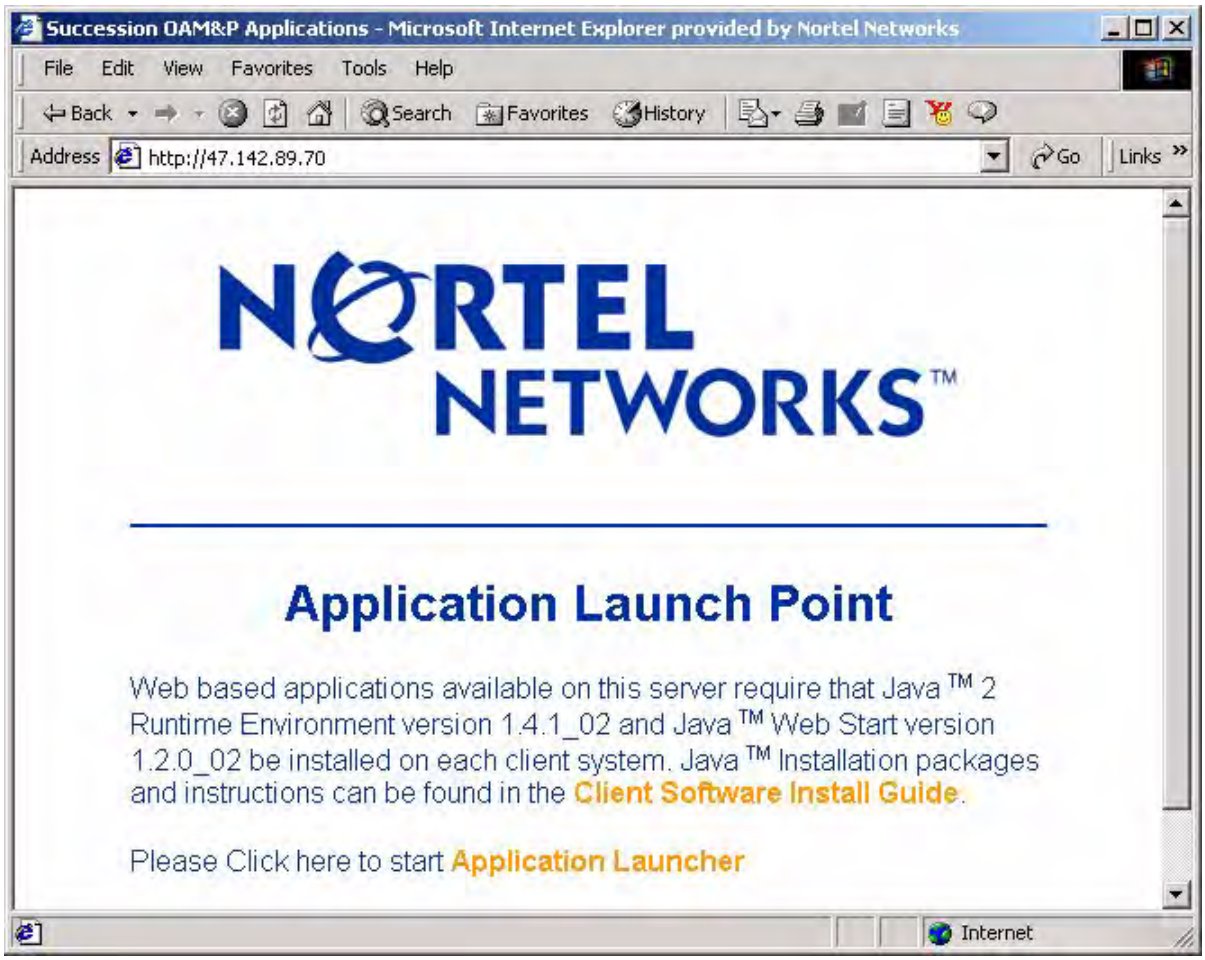
2 Access the CS 2000 Management Tools server by typing

>http://<host>

where

<host>
is the name or IP address of the CS 2000 Management Tools server where the CS2M software package is installed

The “Application Launch Point” page appears.



3 Refer to the following table to determine your next step.

If	Do
you have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 9
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 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 1.4.1_02 and JWS 1.2.0_02 installed	step 8
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 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 the **Back** button to return to the “Client Software Installation” page.

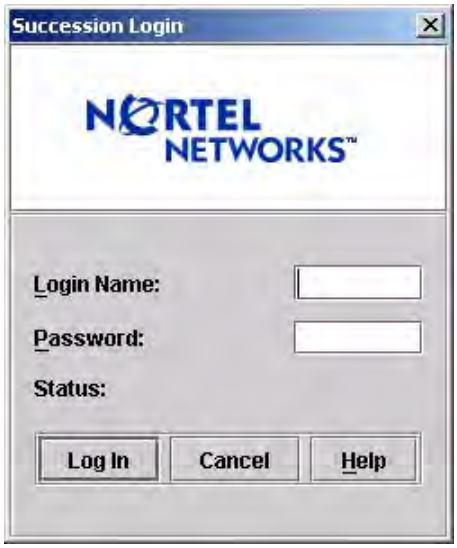
7 Click **Java 2 Runtime Environment Software Download** under “Microsoft Windows” or “Sun Solaris” to download and install the software.

Note: You must have administrative privileges to install the software on the workstation.

8 Click the **Back** button to return to the “Application Launch Point”.

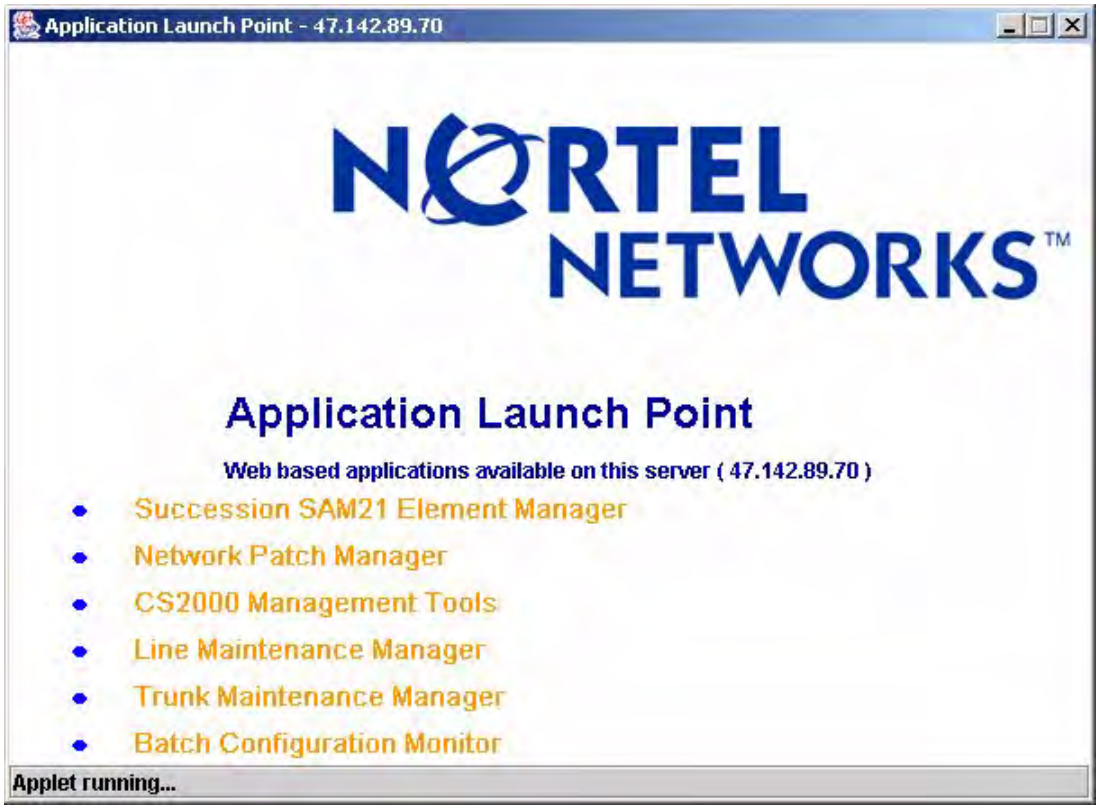
9 Click **Application Launcher**.

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 on the link for the application you want to launch.

The interface for the application you launched, is displayed.

Note: If you delay clicking on an application link by 5 minutes or more after you log in, the login window will appear requiring you to log in again.

12 You have completed this procedure.

Launching applications from the JWS Application Manager

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.

At your workstation

1 Launch the Java Web Start Application Manager.

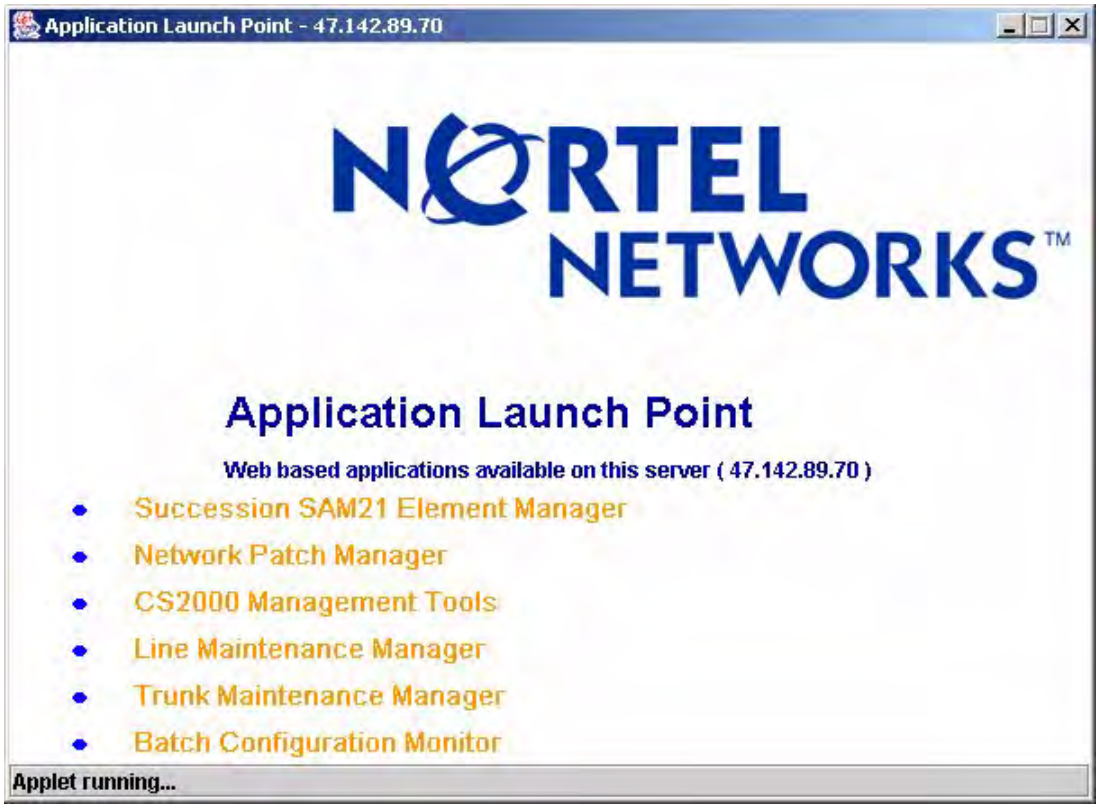
Note: If you do not see the downloaded applications as shown in the example above, on the **View** menu, click **Downloaded Applications**.

2 Double click on the Application Launch Point you want to access, or select the Application Launch Point and click **Start**.

The Login window appears.

3 Enter your user name and password, then click **Log In**.

The Application Launch Point, similar to following, appears.



4 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

5 You have completed this procedure.

Launching applications from a desktop icon or Start menu (Windows only)

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.

At your workstation

1 Perform step a to launch an application from a desktop icon, or b to launch an application from the Start menu.

a To launch a CS 2000 Management Tools client application from a desktop icon, locate the short-cut icon on your desktop, and double click on it to start the application.

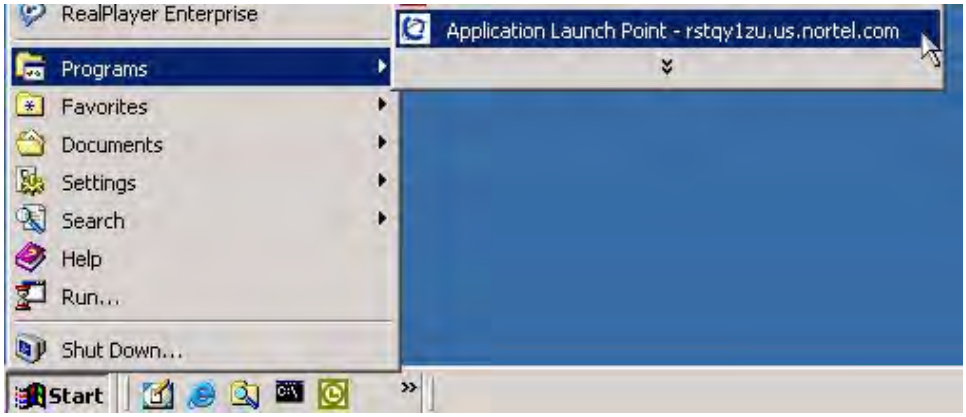
Note: For short-cut icons to be present on your desktop, you must have the right settings under the Shortcut Options tab, which is accessed through **File->Preferences** in the JWS Application Manager.

The Login window appears.

Proceed to step 2.

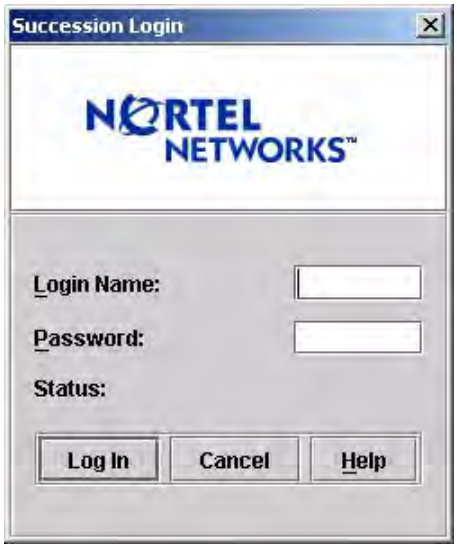
OR

b To launch a CS 2000 Management Tools client application from the Start menu, click **Start->Programs**, then click on the CS 2000 Management Tools client application you want to launch.

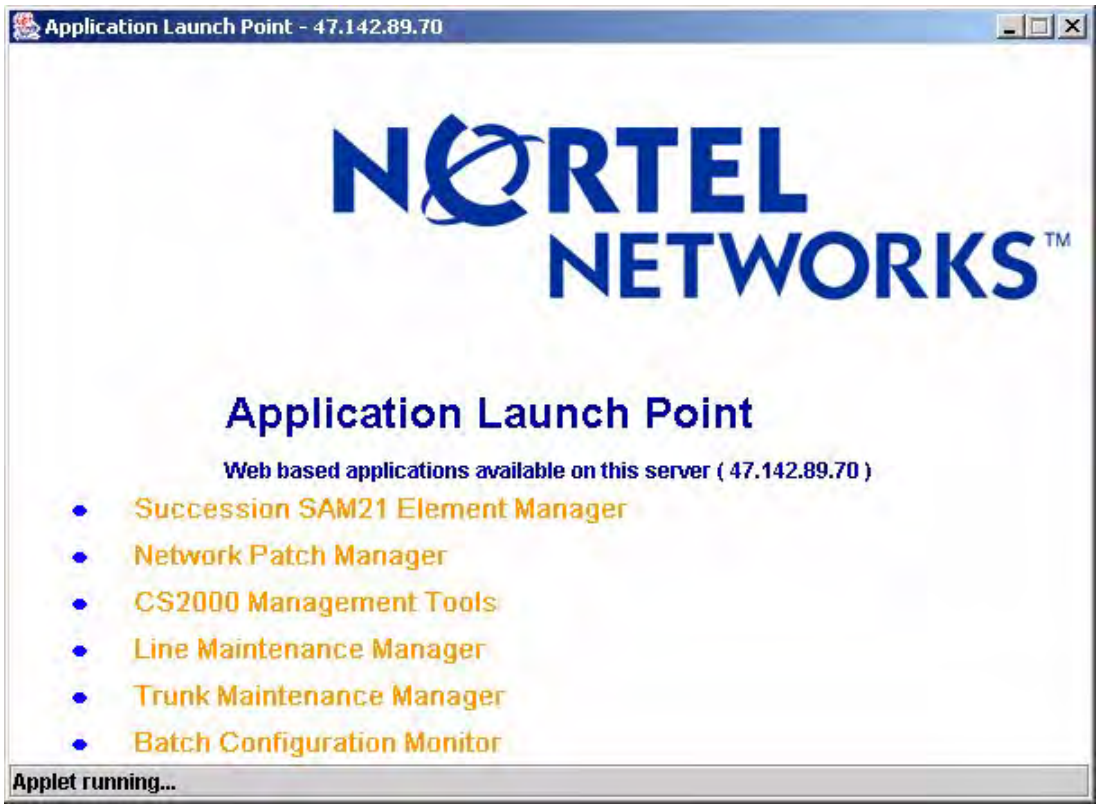


The Login window appears.

2 Enter your user name and password, then click **Log In**.



The Application Launch Point, similar to following, appears.



3 Click on the link for the application you want to launch.

The interface for the application you launched, is displayed.

4 You have completed this procedure.

Launching specific applications using a URL

ATTENTION

You must have Java™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java™ Web Start (JWS) version 1.2.0_02 installed to launch the applications. If this is the first time you are launching an application, use the first method provided in this procedure Launching applications from a web browser on page 246.

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
Trunk Maintenance Manager	http://<host>/sesm/tmm.html
Batch Configuration Monitor	http://<host>/sesm/bpt.html
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 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.

Additional information

The GUI-based client applications (CS2000 Management Tools, Line Maintenance Manager, Network Patch Manager, and Succession SAM21 Element Manager) connect to their corresponding server-side application through a Socks proxy.

Note: The Trunk Maintenance Manager (TMM) and Batch Configuration Monitor do not use a Socks proxy.

If, when you launch a client application that connects through a Socks proxy, you 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 re-launch 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).

Note 1: You can also access the NPM CLUI from the Integrated Element Management System (EMS) when the Integrated EMS is present in the office. Refer to the Integrated EMS Basics document, NN10329-111.

Note 2: The Network Patch Manager also has a graphical user interface (GUI). Refer to procedure Launching CS 2000 Management Tools client applications on page 244 in this document.

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 a Sun server in ATM/IP Solution-level Security and Administration, NN10402-600.

Action

Perform the following steps to complete this procedure.

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 where NPM resides

2 When prompted, enter your user ID and password.

3 Start the NPM CLUI by typing

```
$ npm
```

and pressing the Enter key.

4 When prompted, enter your user ID and password.

Example response:

```
Entering shell mode: Enter 'npm' commands, help
or quit to exit.

npm>
```

5 You have completed this procedure.

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

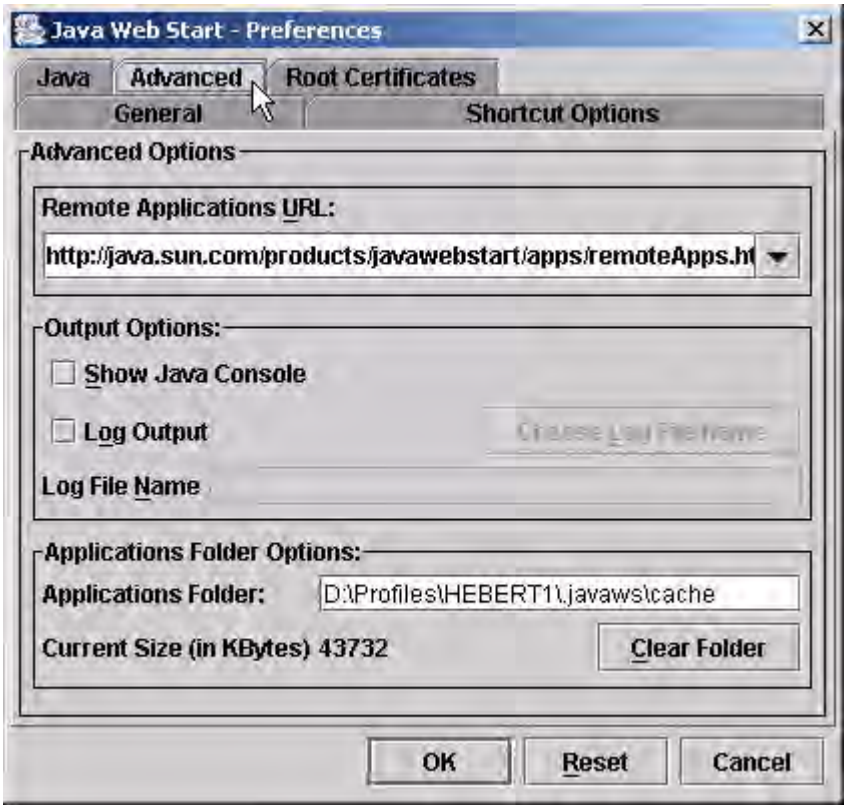
Perform the following steps to complete this procedure.

At your workstation

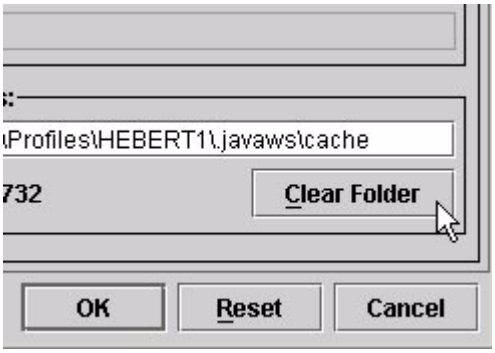
1 Access the Java Web Start Application Manager.

2 Access the Preferences panel by clicking **File->Preferences**.

3 Access the Advanced panel by clicking the **Advanced** tab.



4 Clear the cache by clicking **Clear Folder**.



5 Confirm you want to clear the cache (remove all downloaded resources) by clicking **Yes**.

6 You have completed this procedure.

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.

Platform

Table Client workstation platforms lists the workstation platform and operating system for each client application.

Client workstation platforms (Sheet 1 of 3)

Application	Invocation	Platform	Operating System
Integrated EMS (JWS mode)	Browser (JWS)	PC	Windows 2000, XP, 2003 to current
		Sun	Solaris 2.7, 2.8, 2.9 to current
Integrated EMS (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

Client workstation platforms (Sheet 2 of 3)

Application	Invocation	Platform	Operating System
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
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

Client workstation platforms (Sheet 3 of 3)

Application	Invocation	Platform	Operating System
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
Preside 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
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 lists required web browser for each client application that uses a browser.

Web browser (Sheet 1 of 2)

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
Note: Nortel Networks supports all versions of browser software officially supported by the browser vendor. Microsoft does not support Internet Explorer on a Solaris client.		

Web browser (Sheet 2 of 2)

Application	Invocation	Browser
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 Networks 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

Client to solution mapping for NA solutions

Client	IAC/W	PT-AAL1	PT-IP	UA-AAL1	UA-IP
Universal Signaling Point Manager	X		X	X	X
Nortel Networks Device Manager	X	X	X	X	X
Preside 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
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
Preside 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)	Page
INSTALLATION		
CS 2000 Management Tools	"Installing Java™ Web Start"	270
CS 2000 SAM21 Manager	"Installing Java™ Web Start"	270
Line Maintenance Manager	"Installing Java™ Web Start"	270
Trunk Maintenance Manager	"Installing Java™ Web Start"	270
Network Patch Manager	"Installing Java™ Web Start"	270
Media Gateway 9000 Manager	"Installing Java™ Web Start"	270
Universal Signaling Point Manager	Installing the USP Manager	275
Nortel Networks Device Manager	Installing the Device Manager	276
CONFIGURATION		
Universal Signaling Point Manager	Configuring the USP Manager	279

Client procedures

Component	Procedure (s)	Page
Nortel Networks Device Manager	Configuring the Device Manager	281
All components	Organizing the clients on multiple switches	285
VALIDATION		
CS 2000 Management Tools	Validating an installation of the CS 2000 Management Tools	294
CS 2000 SAM21 Manager	Validating an installation of the CS 2000 SAM21 Manager	307
Line Maintenance Manager	Validating an installation of the LMM	338
Trunk Maintenance Manager	Validating an installation of the TMM	342
Network Patch Manager	Validating an installation of the Network Patch Manager	314
Media Gateway 9000 Manager	Validating an installation of the MG 9000 Manager	321
Universal Signaling Point Manager	Validating an installation of the USP Manager	326
Nortel Networks Device Manager	Validating an installation of the Device Manager	332

Installing Java™ Web Start

Application

This procedure describes how to determine if you need to install Java™ Web Start and how to perform the installation.

Web based applications available on several element management servers require that Java™ 2 Runtime Environment version 1.4.1_02 and Java™ Web Start be installed on each client system. Java™ Web Start is included with the Java™ 2 Runtime Environment version 1.4.1_02. The applications that require this software include the following:

- CS2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- CS2000 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 the Basics document.

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

At your workstation

1 Launch your web browser.

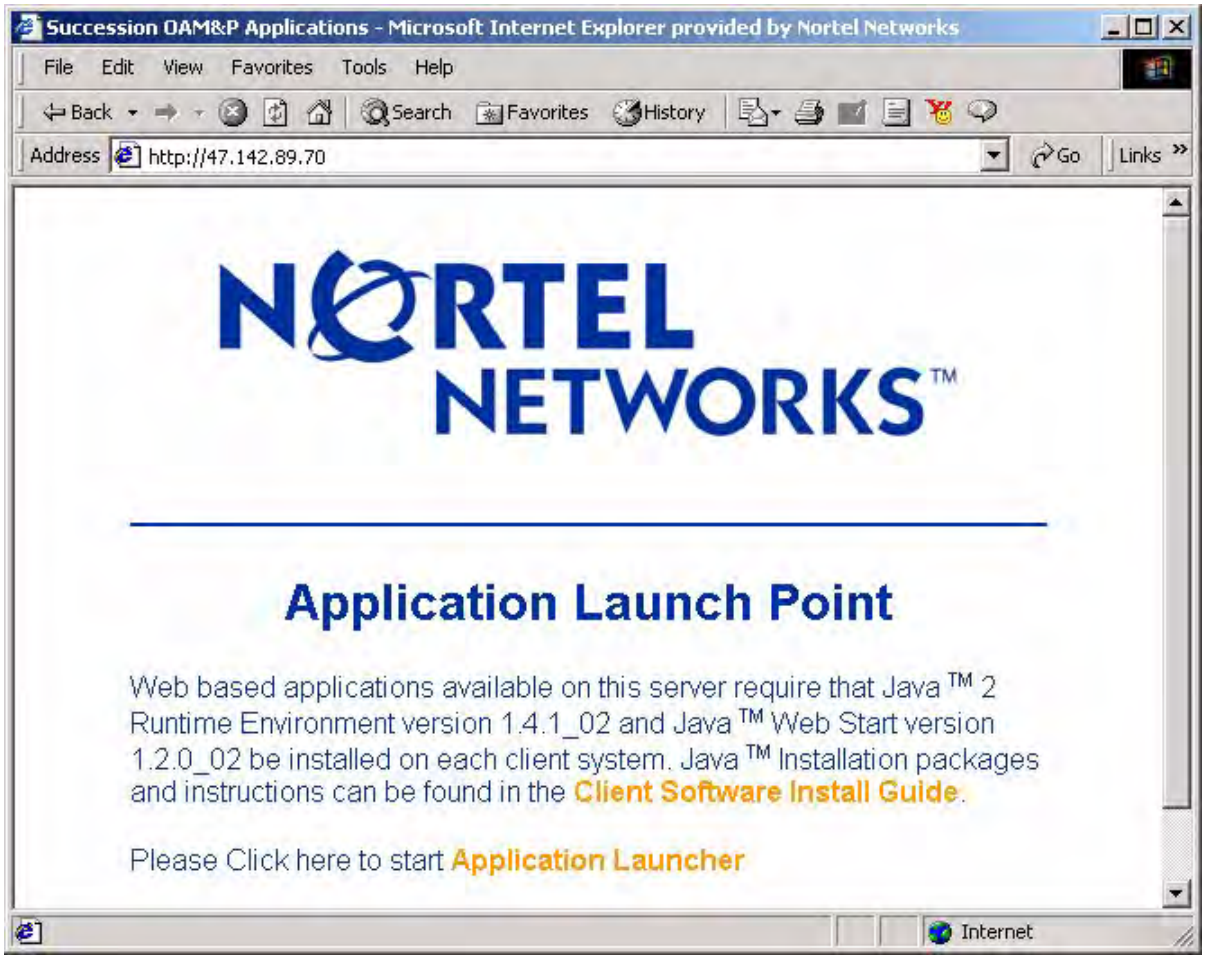
2 Access the server where the CS 2000 Management Tools or the MG 9000 Manager software is installed by typing

>http://<host>

where

<host>
is the name or IP address of the server where the CS 2000 Management Tools or MG 9000 Manager 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 1.4.1_02 and JWS 1.2.0_02 installed	you have completed this procedure
you do not have JRE 1.4.1_02 and JWS 1.2.0_02 installed	step 3

4 Click **Java 2 Runtime Environment Install Guide** under “Microsoft Windows” or “Sun Solaris” for system requirements and installation instructions.

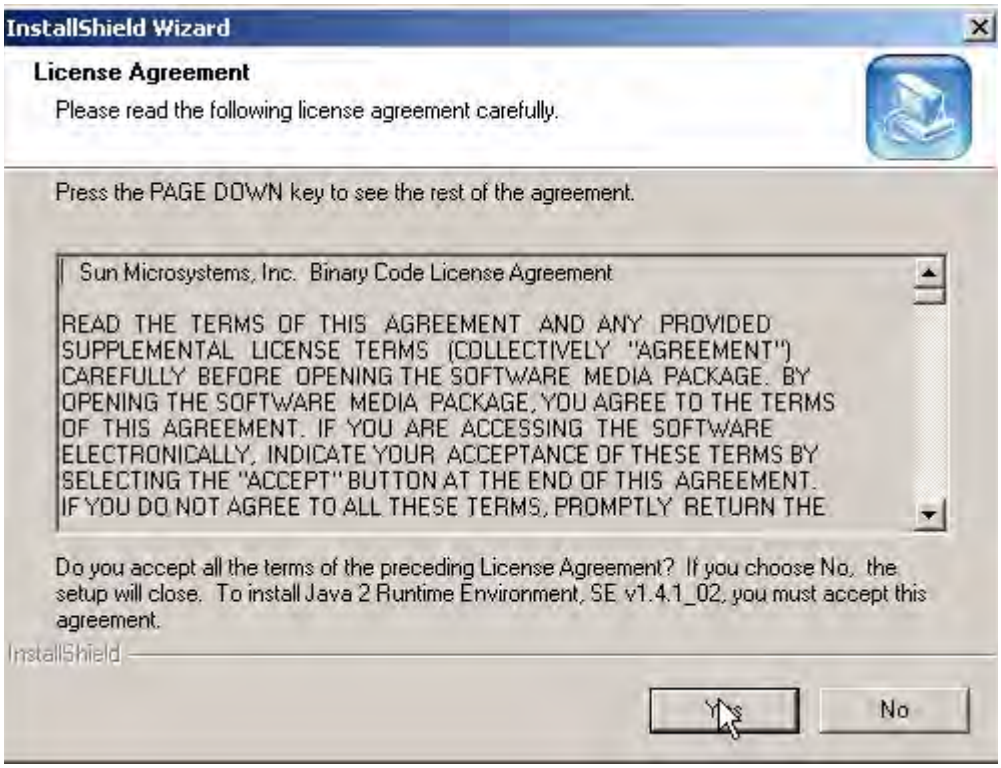
5 Once you have read through the “Java 2 Runtime Environment Install Guide”, click the **Back** button to return to the “Client Software Installation” page.

6 Click **Java 2 Runtime Environment Software Download** under “Microsoft Windows” or “Sun Solaris” to download and install the software.

Note: You must have administrative privileges to install the software on the workstation.

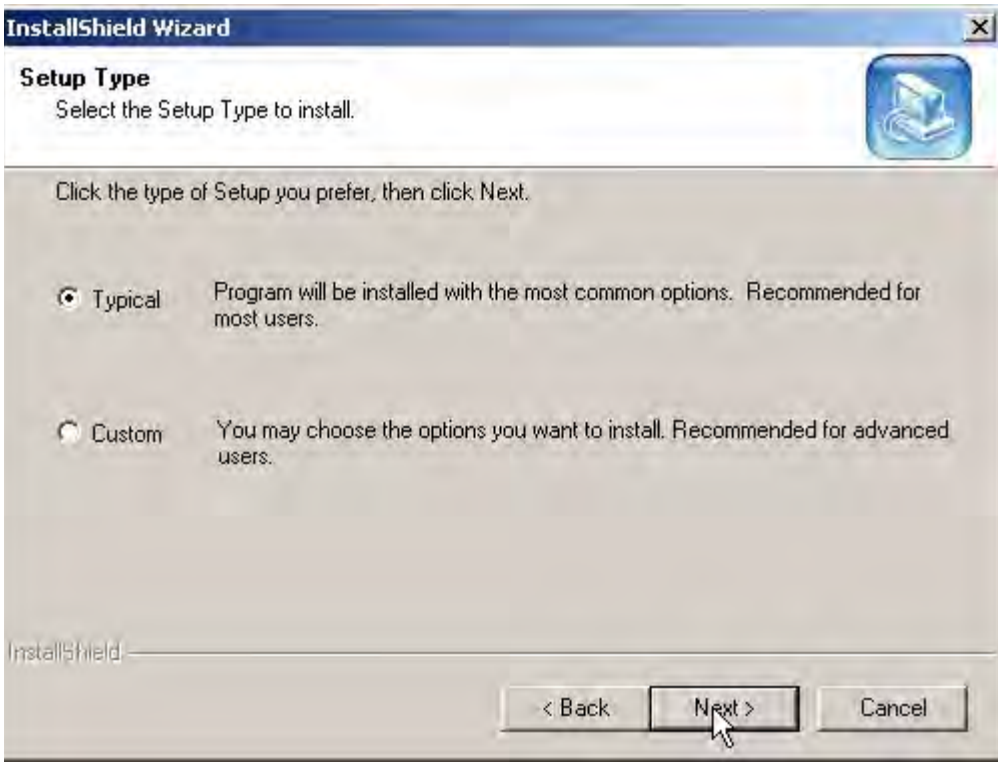
7 Either save the executable file to your computer and run it, or run it from its current location.

8 Read the terms of the license agreement. If you agree to terms, click **Yes**.



Note: 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.

Installing the USP Manager

You must install Windows client software on each remote Windows workstation before you can use the remote reachthrough 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.

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 Networks 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.

Installing the USP Manager client

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.

Installing the Device Manager

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.

> ***Note:*** 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.x.x in order to access Passport 8000 Series switches running switch software version 3.3.

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 1.3.1_03 or higher installed. After the JRE is installed, you can upgrade your system to later versions of Device Manager without installing the JRE again.

Installing the Device Manager software

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 procedure	step 7
not performed the Installing Java™ Web Start procedure	step 6

6 Install the JRE by performing the following steps:

Note: If you have already performed the Installing Java™ Web Start procedure, skip this step.

a Double-click the j2re-1_3_1_03-win.exe 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.

Note: 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.

Configuring the USP Manager

This procedure demonstrates how to configure the USP Manager after you have installed it. You must perform this procedure before launching the USP Manager.

Configuring the USP Manager client

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.

Configuring the Device Manager

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.

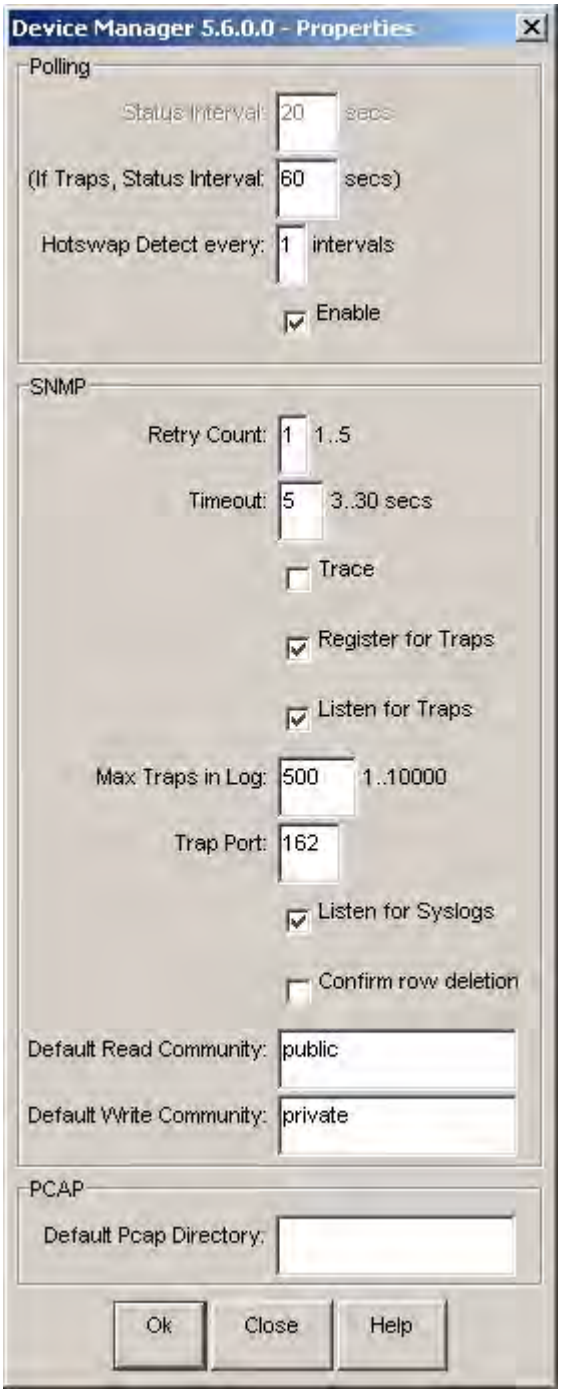
Setting the Device Manager properties

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 table below 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.

Properties dialog box fields

Field	Description
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.
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.

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.

Note: This procedure is written for use with Internet Explorer. Performing the procedure with Netscape Navigator would entail similar, but slightly different steps.

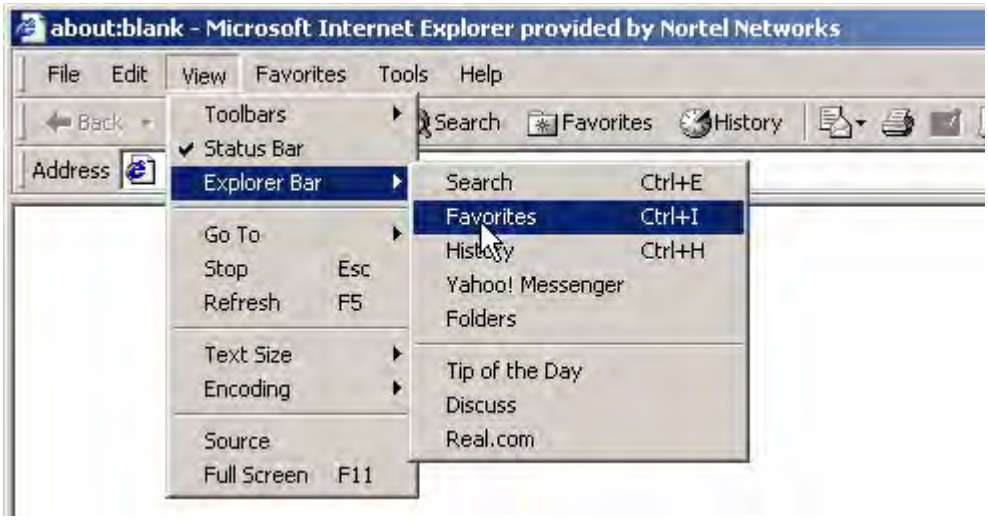
Prerequisites

Action

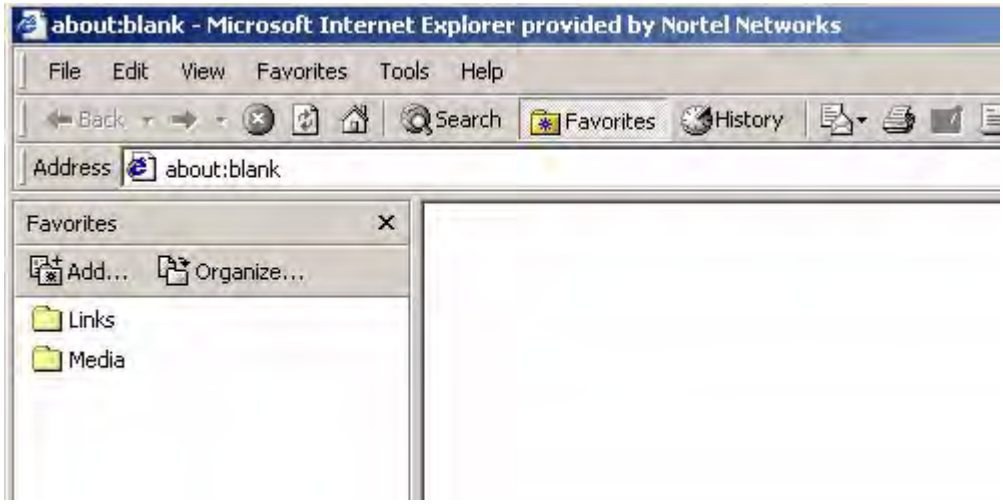
At your workstation

1 Launch Internet Explorer.

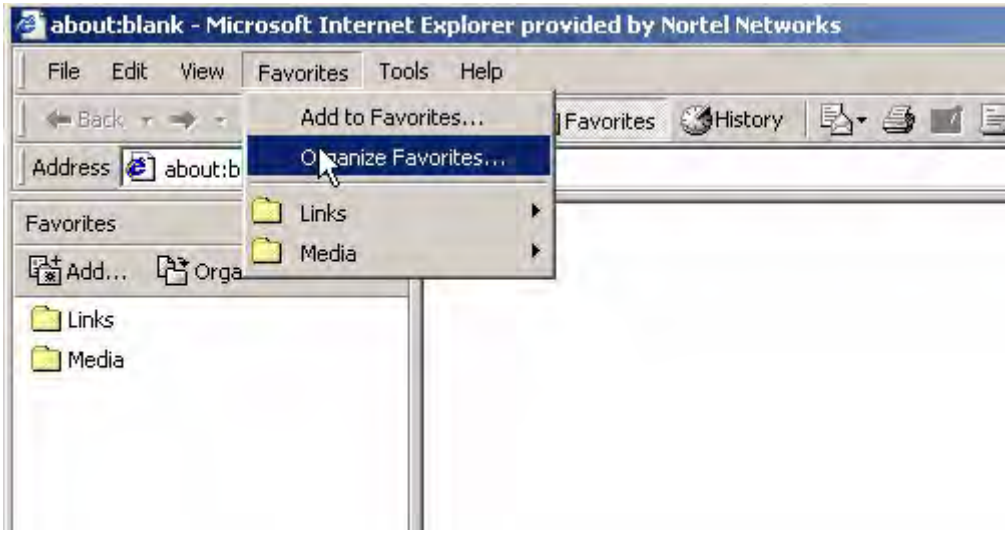
2 From the **View** menu, click **Explorer Bar** then **Favorites**.



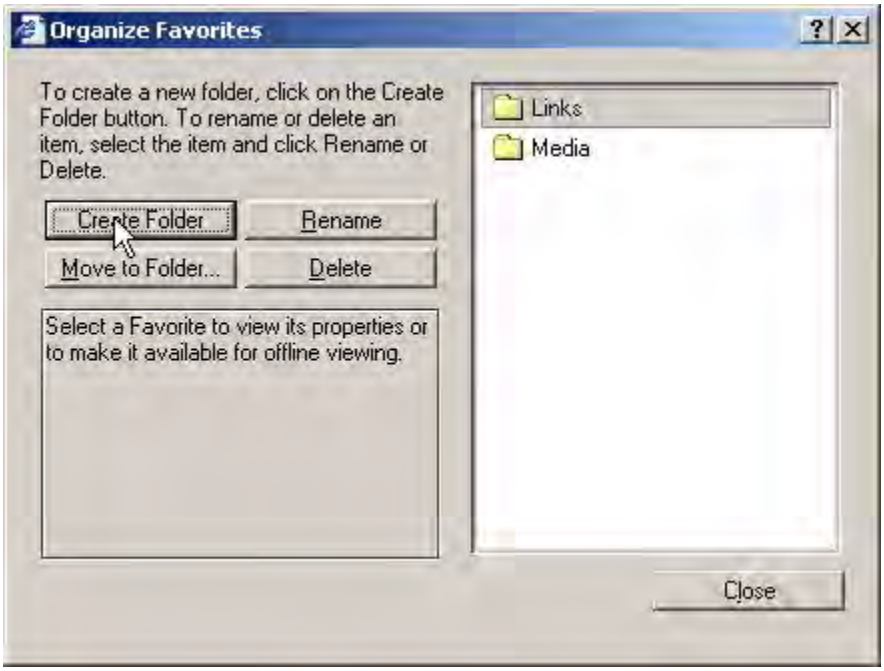
The favorites for the browser should appear in the left side of the browser window.



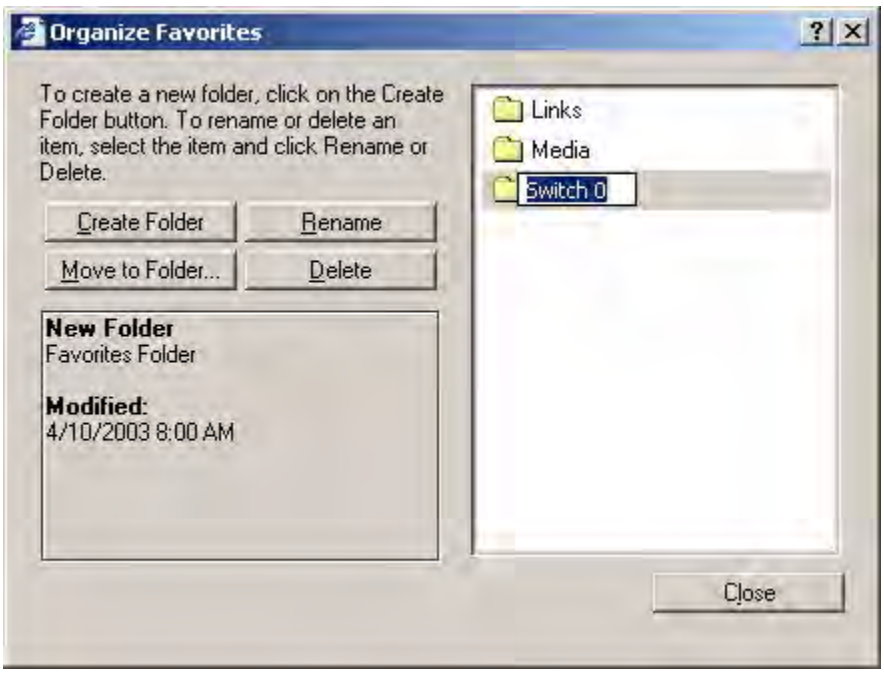
3 From the **Favorites** menu, click **Organize Favorites...**.



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 Tools and MG 9000 Manager client applications as follows:

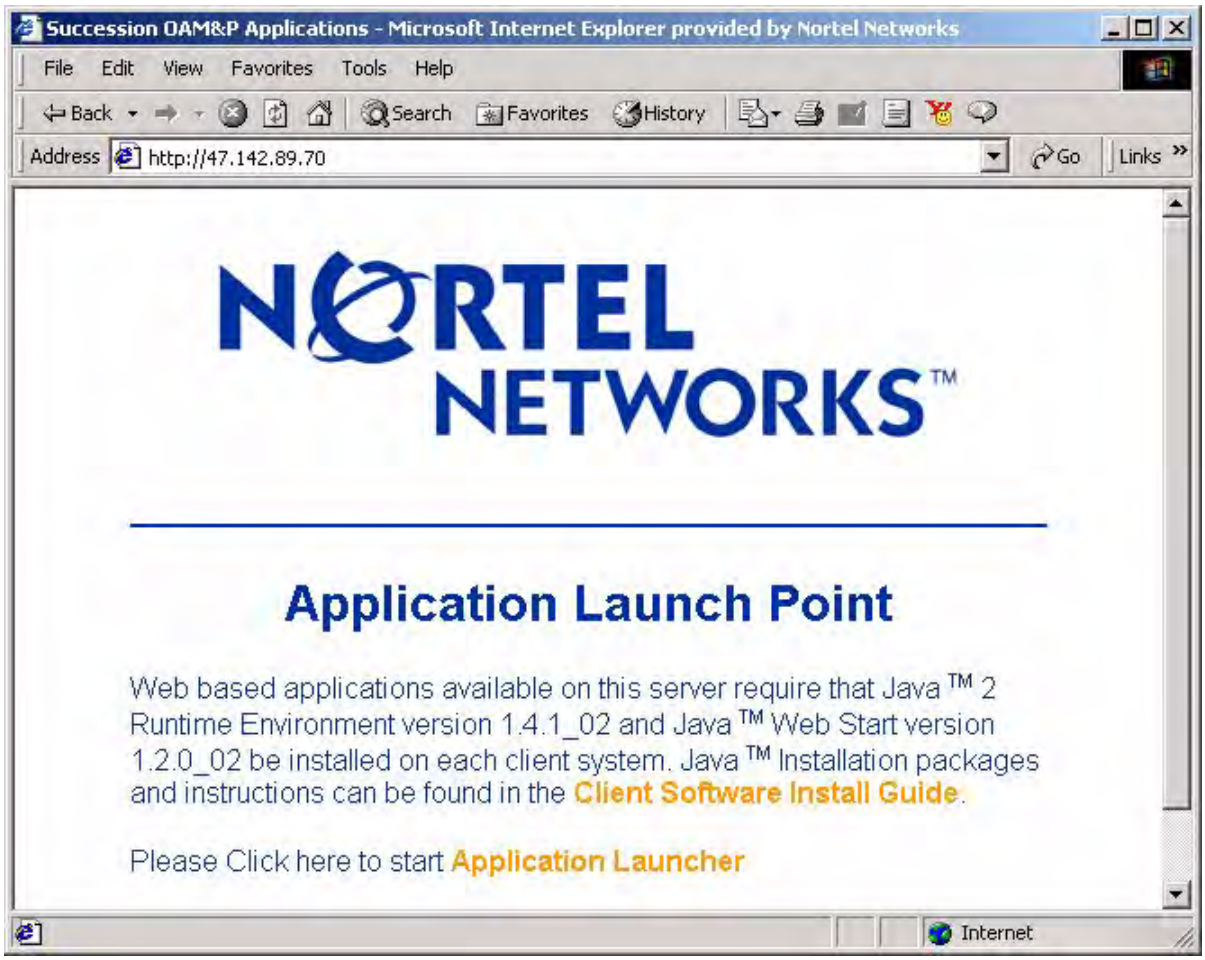
a Access the server where the CS 2000 Management Tools or the MG 9000 Manager software is installed by typing

http://<host>

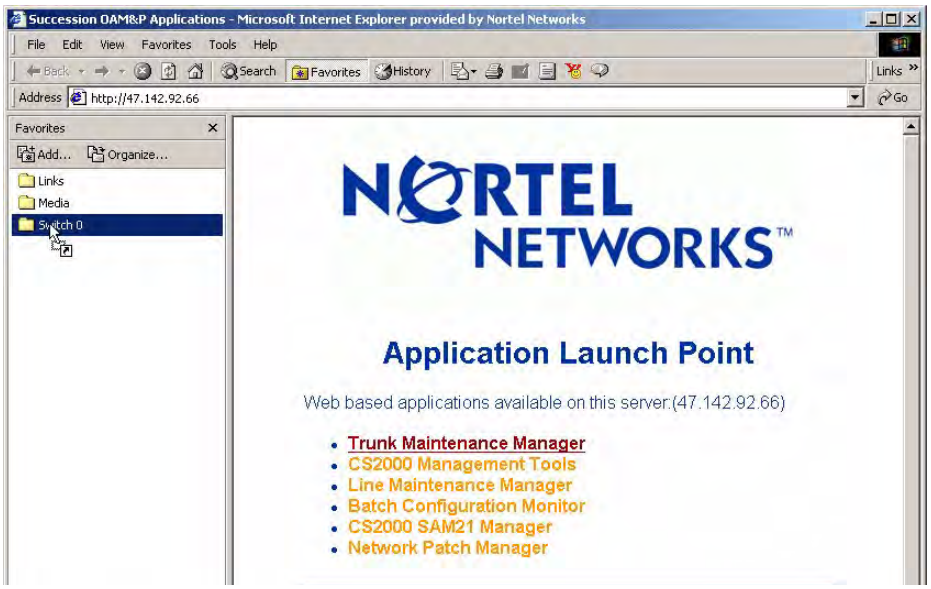
where

<host>
is the name or IP address of the server where the CS 2000 Management Tools or MG 9000 Manager software 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.



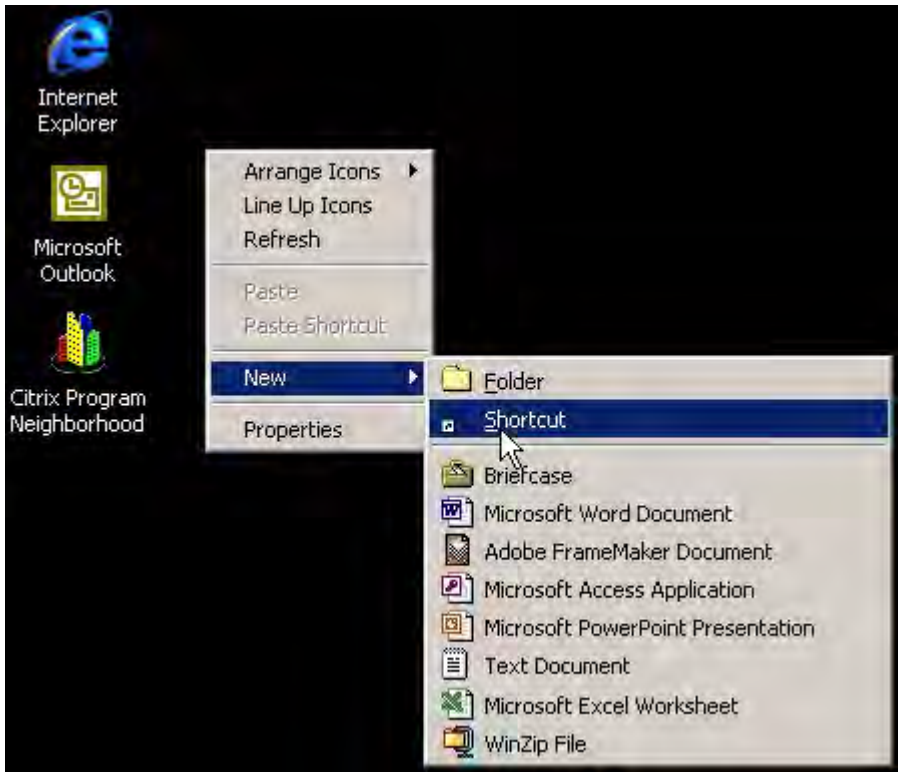
c In the Favorites pane on the browser, right click on the folder you created in step 4 and click **Expand**. The Application Launcher link should now appear under the folder name.

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 Mgr”.

7 Create a link to the core as follows:

a Right-click on your desktop, click **New**, then click **Shortcut**.



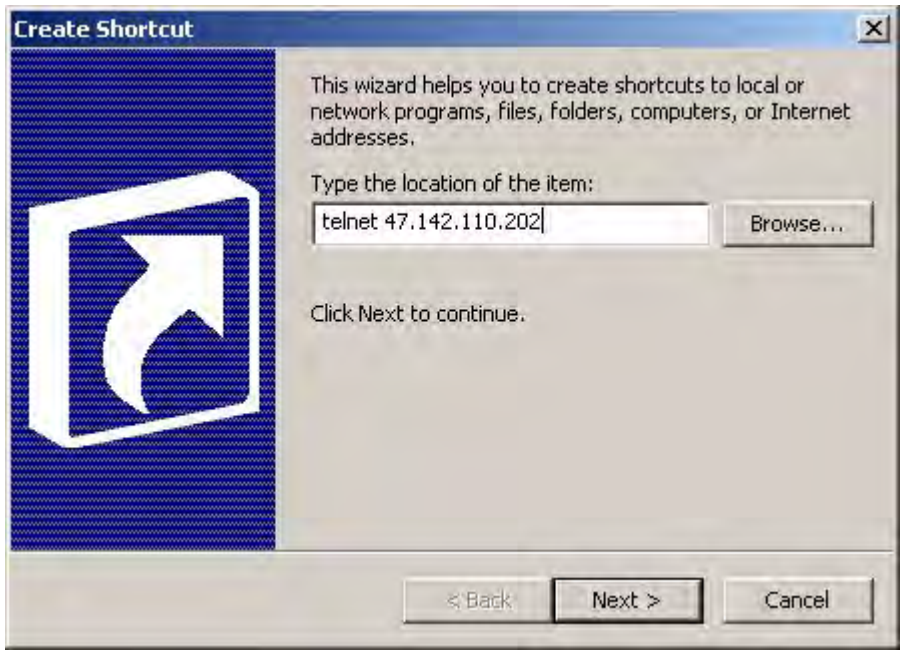
b When prompted for the location of the item, enter “telnet <core_ip>”, then click **Next**.

where

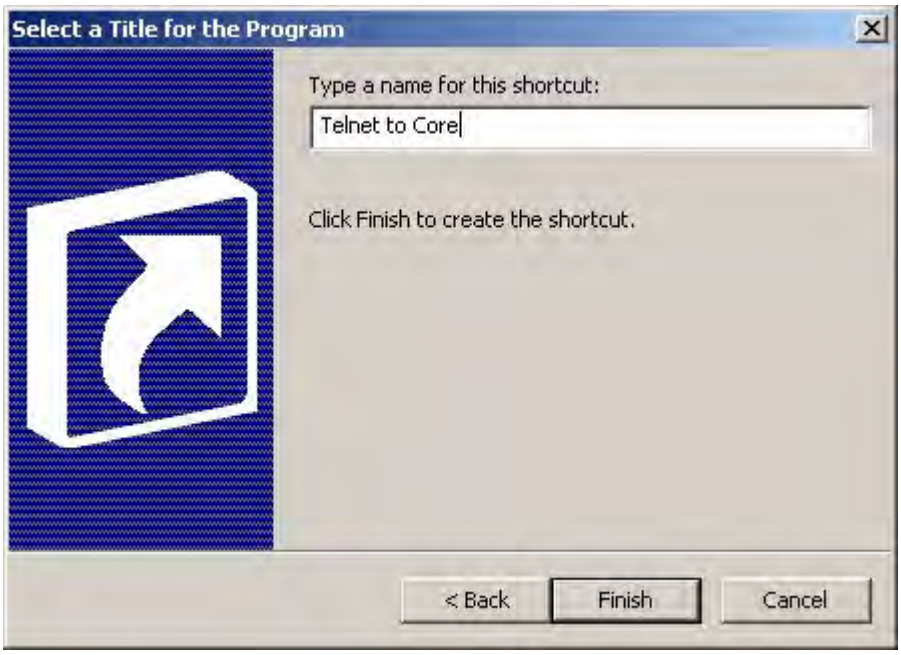
core_ip
is the Core IP address

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

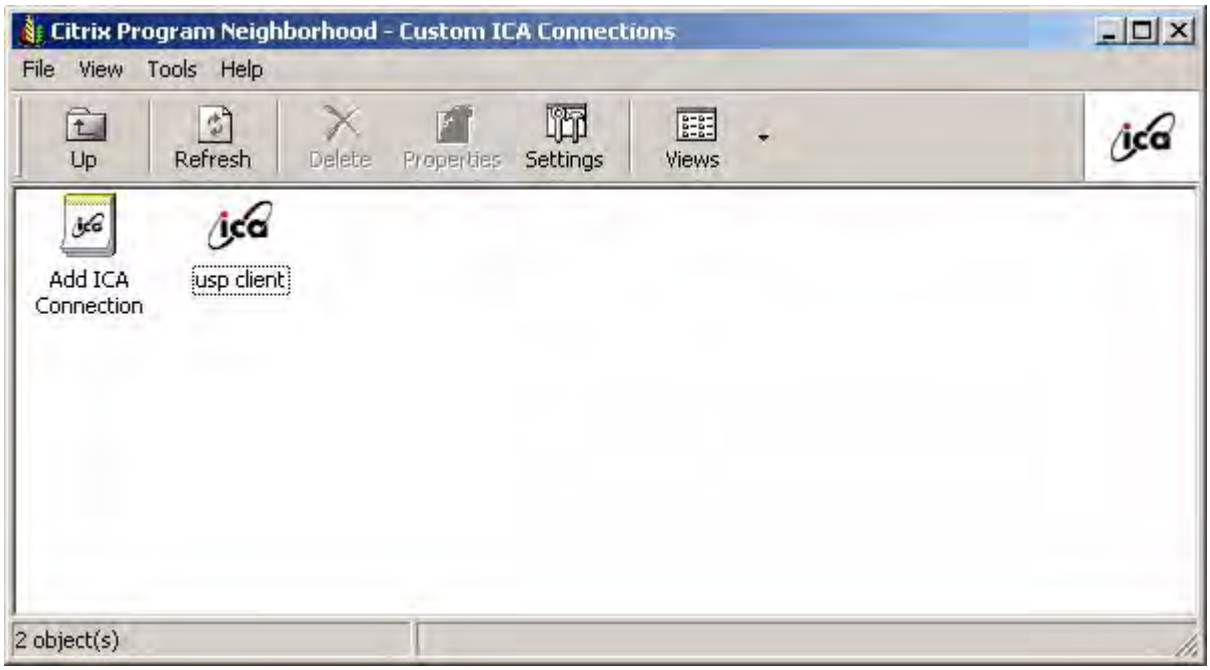
passport_address
is the IP address for the Passport server

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.

10 You have completed this procedure.

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 CS2000 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

At your workstation

1 Launch your web browser.

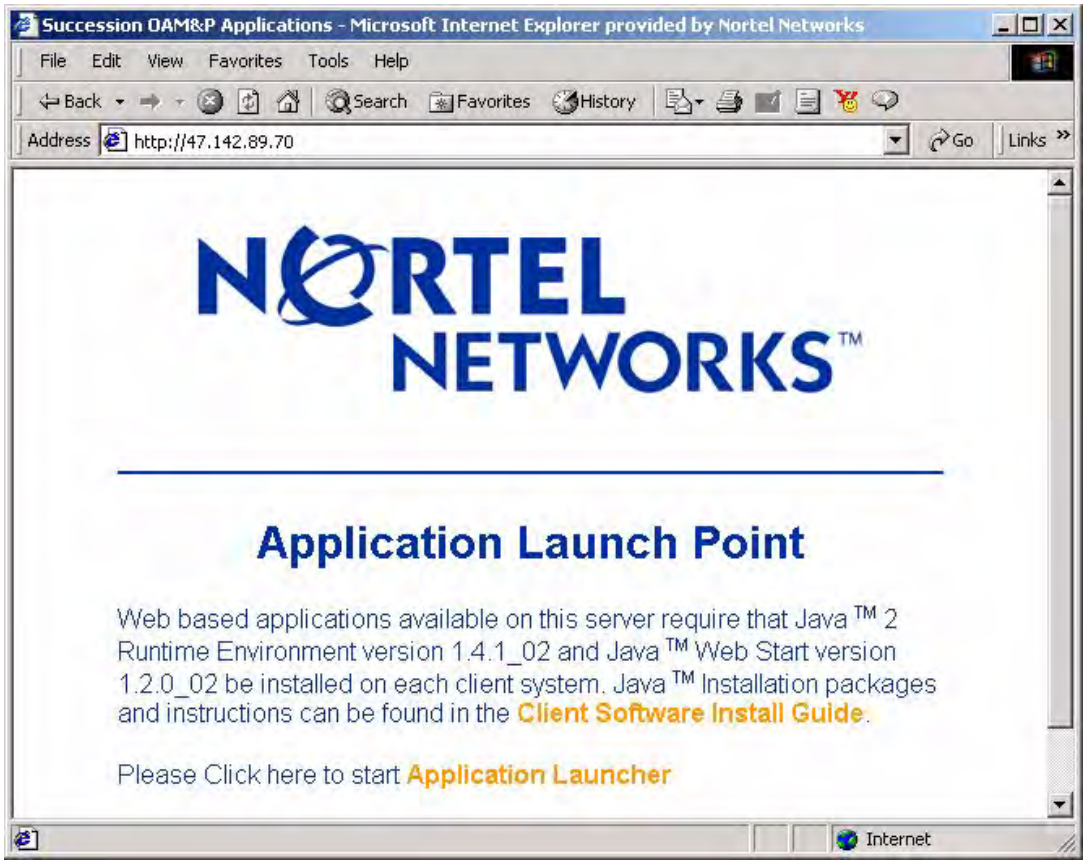
2 Access the server where the CS 2000 Management Tools reside by typing

>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.

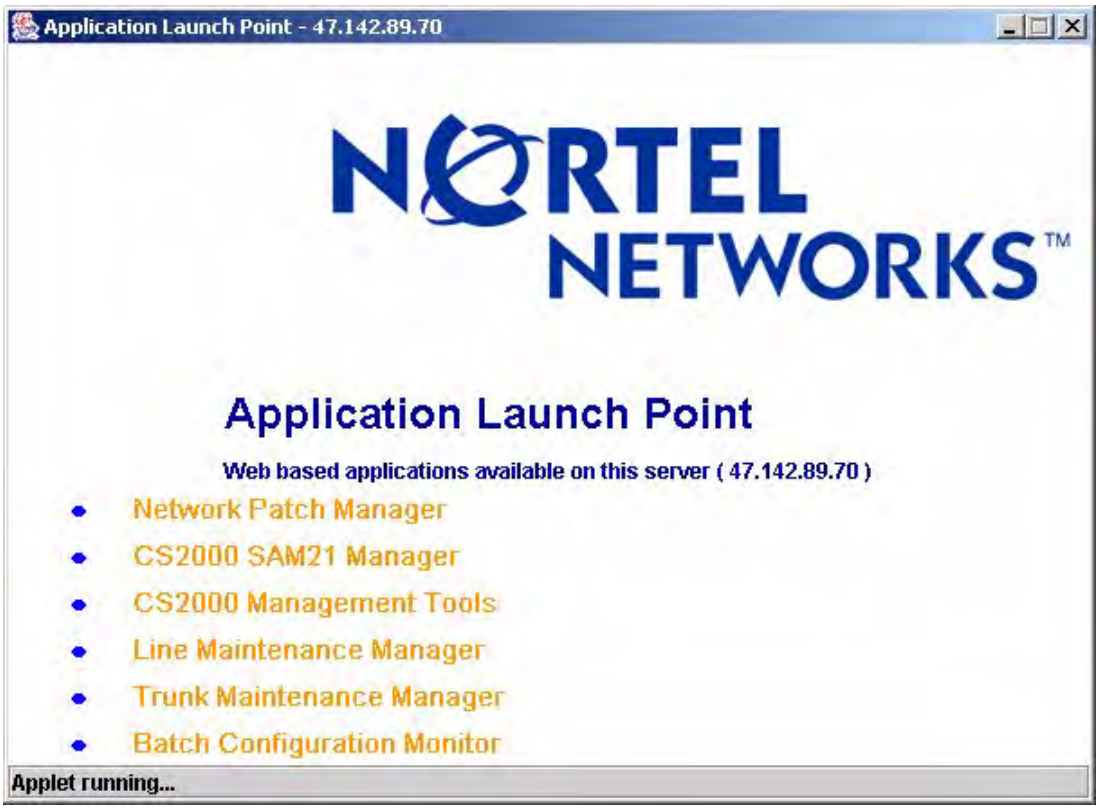


3 Click **Application Launcher**.

The Login window appears.

4 Enter your user name and password, then click **Log In**.

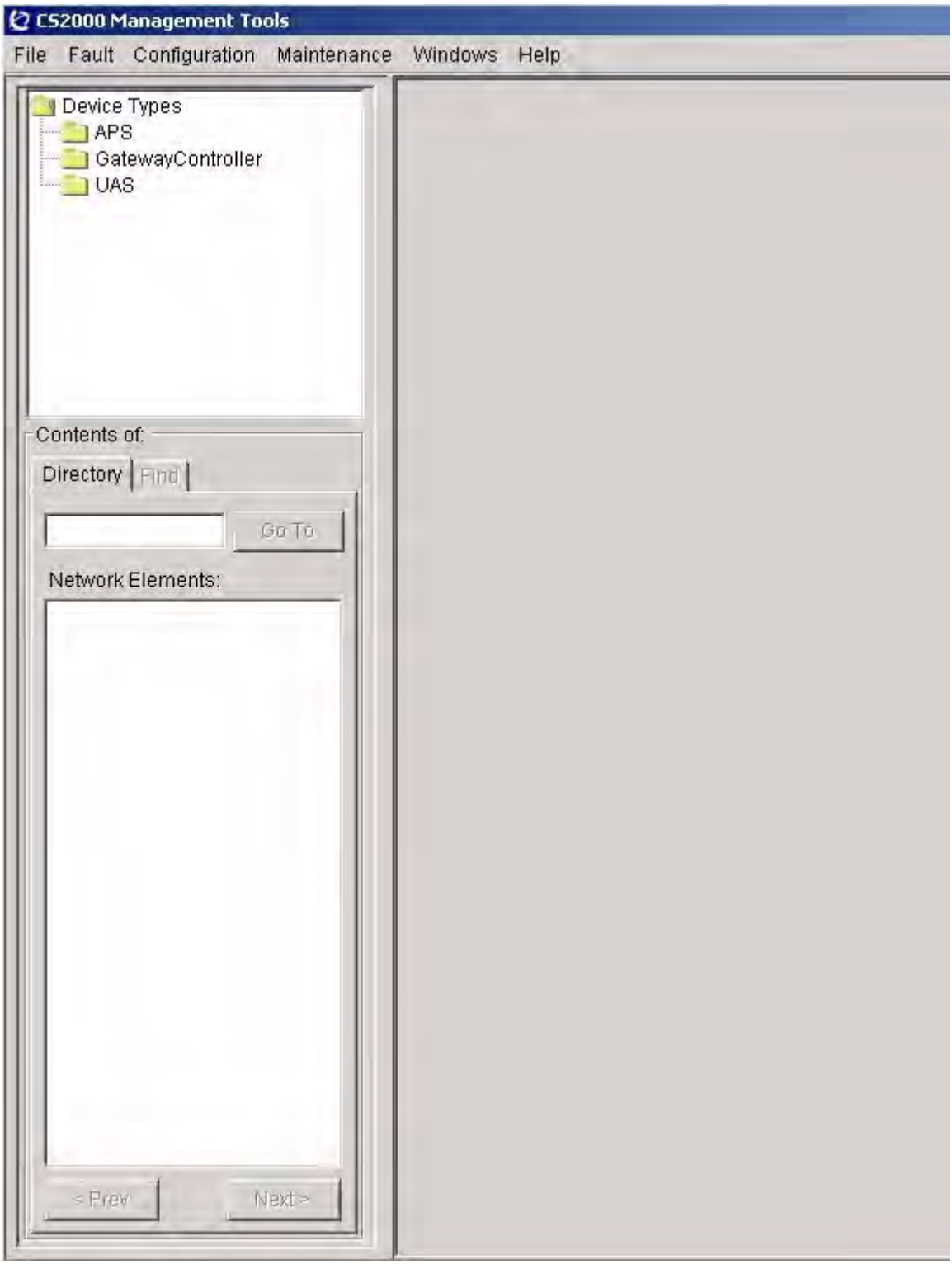
The Application Launch Point, similar to following, appears.



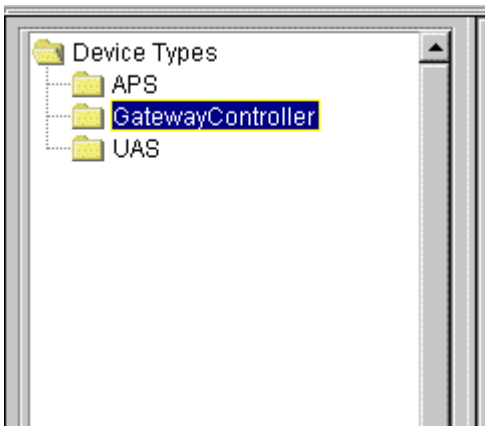
5 Click **CS2000 Management Tools**.

The CS2000 Management Tools GUI, similar to following, appears.

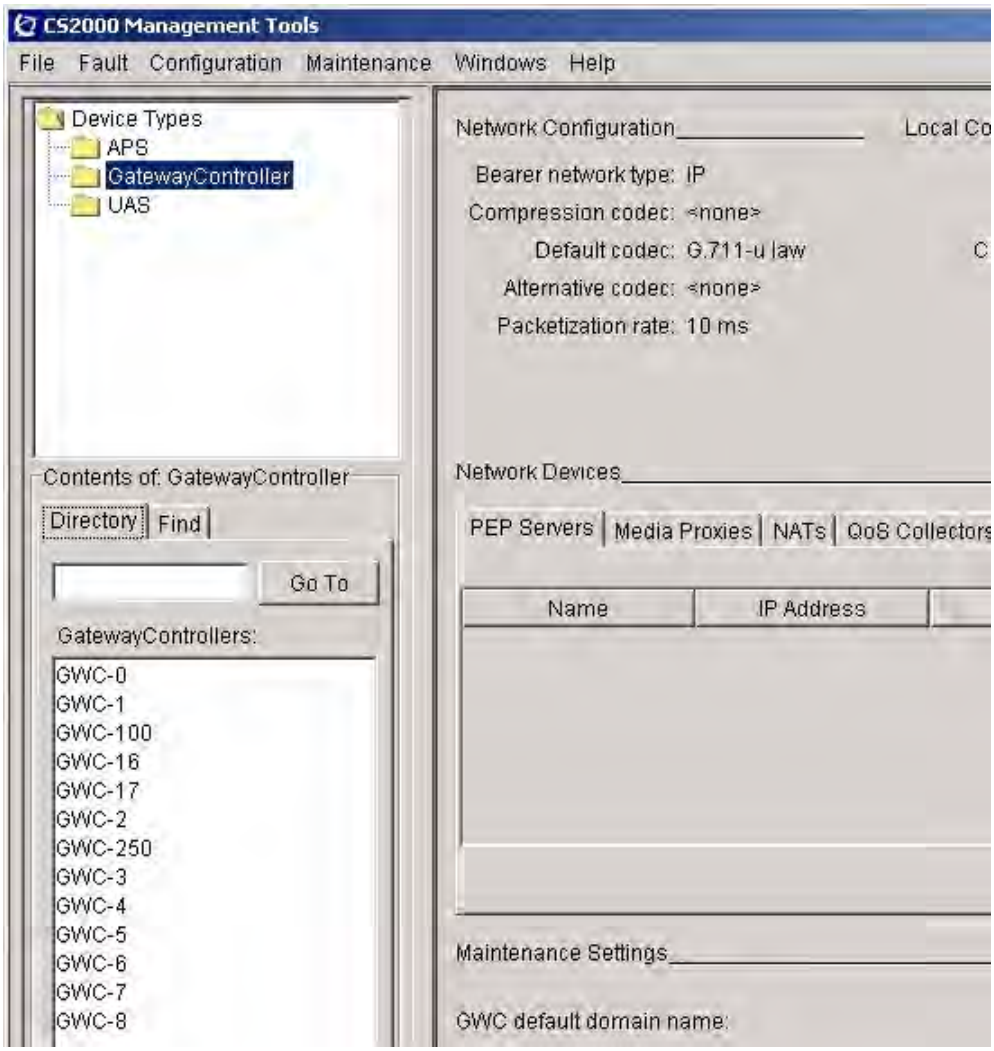
CS2000 Management Tools GUI



6 From the Device Types window, click **Gateway Controller**.



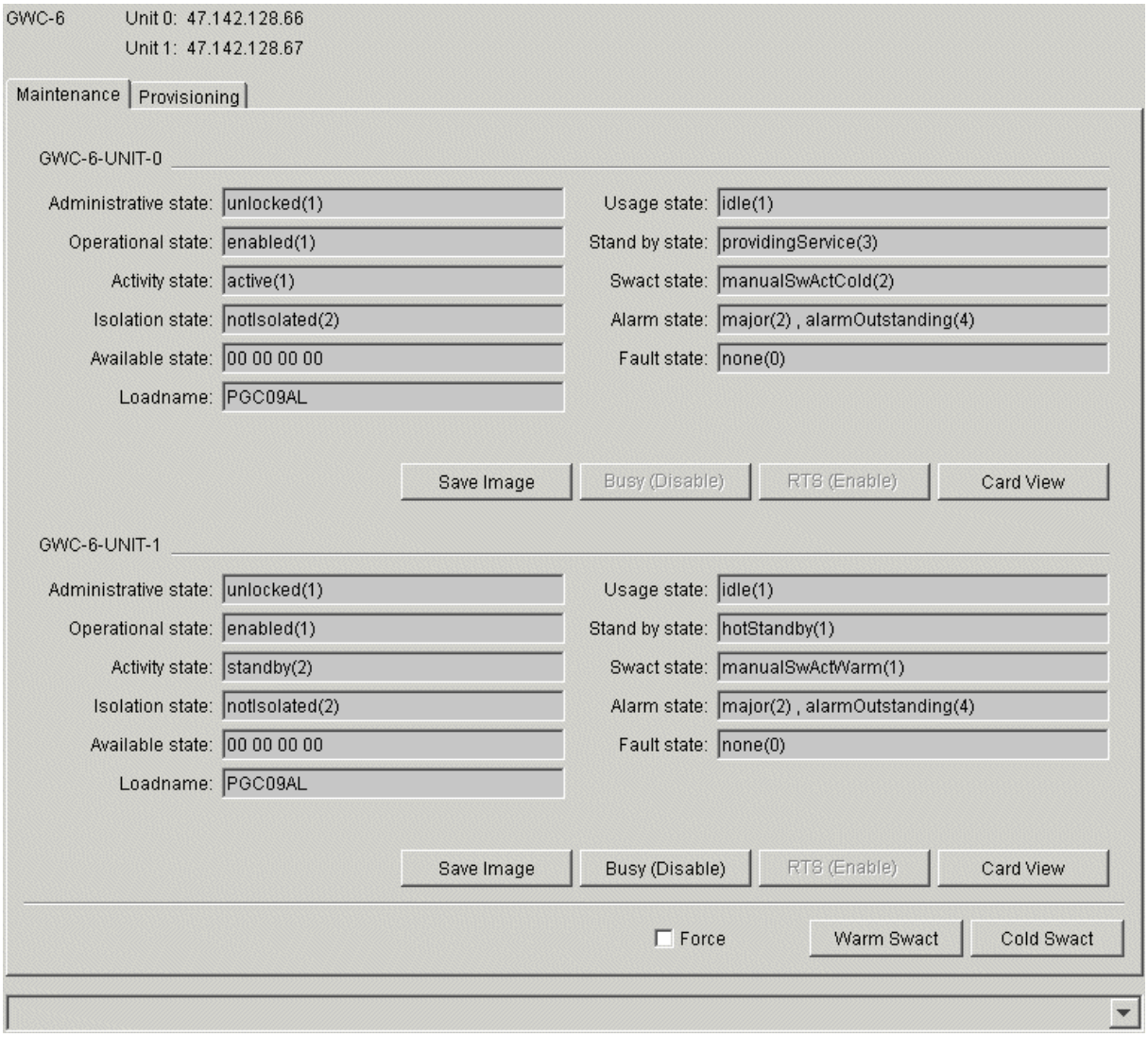
The Network View of the CS 2000 GWC Mgr appears in the main window. A list of GWC devices appear in the Contents window.



7 Access the Node View of the CS 2000 GWC Mgr by clicking on one of the GWC devices.

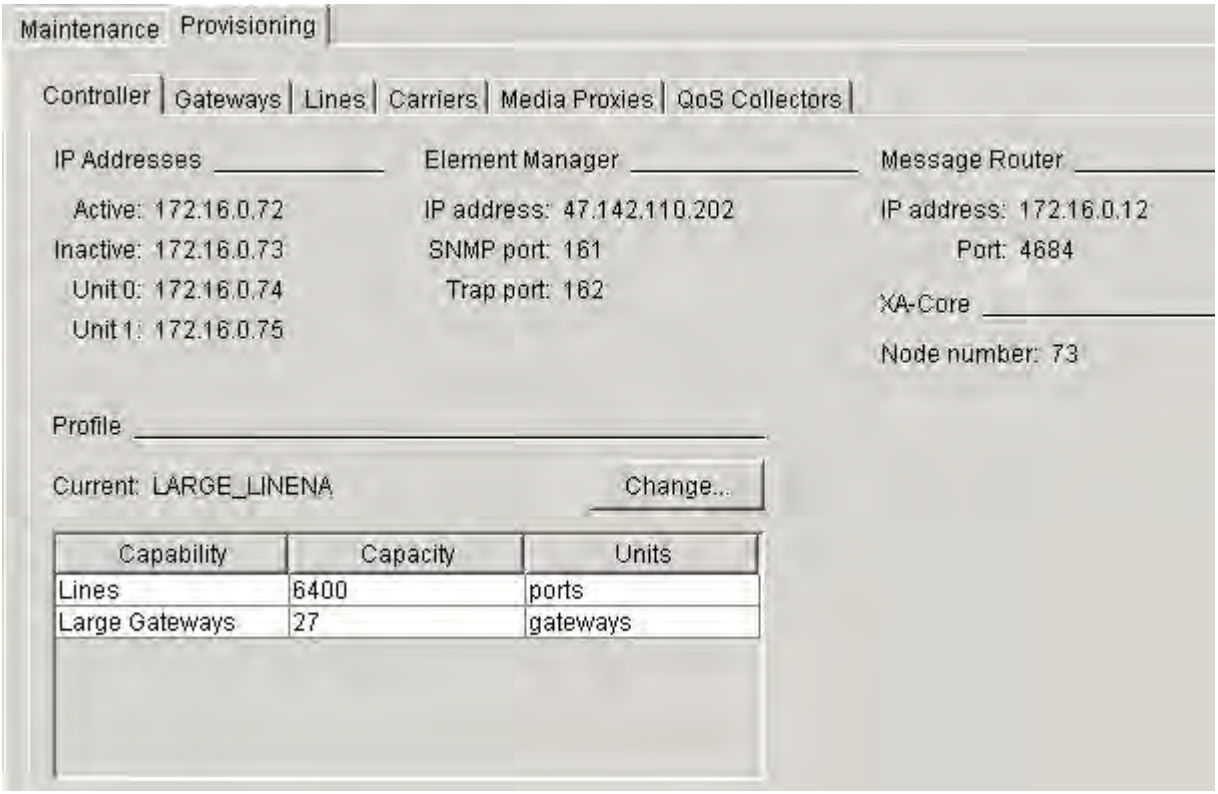
The Node View of the CS 2000 GWC Mgr will appear in the main window.

CS 2000 GWC Mgr



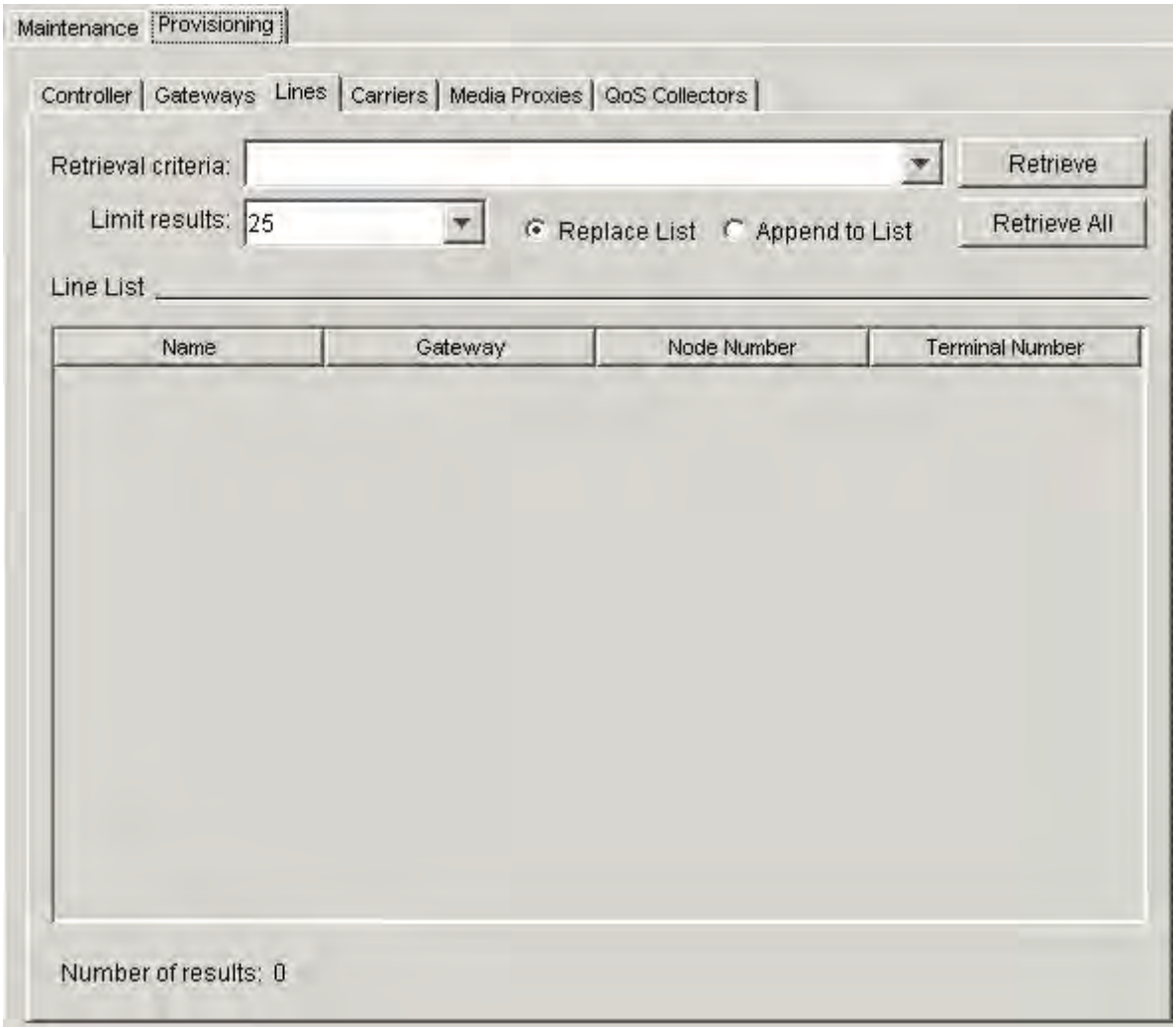
8 Click on the Provisioning tab to bring up the Provisioning view.

Provisioning tab



9 Click on the Lines tab to bring up the Lines view

Lines tab



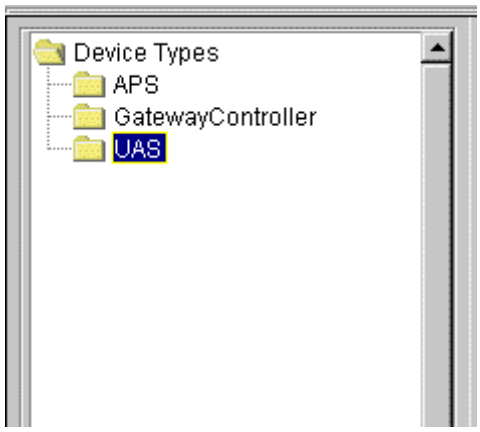
10 To validate the CS 2000 GWC Manager, click on the Retrieve All button to verify that the manager communicates with the GWC.

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

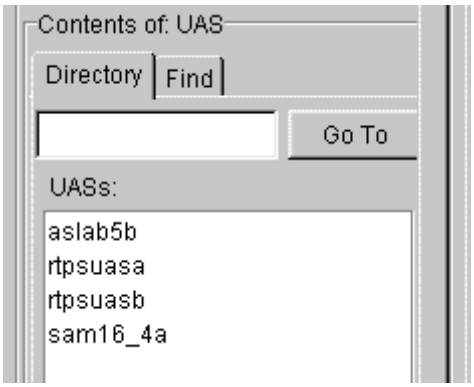
11 From the Device Types window, click **UAS**.

Selecting UAS



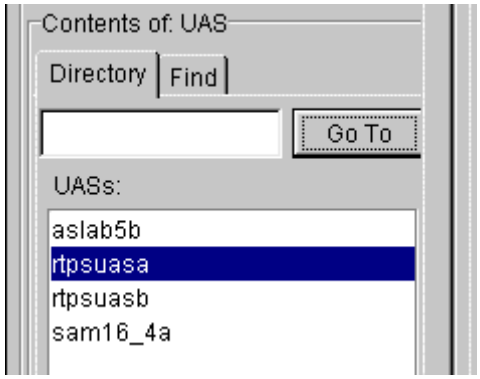
A list of UAS devices will appear in the Contents window.

UAS devices



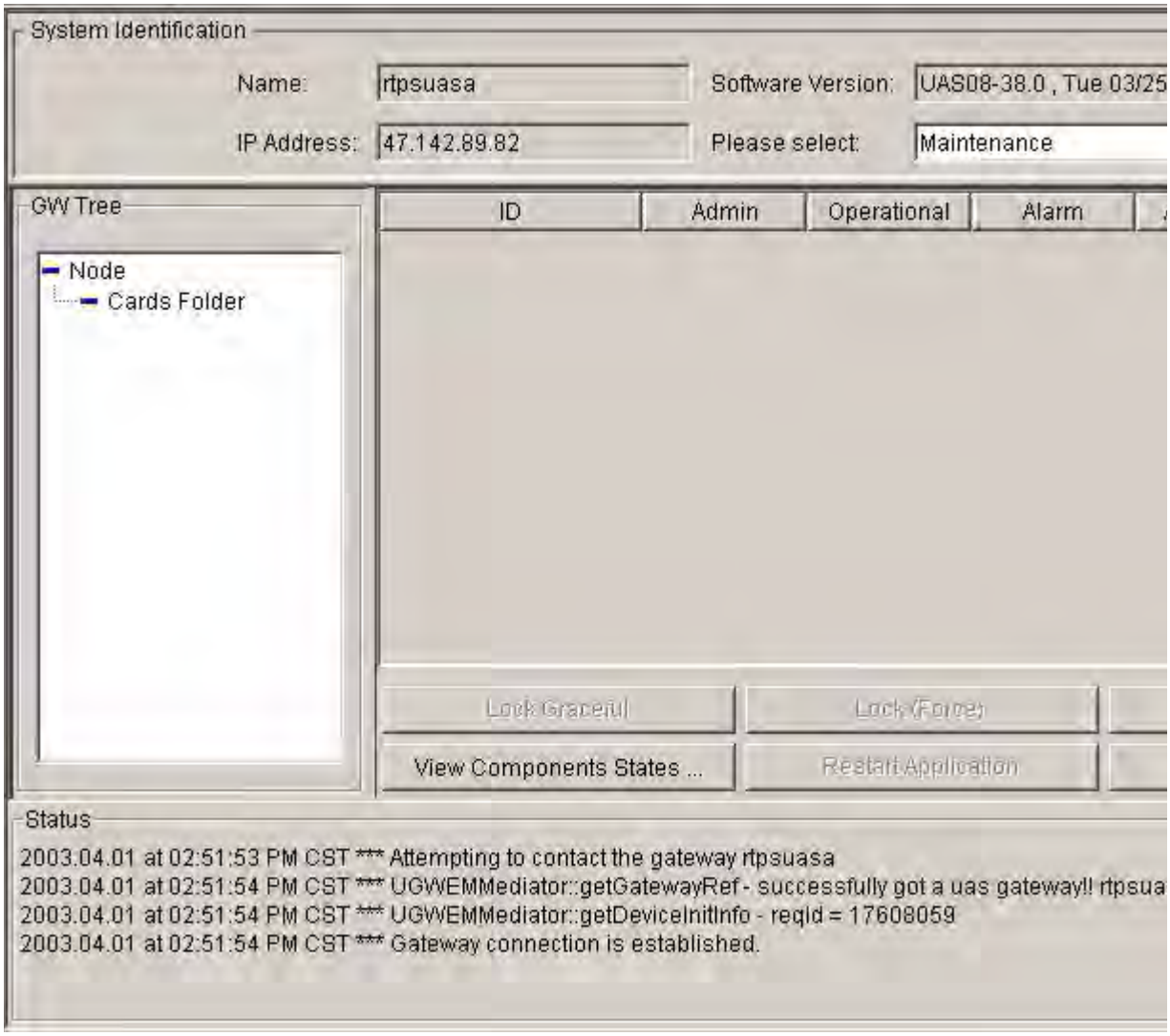
12 Access the UAS Mgr by clicking on one of the UAS devices.

Accessing the UAS Mgr



The UAS Mgr will appear in the main window.

UAS Mgr



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.

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 CS2000 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

At your workstation

1 Launch your web browser.

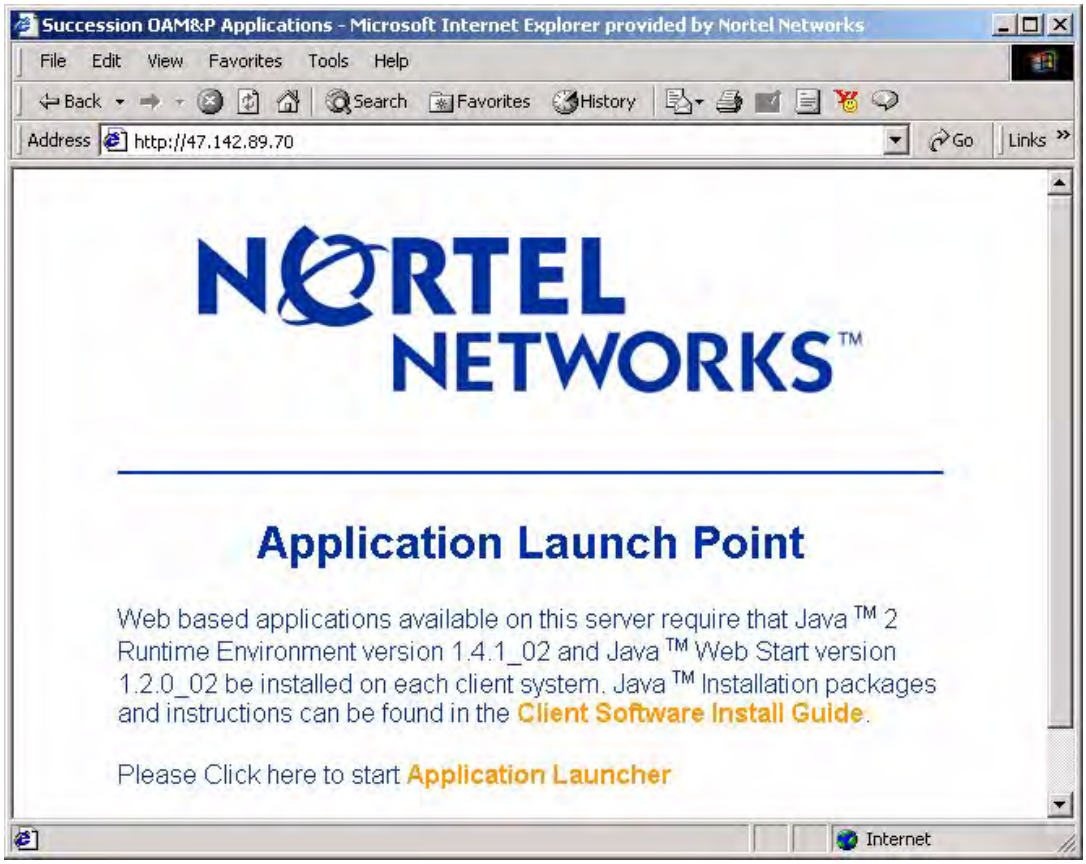
2 Access the server where the CS 2000 SAM21 Manager resides by typing

>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.

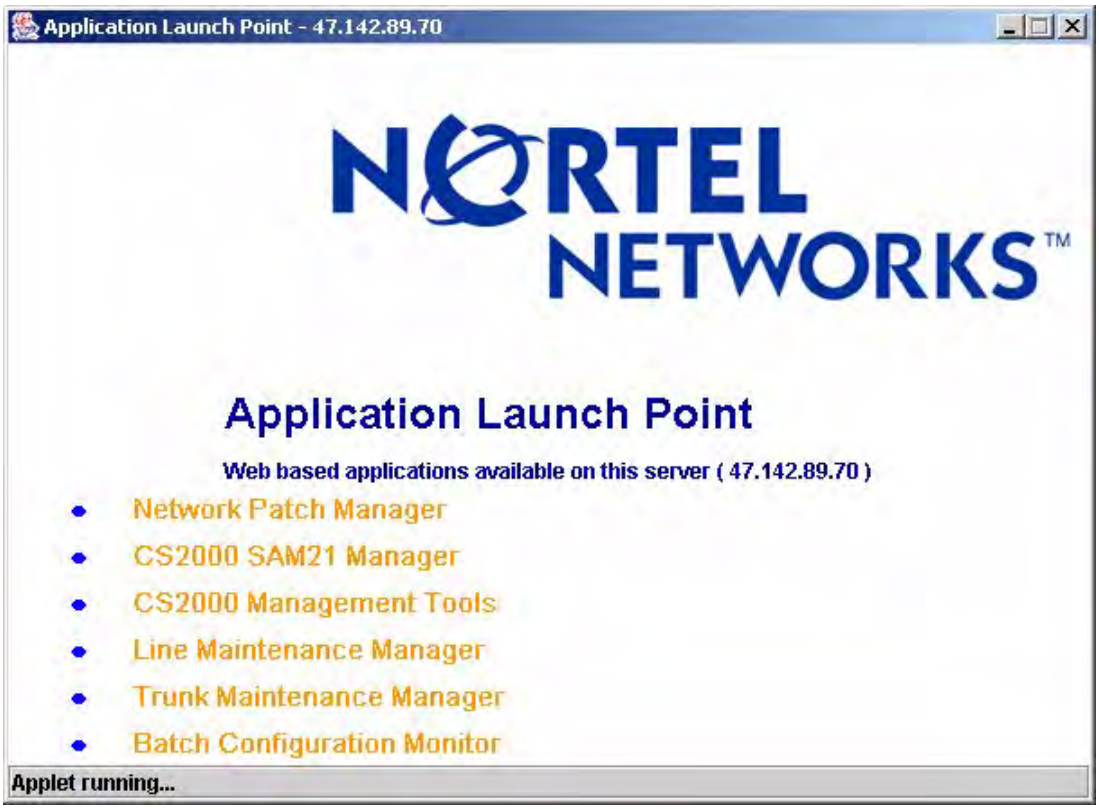


3 Click **Application Launcher**.

The Login window appears.

4 Enter your user name and password, then click **Log In**.

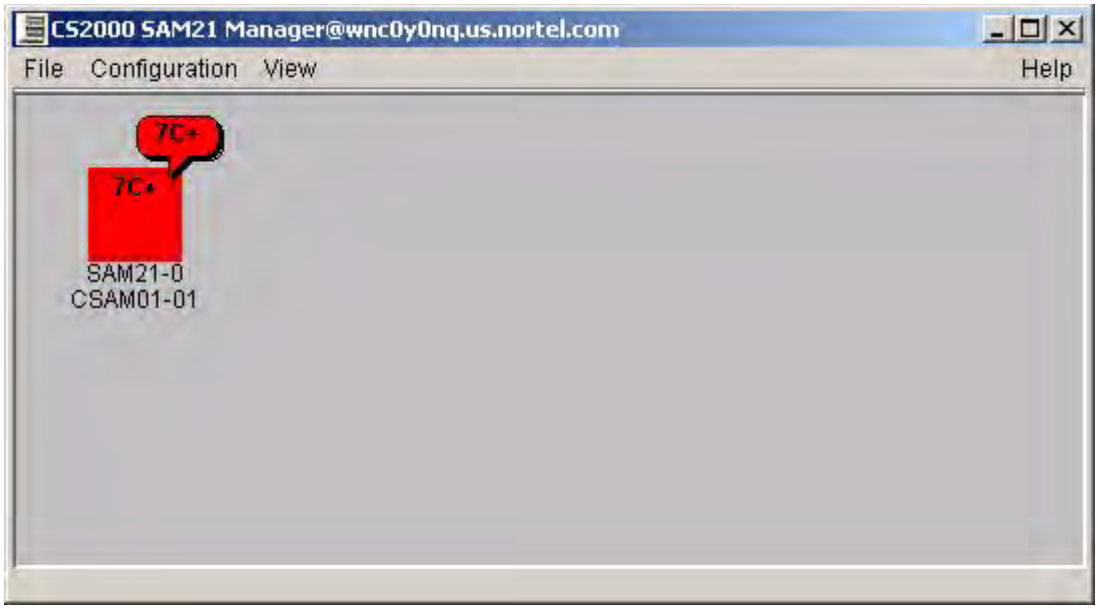
The Application Launch Point, similar to following, appears.



5 Click **CS2000 SAM21 Manager**.

The Subnet View, similar to the following, appears.

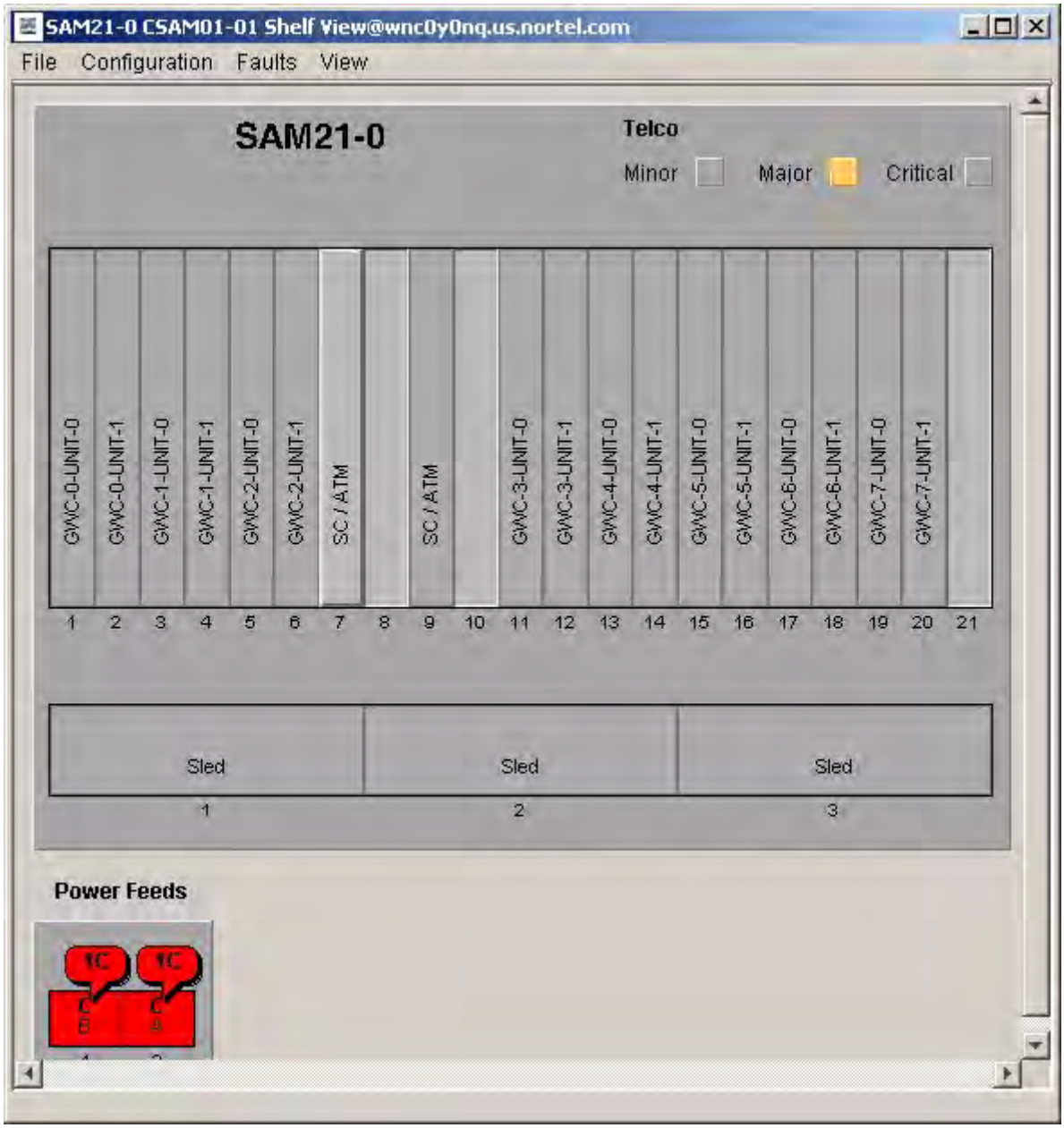
Subnet View



If 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.

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.

Note: 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

At your workstation

1 Launch your web browser.

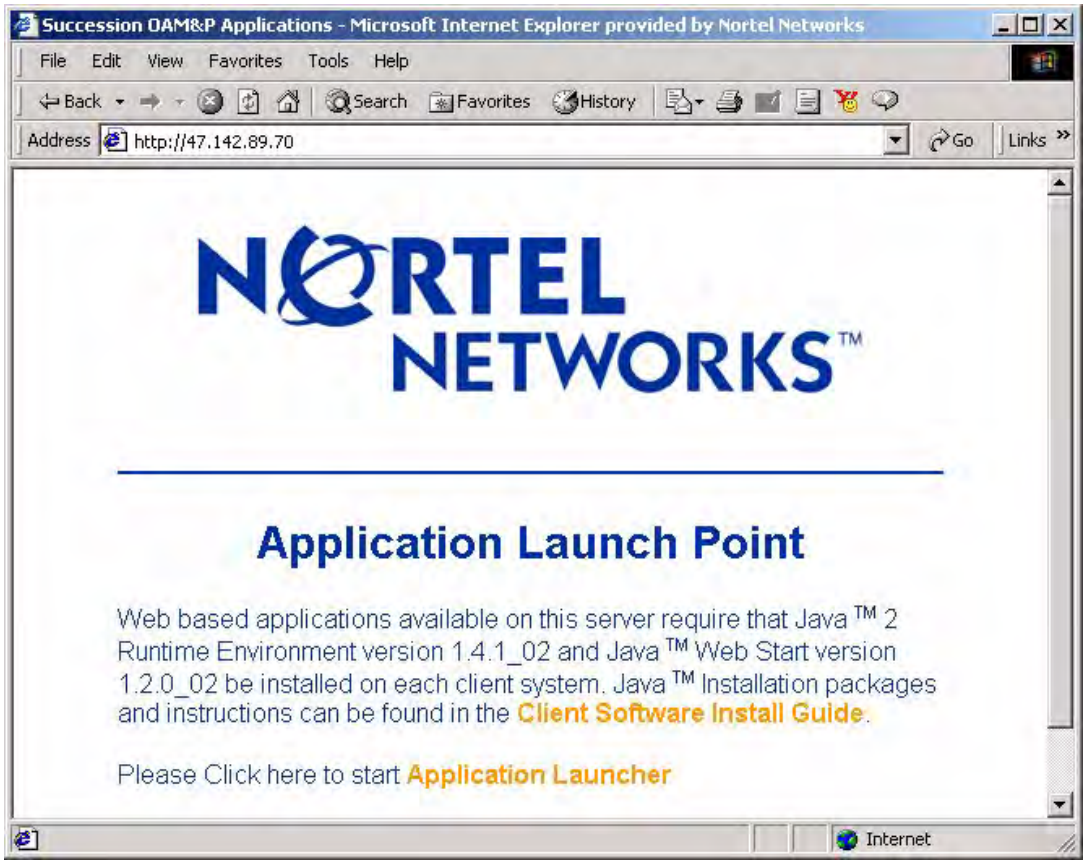
2 Access the server where the NPM software resides by typing

>http://<host>

where

<host>
is the name or IP address of the server where the NPM software resides

The “Application Launch Point” page appears.

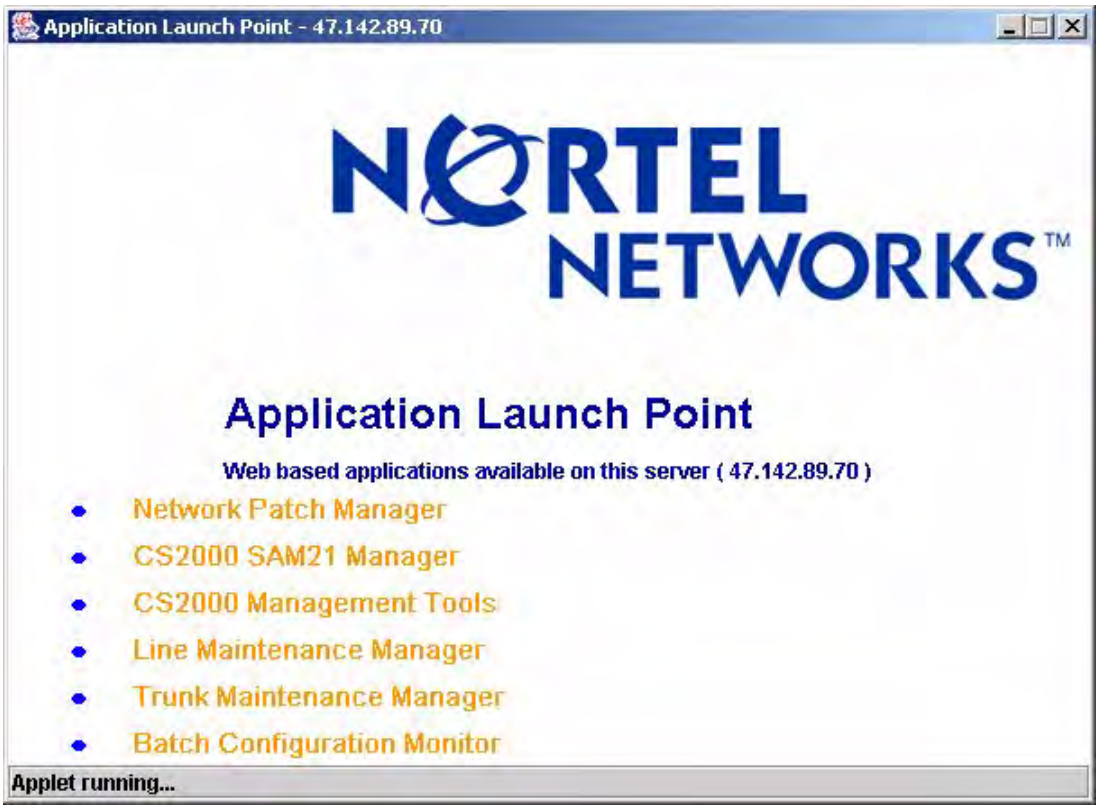


3 Click **Application Launcher**.

The Login window appears.

4 Enter your user name and password, then click **Log In**.

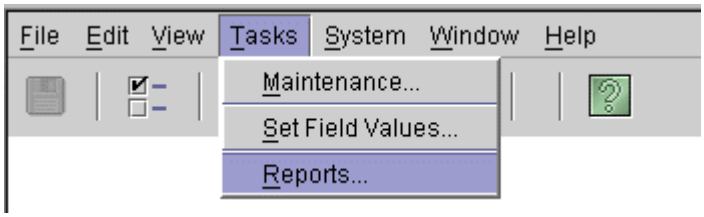
The Application Launch Point, similar to following, appears.



5 Click **Network Patch Manager**.

The NPM GUI appears.

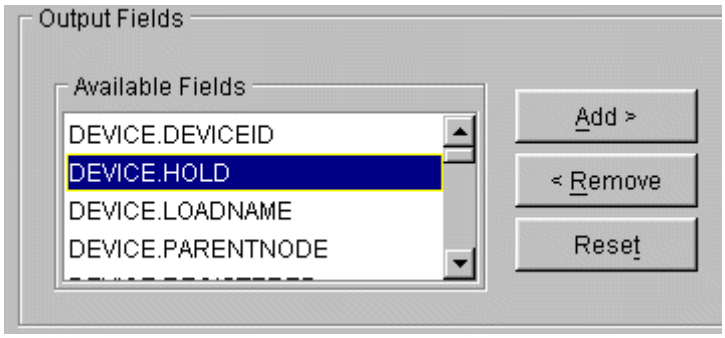
6 On the **Tasks** menu, click **Reports...**.



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.

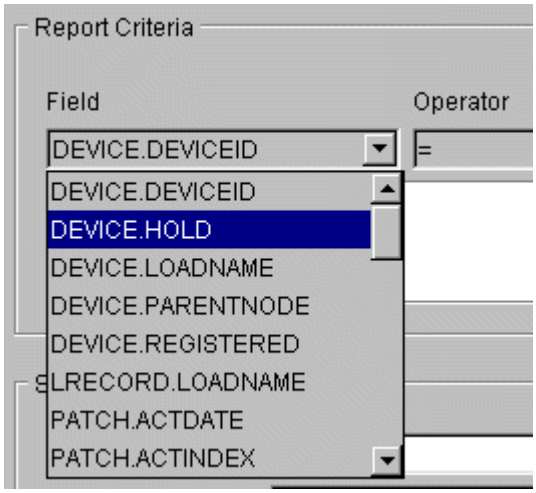
8 Enter the search criteria for the report.

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

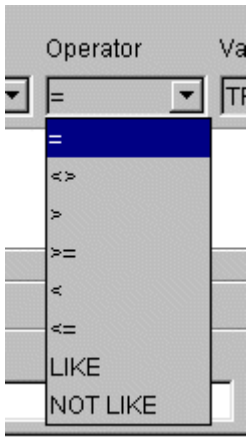


b Select the operator from the Operator Combo box. The table below lists the supported operators and their meaning.

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 (%)

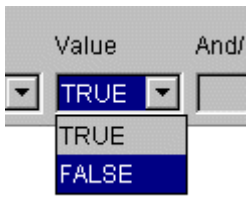
Selecting the operator



c In the Value Combo Box, select the value or enter the value manually.

Note: 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



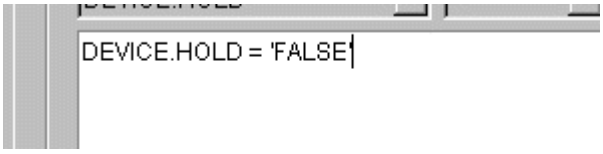
d To combine multiple criteria statements, select the AND or the OR options from the And/Or combo box.

e Go to step 11.

10 Enter the search criteria in the text area below the combo boxes.

Note: Parenthesis “()” may be inserted to define precedence for multiple criteria statements.

Entering search criteria manually

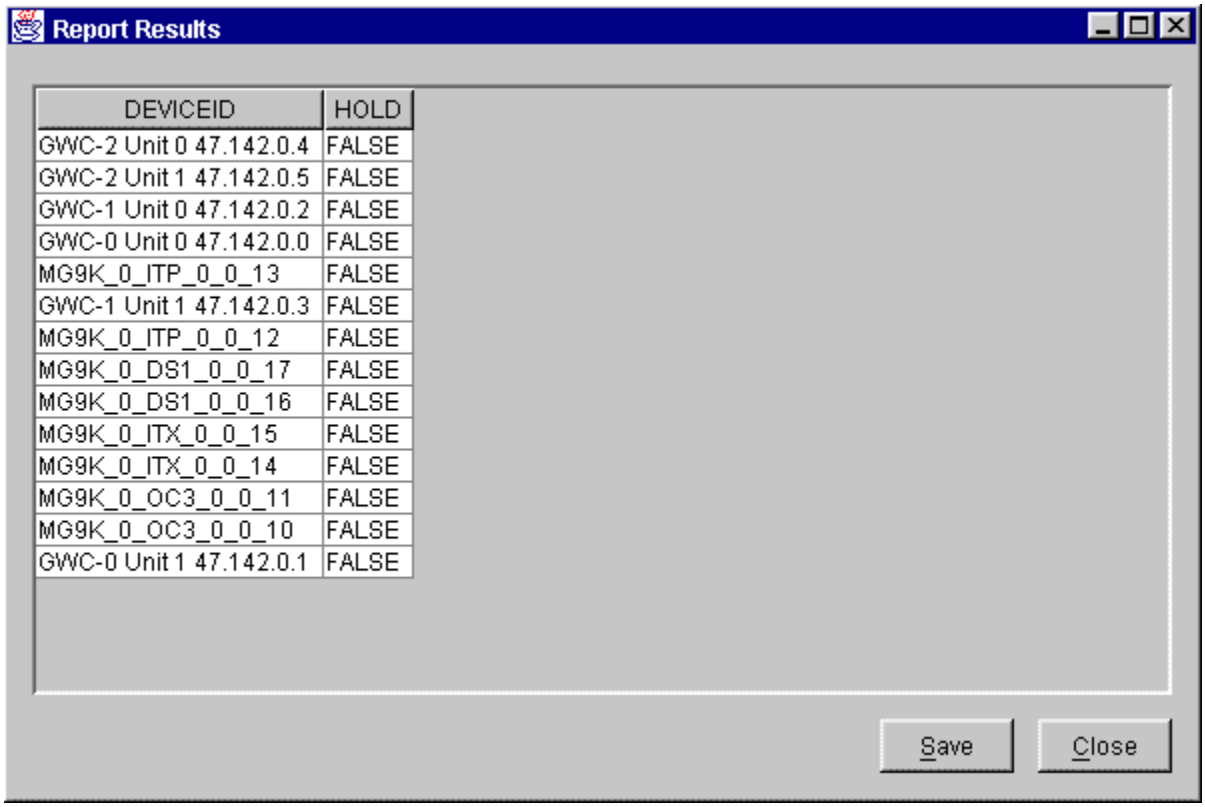


11 Execute the report by pressing the Execute button.

12 After the report data has been received, the Report Results window will be displayed.

Note: 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.

Validating an installation of the MG 9000 Manager

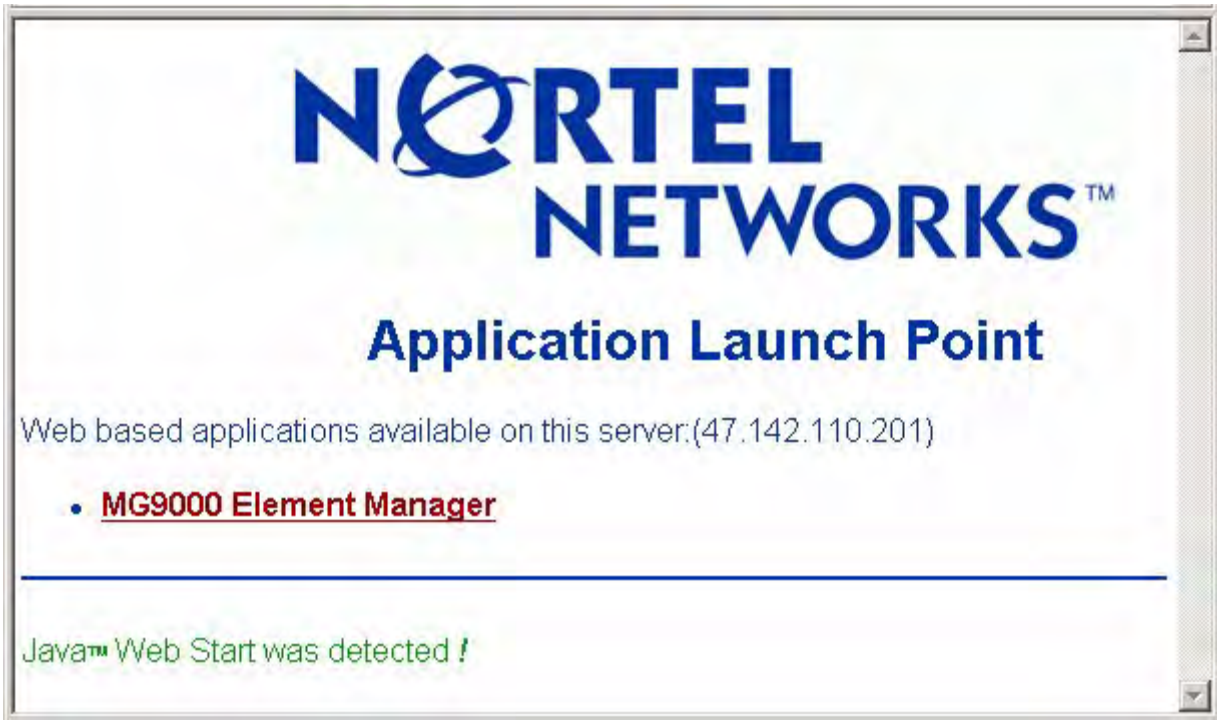
Validating the MG 9000 Manager installation involves logging into the MG 9000 Manager, verifying the shelves appear, and verifying any alarms on the shelves also appear in the Alarm Manager.

Validating the MG 9000 Manager installation

At a web browser

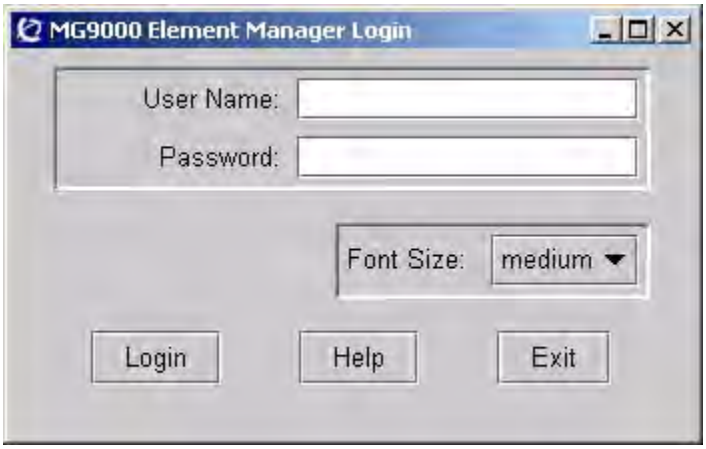
1 Access the Application Launch Point on the server on which you installed the MG 9000 Manager.

MG 9000 Application Launch Point



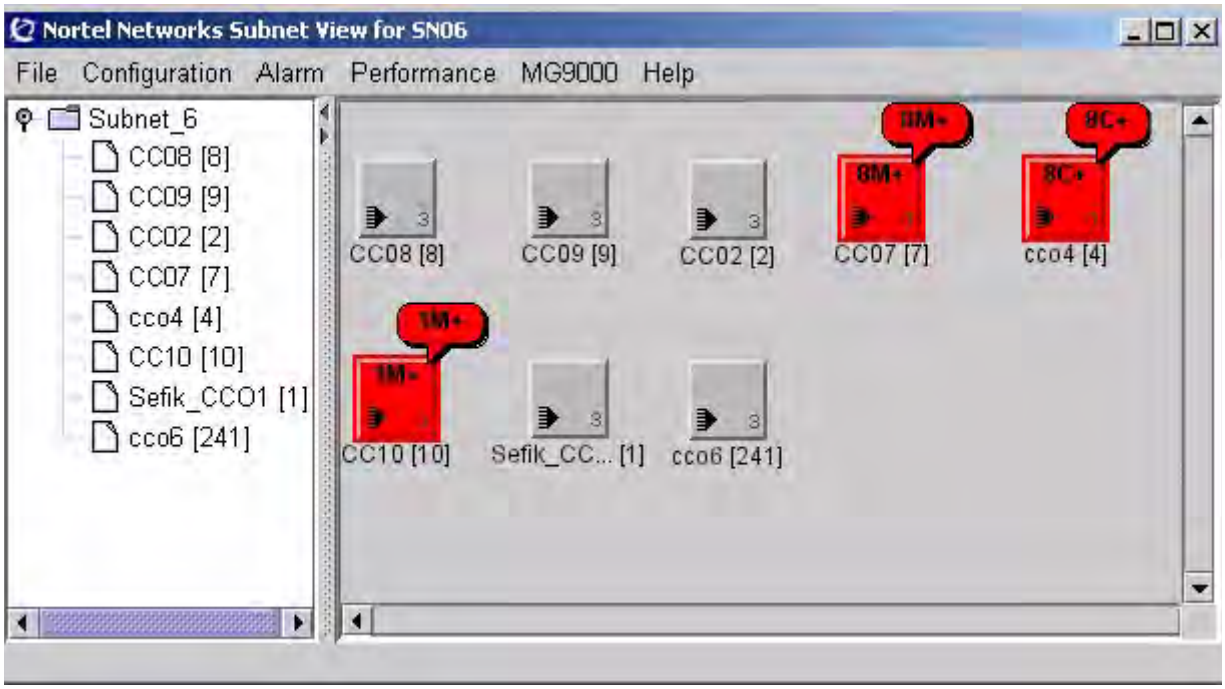
2 Click on the link for the MG 9000 Element Manager. Once the application loads, you will be asked to for a User Name and Password to access the manager.

Login screen



3 Verify that the Subnet View appears.

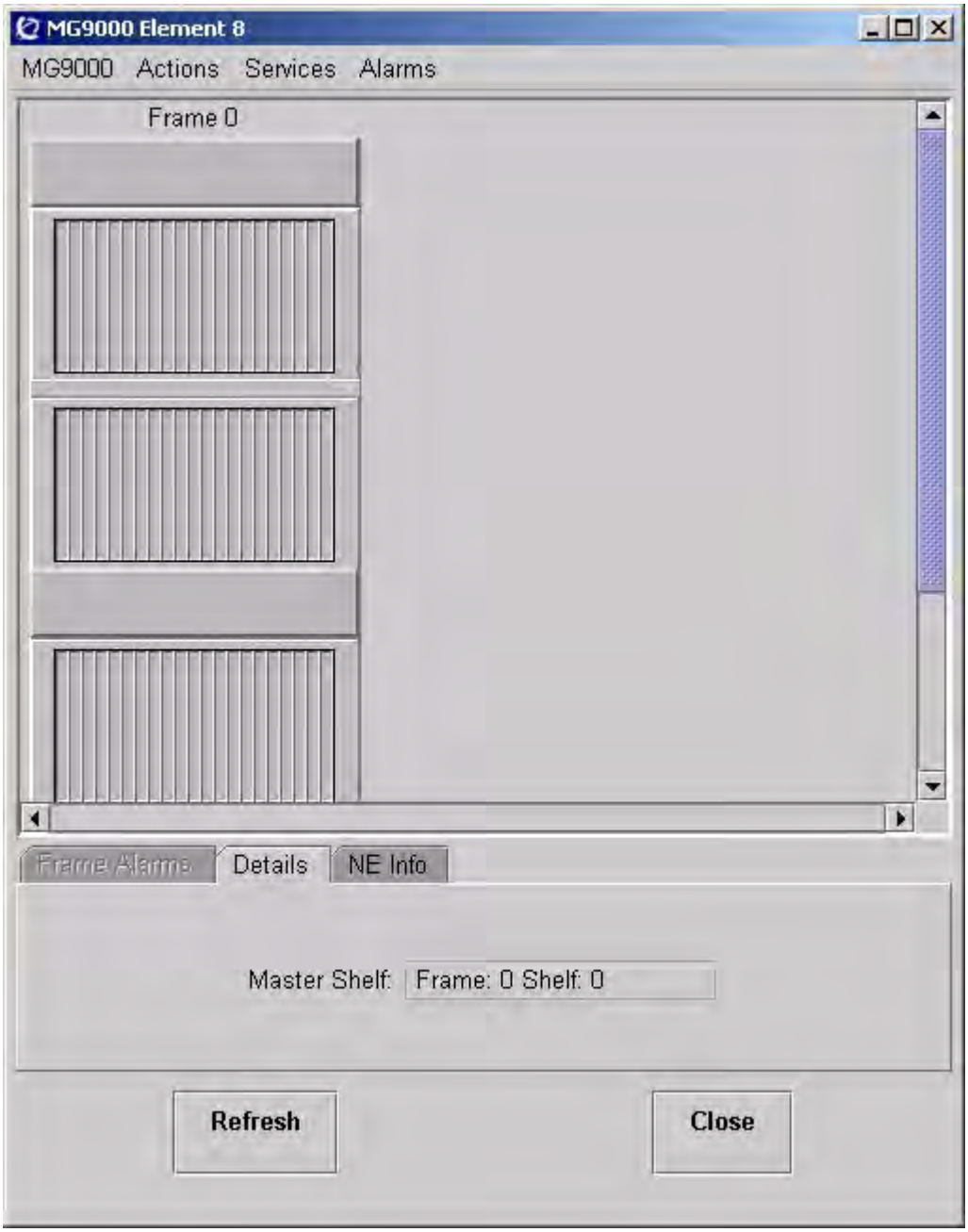
Subnet View for (I)SN06



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

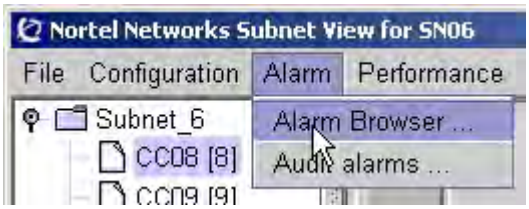
5 Close the Element view and return to the Subnet View.

6

If there are	Do
no alarms present on the subnet view	step 10
alarms present on the subnet view	step 7

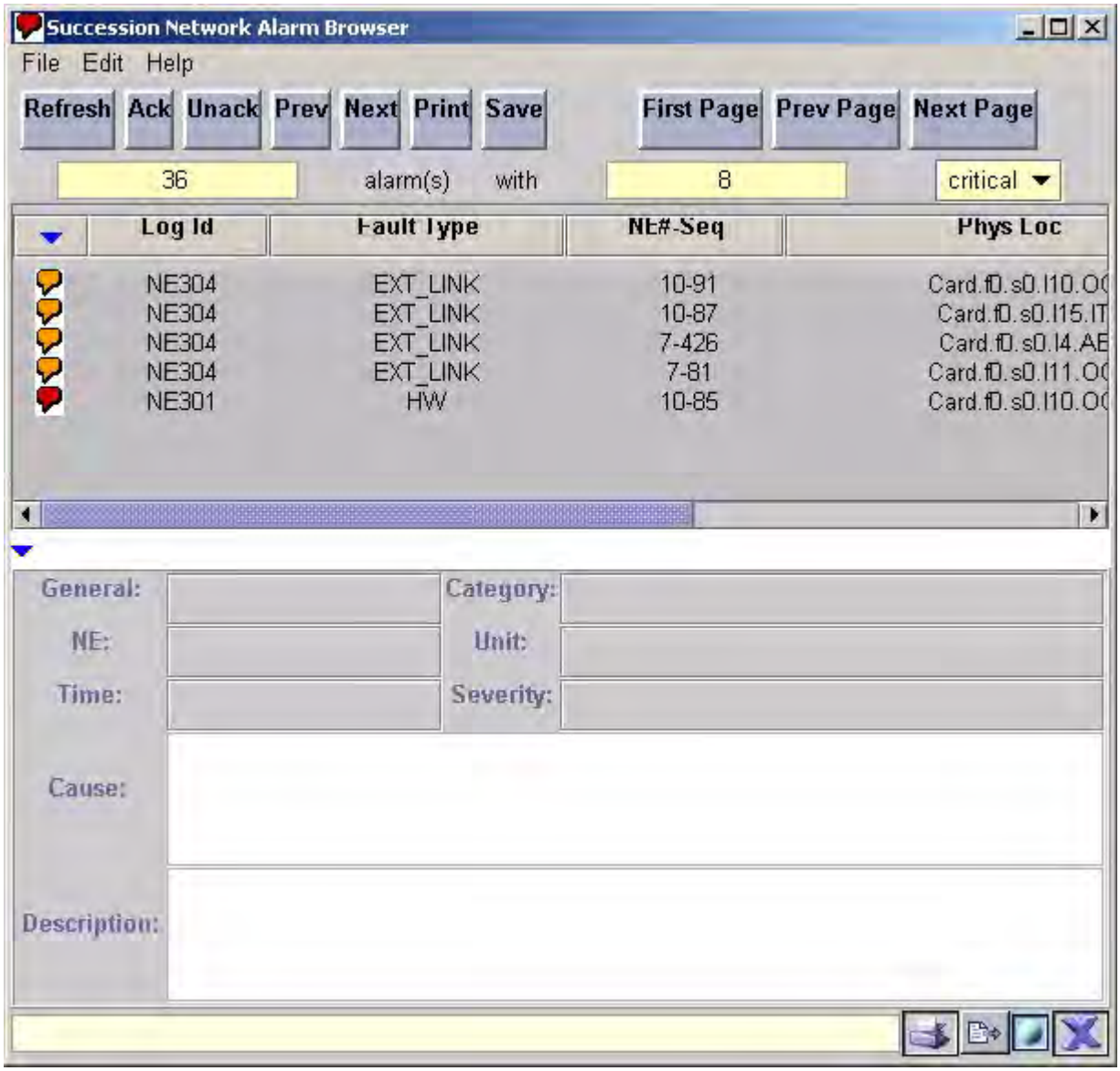
7 Access the Alarm Browser by clicking on the Alarm Browser item in the Alarm menu.

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.

Validating an installation of the USP Manager

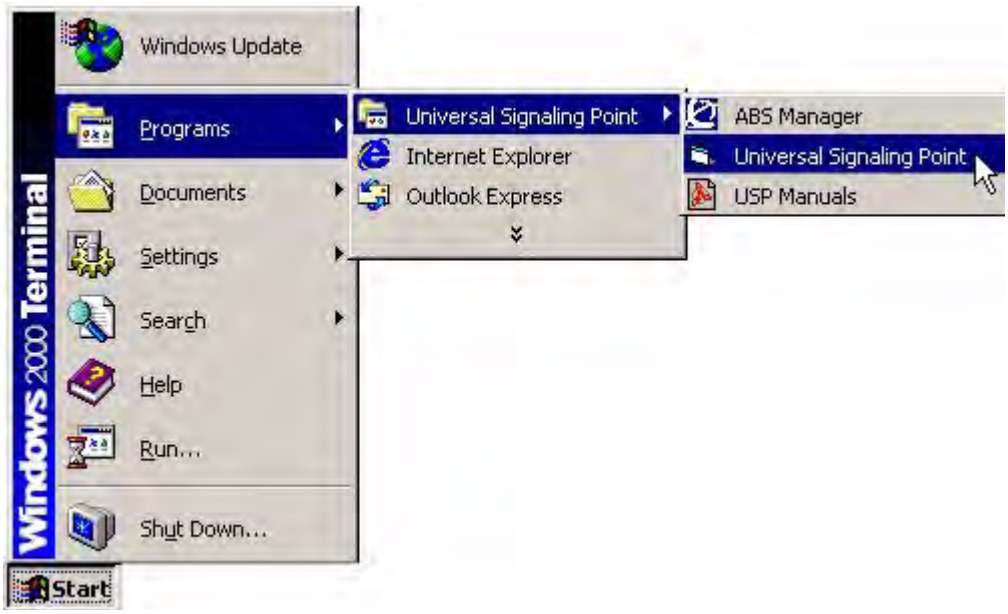
Validating the USP Manager installation involves logging into the USP manager, connecting to the shelves, and verifying the alarm data.

Validating the USP Manager installation

At the client workstation

1 Access the USP Manager by selecting the Universal Signaling Point item from the Universal Signaling Point menu on the Start menu.

Launching the USP Manager

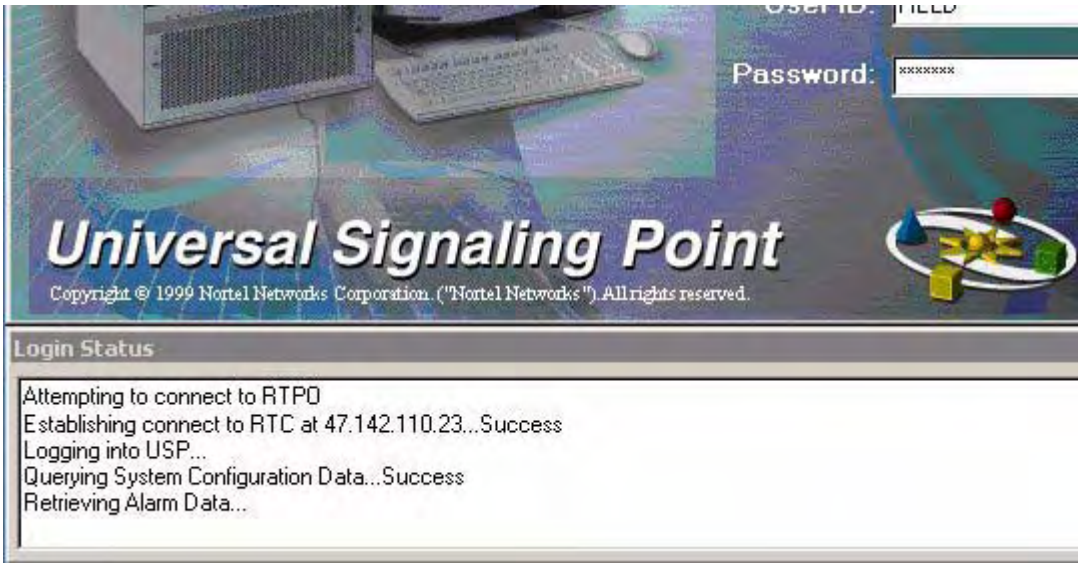


2 The USP Manager login screen will open. Select a site from the drop down menu and enter a User ID and password. Then press the Connect button.

Login screen

3 Observe the Login Status window below the Login screen.

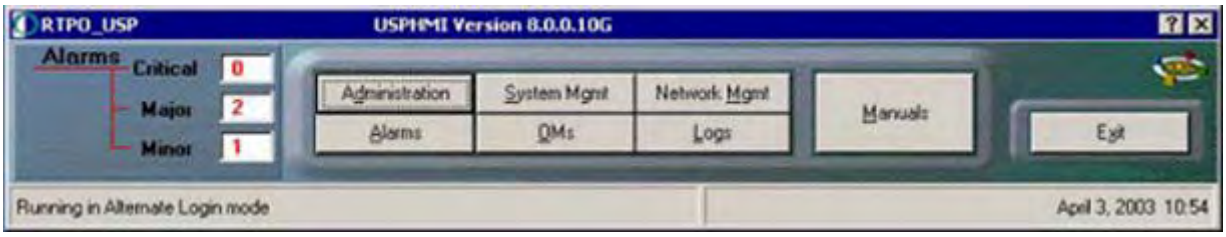
USP Manager login status



If you	Do
connect to the USP manager	step 4
fail to connect to the USP manager	step 11

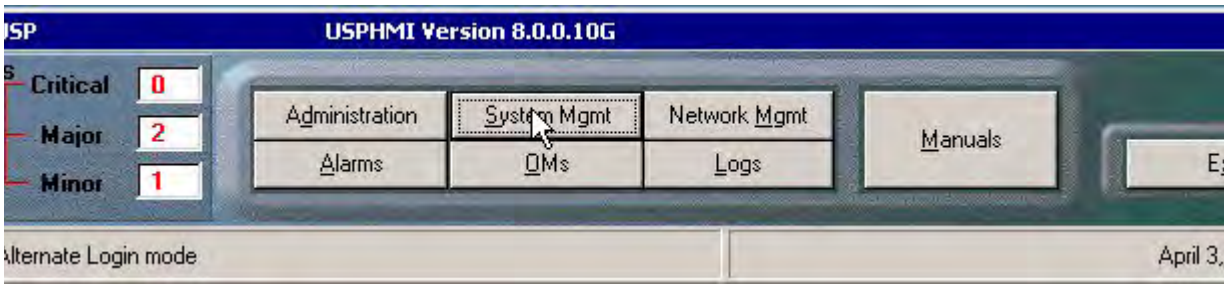
4 The USP Manager client GUI will appear.

USP Manager GUI



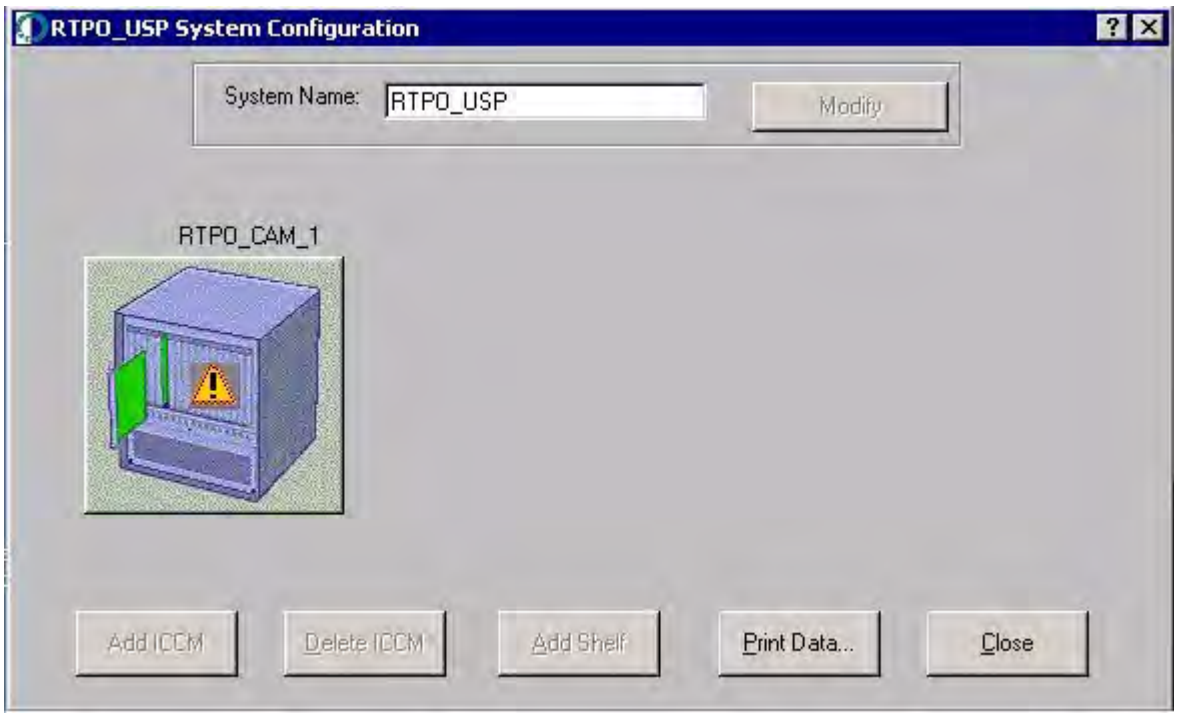
5 Access the System Configuration window by clicking the System Management button.

Accessing the System Configuration window



6 Verify that all provisioned USP shelves appear in the window.

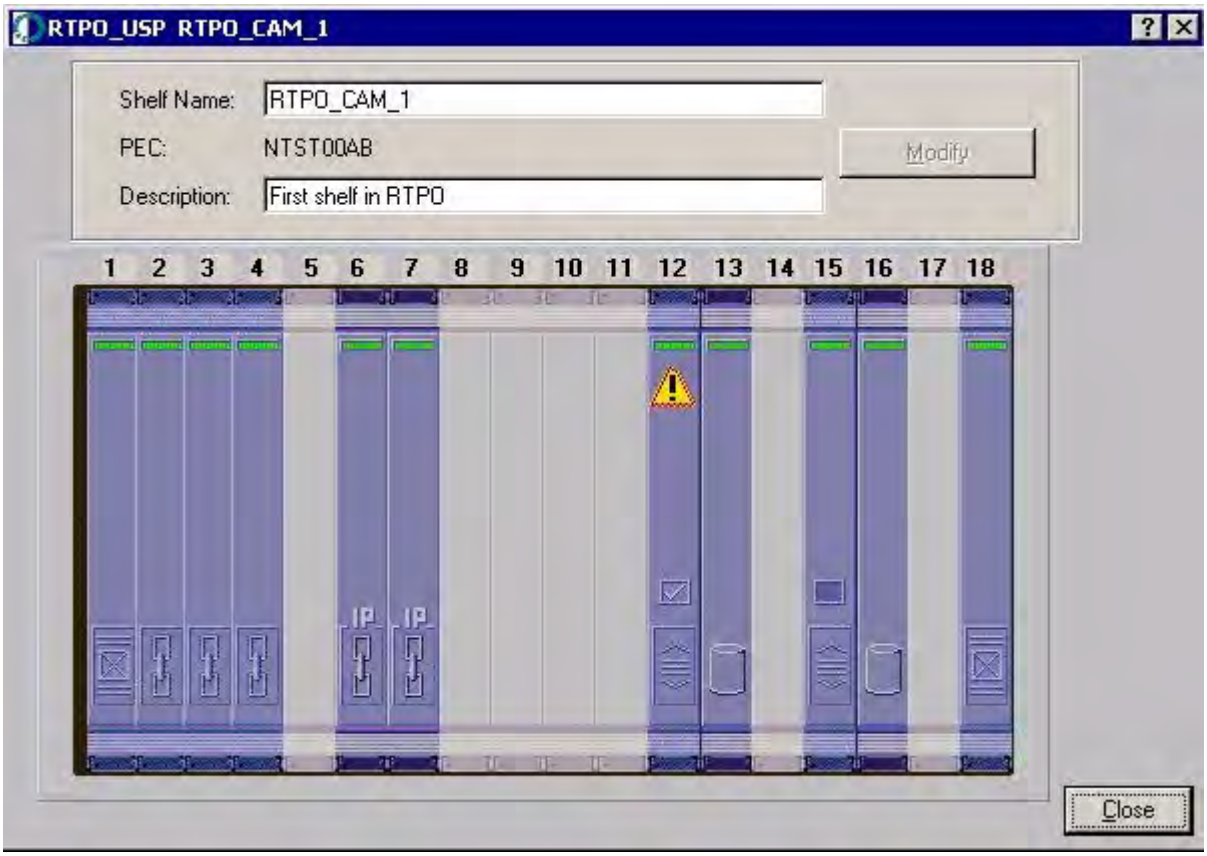
System Configuration window



If all provisioned USP shelves	Do
appeared in the window	step 7
did not appear in the window	step 11

7 Double click on a shelf to bring up the shelf view.

Shelf view



If the shelf	Do
appears correctly	step 8
does not appear correctly	step 11

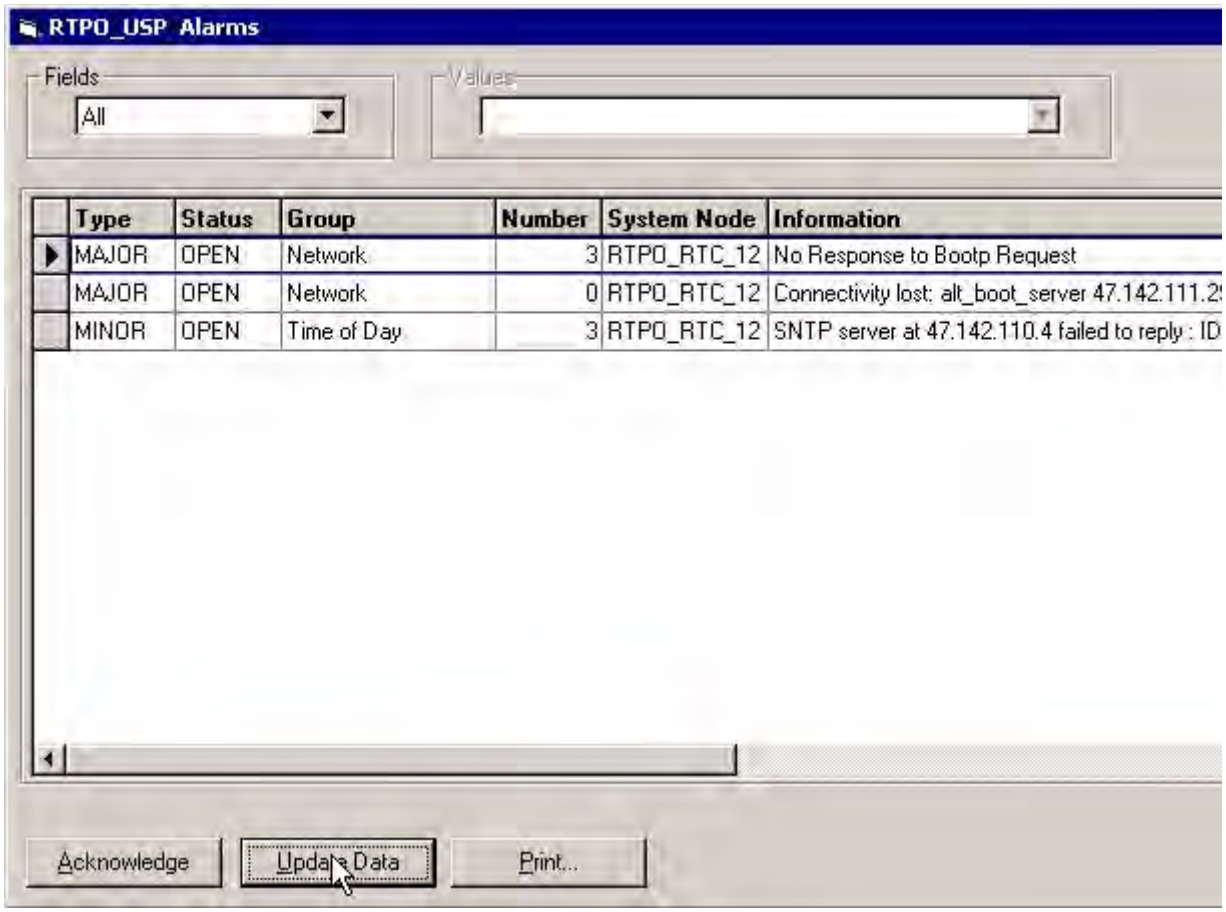
8 Close the Shelf view and System Configuration window by clicking the Close button on each.

9 Access the Alarms window by clicking on the Alarms button.

Accessing the Alarms window

10 When the Alarms window opens. Click on the Update Data button to verify communication between the client and server.

Updating the alarms



If the alarm data	Do
updates with no errors	step 12
updates with errors	step 11

11 Contact your next level of support.

12 You have completed this procedure.

Validating an installation of the Device Manager

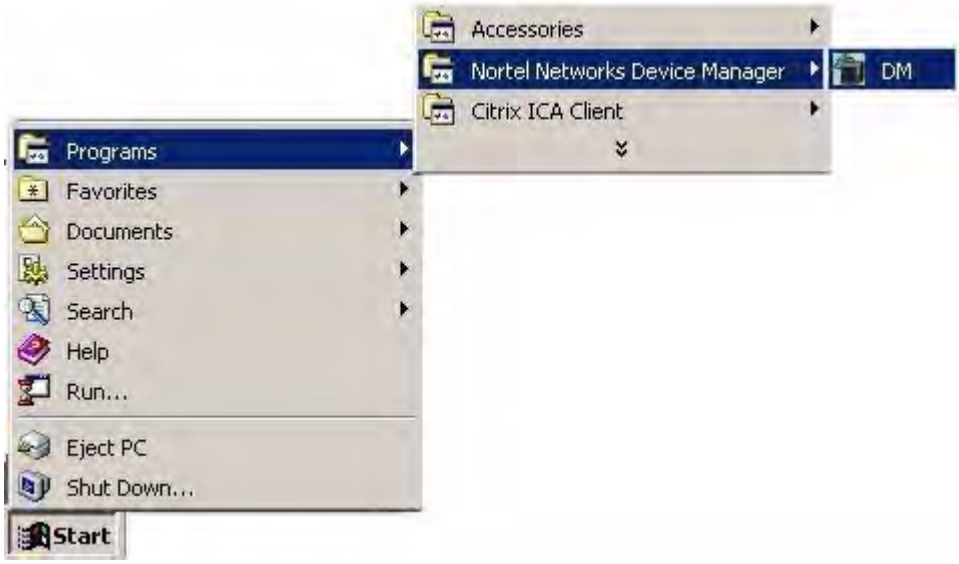
Validating the Device Manager installation involves logging into the Device Manager client and running diagnostics to verify connection between the client and server.

Validating the Device Manager installation

At a WIndows PC

1 Using the Windows Start menu, access the Device Manager by selecting the DM item from the Nortel Networks Device Manager menu.

Accessing the Device Manager Application

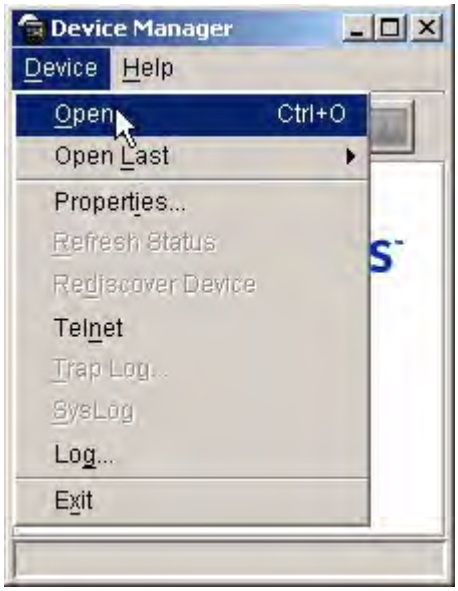


2 The Device Manager application client window will appear.

Device Manager application client

3 Select the Open item from the Device menu.

Selecting the Open item

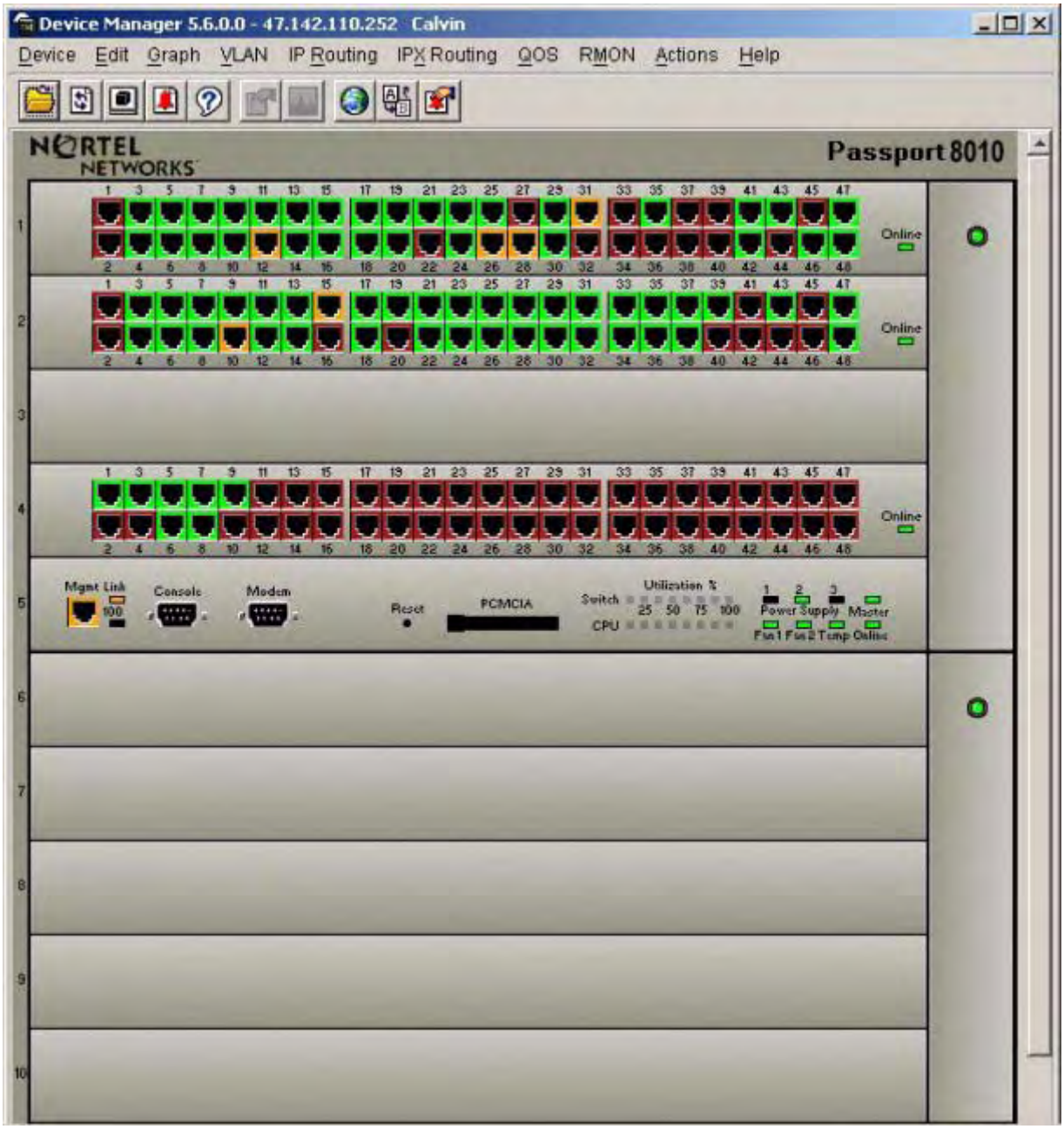


4 In the Open Device window, enter the IP address of the Device to which you wish to connect and click the Open button.

Open Device window

5 The Device Manager GUI will appear.

Device Manager GUI



6 Verify that the client GUI appears.

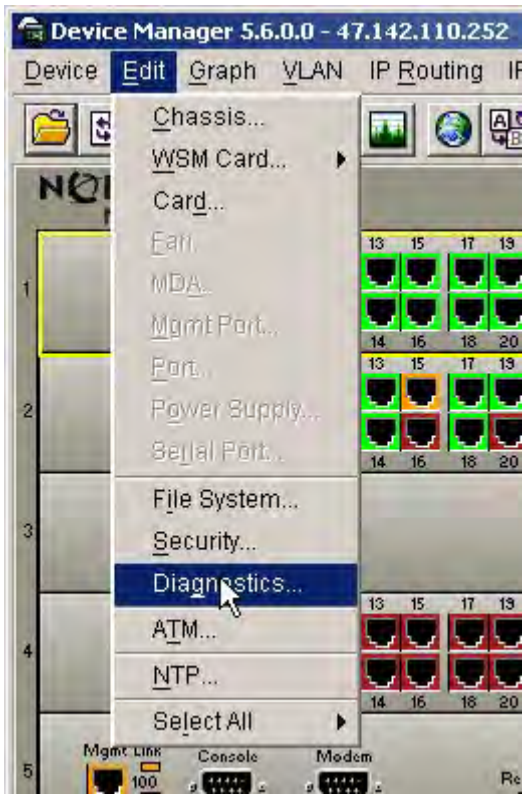
If the Device Manager client	Do
appears	step 7
does not appear	step 11

7 Select one of the ports by clicking on it with the left mouse button.

Selecting a port

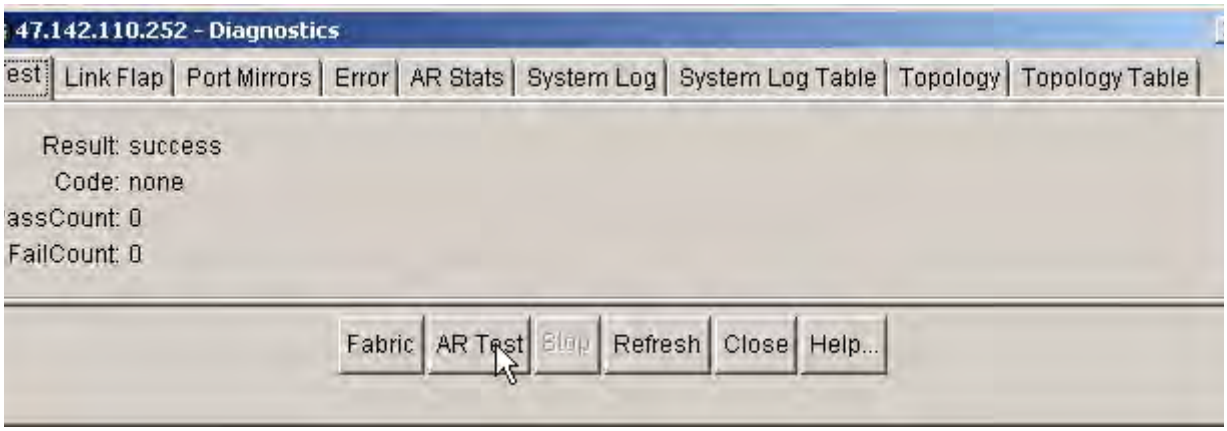
8 Select the Diagnostics item from the Edit menu.

Selecting Diagnostics



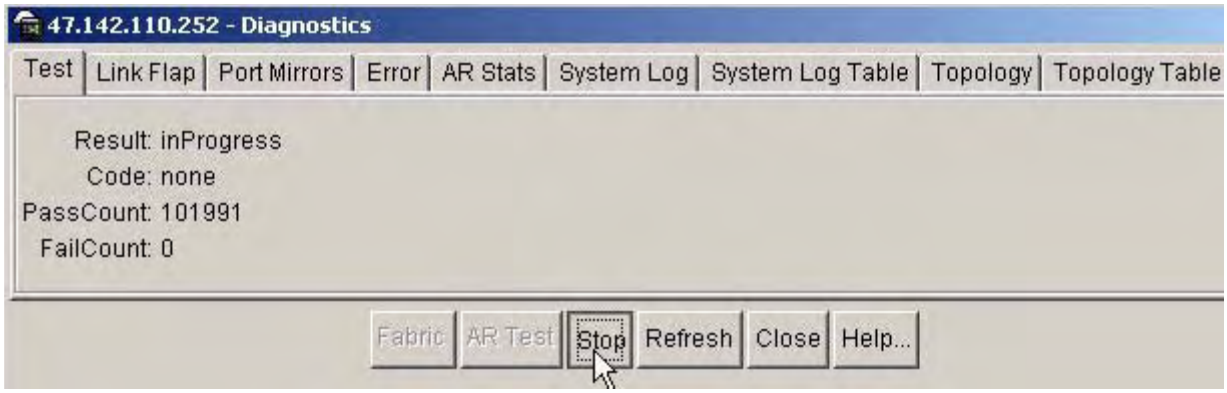
9 Start an AR test by clicking on the AR Test button.

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.

Validating an installation of the LMM

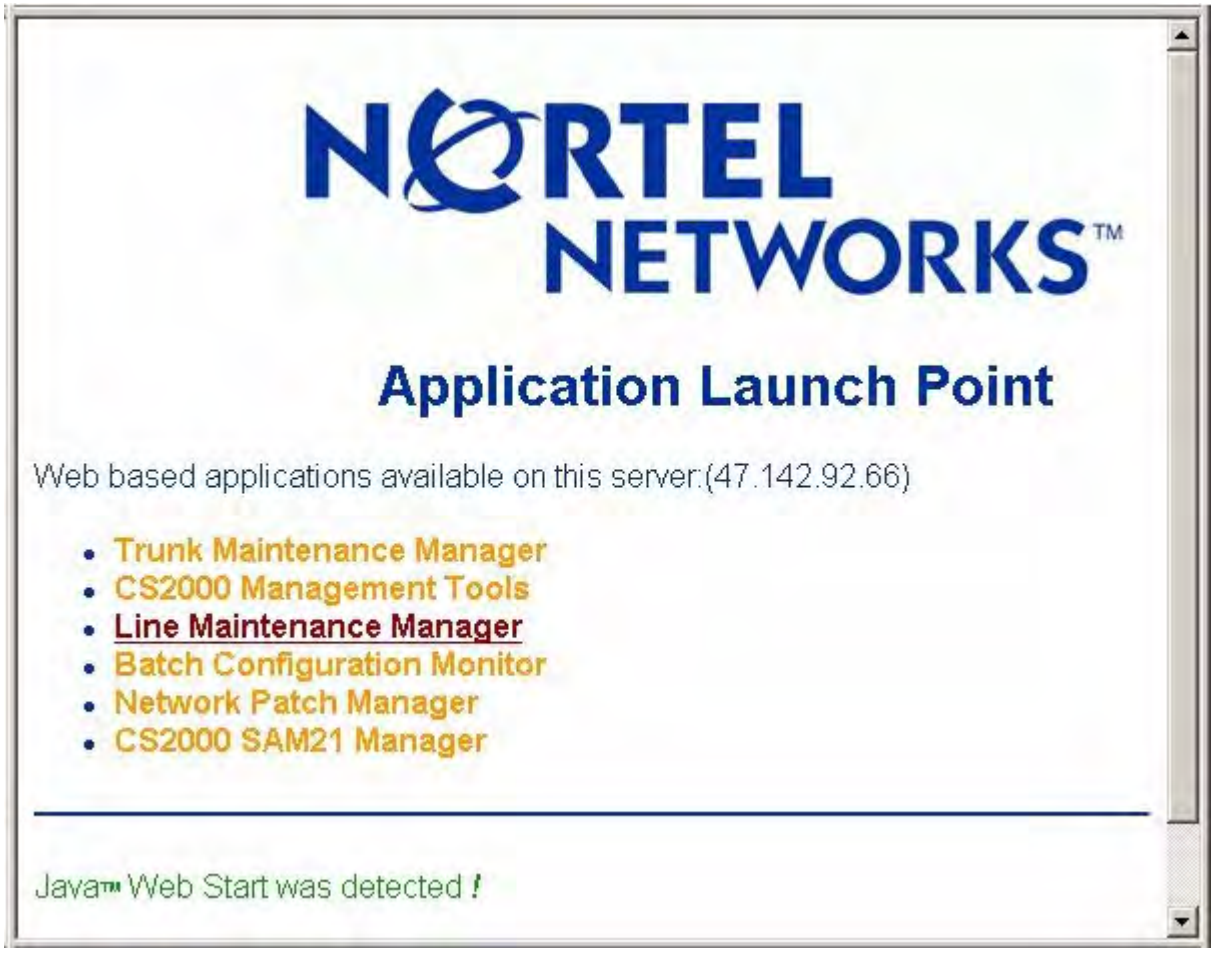
Validating the LMM installation involves logging into the LMM and checking the connection between the client and server.

Validating the LMM installation

At a web browser

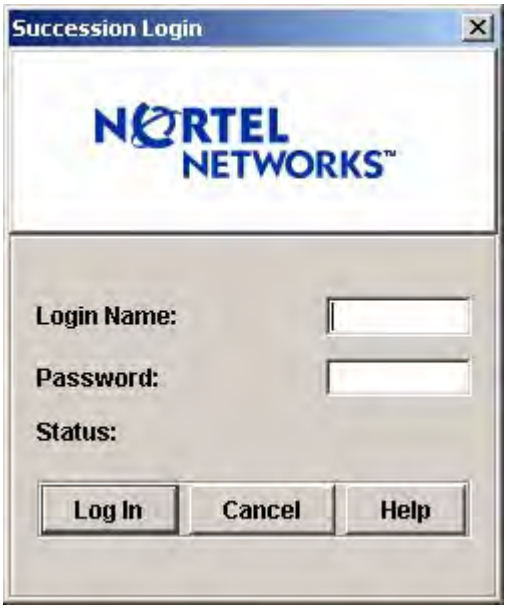
1 Access the Application Launch Point on the server on which you installed the LMM.

LMM Application Launch Point



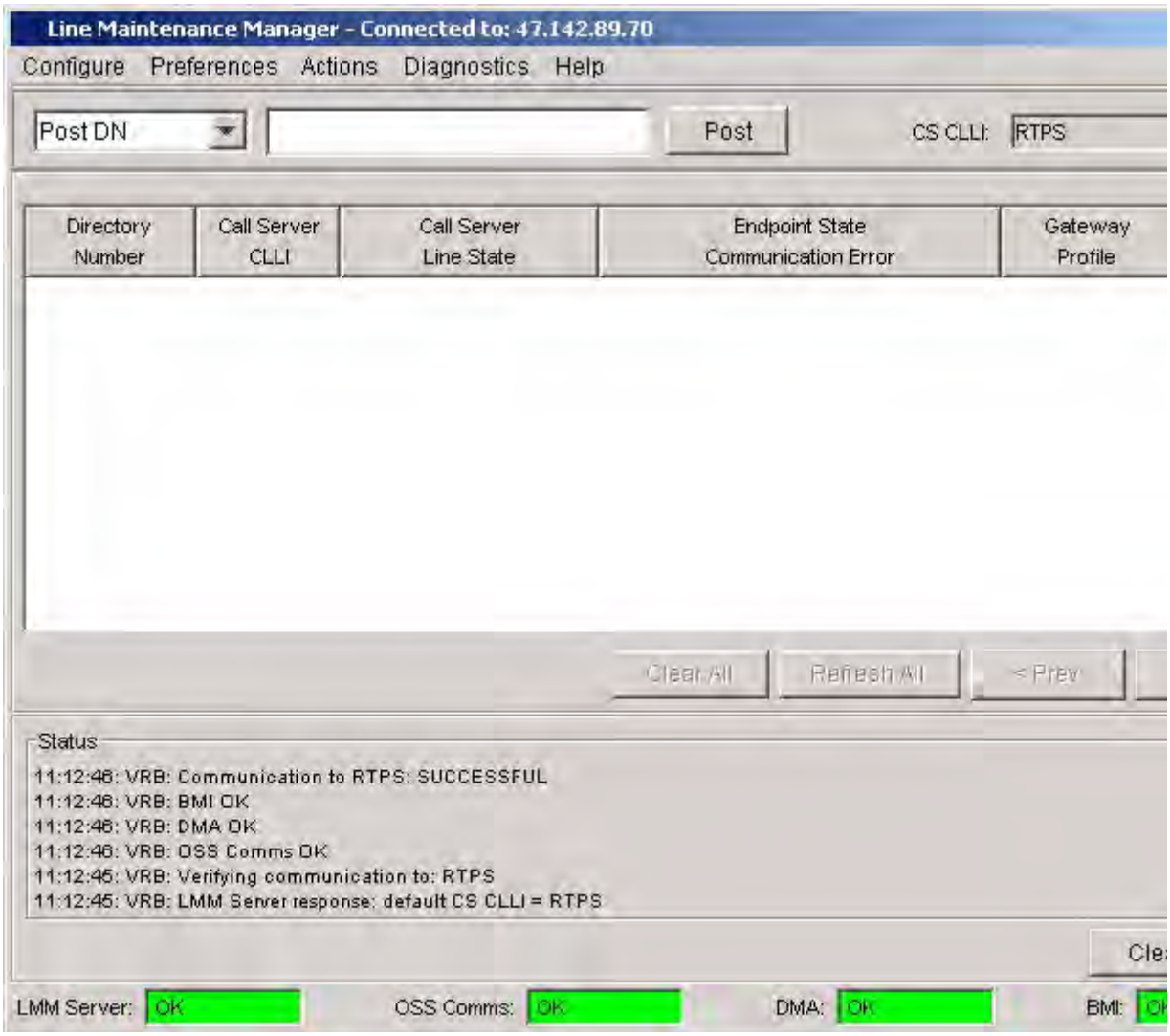
2 Click on the link for the Line Maintenance Manager. Once the application loads, you will be asked to for a User Name and Password to access the manager.

Login screen



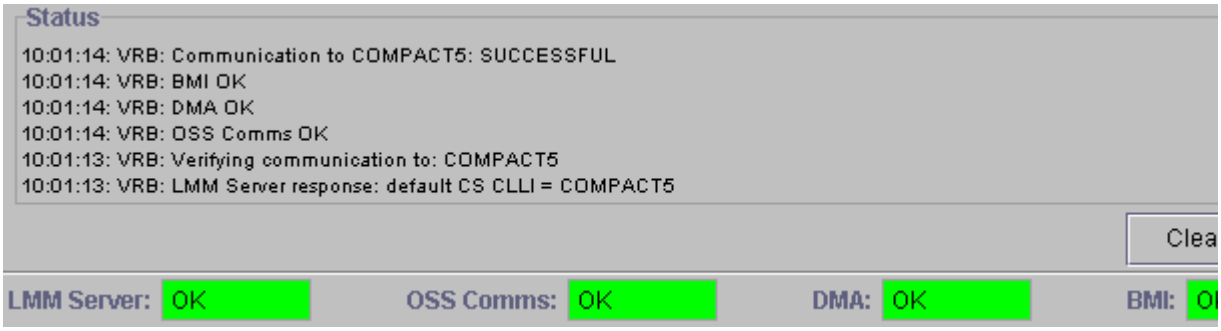
3 The LMM GUI will appear.

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.

Validating an installation of the TMM

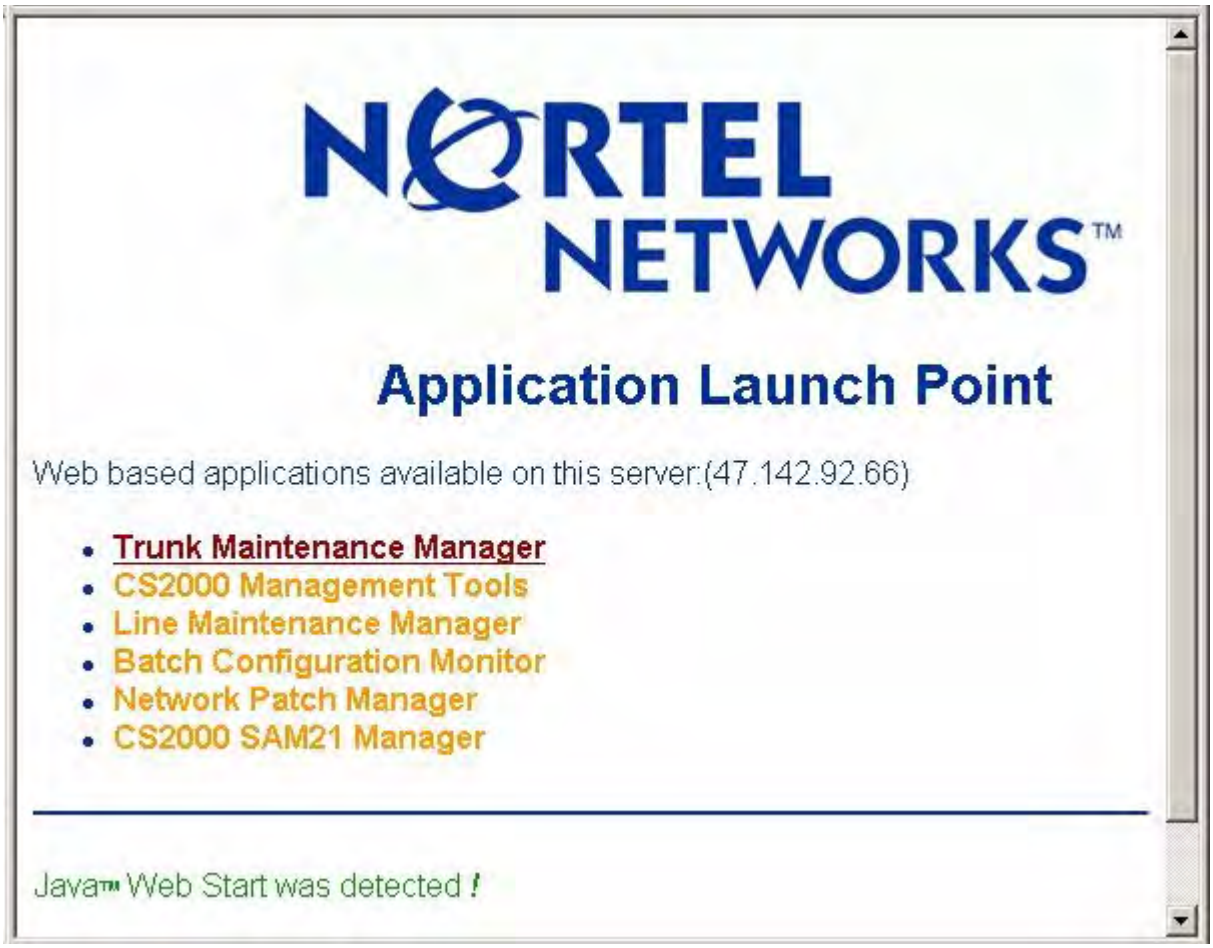
Validating the TMM installation involves logging into the TMM client and verifying that the links in the client window work properly.

Validating the TMM installation

At a web browser

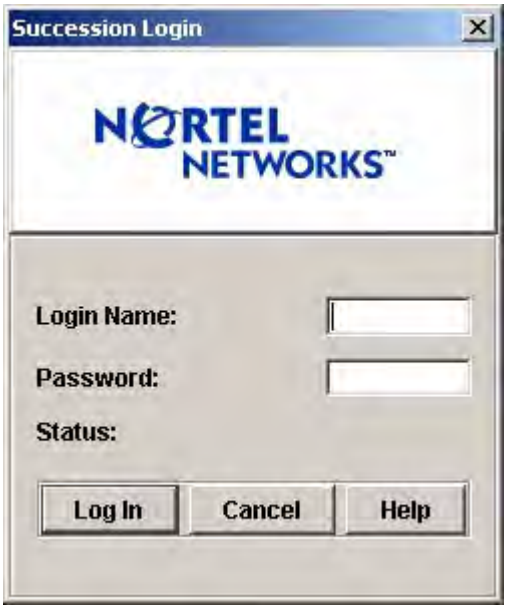
1 Access the Application Launch Point on the server on which you installed the TMM.

TMM Application Launch Point



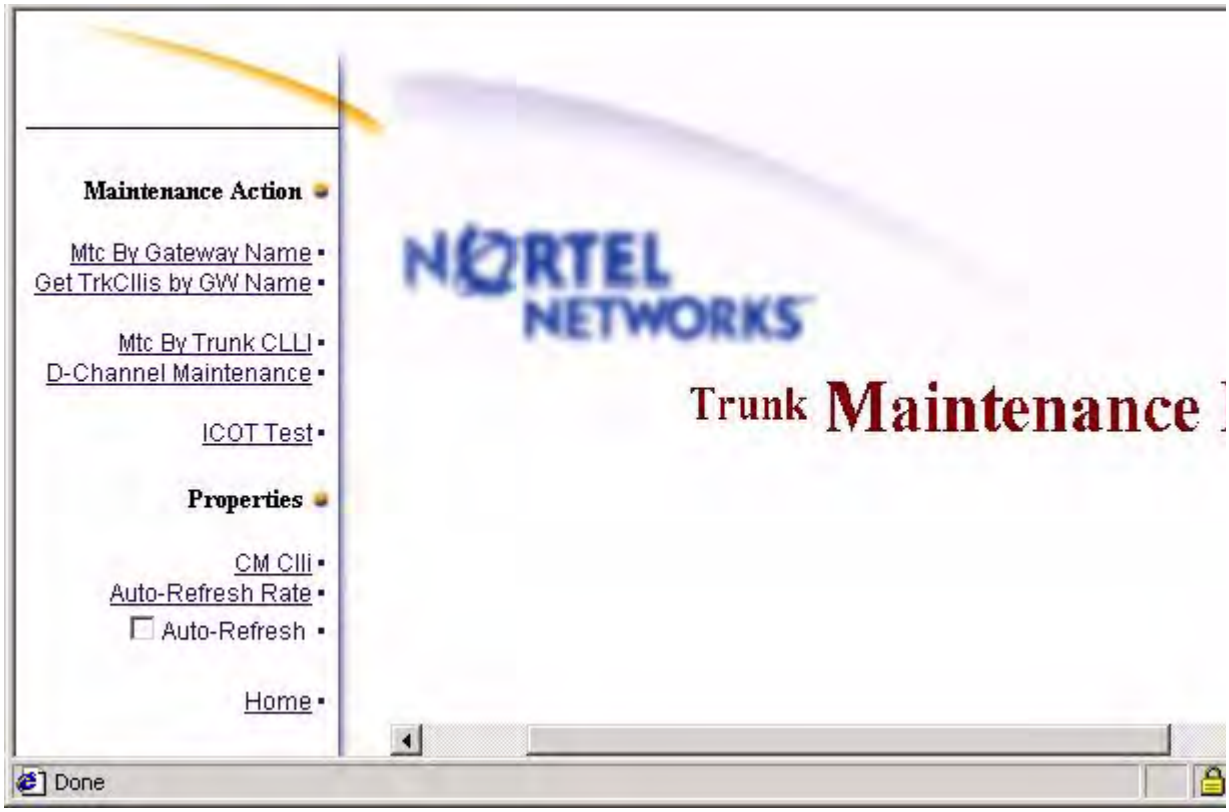
2 Click on the link for the Trunk Maintenance Manager. Once the application loads, you will be asked to for a User Name and Password to access the manager.

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.