P0911818

Nortel Networks Symposium Call Center Server

for DMS/MSL-100
Administrator's Guide

Product release 3.0	Standard 1.0	April 2000

NORTEL NETWORKS™

How the world shares ideas.

P0911818

Nortel Networks Symposium Call Center Server

for the DMS/MSL-100
Administrator's Guide

Publication history

Contents

13   Restoring data   335

14   Controlling the server from a client PC   403

Chapter 1

Getting started

In this chapter

Overview

Introduction

The *Nortel Networks Symposium Call Center Server Administrator's Guide* provides information on how to configure, and manage the configuration of, your Symposium Call Center Server. In addition, the *Administrator's Guide* provides information on software maintenance tasks, such as alarm monitoring and backing up and restoring the database.

Restrict access to this guide

This guide contains sensitive information about maintaining your Symposium Call Center Server, including passwords, procedures, and information that could damage the system if not used correctly. Nortel Networks recommends that access to this guide be restricted to senior administrators only.

Optional features

Some of the features described in this guide are optional. To determine which features you have access to, Nortel Networks supplies a special code called a keycode that you use when you install the Symposium Call Center Server software. Fields and commands for features that you did not purchase are not available.

Skills you need

Nortel Networks product knowledge

Knowledge of, or experience with, the following Nortel Networks products will be of assistance when administering the Symposium Call Center Server:

- the Symposium Call Center Server
- the DMS-100 family of switches or the MSL-100 switch

PC experience or knowledge

Knowledge of, or experience with, the following PC products will be of assistance when administering the Symposium Call Center Server:

- Microsoft Windows 95, Windows 98, or Windows NT 4.0 Workstation

Other experience or knowledge

Other types of experience or knowledge that might be of use include:

- analytical skills
- knowledge of your call center organizational structure and your call center objectives

Section A: Call center setup and management tasks

In this section

Switch configuration tasks

Introduction

Before you can use the Symposium Call Center Server with the switch, you must configure the switch.

Note: To use the Symposium Call Center Server with your switch, you require the Intelligent Call Manager (ICM) on the switch. For more information about ICM, refer to the ICM documentation.

Switch configuration tasks

You must perform the following tasks to configure the switch for the Symposium Call Center Server.

- Configure the server logon process.
- Configure RAN and music routes, including routes for forced incoming and overflow announcements in table ACDRTE, and call treatments in table AUDIO.
- Configure the ACD groups in table ACDGRP.
- Configure the ACD subgroups in table ACDSGRP.
- Configure ACD-DNs in table DNROUTE.

  Note: Before defining ACD DNs, you must define the area code and office code in the table TOFCNAME.
- Configure agent and supervisor phonesets using the SERVORD utility.

  Note: Before you can configure phonesets, you must define the NCOS in table NCOS, and features for the customer group in table CUSTHEAD.
- Define agent logon IDs in table ACDLOGIN.

For detailed instructions, refer to the *Symposium and DMS Switch Guide* or *Symposium and MSL-100 Switch Guide*.

Initial setup tasks

Introduction

Initial setup tasks include all of those tasks required to create a system that performs in the manner required to meet your call center objectives. (For help in planning and setting up a new system, refer to the *Symposium Call Center Server Setup Guide*.)

Initial setup tasks

The following table lists initial setup tasks.

Task	For more information, see
Installing the Symposium Call Center Server Client	*Software Installation and Upgrade Guide*
Setting up security—defining access classes and giving users authority to connect to the server and perform various functions.	"Adding access classes" on page 29 and "Adding desktop user accounts" on page 47
Administering the switch (CDNs, music/RAN routes, phonesets, voice ports, activity codes, and DNISs)	"Adding CDNs" on page 79, "Adding music/RAN routes" on page 87, "Adding phonesets" on page 93, "Adding voice ports" on page 100, "Adding activity codes" on page 109, "Adding DNISs" on page 115
Creating threshold classes to control how statistics are pegged in reports and how they appear in displays	"Adding threshold classes" on page 122
Configuring which historical statistics are collected and how long they are stored, and customize real-time displays	"Real-time displays" on page 137 and "Configuring historical statistics collection" on page 152
Creating call presentation classes	"Adding call presentation classes" on page 165

Task	For more information, see
Creating skillsets	"Adding skillsets" on page 182
Creating supervisors	"Adding or changing supervisors" on page 194
Creating agents	"Adding agents" on page 205
Creating scheduled agent to supervisor assignments	"Adding agent to supervisor assignments" on page 221
Creating scheduled agent to skillset assignments	"Adding agent to skillset assignments" on page 233
Generating reports	*Historical Reporting and Data Dictionary Guide*
Scheduling regular system backups	*"Scheduling a backup" on page 291*
Creating scripts	*Scripting Guide*

Ongoing call center management tasks

Introduction

From time to time, changes in your call center require changes to the configuration of the server. During system installation, the installer created a default system administrator. You can add other system administrators. You must add users, user groups, and application administrators, as required, so that others can use the system.

Ongoing call center management tasks

The following table lists ongoing call center management tasks.

Task	For more information, see
Adding and maintaining threshold classes to control how statistics are treated in reports, statistics, and displays	Chapter 4, "Managing threshold classes"
Administering the switch (CDNs, music/ RAN routes, phonesets, voice ports, activity codes, and DNISs)	Chapter 3, "Administering the switch"
Change the historical statistics collection and real-time displays configuration	Chapter 5, "Working with displays and statistics"
Adding and maintaining call presentation classes and skillsets	Chapter 6, "Managing skillsets and call presentation"
Adding and maintaining supervisors	Chapter 7, "Managing supervisors"
Adding and maintaining agents	Chapter 8, "Managing agents"
Adding and maintaining agent to supervisor assignments	Chapter 9, "Managing agent to supervisor assignments"
Adding and maintaining agent to skillset assignments	Chapter 10, "Managing agent to skillset assignments"

Task	For more information, see
Generating reports and using real-time displays	*Historical Reporting and Data Dictionary Guide*
Scheduling regular system backups	Chapter 12, "Backing up data"
Creating and maintaining scripts	*Scripting Guide*

Section B: Managing the server

In this section

Accessing Windows NT Administrative Tools

To access a Windows NT administrative tool

1   Logon to the server as Administrator.

2   Choose Start → Programs → Administrative Tools (Common) and select the tool you want to run.

List of Administrative Tools

The following are among the tools available from the Windows NT Administrative Tools menu:

- Backup
- Disk Administrator
- Event Viewer
- Performance Monitor
- User Profile Editor
- User Manager
- Server Manager
- Windows NT Diagnostics

For more information, consult your Windows NT documentation.

Shutting down or restarting the server

Introduction

Follow the procedures in this section to shut down the Symposium Call Center Server properly.

CAUTION

Risk of file corruption

Do not press the power button on the front of the server to shut down your system as this can result in

- file corruption
- failure to deacquire resources
- loss of statistics for the current interval

Always use the procedure described in this section to shut down the server.

To shut down or restart the Symposium Call Center Server

1   Choose Start → Shutdown.

Result: The Shut Down Windows dialog box appears.

2   To turn off the server, select Shut down. To restart the server, select
Restart, then click Yes.

Result: If you are shutting down the server, the Symposium Call Center
Server shuts downs and powers off. If you are restarting the server, the
server shuts down and then begins starting up.

ATTENTION	If you are going to work on the inside of the server, follow safety precautions described in the *Meridian Application Server Installation and Maintenance Guide* for your hardware platform.

Managing the date and time

Introduction

The Symposium Call Center Server is the master clock. It does not derive its time from the switch.

Note: After a time change, you must restart the server.

For more information refer to one of the following guides:

- *Symposium Call Center Server and the DMS-100 Switch Guide*
- *Symposium Call Center Server and the MSL-100 Switch Guide*

To view the system date, time, and time zone from the client PC

1 From the SMI window, double-click the time at the bottom right corner of the SMI window.

Result: The System Date and Time property page appears.
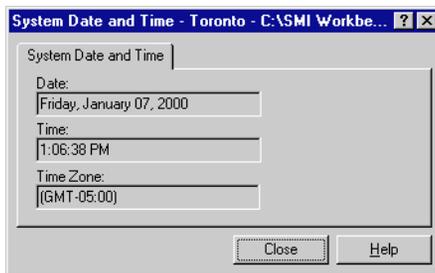
2 Click Close to return to the SMI window.

Section C: Using SMI Workbench

In this section

Adding servers

Introduction

This section introduces you to the System Management Interface (SMI) Workbench. Through the SMI Workbench, you access the SMI window, which contains all of the functions available on the Symposium Call Center Server.

Note: Existing MAT systems for Symposium Call Center Server are exported to SMI systems during client software installation or upgrade. If you require more information, refer to the *Software Installation and Upgrade Guide*.

Using a dial-up connection to the server

Client PCs that are not on the same LAN as the server must use Dial-Up Networking to establish a network connection. For instructions, refer to the *Software Installation and Upgrade Guide*.

Note: You cannot generate reports across a dial-up (PPP) connection.

To add a server

1   From the Windows Start menu, choose Programs → SMI Workbench.

2   Double-click Add System.

   Result: The Add System dialog box appears.
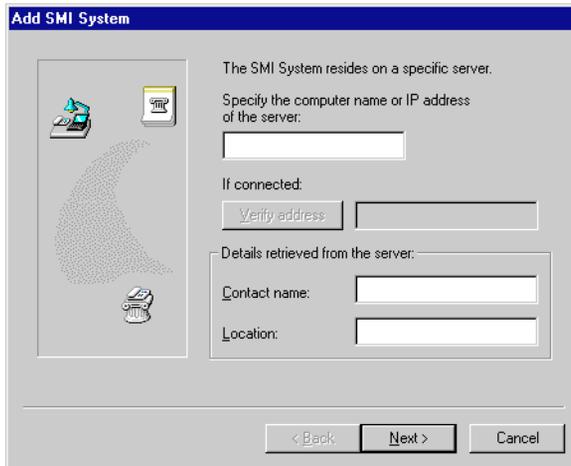
3   Enter the computer name or the IP address of the server you want to access.

   Note: For a dial-up connection, enter the IP address.

4   If the client PC has a network connection to the server, click Verify Address to verify that the computer name or IP address is correct and reachable.

5   Click Next.
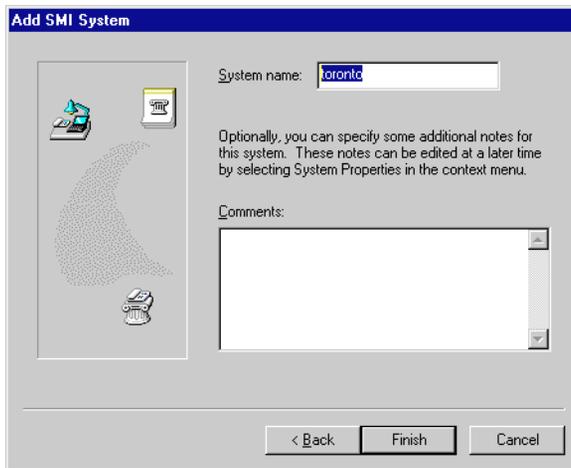
6   (Optionally) Enter notes or a comment that describes this SMI system.

7   Click Finish.

Result: The server appears in the SMI Workbench folder.

To group servers by location

Group servers by location if the client PC is used to administer servers in different physical locations.

To group SMI systems, create sub-folders in the SMI Workbench folder. Name these sub-folders by the site (location) names. Click and drag the servers into the appropriate folders.

Logging on to the server

Introduction

To access the Symposium Call Center Server client functions, you must log on to the server.

To log on

1 Double-click the server in the SMI Workbench folder (or double-click the desktop shortcut, if one is available).

Result: The SMI Login dialog box appears.
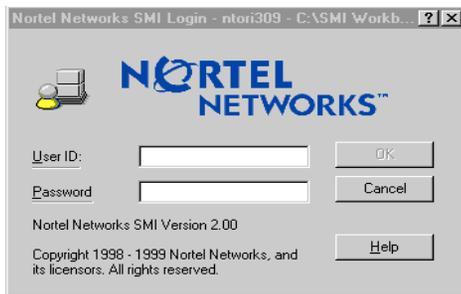
2 In the User ID box, type your user ID.

3 In the Password box, type your password.

4 Click OK.

Result: The Login dialog box closes and the SMI window appears.

Overview of the SMI window

Introduction

The SMI window displays a tree of system administration tasks to which you have access. This window is displayed after you log in to the server.

The SMI window

The following figure shows the SMI window. The contents of the window depend on the system administration tasks available and your access permissions. Your SMI window might look different than the example below.
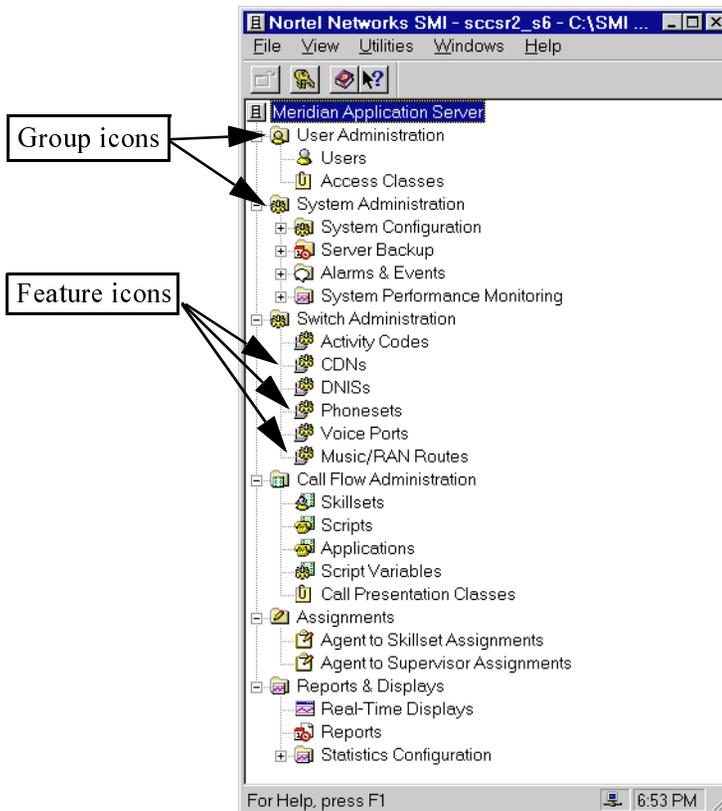
Chapter 2

Managing security

In this chapter

Overview of managing security

Introduction

Today, much information that is vital to a company's well-being is transmitted over networks. These networks must be protected so that only authorized users can access, change, or delete information.

The system administrator is responsible for establishing and maintaining system security. The administrator sets up security by assigning users logon passwords and access classes. By assigning the appropriate access classes to the appropriate users, the administrator can help ensure system security.

Example

You might want to restrict access to call-by-call reports to senior administrators, since stored call-by-call data, such as caller-entered keypad input, might contain confidential information. To restrict access, define an access class with the ability to generate reports and access call-by-call data. Then assign this access class to senior administrators only.

Assumption

This chapter assumes that you understand Microsoft Windows NT security.

Setting up security

To set up security, perform these tasks:

1. Define access classes.

2. For each access class, select the Symposium Call Center Server functions that members of that class may use. For a complete list of functions and privileges, see "Functions and privileges" on page 35.

3. Create desktop user accounts for users who require access to Symposium Call Center Server functions.

4.   Assign access classes to user accounts, giving users the privileges they need to perform their jobs.

Password retry lockout

Users are locked out of the system if they attempt to logon more than three consecutive times using an invalid password. (This is based on Windows NT settings configured during the installation.) To restore a user's access to the system, an administrator must reset the password retry count to zero. For more information, see "To restore a user's access to the server" on page 52.

If the locked-out user is an administrator, another administrator must restore access.

Note: If there is no other administrator, only Nortel Networks support staff can reset the account. Therefore, be sure to create at least two users with administrator privileges.

Section A: Working with access classes

In this section

Overview of access classes

Introduction

An access class is a set of privileges for the various functions available for the Symposium Call Center Server.

Example

If you want a shift supervisor to monitor agent performance by viewing real-time statistics, you could do the following tasks:

■ Define an access class called Real_Time_View that provides view access to real-time displays, but no other access.

■ Give the shift supervisor a desktop account.

■ Assign them to the Real-Time_View access class.

Default access classes

The installation process creates three default access classes:

■ **adminGroup:** Users belonging to this class have administrator access to the system and can access all functions.

■ **Call Center Admin:** Users belonging to this class can access all functions except the switch administration functions (such as configuring phonesets and CDNs) and system administration functions (such as backup, restore, and the alarm monitor).

■ **Supervisor:** Users belonging to this class can view and change reporting agents, create and run reports, and create and view real-time displays.

Adding access classes

To add an access class

1   From the SMI window, choose User Administration → Access Classes.

   Result: The Access Classes window appears.

2   Choose File → New.

   Result: The New Access Class property sheet appears.

3   In the Name box, type a name for the access class. Use a descriptive name that describes the type of user that will have this access level or the type of privileges available at this access level.

4   In the Comments box, enter additional, optional information about the access class.

5   Click the Access tab.

Result: The Access page appears, showing the available Symposium Call Center Server functions and the level of access that members of this access class have for each function.
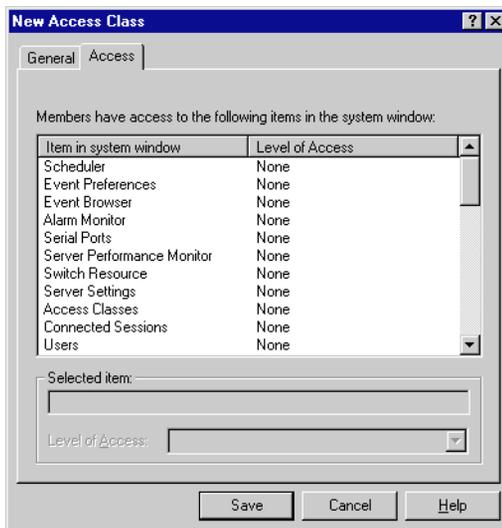
Notes:

■   Most of the items in this list correspond to items in the SMI window.

■   After you assign users to an access class, a third tab appears, named "Members." This tab shows you all the users who belong to the access class.

6   Select a function you want to make available to this access class. For a list of functions and available access levels, see "Functions and privileges" on page 35.

Result: The selected function appears in the Selected item box.

7   Choose the desired level of access for that function.

8   Repeat steps 6 and 7 for each function you want this access class to have.

9   Click Save.

Result: You return to the Access Classes window.

10 To return to the SMI window, choose File → Close.

Viewing the members of an access class

To view the members of an access class

1   From the SMI window, choose User Administration → Access Classes.

   Result: The Access Classes window appears.

2   Select the access class for which you want to display the members.

3   Choose File → Properties.

   Result: The Access Class Properties property sheet appears.

4   Click the Members tab.
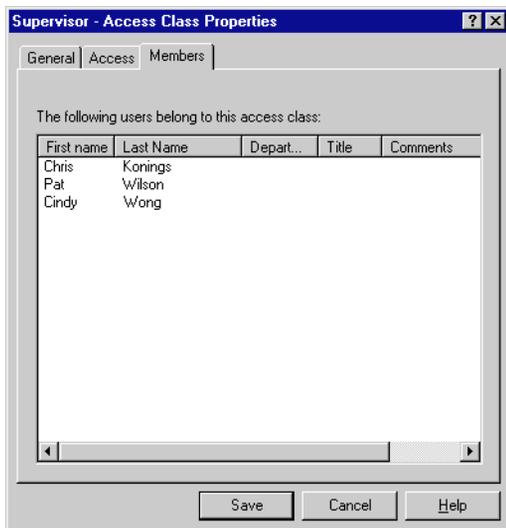
5   Click Save.

Result: You return to the Access Classes window.

6   To return to the SMI window, choose File → Close.

Other procedures for access classes

To change the properties of an access class

From the Access Classes window, select the access class you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview the list of access classes

From the Access Classes window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print the list of access classes

From the Access Classes window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete an access class

Note: You cannot delete the AdminGroup or any access class that has members.

From the Access Classes window, select the access classes you want to delete and choose File → Delete.

Functions and privileges

Function	Privilege	Description
Access Classes	View	Allows users to display the Access Classes window and view the properties for any access class.
	Edit	Allows users to display the Access Classes window and view and change properties for any access class.
	Create/Delete	Allows users to display the Access Classes window and view, change, add, and delete access classes.
Activity Codes	View	Allows users to display the Activity Codes window and view properties for all activity codes.
	Edit	Allows users to display the Activity Codes window and view and change properties for all activity codes.
	Create/Delete	Allows users to display the Activity Codes window and view, change, add, and delete activity codes.
Agent Threshold Classes	View	Allows users to view the Agent Threshold Classes property sheet for agent threshold classes.
	Edit	Allows users to view and change properties for agent threshold classes.
	Create/Delete	Allows users to view, change, add, and delete properties for agent threshold classes.

Function	Privilege	Description
Agent to Skillset Assignments	View own agents only	Allows users to display the list of assignments containing their reporting and associated agents in the Agent to Skillset Assignments window and view the properties, schedules, and matrixes for these assignments. The matrix specifies agents' priority for a skillset.
	View and assign own agents only	Allows users to display the Agent to Skillset Assignments window and view, change, add, and delete properties, schedules, and matrixes for assignments created for their reporting and associated agents.
	View all agents	Allows users to display the Agent to Skillset Assignments window and view properties, schedules, and matrixes for assignments created for all agents.
	View and assign all agents	Allows users to display the Agent to Skillset Assignments window and view, change, add, and delete properties, schedules, and matrixes for assignments created for all agents.
Agent to Supervisor Assignments	View all agents	Allows users to display the Agent to Supervisor Assignments window and view properties and schedules for all assignments.
	View and assign all agents	Allows users to display the Agent to Supervisor Assignments window and view, change, add, and delete properties and schedules for all assignments.
Alarm Monitor	View	Allows users to open the Alarm Monitor and view event details for system alarms.
	Create/Delete	Allows users to open the Alarm Monitor, view event details for system alarms, and clear and acknowledge alarms.

Function	Privilege	Description
Application Threshold Classes	View	Allows users to view the Application Threshold Classes property sheet for application threshold classes.
	Edit	Allows users to view and change properties for application threshold classes.
	Create/Delete	Allows users to view, change, add, and delete properties for application threshold classes.
Applications	View	Allows users to display the Applications window and view the properties of any application.
	Edit	Allows users to display the Applications window and view and change the properties of any application.
Backup Devices	View	Allows users to display the Backup Devices window and view the list of available backup devices.
	Edit	Allows users to display the Backup Devices window and view and change the properties of backup devices.
	Create/Delete	Allows users to display the Backup Devices window and view, change, and delete backup devices.
Backup Scheduler	View	Allows users to display the Backup Scheduler window and view the scheduled date and time of backups.
	Edit	Allows users to display the Backup Scheduler window and view and change the scheduled date and time of backups.
	Create/Delete	Allows users to display the Backup Scheduler window and view, change, and delete scheduled backups.

Function	Privilege	Description
Call Presentation Classes	View	Allows users to display the Agent Call Presentation Classes window and view the properties for all call presentation classes.
	Edit	Allows users to display the Agent Call Presentation Classes window and view and change the properties for all call presentation classes.
	Create/Delete	Allows users to display the Agent Call Presentation Classes window and view, change, add, and delete call presentation classes.
CDNs	View	Allows users to display the CDNs window and view properties for all CDNs.
	Edit	Allows users to display the CDNs window and view and change properties for all CDNs.
	Create/Delete	Allows users to display the CDNs window and view, change, add, delete, acquire, and deacquire CDNs.
Connected Sessions	View	Allows users to display the Connected Sessions window.
	Edit	Allows users to display the Connected Sessions window.
	Create/Delete	Allows users to display the Connected Sessions window and log off connected users.
DNISs	View	Allows users to display the DNISs window and view properties for all DNISs.
	Edit	Allows users to display the DNISs window and view and change properties for all DNISs.
	Create/Delete	Allows users to display the DNISs window and view, change, add, and delete DNISs.
Emergency Help	View	Allows users to open the Emergency Help window.

Function	Privilege	Description
Event Browser	View	Allows users to open the Event Browser and view all informational, critical, minor, or major events.
Event Preferences	View	Allows users to view event preferences configured for event codes.
	Edit	Allows users to view event preferences and increase or decrease their severity.
	Create/Delete	Allows users to create event preferences; increase or decrease their severity; and delete event preferences.
Formulas	View	Allows users to display the Formulas window and view properties for all formulas.
	Edit	Allows users to display the Formulas window and view and change properties for all formulas.
	Create/Delete	Allows users to display the Formulas window and view, change, add, and delete formulas.
Historical Statistics	View	Allows users to view the Historical Statistics property sheet. This property sheet determines the type of historical statistics collected, and how long they are stored.
	Edit	Allows users to view and change the Historical Statistics properties.

Function	Privilege	Description
Maintenance	View	Allows users to monitor the status of server components, perform maintenance operations, and run diagnostics.
Music/RAN Routes	View	Allows users to display the Music/RAN Routes window and view properties for all music/RAN routes.
	Edit	Allows users to display the Music/RAN Routes window and view and change properties for all music/RAN routes.
	Create/Delete	Allows users to display the Music/RAN Routes window and view, change, add, delete, acquire, and de-acquire music/RAN routes.
Nodal Threshold Class	View	Allows users to view the Nodal Threshold Classes property sheet for the nodal threshold class.
	Edit	Allows users to view and change properties for the call center summary threshold class.
Phonesets	View	Allows users to display the Phonesets window and view properties for all phonesets.
	Edit	Allows users to display the Phonesets window and view and change properties for all phonesets.
	Create/Delete	Allows users to display the Phonesets window and view, change, add, delete, acquire, and deacquire phonesets.

Function	Privilege	Description
Real-Time Displays	View own agents	Allows users to view reporting and associated agents in the real-time displays.
	View own agents–create displays	Allows users to view reporting and associated agents in the real-time displays, and view and change the properties of real-time display definitions.
	View all agents–create displays	Allows users to view all agents in the real-time displays
	View all agents–create displays	Allows users to view all agents in the real-time displays, and view and change the properties of real-time display definitions.
Real-time Statistics	View	Allows users to view the Real-time Statistics Configuration property sheet. This property sheet determines the type of real-time statistics collected, and the viewing mode.
	Edit	Allows users to view and change the Real-time Statistics Configuration properties.
Reports	Create and run any report	Allows users to display the Reports window. In combination with one of the following options, allows users to generate reports.
Reports– Agent Performances	Create and run any report	Allows users to modify the properties (including the schedule and selection criteria) of standard and user-defined performance reports, and produce ad hoc performance reports.
Reports–Call by Call	Create and run any report	Allows users to modify the properties (including the schedule) of standard and user-defined call-by-call reports, and produce ad hoc call-by-call reports.
Reports– Other	Create and run any report	Allows users to modify the properties of standard and user-defined configuration reports, and produce ad hoc configuration reports.

Function	Privilege	Description
Scheduler	View	Allows users to display the Scheduler window and view the scheduled date and time of scheduled events. These events include all server activities that are scheduled to run unattended, including report generation, agent to skillset and agent to supervisor assignments, and backups.
	Edit	Allows users to display the Schedule window and view and change the date and time of scheduled events.
	Create/Delete	Allows users to display the Schedule window and view, change, and delete scheduled events.
Script Variables	View	Allows users to view the Script Variables window and view the properties of any script variable.
	Edit	Allows users to view the Script Variables window and view and change the properties of any script variable.
	Create/Delete	Allows users to view the Script Variables window and view, change, add, and delete script variables.
Scripts	View	Allows users to display the window and view scripts in the Script Editor.
	Edit	Allows users to display the window and view and change scripts in the Script Editor.
	Create/Delete	Allows users to display the window, view and change scripts in the Script Editor, as well as add and delete scripts.
Serial Ports	View	Allows users to display the Serial Ports window and view properties for all serial ports.
	Edit	Allows users to display the Serial Ports window and view and change properties for all serial ports.

Function	Privilege	Description
Server Performance Monitor	View	Allows users to display the Server Performance Monitor. This monitor displays information about processing capacity, memory, and storage space.
Server Settings	View	Allows users to display detailed information about the server, such as the software release it is running and its serial number.
Skillset Threshold Classes	View	Allows users to view the Skillset Threshold Classes property sheet for skillset threshold classes.
	Edit	Allows users to view and change properties for skillset threshold classes.
	Create/Delete	Allows users to view, change, add, and delete properties for skillset threshold classes.
Skillsets	View	Allows users to display the Skillsets window, view the properties for all skillsets, and view the Global Settings.
	Edit	Allows users to display the Skillsets window, view and change the properties for all skillsets, and view and change the Global Settings.
	Create/Delete	Allows users to display the Skillsets window, view change, add, and delete skillsets, and view and change the Global Settings.
Switch Resource	View	Allows users to view the Switch Resource properties. These properties display information about the switch type.
	Edit	Allows users to view and change the Switch Resource properties.

Function	Privilege	Description
Users	View reporting agents only	Allows users to display the Users window and view properties for reporting agents.
	View and edit reporting agents only	Allows users to display the Users window and view and change properties for reporting agents.
	Edit all agents–create agents only	Allows users to display the Users window and view, change, create, and delete any agents.
	View all users	Allows users to display the Users window and view properties for all desktop users, supervisors, and agents.
	Edit all users	Allows users to display the Users window and view and change properties for all desktop users, supervisors, and agents.
	Edit all users– create any type	Allows users to view the Users window and view, change, add, and delete desktop users, supervisors, and agents.
Voice Ports	View	Allows users to display the Voice Ports window and view properties for all voice ports.
	Edit	Allows users to display the Voice Ports window and view and change properties for all voice ports.

Section B: Working with desktop user accounts

In this section

Overview of desktop user accounts

Introduction

A desktop user account is an account that uses the client application to access the Symposium Call Center Server. You must create a desktop user account for each user who requires access to the server. You must also assign each account to the access class that gives the user the privileges she or he needs to perform his or her job.

Adding desktop user accounts

Introduction

When you create a desktop user account, the account is assigned the default password, **password**. When the user logs on to the server, he or she is prompted to change the password. The user can also change his or her password by logging on to the server and choosing Utilities → Change Password.

To add desktop user accounts

1 From the SMI window, choose User Administration → Users.

   Result: The Users window appears.

2   Choose File → New.

Result: The User Configuration dialog box appears.

3   Click Desktop.

Note: If this user will also have Agent capabilities, select Call Center Agent (for more information about setting up agents, see Chapter 8, "Managing agents"). If this user will also have Supervisor capabilities, select Call Center Supervisor (for more information about setting up supervisors, see Chapter 7, "Managing supervisors").

4   Click OK.

Result: The New User property sheet appears.
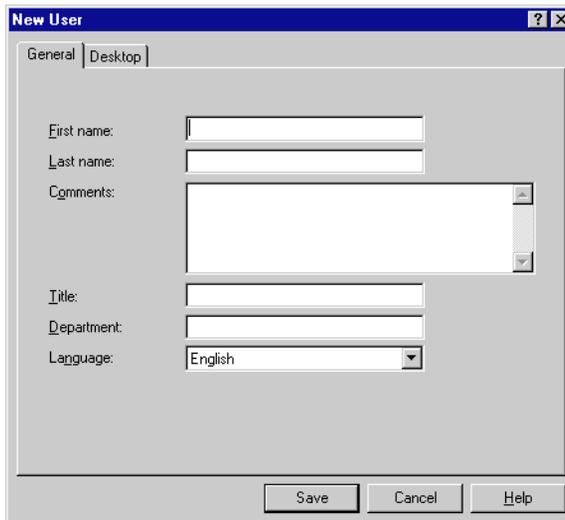
5   Enter the user's contact information in the fields on the General property page.

6   Click the Desktop tab.
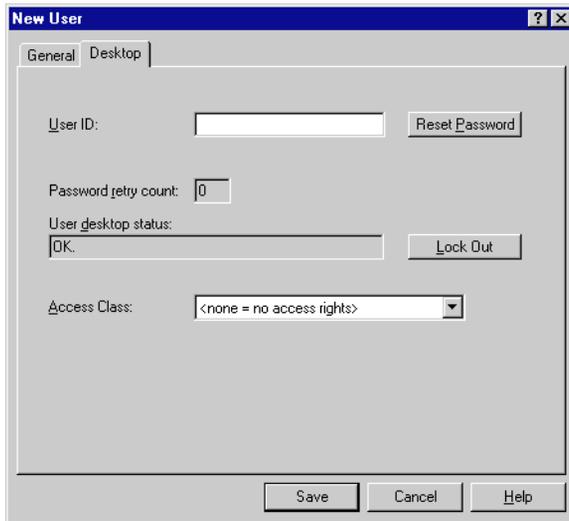
Result: The Desktop property page appears.

7   Enter information into the following boxes:

User ID: The user ID with which the desktop user will log on to the server. You cannot change the user ID after you save the user account.

Note: You may need to confirm that the user ID (login ID) is configured at the switch, before the user can log on to the system.

Access Class: The access class to which you want to assign the user.

Note: The access class must already exist (for more information about adding access classes, see "Adding access classes" on page 29).

Password retry count: The desktop Password retry count shows the number of times the user has tried to log on, and failed. Once a user is locked out, you must set the password retry count to zero. To do this, restore the User desktop status to OK by clicking Restore.

User desktop status: The User desktop status shows whether the user currently has access to the system. A user's status can be OK or Locked Out. Users are locked out under the following conditions:

- when the system administrator locks them out manually, as in the preceding example (see "Controlling access to the server" on page 51)

- when the user tries and fails to log on the maximum number of times

8 Click Save to save your settings and return to the Users window.

Note: If you click Save before you enter the necessary information, you are prompted to complete the required fields.

Result: The new user appears in the list of users.

9 To return to the SMI window, choose File → Close.

Controlling access to the server

Introduction

This section provides instructions for restricting and restoring access to the server for individual desktop users.

To prevent users from accessing the server

ATTENTION	If the desktop user you want to lock out is currently logged on, log the desktop user off (see "Logging users off" on page 61).

1   From the SMI window, choose User Administration → Users.

Result: The Users window appears.

2   Select the user you want to prevent from accessing the system.

3   Choose File → Properties.

Result: The User Properties property sheet appears.

4   Click the Desktop tab.

Result: The Desktop property page appears.
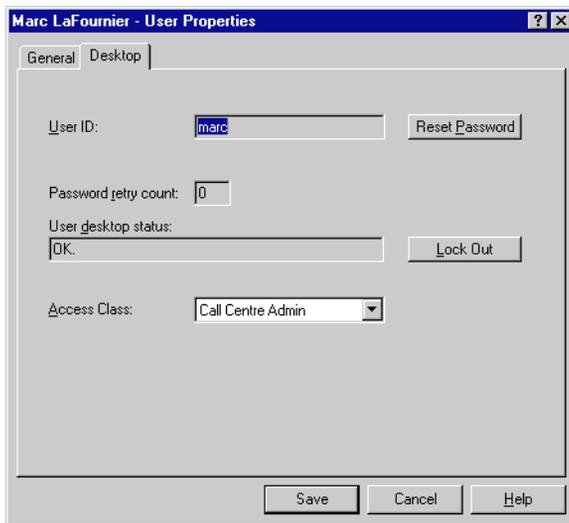
5   Click Lock Out.

Result: The User desktop status changes to Locked out by an administrator. This continues to be the current status of the user until an administrator restores it to OK. The Lock Out button changes to Restore.

6   Click Save.

Result: You return to the Users window.

7   To return to the SMI window, choose File → Close.

To restore a user's access to the server

Note: Use this procedure when a user is locked out of the system after exceeding the password retry count, or after an administrator manually locks out a user.

1   From the SMI window, choose User Administration → Users.

Result: The Users window appears.

2   Select the user whose access you want to restore.

3   Choose File → Properties.

   Result: The User Properties property sheet appears.

4   Click the Desktop tab.
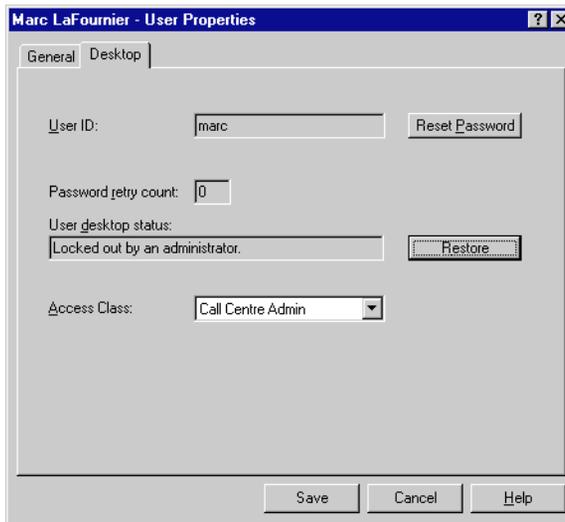
5   Click Restore.

   Result: The User desktop status changes to OK. The Restore button changes to Lock Out.

6   Click Save.

   Result: You return to the Users window.

7   To return to the SMI window, choose File → Close.

Resetting desktop passwords

When to use

Follow this procedure when a user has forgotten his or her desktop password. By resetting the user's password, you restore the default password, which is "password." Once the user is able to logon again, then he or she needs to change the default password.

Notes:

■   You cannot change a user's password. To change his or her password, the user logs on to the server, and choose Utilities → Change Password.

■   When you reset the user's desktop password, he or she might be locked out of the server. If this happens, restore the user (see "To restore a user's access to the server" on page 52).

To reset the desktop password

1   From the SMI window, choose User Administration → Users.

Result: The Users window appears.

2   Select the user whose desktop password you want to reset.

3   Choose File → Properties.

Result: The User Properties property sheet appears.

4   Click the Desktop tab.

      Result: The Desktop property page appears.
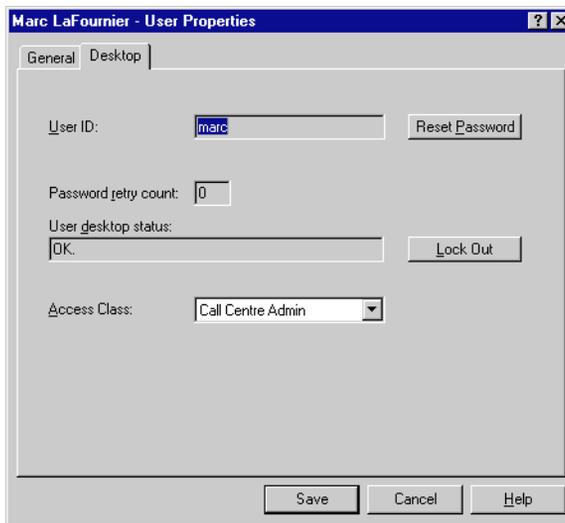
5   Click Reset Password.

      Result: A dialog box appears indicating that the user will have to use the password "password" to log on next time.

6   Click Yes to confirm.

7   Click Save.

      Result: You return to the Users window.

8   To return to the SMI window, choose File → Close.

Other procedures for desktop users

To change the capabilities of a desktop user

You can assign or revoke supervisor and agent capabilities for a desktop user.

From the Users window, select the desktop user you want to change, and choose File → Configuration.

For step-by-step instructions, press F1 to access the online Help.

To the properties of a desktop user

ATTENTION   Ensure that the user is not logged on when you change his or her access class. If the user is logged on, the server logs the user off when you make the change.

From the Users window, select the desktop user you want to change, and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview the list of users (including desktop users)

From the Users window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print the list of users (including desktop users)

From the Users window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete a desktop user

Note: If you delete a user who is currently logged on, the user is automatically logged off.

On the Users window, select the desktop user you want to delete, and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Section C: Managing user sessions

In this section

Viewing connected users

When to use

Follow the procedure in this section to check the status of a desktop user's connection to the server.

To view a list of connected users

1   From the SMI window, choose System Administration → System Configuration → Connected Sessions.

Result: The Connected Sessions window appears. This list displays how many desktop users are connected, their user IDs, where users are connected from (their network address), and the time of their last activity on the system.

2   To return to the SMI window, choose File → Close.

To print a list of connected users

Choose File → Print from the Connected Users window.

The list tells you how many desktop users are connected, where they are connected from (network address), and their user IDs. For step-by-step instructions on printing, access the online Help.

Logging users off

When to use

Follow the procedure in this section to disconnect a user from the server.

Note: This procedure disconnects and logs users off immediately. The disconnected user is not warned.

To log a user out

1   From the SMI window, choose System Administration → System Configuration → Connected Sessions.

Result: The Connected Sessions window appears.
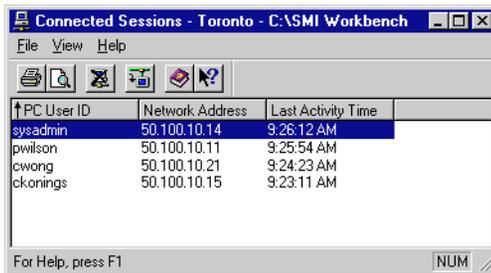
2   Select the PC User ID of the user you want to disconnect.

3   Choose File → Disconnect Session.

Result: You are prompted to confirm that you want to disconnect the user, since this action logs the user off immediately.

4   Click Yes.

Result: You return to the Connected Sessions window. The user is no longer on the list.

5   To return to the SMI window, choose File → Close.

Section D: Maintaining system security

In this section

Changing Nortel Networks user account passwords

Introduction

To maintain system security, change passwords regularly and store them in a secure location.

Default accounts and passwords

The following Windows NT accounts are created on the server during the installation procedures at the factory.

- Administrator
- NGenSys
- NGenDist
- NGenDesign

For more information about these accounts and their passwords, refer to the *Installation and Upgrade Guide*.

ATTENTION   The on-site installer is instructed to change all default passwords as part of the on-site installation procedures.

All passwords can be changed by using the procedures in this section. Change all passwords regularly to maintain system security.

If server software is reinstalled, the default accounts and passwords are recreated and passwords must be changed.

When to change passwords

Passwords should be changed at the following times:

- during the initial system setup after the operating system is installed

- at regular intervals for maximum security
- if you experience trouble logging on to Windows NT
- if server software is reinstalled (the default accounts and passwords are recreated, so passwords must be changed)

Note: If you require support from Nortel Networks or your distributor, you must tell them the new passwords.

Password guidelines

Write down any new passwords and store them in a secure place for future reference. Passwords are case-sensitive.

New passwords should be

- unique
- alphanumeric (they should contain at least one number)
- a minimum of six characters
- not nouns

Example
xyd45fst

To change the Administrator password

1   Log on as Administrator.

2   Press Ctrl-Alt-Del.

   Result: The Windows NT Security dialog box appears.

3   Click Change Password.

Result: The Change Password dialog box appears.

4   In the Old Password box, enter the current password.

5   In the New Password box, enter the new password.

Note: Ensure the password meets the requirements described earlier in "Password guidelines" on page 65.

6   In the Confirm Password box, enter the new password again.

7   Click OK.

Result: A dialog box appears indicating that the password has been successfully changed.

8   Click OK.

Result: You return to the Windows NT Security dialog box.

9   Click Cancel to close the Windows NT Security dialog box.

10   Record the password and store it in a safe, secure place away from the server.

To change the NGenDist and NGenDesign passwords

Note: You are not required to change the NGenSys password. If you change the NGenSys password, you must apply the same password change to the MAS Backup/Restore service.

1   Log on as Administrator.

2   Click Start → Programs → Administrative Tools (Common) → User Manager for Domains.

Result: The User Manager window displays a list of available user accounts, including NGenDist and NGenDesign.

3 Double-click the NGenDist icon.

   Result: The User Properties window appears.

4 In the Password field, type the new password.

   Note: Ensure that you use a password that contains a combination of numbers and letters (see "Password guidelines" on page 65).

5 In the Confirm Password field, type the same password entered in the Password field.

6 Click OK to close the User Properties window.

7 Repeat steps 3 to 6 for NGenDesign.

8 Select Exit to save changes.

9 Record these passwords and store them in a secure place away from the server.

   Note: If you have changed the NGenSys password, continue with the following procedure.

To change the NGenSys password for MAS Backup/Restore service

   Note: This procedure is required only if you change the Windows NT user account password for NGenSys.

1 Click Start → Settings → Control Panel.

2 Double-click Services.

   Result: The Services dialog box appears.
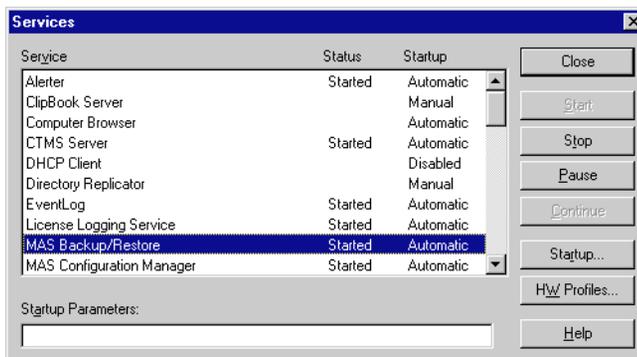
3 Scroll to MAS Backup/Restore service and select it.

4 Click Startup.

Result: The Service dialog box appears.

5 In the Log On As section, fill in the Password and Confirm Password boxes with the current NGenSys password.

Note: Use the same password you assigned to NGenSys in "To change the NGenDist and NGenDesign passwords" on page 66.

Changing pcANYWHERE32 passwords

Introduction

During the installation and configuration of pcANYWHERE32, you specify logon passwords. To maintain security, you can change these passwords periodically.

Note: To simplify the remote logon process, Nortel Networks recommends that you match the pcANYWHERE32 caller passwords for NGenDist and NGenDesign to the Nortel Networks user account passwords for NGenDist and NGenDesign. Change the pcANYWHERE32 passwords when you change the Nortel Networks user account passwords for NGenDist and NGenDesign.

To change passwords

1   Choose Start → Programs → pcANYWHERE32 → pcANYWHERE.

   Result: pcANYWHERE32 starts.

2   Select Be a Host PC.

3   Click Network.

   Note: Do not double-click the icon or you will begin a pcANYWHERE32 session.

4   Choose File → Properties.

   Result: The Network Properties sheet appears.

5   Click the Callers tab.

6   Click Specify individual caller privileges.

7   Right-click the NGenDist icon, and then choose Properties.

8   Click the Settings tab.

9   In the Password field, type a new NGenDist password.

10   In the Confirm Password field, type the NGenDist password again.

11   Click Apply.

12   Click OK.

13   Click the NGenDesign icon.

14   Repeat steps 8 to 12 to create a new password for NGenDesign.

15   Click OK to return to the main pcANYWHERE32 window.

16   Exit pcANYWHERE32.

Checking server events for suspicious activity

Security events

Security auditing is enabled on the server. Suspicious actions by a user are logged as event code 40593 in the Event Browser in the SMI window on the client and in the security log in the Windows NT Event Viewer. The severity of the event depends on the severity of the condition that caused the event. If the severity is information, the event does not appear in the Alarm Monitor.

Chapter 3

Administering the switch

In this chapter

Overview

Acquired resources

Certain resources must be configured to enable Symposium Call Center Server to acquire them from the switch. These resources include

- CDNs (Controlled Directory Numbers)
- phonesets
- voice ports

When you configure these resources on the server, you add them to a catalog maintained by the server. At startup, or whenever you make a change to the catalog of resources (for example, if you add a phoneset), the server acquires these resources. When you acquire a resource, the switch sends messages, regarding the resource, to Symposium Call Center Server.

States of acquisition

The following table describes the states of acquisition:

IF the current state is	THEN
Not Acquired	The resource has just been created or deacquired.
Acquired-Pending	There is a request into the system to acquire the resource.
Acquired	The resource is acquired from the switch.
Acquired without Secondary DN (phonesets)	The server was not able to acquire the secondary DN.
Acquired Login (voice port)	The voice port has been acquired, and is in login state.
Acquired Logout (voice port)	The voice port has been acquired, and is in logout state.

IF the current state is	THEN
Acquired-Failed	A problem occurred during an attempt to acquire the resource. The server is unable to acquire it.
Deacquired-Pending	There is a request in the system to deacquire the resource.
Deacquired-Failed	There is a problem deacquiring the resource from the switch, and the system is unable to deacquire it.
Deacquired without Secondary DN (phoneset)	A phoneset that was in Acquired without Secondary DN state has been deacquired.
Deacquired failed on Secondary DN (phoneset)	A problem occurred during deacquisition of the phoneset, because the server was unable to deacquire the secondary DN.

Note: A change in the status of an acquisition is not automatically reflected in the resource window. To view the current status of the acquisition of a switch resource, select Refresh on the View menu.

Other resources

To make your reports easier to understand, you can assign names to the following resources:

- music/RAN (Recorded ANnouncement) routes

- activity (line of business) codes

- DNISs

ATTENTION	Information that is configured at the switch must match the configuration on the Symposium Call Center Server to ensure that the switch and the system can communicate and function properly.

Section A: Working with CDNs

In this section

Overview of CDNs

Introduction

A controlled directory number (CDN) enables incoming calls to be queued into the switch and enables messages to be sent to Symposium Call Center Server regarding these calls.

To ensure that the Symposium Call Center Server can track when calls are terminated at that CDN, you must first add a CDN at the switch, then at the server, then the system must acquire it.

Adding CDNs

Introduction

To enable the server to acquire a CDN, you must

1.   Define the CDN at the switch.

2.   Add the CDN on the Symposium Call Center Server.

ATTENTION   If you want agents to be able to identify the source site of incoming network calls, follow these steps:

1 Configure a network CDN for each source site. Assign a CDN Name that identifies the source site.

2 Tell the source site administrator which network CDN (dialable DN) to use to route calls to your site.

3 Configure your phoneset displays to display the CDN name

Before you begin

Make sure that the CDN is configured in the DNROUTE table on the switch. For more information, refer to the *Symposium and DMS Switch Guide* or the *Symposium and MSL-100 Switch Guide*.

To add a CDN

1   From the SMI window, choose Switch Administration → CDNs.

Result: The CDNs window appears.
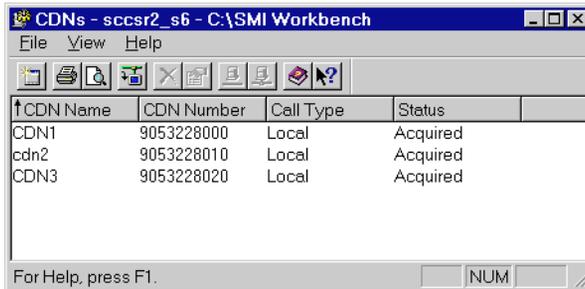
2   Choose File → New.

Result: The CDN Properties property sheet appears.
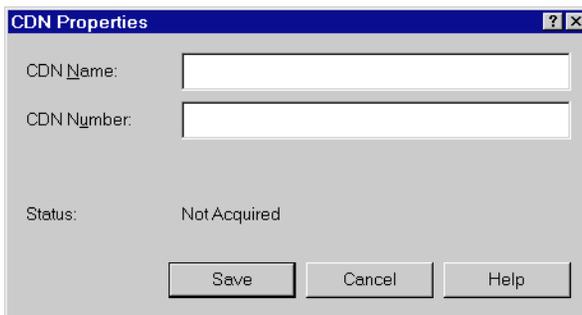
3   Enter information into the following boxes:

CDN Name: The name of the CDN, as it appears on reports.

CDN Number: The number that is passed to the switch in requests to acquire or deacquire the CDN. This number must be ten digits, and must match the number that is configured at the switch.

4   Click Save.

Result: The new CDN is added to the list in the CDNs window. It has the status Not Acquired.

5   To return to the SMI window, choose File → Close.

After you finish

Now that you have added the CDN, you must acquire it to enable the system to track calls terminated on it. To acquire the CDN, see "Acquiring and deacquiring CDNs" on page 82.

Acquiring and deacquiring CDNs

Introduction

Follow this procedure to request the system to acquire or deacquire a CDN. The Symposium Call Center Server must acquire a CDN so that it can track when calls are terminated at that CDN.

Note: Nortel Networks recommends that you deacquire a CDN before you configure it on the switch.

Before you begin

Make sure the CDN has been configured on the switch and added on the Symposium Call Center Server (see "Adding CDNs" on page 79).

To acquire or deacquire a CDN

1   From the SMI window, choose Switch Administration → CDNs.

    Result: The CDNs window appears.

2   Select the CDN you want to acquire or deacquire.

3   If you want to acquire the CDN, choose File → Acquire. If you want to deacquire the CDN, choose File → deacquire.

4   To refresh the CDN status on the display, choose View → Refresh.

5   Click Save.

    Result: You return to the CDNs window.

6   To return to the SMI window, choose File → Close.

Other procedures for CDNs

To change the name of a CDN

Notes:

1. You must deacquire a CDN before you change its name.

2. You cannot change the number assigned to a CDN once it has been saved. You must delete the CDN and recreate it with a new number.

Select the CDN you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview a list of CDNs

From the CDNs window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print a list of CDNs

From the CDNs window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete a CDN

Notes:

1. Before deleting a CDN, make sure that its status is one of the following: Not-Acquired, Acquired-Failed, or De-acquired-Failed.

2. This procedure does not delete the CDN from the switch.

On the CDNs window, select the CDNs you want to delete and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Section B: Working with music/RAN routes

In this section

Overview of music/RAN routes

Introduction

A music/RAN route is a resource installed on the switch that offers music or a recorded announcement to callers on hold. Callers can be transferred to music and RAN routes in one of the following ways:

- by the switch
- by a Symposium Call Center Server script
- by an agent

If you want to include a music/RAN route name on reports, you must define the route on the Symposium Call Center Server.

Adding music/RAN routes

Introduction

You must define music/RAN routes on the Symposium Call Center Server to enable the route names to appear on reports.

Before you begin

Make sure the route is configured in table ACDRTE on the switch. For more information, refer to the *Symposium and DMS Switch Guide* or the *Symposium and MSL-100 Switch Guide*.

To add a music/RAN route

1 From the SMI window, open Call Center Management → Switch Administration → Music/RAN Routes.

Result: The Music/RAN Routes window appears.
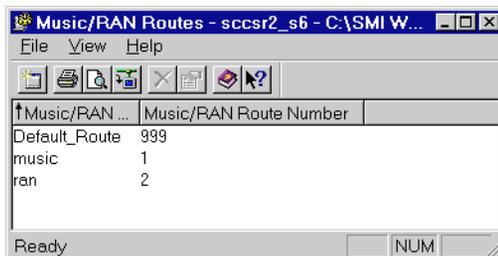
2   Choose File → New.

Result: The Music/RAN Routes Properties property sheet appears.

```
┌──────────────────────────────────────────────────────────────┐
│ Music/RAN Route Properties                              ? ☒   │
├──────────────────────────────────────────────────────────────┤
│ ┌─────────┐                                                    │
│ │ General │                                                    │
│ ├─────────┴───────────────────────────────────────────────┐   │
│ │                                                           │   │
│ │   Music/RAN Route Name:      ┌──────────────────────┐    │   │
│ │                              │                      │    │   │
│ │                              └──────────────────────┘    │   │
│ │   Music/RAN Route Number:    ┌──────────────────────┐    │   │
│ │                              │                      │    │   │
│ │                              └──────────────────────┘    │   │
│ │                                                           │   │
│ └───────────────────────────────────────────────────────────┘ │
│                      ┌────────┐   ┌────────┐   ┌────────┐      │
│                      │  Save  │   │ Cancel │   │  Help  │      │
│                      └────────┘   └────────┘   └────────┘      │
└──────────────────────────────────────────────────────────────┘
```

3   Enter information in the following boxes:

Music/RAN Route Name: The route name, as it appears on reports.

Music/RAN Route Number: The number of the music or RAN route, as it is configured at the switch.

4   Click Save.

Result: The route is added to the list in the Music/RAN Routes.

5   To return to the SMI window, choose File → Close.

Other procedures for music/RAN routes

To change the name of a music/RAN route

Note: You cannot change the number assigned to a music/RAN route once it has been saved. You must delete the route and recreate it with a new number.

On the Music/RAN Routes window, select the route you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview the list of music/RAN routes

From the Music/RAN Routes window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print the list of music/RAN routes

From the Music/RAN Routes window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete music/RAN routes

On the Music/RAN Routes window, select the routes you want to delete, and choose File → Delete.

Note: This procedure does not delete the route from the switch.

For step-by-step instructions, press F1 to access the online Help.

Section C: Working with phonesets

In this section

Overview of phonesets

Introduction

You must add and acquire each phoneset at which agents and supervisors will log on to the system. When the Symposium Call Center Server acquires a phoneset, the switch begins sending messages about the phoneset to the server.

Agent and supervisor phonesets

On the switch, each phoneset is associated with an ACD subgroup. Configure one phoneset in that subgroup as a supervisor set. Configure the remaining phonesets as ACD sets. An agent in the subgroup can log in at any ACD phoneset associated with the subgroup.

You associate agents and supervisors using the Agent to Supervisor application. For more information, see Chapter 9, "Managing agent to supervisor assignments."

Adding phonesets

Introduction

You must add and acquire each phoneset that you want to use with the Symposium Call Center Server so that the switch can send messages to the server when an agent logs on to the phoneset.

Before you begin

Configure the phoneset on the switch with the SERVORD utility. For more information, refer to the *Symposium and DMS Switch Guide* or the *Symposium and MSL-100 Switch Guide*.
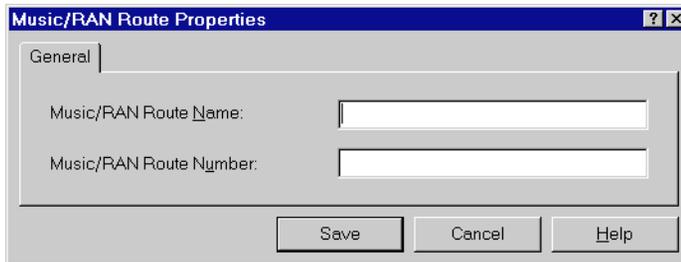
To add a new phoneset

1   From the SMI window, choose Switch Administration → Phonesets.

Result: The Phonesets window appears.
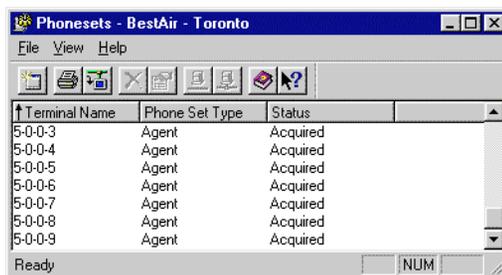
2   Choose File → New.

Result: The Phoneset Properties property sheet appears.
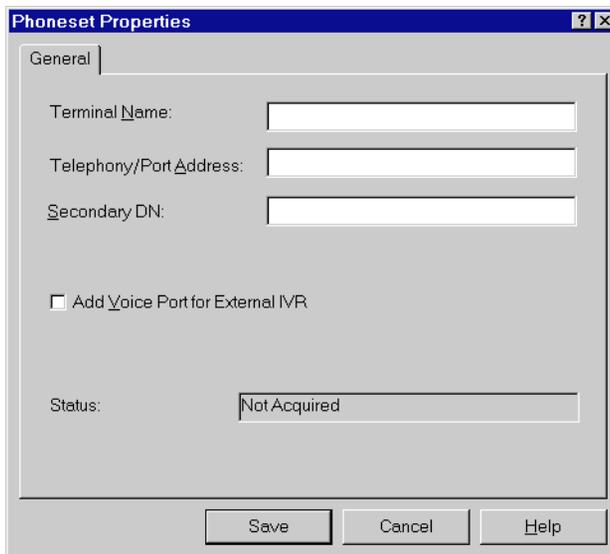
3   Enter information into the following boxes:

Terminal Name: The name of the phoneset, as it will appear on reports.

Telephony/Port Address: The address of the ACD phoneset on the telephony server. This must match the Position ID configured on the switch.

Secondary DN: The DN at which the agent can be reached for non-ACD calls.

4   Ensure that the Add Voice Port box is unchecked.

5   Click Save.

Result: The phoneset is added to the list in the Phonesets window. It has the status Not Acquired.

6   To return to the SMI window, choose File → Close.

After you finish

After adding the phoneset, you must acquire it so that the switch sends messages to the system when an agent logs on to the phoneset.

Acquiring and deacquiring phonesets

Introduction

You must acquire each phoneset, so that the switch sends a message to the system when an agent logs on to the phoneset.

Note: Nortel Networks recommends that you deacquire a phoneset before you configure it on the switch.

Before you begin

Make sure that the phoneset is configured on the switch, and has been added on the Symposium Call Center Server (see "Adding phonesets" on page 93).

To acquire or deacquire a phoneset

1 From the SMI window, choose Switch Administration → Phonesets.

   Result: The Phonesets window appears.

2 Select the phoneset you want to acquire or deacquire.

3 If you want to acquire the phoneset, choose File → Acquire. If you want to deacquire the phoneset, choose File → De-acquire.

   Result: The phoneset status changes to Acquired (or Deacquired) pending.

4 To refresh the phoneset status on the display, choose View → Refresh.

5 To return to the SMI window, choose File → Close.

Other procedures for phonesets

To change the name of a phoneset

Notes:

1. You must deacquire a phoneset before you change its properties.

2. You cannot change the telephony/port address or secondary DN assigned to a phoneset. To change these properties, delete the phoneset and recreate it.

On the Phonesets window, select the phoneset you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview the list of phonesets

From the Phonesets window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print the list of phonesets

From the Phonesets window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete a phoneset

Notes:

1. Before deleting the phoneset from the system, ensure that the phoneset status is either Not-Acquired, Deacquire Failed, or Acquired-Failed. You cannot delete a phoneset if it is Acquired.

2. This procedure does not delete the phoneset from the switch.

On the Phonesets window, select the phoneset you want to delete and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Section D: Working with voice ports

In this section

Adding voice ports

Introduction

A voice port is defined as a 2500 phoneset for third-party IVR systems. To add a voice port, you must add a phoneset and then configure it as a voice port.

Limitations

You can define up to 500 voice ports.

Before you begin

Make sure that the voice port is configured on the switch. For more information, refer to the *Symposium and DMS Switch Guide* or the *Symposium and MSL-100 Switch Guide*.

To add a phoneset for voice port

1   From the SMI window, choose Switch Administration → Phonesets.

Result: The Phonesets window appears.

2   Choose File → New.

Result: The Phoneset Properties property page appears.

3   Enter information into the following boxes:

Terminal Name: The name of the phoneset, as it will appear on reports.

Telephony/Port Address: The address of the voice port on the telephony server. This must match the Position ID configured for the voice port on the switch.

4   Ensure that the Add Voice Port box is checked.

5   Click Save.

Result: The phoneset is added to the list in the Phonesets window.

6   To return to the SMI window, choose File → Exit.

To add a voice port

1   From the SMI window, choose Switch Administration → Voice Ports.
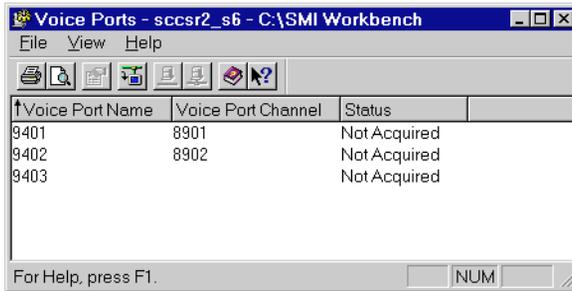
Result: The Voice Ports window appears.

2   From the Voice Ports window, select the phoneset that you added.

3   Choose File → Properties.

Result: The Voice Port Properties property sheet appears.
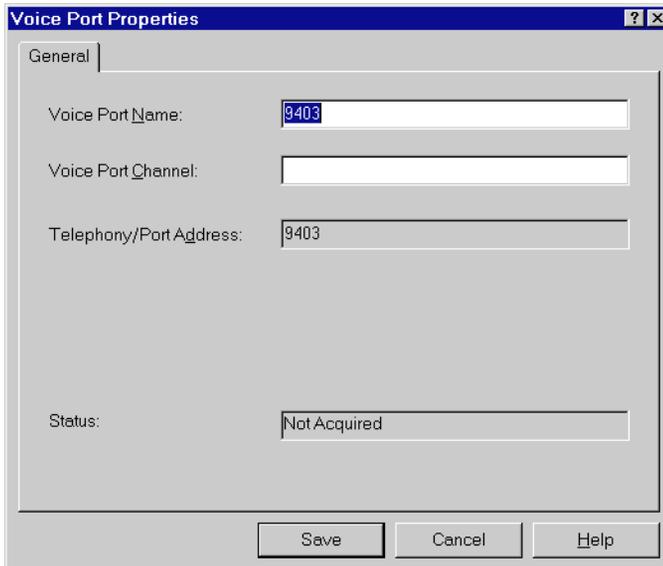
4   Enter information into the following boxes:

Voice Port Name: The name of the voice port as it appears on reports, if it is different from the phoneset name.

Voice Port Channel: The number that is passed to the telephony server in requests to acquire or deacquire the voice port.

5 Click Save.

6 The voice port channel number is added to the list in the Voice Ports window.

7 To return to the SMI window, choose File → Close.

After you finish

After adding voice port, you must acquire it so that the switch sends messages to the system.

Acquiring and deacquiring a voice port

To acquire or deacquire a voice port

Note: Nortel Networks recommends that you deacquire a voice port before you configure it on the switch.

1   From the SMI window, choose Switch Administration → Voice Ports.

Result: The Voice Ports window appears.

2   Select the voice port you want to acquire or deacquire.

3   If you want to acquire the voice port, choose File → Acquire. If you want to deacquire the voice port, choose File → De-acquire.

4   To refresh the voice port status on the display, choose View → Refresh.

Other procedures for voice ports

To change the name of a voice names

Note: You cannot change the channel or telephony/port (phoneset ID) address assigned to a voice port. To change these properties, you must delete the voice port and recreate it with the new channel.

On the Voice Ports window, select the voice port you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview a list of voice ports

From the Voice Ports window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print a list of voice ports

From the Voice Ports window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete a voice port

Note: Before deleting a voice port from the system, ensure that the voice port status is either Not-Acquired, Deacquire Failed, or Acquired-Failed.

On the Voice Ports window, select the voice port you want to delete and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Section E: Working with activity codes

In this section

Overview of activity codes

Introduction

An activity (line of business) code is a number that an agent enters on the phoneset keypad during a call. The system uses activity codes to keep track of the amount of time that is spent on the various types of incoming calls, for example, Sales or Service calls. You can then generate reports on activity codes.

System default activity code

The server ships with a system default activity code, which cannot be changed or deleted. The system default activity code is assigned to calls that are not queued to a skillset and if no other activity code is assigned.

Adding activity codes

Introduction

You can use activity codes to track time spent on different types of calls. If you do not create activity codes, agents can still enter activity code numbers and the system will report on them. However, when you run Activity Code reports, no names will appear on the reports.

Limitations

You can define up to 4998 activity codes.

Before you begin

Before you add an activity code, ensure that the line of business (LOB) feature is enabled on the switch. For more information, refer to the *Symposium and DMS Switch Guide* or the *Symposium and MSL-100 Switch Guide*.

To add an activity code

1   From the SMI window, choose Switch Administration → Activity Codes.

Result: The Activity Codes window appears.
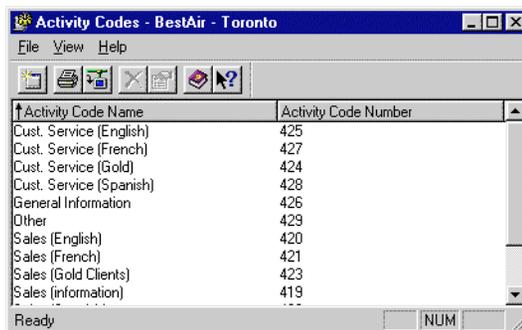
2   Choose File → New.

Result: The Activity Code Properties property sheet appears.

3   Complete the General property page by entering information into these boxes:

Activity Code Name: The name of the activity code, as it will appear on reports.

Activity Code Number: The number the agent will enter at a phoneset to select this activity code.

4   Click Save.

Result: The new activity code is added to the list in the Activity Codes window.

5   To return to the SMI window, choose File → Close.

Other procedures for activity codes

To change the name of an activity code

Note: You cannot change the number assigned to an activity code once it has been saved. To change the number, delete the activity code and recreate it with a new number.

On the Activity Codes window, select the activity code you want to and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview a list of activity codes

From the Activity Codes window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print a list of activity codes

From the Activity Codes window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete an activity code

Note: You cannot delete the System_Default_Activity_Code.

From the SMI window, on the Activity Codes window, select the activity code you want to delete and choose File → Delete.

Section F: Working with DNISs

In this section

Overview of DNISs

Introduction

You can report on the numbers (CDNs, ACD-DNs, and Supplementary DNs) dialed by your customers, using the Dialed Number Identification Service (DNIS). You must define each DNIS on which you wish to report.

Adding DNISs

Before you begin

Before you configure a new DNIS, ensure that the CDN, ACD-DN, or Supplementary DN is configured in the DNROUTE table on the switch. For more information, refer to the *Symposium and DMS Switch Guide* or the *Symposium and MSL-100 Switch Guide*.

Limitations

The server supports up to 10 000 DNISs.

To add a DNIS

1 From the SMI window, choose Switch Administration → DNISs.
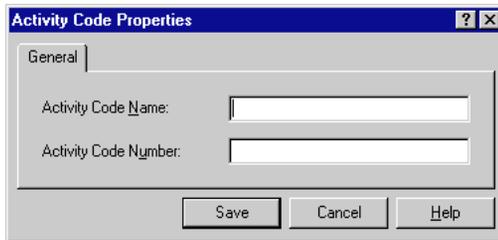
Result: The DNISs window appears.

2   Choose File → New.

   Result: The DNIS Properties property page appears.
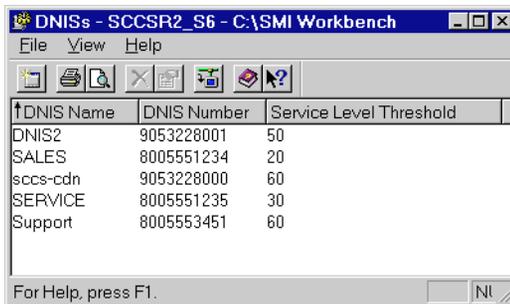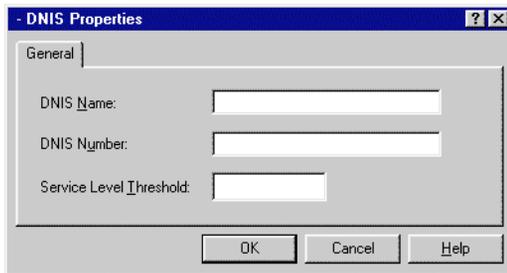
```
- DNIS Properties                                        [?][X]

  General

    DNIS Name:              [                              ]

    DNIS Number:            [                              ]

    Service Level Threshold: [           ]

                    [    OK    ]  [  Cancel  ]  [  Help  ]
```

3   Complete the General property page by entering information into these
         boxes:

   DNIS Name: The name of the DNIS, as it will appear on reports.

   DNIS Number: The ACD-DN, CDN, or Supplementary DN number, as it is
   configured on the switch. This number must be ten digits in length.

   Service Level Threshold: Specify the time (in seconds) within which all
   calls coming through on this DNIS should be answered or abandoned. This
   threshold value is used in real-time displays.

4   Click Save.

   Result: The DNIS appears in the list in the DNISs window.

5   To return to the SMI window, choose File → Close.

Other procedures for DNISs

To change the properties of a DNIS

Note: You cannot change the number assigned to a DNIS once it has been saved. You must delete the DNIS and recreate it with a new number.

On the DNISs window, select the DNIS you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview the list of DNISs

From the DNISs window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print the list of DNISs

From the DNISs window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete a DNIS

On the DNISs window, select the DNIS you want to delete and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Note: For the 3905 phoneset display, the Symposium Call Center Server supports 24 characters on the first line, and 18 characters on the second line.

Chapter 4

Managing threshold classes

In this chapter

Overview

Introduction

A threshold class is a set of options that specifies how statistics are treated in reports and real-time displays.

You can define threshold classes to apply different standards to different types of agents, skillsets, and so on. For example, you can create different agent threshold classes for customer service trainees and for senior customer service representatives. You can also create different skillset threshold classes for weekday performance and weekend performance.

The following types of threshold classes are available:

- agents
- skillsets
- applications
- nodal

Many of these threshold class types contain two types of thresholds: pegging thresholds (used for reports) and display thresholds (used for real-time displays).

Pegging thresholds

Pegging thresholds are used to accumulate historical statistical data. In a threshold class, you define a value that represents a cutoff limit for statistics such as short calls or the delay time before a call is answered or abandoned. Pegging thresholds allow you to define the length of a short call and the minimum delay before answer/abandon that you want to peg.

For example, you can create a skillset threshold that defines a short call as a call of less than ten seconds. Any calls that are less than ten seconds, and that are directed to skillsets with this threshold, are pegged as short calls and appear on short call reports.

Display thresholds

For display thresholds, you define two values—the low end and the high end of the normal range. When you create a real-time display, you can use colors to identify whether the value of the statistic is less than the low value, between the low and high value, or greater than the high value.

For example, in a skillset threshold class, you can specify low and high values for the Agent Available statistic. You might set the low value to 2, and the high value to 6. You can create a real-time display that displays this statistic in red if it is less than 2, in black if it is 3 to 6, and in blue if it is greater than 6.

Types of statistics available

The statistics that are available for a threshold class vary depending on the threshold class type. For a list of statistics by threshold class type, see "Thresholds" on page 126.

Adding threshold classes

When to use

Follow the procedures in this section to add a threshold class, add a threshold, and print a list of threshold classes.

To add a threshold class

1   From the SMI window, choose Reports & Displays → Statistics Configuration.

2   Double-click the threshold class type you want to configure (for example, Skillset Threshold Classes).

Result: The Thresholds Classes window for the selected threshold class type appears.
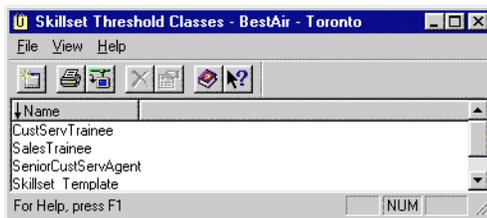
3   Choose File → New.

Result: A Skillset Threshold Class Properties page appears.

4   Enter the threshold class name.

5   Continue with the following procedure to add thresholds to a threshold class.

To add a threshold

1   From the Add Threshold drop-down list, select the statistic for which you want to define thresholds.

2   Click Add.

Result: The new statistic is added to the list of thresholds.

3   Enter information into the following boxes:

Level 1: For a display threshold, enter the value for the low end of the normal range. For a pegging threshold, enter the cutoff value for this statistic.

Level 2: Display thresholds only. Enter the value for the high end of the normal range.

4   Repeat steps 1 to 3 for each statistic for which you want to define thresholds.

5   Click Save.

   Result: The property page closes and the new threshold class appears in the Thresholds Classes window.

6   To return to the SMI window, choose File → Close.

Other procedures for threshold classes

Introduction

After you define a threshold class, you can change it or delete it. You can also print a list of threshold classes.

To rename a threshold class or add, delete, or change thresholds

Note: You cannot rename a threshold class if it is currently assigned to any objects.

On the Threshold Classes window, select the threshold class you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview a list of threshold classes

From the Threshold Classes window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To print a list of threshold classes

From the Threshold Classes window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To delete threshold classes

Note: You cannot delete a threshold class if it is currently assigned to any objects.

On the Threshold Classes window, select the threshold class and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Thresholds

Agent thresholds

Active

Type: Display

Description: Defines upper- and low-level thresholds for the Active state. Agents are in active state when they are handling a call on their Incalls key.

Busy

Type: Display

Description: Defines upper- and low-level thresholds for the Busy state.

Call Present

Type: Display

Description: Defines upper- and low-level thresholds for the Call Present state. Agents are in Call Present states when a call is ringing at their phonesets.

Consultation

Type: Display

Description: Defines upper- and low-level thresholds for the Consultation state. Agents are in Consultation state when they are in conference with another agent.

Emergency

Type: Display

Description: Defines upper- and low-level thresholds for the Emergency state. Agents go into Emergency state when they press the Emergency key on their phoneset.

Idle

Type: Display

Description: Defines upper- and low-level thresholds for the Idle state. Agents are in Idle state when they are waiting for a call.

Logout

> **Description:** Display

> **Type:** Defines upper- and low-level thresholds for the Logout state.

Not Ready

> **Type:** Display

> **Description:** Defines upper- and low-level thresholds for the Not Ready state. Agents go into Not Ready state when they press the Not Ready key.

Variable Wrap

> **Type:** Display

> **Description:** Defines upper- and lower- level thresholds for the Variable Wrap state. Agents go into Variable Wrap state if the variable wrap option is configured on the switch.

Walkaway

> **Type:** Display

> **Description:** Defines upper- and low-level thresholds for the Walkaway state. Agents go into Walkaway state when they go into Not Ready state with a reason code other than zero.

Application thresholds

%Abandoned_Aft_Threshold

> **Type:** Display

> **Description:** The percentage of calls abandoned for an application that are abandoned after the service level threshold.

%_Calls_Abandoned

> **Type:** Display

> **Description:** The percentage of calls offered for an application that are abandoned.

%Service Level

    Type: Display

    Description: The percentage of incoming calls answered within the period specified in the threshold class associated with this application.

Average_Abandon_Delay

    Type: Display

    Description: The average wait experienced by calls that were abandoned for an application.

Average_Answer_Delay

    Type: Display

    Description: The average wait experienced by calls that were answered for an application.

Calls Abandoned

    Type: Display

    Description: The number of calls abandoned for an application.

Calls Abandoned Delay

    Type: Display

    Description: The average wait experienced by calls that were abandoned for an application.

Calls Abdnd Aft Threshold

    Type: Display

    Description: The number of calls abandoned for an application after experiencing a delay greater than or equal to the service level for the application.

Calls Answd Aft Threshold

    Type: Display

    Description: The number of calls answered for an application after experiencing a delay greater than or equal to the service level for the application.

Calls Answd Dly At Skillset

Type: Display

Description: The delay time experienced by all calls from the time the call is first queued against the first skillset until it is answered.

Calls Answered

Type: Display

Description: The number of calls answered for an application.

Calls Answered Delay

Type: Display

Description: The total wait experienced by all calls answered for an application.

Calls Given Terminate

Type: Display

Description: The number of calls terminated with one of the following treatments:

- given force busy, force overflow, force disconnect, route to, or default treatment

Calls Offered

Type: Display

Description: The number of calls offered for an application.

Calls Waiting

Type: Display

Description: The number of calls for an application that are currently waiting to be answered.

Max Waiting Time

Type: Display

Description: The amount of time that the oldest call for an application has been waiting to be answered.

Service Level Threshold

Type: Pegging

Description: The number of seconds specified in your service level objective for this application. For example, if your service level objective is "eighty percent of calls are answered within 20 seconds," enter 20 here.

ShortCall

Type: Pegging

Description: The length, in seconds, of a short call for this application.

Waiting Time

Type: Display

Description: The total wait experienced by all calls for an application that are currently waiting.

Nodal thresholds

Calls Answered

Type: Display

Description: The number of calls answered at this site.

Calls Offered

Type: Display

Description: The number of calls offered at this site.

Calls Waiting

Type: Display

Description: The number of calls waiting at this site.

Skillset thresholds

%Service Level for Ans Calls

Type: Display

Description: The percentage of answered calls answered within the period defined in the threshold class for this skillset.

Agent Available

> **Type:** Display

> **Description:** The number of agents currently in Waiting state.

Agent In Service

> **Type:** Display

> **Description:** The number of agents assigned to a skillset who are currently logged on.

Agent Not Ready

> **Type:** Display

> **Description:** The number of agents logged on for a skillset who are currently in Not Ready state.

Agents On ACD-DN Call

> **Type:** Display

> **Description:** The number of agents logged on for a skillset who are currently handling ACD calls.

Agent On DN call

> **Type:** Display

> **Description:** The number of agents logged on for a skillset who are currently handling a DN call.

Agent on In call

> **Type:** Display

> **Description:** The number of agents logged on for a skillset who are currently handling a Symposium Call Center Server call.

Agents On Other Skillset Call

> **Type:** Display

> **Description:** The number of agents logged on for a skillset who are currently handling calls for skillsets other than this skillset.

> **Notes:**

> ■ Agents can be assigned to multiple skillsets.

■   Other skillsets can be local skillsets designed specifically for call handing at your location, or system skillsets that can be assigned from any site. An example of a system skillset is Agent Queue To.

Agents On This Skillset Call

Type: Display

Description: The number of agents logged on for a skillset who are currently handling a call for this skillset.

Agent Unavailable

Type: Display

Description: The number of agents logged on for a skillset who are unavailable to take calls.

Average_Answer_Delay_S

Type: Display

Description: The average wait experienced by calls answered for a skillset, from the time they were queued to the skillset to the time they were answered.

Calls Answd Aft Threshold

Type: Display

Description: The number of calls answered for a skillset after experiencing a delay greater than or equal to the service level for the skillset.

Calls Answered

Type: Display

Description: The number of calls answered for a skillset.

Calls Waiting

Type: Display

Description: The number of calls for a skillset that are currently waiting to be answered.

Expected Wait Time

Type: Display

Description: The total time a new call is expected to wait before being answered by an agent with the required skillset.

Longest Wait Since Last Call

Type: Display

Description: The longest idle time for all agents who are currently waiting to answer calls for a skillset. This idle timer is reset whenever a call is answered. For example, the longest waiting time since last call is currently 14 seconds; Mary and Jim have been idle 14 and 10 seconds, respectively. A call arrives and is presented to Mary. Her idle timer is set to 0, and the longest wait time is reset to 10. This statistic includes time that agents are in Not Ready state.

Longest Wait Since Login

Type: Display

Description: The longest waiting time of all idle agents who are currently waiting to answer calls for a skillset. This idle timer is reset when the agent logs on to the skillset. Waiting time is incremented until the agent answers a call. After the call ends, waiting time is incremented until the agent answers the next call.

Max Wait Time

Type: Display

Description: The amount of time that the oldest call for an application has been waiting to be answered.

Service Level Threshold

Type: Pegging

Description: The number of seconds specified in your service level objective for this skillset. For example, if your service level objective is "eighty percent of calls are answered within 20 seconds," enter 20 here.

ShortCall

Type: Pegging

Description: The length of a short call, in seconds, for this skillset.

Total Answered Delay

Type: Display

Description: The total wait experienced by all calls answered for a skillset from the time they were queued to the skillset until they were answered.

Total Wait Time

Type: Display

Description: The total waiting time for all calls for a skillset that are currently waiting.

Chapter 5

Working with displays and statistics

In this chapter

Section A: Real-time displays

In this section

Overview

Introduction

Real-time displays provide up-to-date statistics for your call center and its resources. You can use these statistics to monitor your call center and determine its effectiveness.

The information that each display shows is determined by the real-time display definition.

Types of real-time displays

The following types of real-time displays are available:

- agent
- application
- skillset
- nodal

Standard display definitions

The Symposium Call Center Server ships with a set of default, or standard, real-time display definitions. The contents of these real-time display definitions are predefined, and cannot be modified. Standard real-time display definitions are stored on the server.

User-defined display definitions

User-defined definitions are ones that you create yourself. You can modify these definitions at any time. They are stored on the client PC.

Statistics groups

The following summarized real-time statistics groups are used to gather real-time call processing data:

- application statistics
- skillset statistics
- agent statistics
- nodal statistics

You can choose the groups for which you will collect statistics. For more information about real-time display statistics groups, see "Configuring real-time statistics collection" on page 143.

Working with real-time displays

Configuring real-time statistics collection

You must configure the server to collect the types of statistics you want to include in your real-time displays. If the server does not collect application statistics, for example, the application real-time displays cannot be opened.

Managing formulas

You can use formulas to create customized real-time statistics fields for use in your real-time displays. To create formulas, you combine existing fields using mathematical operators.

Creating real-time displays

You can create user-defined real-time display definitions to display the type of information you need to monitor your call center. For more information, see the *Supervisor's Guide*.

Managing real-time displays

You can change, print a list of, or delete user-defined real-time display definitions. For more information, see the *Supervisor's Guide*.

Using real-time displays

You can view, sort, and print real-time displays. Supervisors can also filter agent and skillset real-time displays to show only their agents, all agents except their agents, or all agents. For more information, see the *Supervisor's Guide*.

Real-time displays and agent keys

Agents should not use the following keys on their phonesets:

- Hotline
- Private line
- Voice call
- Dial Intercom

The use of these keys results in incorrect agent statuses on the real-time displays.

Emergency key and consultations (DMS switch)

When an agent is in consultation with another agent (for example, during a transfer or conference), he or she cannot use the Emergency key. However, when the other agent drops off the call, this key become available again.

Managing real-time statistics collection

Introduction

The Symposium Call Center Server provides you with real-time statistics such as

■ agents available or unavailable in a skillset

■ calls waiting

■ expected waiting time

To use the real-time statistics feature of the Symposium Call Center Server, you must configure real-time statistics collection and create real-time displays.

Configuring real-time statistics collection

Real-time statistics are collected to monitor the performance of a call center as it happens. When you configure real-time statistics collection, you choose

■ the statistics groups for which statistics are to be collected

■ viewing modes for the different statistics groups (moving window or interval to date)

■ the start time and length of the interval in which real-time statistics are accumulated

■ the frequency with which real-time statistics are refreshed

Viewing modes

Moving window mode
In moving window mode, statistics shown represent the last ten minutes of system activity.

Interval to date mode
In interval-to-date mode, statistics are collected only for the current interval. When the interval is over, data fields initialize to zero and collection begins for the next interval.
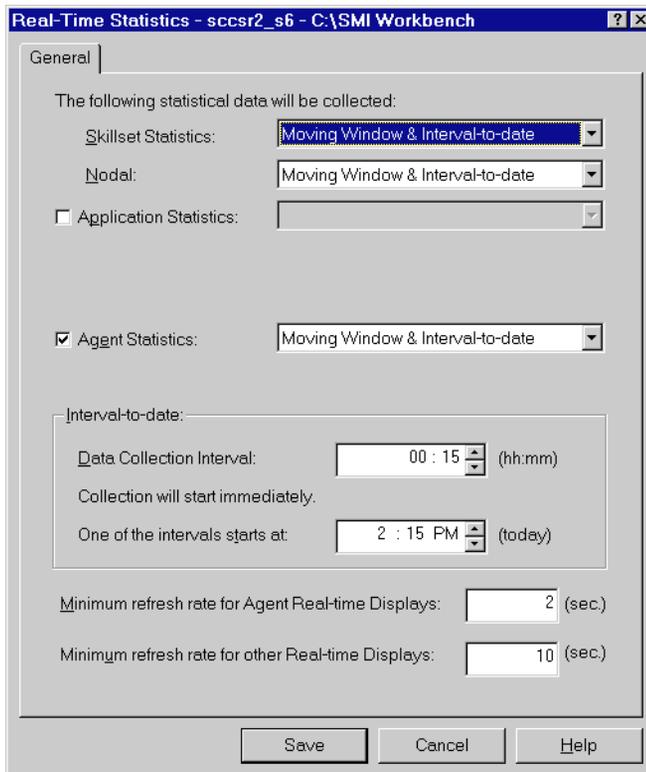
Refresh rates

The minimum refresh rate for the collection of real-time statistics data is applied to real-time displays across the entire system. A unique refresh rate can be defined for each individual real-time display, but it cannot be less than the minimum refresh rate defined for the entire system.

Configuring real-time statistics collection

To configure real-time statistics collection

1 From the SMI window, choose Reports & Displays → Statistics Configuration → Real-Time Statistics.

Result: The Real-Time Statistics Configuration property sheet appears.

2 On the General property page, make the desired changes to the general properties. You can change the following properties:

Skillset Statistics: The mode for skillset statistics collection. (For more information about modes, see "Overview" on page 138).

Nodal: The mode for nodal statistics collection.

Application Statistics: Whether to collect application statistics, and the mode for application statistics collection.

Agent Statistics: Whether to collect agent statistics, and the mode for agent statistics collection.

Data Collection Interval: The length of the period in which real-time statistics are accumulated. To ensure that intervals start at the same time each day, interval lengths can be one of the following: 15 minutes, 30 minutes, 45 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 6 hours, 8 hours, 12 hours, and 24 hours.

One of the intervals starts at: The start time for one of the intervals during a day. The system uses this information to calculate the start times of all other intervals.

For example, a system administrator is modifying the real-time statistics data at 3:00 p.m. He specifies four hours as the interval duration. Since the agents' shifts begin at 9:00 a.m., he wants one of the intervals to start every day at that time. He enters 9:00 a.m. as the value for this field. The system automatically calculates the start time for all other intervals to be 1:00 p.m., 5:00 p.m., 9:00 p.m., and 1:00 a.m. The change takes effect immediately, so at 5:00 p.m. the next interval begins.

Minimum refresh rate for Agent Real-time Displays: The minimum refresh rate for agent real-time displays.

Minimum refresh rate for other Real-time Displays: The minimum refresh rate for displays other than agent displays.

3   Click Save to save your changes.

Note: Nodal and skillset statistics are automatically collected by the system.

Managing formulas

Introduction

Use formulas to create custom real-time statistics fields by combining existing statistics fields with mathematical operators. For example, you can create a customized formula for calculating the service level.

These custom fields can be selected and used in your real-time displays. You can also define display thresholds for customized formulas.
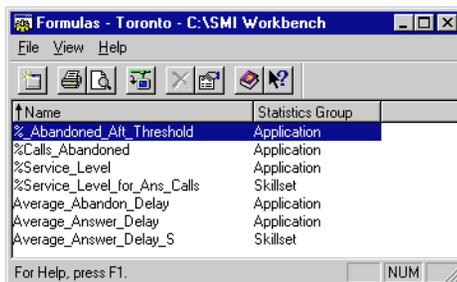
ATTENTION

Custom fields created by using formulas cannot be used in reports.

To create formulas

1   From the SMI window, choose Reports & Displays → Statistics Configuration → Formulas.

Result: The Formulas window appears.

2   Choose File → New.

3   Choose the statistics class (Agent, Skillset, Application, or Nodal) that you want to use.

Result: The Formula Properties property sheet appears.

4   Enter information into the following fields:

Formula Name: The name of your formula.

Comment: Optional. Additional information about the formula.

Definition: The definition of the formula. To add a variable, select it from the Column Name box. To add numbers or arithmetic operators to the definition, click on them. For example, to create a customized formula for service level, you might enter: Calls Answered – Calls Answered Aft Threshold / Calls Answered. The definition can be up to 250 characters long.

Notes:

- When you select a variable, it is placed in the Definition field, with a percent symbol (%) preceding it. The percent symbol identifies it as a variable; the symbol is not an operator.

- Not all operations buttons can be used at all times. Operations buttons that are not available appear dimmed.

- When you click the Max or Min button, an open bracket is automatically inserted.

5   Click Save to save your changes.

Result: The new formula is added to the list in the Formulas window.

6   To return to the SMI window, choose File → Close.

Other procedures for formulas

To change a formula

Note: You cannot change standard formulas.

On the Formulas window, select the formula and choose File → Open.

For step-by-step instructions, press F1 to access the online Help.

To print a formula

On the Formulas window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete a formula

Note: You cannot delete standard formulas.

On the Formulas window, select the formula and choose File → Delete.

For step-by-step instructions, click F1 to access the online Help.

CAUTION

Risk of data loss
The formula you are deleting might be used in existing real-time displays. If you delete a formula that is used in a display, then columns containing the formula appear as blank.

Section B: Managing historical statistics

In this section

Overview of historical statistics collection

Introduction

The Symposium Call Center Server enables you to report on such historical statistics as

- the number of calls an agent took during a specified period
- the number of calls that abandoned before an agent became available
- (optionally) call events

However, to do so, you must configure the server to collect these statistics.

Note: Call-by-call statistics are available only if you purchased the call-by-call statistics option, and the option has been activated using a keycode. The call-by-call statistics option is not available on a 2-Gbyte system.

Configuring historical statistics collection

When you configure historical statistics collection, you can choose

- the types of statistics to be collected
- the values for system parameters, such as number of agent positions, number of skillsets, and number of calls per hour
- how long historical statistics are stored on your system
- the applications for which call-by-call statistics are collected

The statistics are stored in the system database. The Historical Statistics Configuration window estimates required disk space for the options you have selected, and displays the amount of disk space available.

Statistics groups

A statistics group is a set of related statistics that can be collected for use in reports and displays. When you configure historical statistics, you choose the statistics groups for which you want to record statistics. The server provides the following statistics groups:

- activity code statistics
- agent performance statistics
- agent by application statistics
- agent by skillset statistics
- application statistics (see below)
- CDN statistics
- DNIS statistics
- music/RAN route statistics
- skillset statistics
- agent login/logout statistics
- call-by-call statistics

To manage your disk space usage, you can vary number and types of statistics you collect.

Applications

An application is a logical entity that represents a script for reporting purposes. The master script, and each script it references (that is, each primary script), has an application with a name that matches the script name.

Configuring historical statistics collection

Introduction

Use this procedure to configure the following options for historical statistics collection:

- the types of statistics to be collected

- the values for system parameters, such as number of agent positions, number of skillsets, and number of calls per hour

- how long historical statistics are stored on your system

- the applications for which call-by-call statistics are collected

This procedure also shows you how to calculate the amount of disk space required by your selected configuration.

Removal of expired statistics

Each day, the server deletes any historical data that has exceeded the allowable age for data of its type (defined on the Duration property page of the Historical Statistics Configuration window). If the size of the statistics database exceeds the size configured during installation, then the server deletes the oldest unexpired data to provide space for new data.

To configure historical statistics collection

1 From the SMI window, choose Reports & Displays → Statistics
Configuration → Historical Statistics.

Result: The Historical Statistics property sheet appears.

2 In the Call Flows box, check the call flow statistics that you want to collect,
and clear those that you don't want to collect. You can select the following
options:

Application: To collect application statistics, such as calls abandoned and
calls answered for an application.

CDN: To collect CDN statistics, such as calls offered to a CDN and calls
terminated on a CDN.

Skillset: To collect skillset statistics, such as active time, calls answered, and calls answered after threshold for a skillset.

Activity Code: To collect activity code (line of business) statistics, such as total call time charged to an activity code.

DNIS: To collect DNIS statistics, such as calls answered and abandoned for a DNIS number.

Music/RAN Route: To collect RAN and music route statistics, such as the number of times a RAN/music route was accessed, and the total amount of time it was in use.

Note: Options selected here apply to all applications defined in the system database. They cannot be applied to a selected group of applications.

3   In the Agent box, check the agent statistics that you want to collect and clear those that you don't want to collect. You can choose to collect the following types of statistics:

Performance: To collect agent performance statistics, such as number of ACD calls answered, conferenced, and transferred.

By-Application: To collect statistics, by agent, for individual applications. Statistics available include calls answered for the application and agent talk time for the application.

By-Skillset: To collect statistics, by agent, for individual skillsets. Statistics available include calls answered and short calls answered.

Login/Logout: To collect agent login and logout statistics.

4   Click the Parameters tab to configure system parameters.

Result: The Parameters property page appears.

For each parameter, this property page contains the following information:

Configured Value: The number to be used to calculate the required database size (for example, estimated number of activity codes).

Purchased Value: The maximum number you can configure (this number is controlled by keycodes).

Measured Value: The number currently defined in the system.

System Value: The maximum number that can be defined in the system, if all available options are installed.

Note: The measured value for skillsets includes the four system skillsets. The measured value for applications includes the system applications. The number varies depending on the options installed on your server, but may include Master_Script, ACD_DN_Application, and System_Application.

5   Click the Parameter Name for which you want to change the configured value. You can change the following parameters:

Active Agents: Purchased Value shows the number of agents logged in at any time. You cannot change the configured value for this parameter. Measured Value and System Value are not applicable to this parameter.

Agent Positions: The number of phonesets defined in the system. Purchased Value is not applicable to this parameter; the number of phonesets is not controlled by a license option.

Skillsets: The number of skillsets defined in the system. Allow for the four system skillsets. For example, if you want to have 25 skillsets, then enter 29 as your configured value.

Calls per hour: The estimated number of calls arriving at the call center within an hour. Measured Value is not applicable to this parameter, as you do not configure the number of calls allowed per hour.

DNISs: The number of DNISs defined in the system.

CDNs: The number of CDNs defined in the system.

Activity Codes: The number of activity codes defined in the system. Allow for the two default activity codes when you configure this value.

Agent Events per Day: The number of agent events (login, logout, walkaway, return from walkaway) that occur in one day. Measured Value is not applicable to this parameter, as you do not configure the number of events allowed per day. This estimate is used to calculate usage of disk space.

RAN Routes: The number of RAN routes defined in the system.

Music Routes: The number of music routes defined in the system.

Applications: The number of applications defined in the system. Based on the options installed on your server, up to five system applications might be installed. Allow for these applications when you configure this value.

Nodes: The number of nodes in the network. (Only one node is supported in the Symposium Call Center Server for DMS/MSL-100.)

IVR ports: The number of voice ports configured on the system.

Note: The values you enter here do not affect the size of the database. However, they do control the number of entities you can add to the database.

6   In the Selected Parameter group box, change the Configured Value as required.

7   Click the Duration tab to define the storage duration.

8   Enter a value for each of the following collection periods:

Interval: The number of days that interval statistics are stored by the system.

Daily: The number of days that daily statistics are stored by the system.

Weekly: The number of weeks that weekly statistics are stored by the system.

Monthly: The number of months that monthly statistics are stored by the system.

IVR Voice Port: The number of days IVR voice port login and logout statistics are stored by the system.

Agent login and logout: The number of days that agent login and logout statistics are stored by the system.

First business day of the week: The day defined as the first business day of the week. Weekly statistics are cumulated automatically at the beginning of the day designated as the first business day.

Length of business day: The number of hours per business day that the system collects historical statistics.

Business week contains: The number of business days per week that the system collects historical statistics.

Call by call: The number of days call-by-call statistics are stored by the system. In a Symposium Call Center Server network, use the same value for all servers in the network.

Note: These values are used to calculate the size of the database. They do not affect statistics collection.

9   Click the Call-by-Call tab to select applications for call-by-call statistics collection.

The list contains all applications defined on your server. You can choose whether to collect call-by-call statistics for local calls, network calls, both, or neither.

10   To change the call-by-call statistics collection method for an application, click in the Call-by-Call column beside the application, and select one of the following options:

■   **local calls**—For calls originating on the local server, collect call event data for local events. Data collection ends when the call terminates.

■   **none**

11   To determine the disk space requirements of your selected configuration, click Calculate.

12   The Required fields are updated to show the disk space requirement of the selected configuration. The Actual fields show the disk space available.

13   Click Save to save your changes.

Note: The Save button is enabled only if the Required value (disk space requirement of the selected configuration) is less than the Actual value (disk space available). If the Save button is not enabled, you must modify your configuration.

Managing skillsets and call presentation

In this chapter

Overview of skillsets and call presentation

Introduction

This chapter provides instructions on how to define and configure call presentation classes and skillsets. These features, in conjunction with scripts, determine how and when calls are presented to agents. To understand the operation of your call center, you must understand how these features function.

Skillsets

A skillset is a set of capabilities necessary to answer a specific type of call. Skillsets are the basic building blocks of skill-based routing. They are used to match callers with the agents who can best meet their needs.

Call presentation

Call presentation is the matching of available agents with calls in the queue. The order in which calls are presented is determined by the following parameters:

- call priority, as specified in the script
- call age

The agent to which a call is presented is determined by the following parameters:

- agents' priority for the skillset to which the call is being presented
- agents' idle time

Section A: Managing call presentation classes

In this section

Overview of call presentation classes

Introduction

Call presentation is the matching of available agents with calls in the queue. How the server presents calls to agents varies depending on the call presentation calls to which the agent belongs. In your agent call presentation classes, you can configure the following options.

Presentation of calls to agents

You can configure calls to be presented to an agent phoneset. If a call is not answered after a specific length of time, it can

- be returned to the skillset queue, or
- remain queued to the agent phoneset until it is answered or abandoned

Conditions for receiving calls

You can choose whether agents can receive incoming calls when they are in Not Ready state on their secondary directory number (DN). (This option must also be configured at the switch.)

Adding call presentation classes

To add a call presentation class

1   From the SMI window, choose Call Flow Administration → Call Presentation classes.

Result: The Call Presentation Classes window opens.

2   Choose File → New.

Result: The Agent Call Presentation Class Properties property sheet appears.
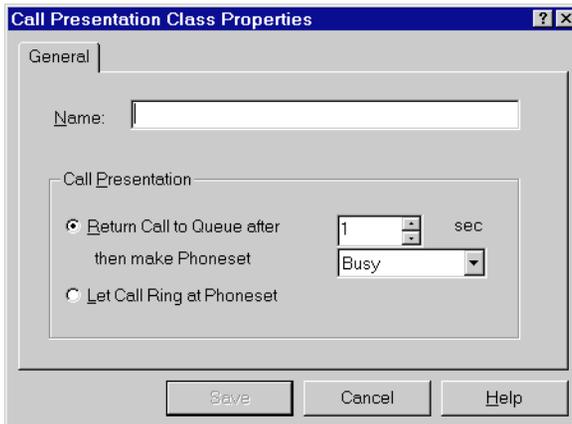
3   Enter information into the following boxes:

Name: The name of the call presentation class, as it will appear in drop-down lists and on reports.

Call Presentation: Select one of the following call presentation options:

- Return Call to Queue After—The call is returned to the queue if not answered within the time you specify. You can also choose the mode in which the phoneset is placed after the call is returned to the queue.

  Note: The time you specify here must be less than the ringing threshold for the ACD group, or the call will be sent to the ACD group's threshold destination.

- Let Call Ring at Phoneset—The call rings at the phoneset until it is answered or abandoned.

4   Click Save.

5   To return to the SMI window, choose File → Close.

Other procedures for call presentation classes

Introduction

After you define a call presentation class, you can change it or delete it. You can also print a list of call presentation classes.

To change call presentation class properties

On the Call Presentation Classes window, select the call presentation class you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview a list of call presentation classes

From the Call Presentation Classes window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To print a list of call presentation class

From the Call Presentation Classes window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To delete call presentation classes

Note: You cannot delete a call presentation class that is assigned to an agent.

On the Call Presentation Classes window, select the call presentation class you want to delete and choose File → Delete.

Section B: Skillsets and skill-based routing

In this section

Skillsets

Introduction

A skillset is a set of capabilities necessary to answer a specific type of call. Skillsets are the basic building blocks of skills-based routing. They are used to match callers with the agents who can best meet their needs.

You can assign agents to skillsets by two methods:

- the agent's Skillsets property page (see "To assign skillsets" on page 211)
- agent to skillset assignments (see Chapter 10, "Managing agent to skillset assignments")

Examples of skillsets

BestAir has several different skillsets:

- **Bookings:** Agents who can accept and change bookings, and provide schedule and rate information.
- **Shipping:** Agents who can arrange for shipment of goods. Additional skillsets include agents who specialize in shipment of perishable food products and hazardous goods, as well as international shipments.
- **Cargo Tracing:** Agents who specialize in the tracing of shipments and personal luggage.
- **BestAir Travel Club:** Agents who can provide information about BestAir Travel Club benefits and air miles.
- **Vacations:** Agents who can book vacation packages. Additional skillsets specialize in **American**, **European**, **Asian**, and **Pacific** vacations.

James Jones is a booking agent with BestAir. He is a member of the Bookings skillset. Through training courses, James has become familiar with the company's vacation package offerings. After completing the courses, he was assigned to the Vacations skillset as well. Through additional courses, travel, and reading, James has developed additional expertise in European travel issues. He is now also a member of the European skillset.

Skill-based routing

Introduction

Skill-based routing uses skillsets to match callers with the agents who can best meet their needs.

Example

Sandra Smith wants to book a vacation to Britain. She has called several airlines to obtain information on

- schedules and fares information
- a British Rail pass
- a list of bed and breakfasts in the cities she is planning to visit
- information about tour packages

All of the airlines were able to provide her with schedules and fares, but most were not able to provide her with general travel information she wanted. They referred her to the British embassy.

However, when she called BestAir, her call was routed to the European skillset and presented to James Jones. James was able to give her information about the British Rail pass, along with a list of bed and breakfasts and a description of the tour packages that are available.

Calls in queue

Introduction

The server must make the following decisions when presenting calls:

■   If multiple agents are available, to which agent will it present the call?

■   If multiple calls are waiting, which call will it present first?

Choosing an agent

If two agents are available to answer an incoming call, the server presents the call to the agent with the highest priority for the skillset to which the call is queued. Skillset priority is based on the agent's skill level for a skillset. An agent with a higher skill level is assigned a higher priority for a skillset, and an agent with a lower skill level is assigned a lower priority. (Priority can range from 1–48.)

If more than one agent has the same priority, the server presents the call to the agent with the greatest idle time. Your administrator can configure the server to base idle time on one of the following conditions:

■   total idle time since logon

■   idle time since last status change

■   idle time since last Symposium Call Center Server or ACD call

Example: Skillset priority

James Jones and Emma Wright are both members of the European skillset. Emma has recently completed training on European vacations and was assigned a priority of 4 for the skillset. However, James has had additional training and experience and was therefore assigned a priority of 1 for the skillset.

Both James and Emma are available when a call is queued to the European skillset. Regardless of how long each of them has been idle, skillset priority determines the best agent to present the call. Since James has a higher priority in the European skillset, the call is presented to him.

Example: Idle time

James Jones, Brandon Woo, and Toni Morelli are members of the European skillset. All three have a priority of 1 for that skillset. James Jones has been idle a total of ten minutes since he logged on to the system. Brandon has been idle seven minutes. Toni Morelli has been idle for five minutes. The following events occur:

11:10:24	James, Toni, and Brandon are all on calls.
11:10:25	Brandon's call ends. Brandon presses Not Ready.
11:10:30	Toni's call ends.
11:10:40	James' call ends.
11:10:45	Brandon presses Not Ready again, to go out of Not Ready state.
11:10:60	Call is queued to the European skillset.

The following table summarizes the idle times.

Agent	Idle time since logon	Idle time since last ACD/Symposium Call Center Server call	Idle time since last status change
James	10 minutes	20 seconds	30 seconds
Brandon	7 minutes	35 seconds	15 seconds
Toni	5 minutes	30 seconds	20 seconds

The following table shows how your configuration of idle time preference affects call queuing.

IF Idle time preference is set to	THEN call is presented to
Idle time since logon	James
Idle time since last ACD/Symposium Call Center Server call	Brandon
Idle time since last status change	Toni

Choosing a call

If two calls are waiting in a skillset queue when an agent for that skillset becomes available, the server presents the call with the highest priority. Priority is determined by call age.

You can configure the server to base call age on either

■   when the call was received by the server (that is, passed to the server from the switch or from an external IVR), or

■   when the call was added to the skillset queue (for example, if a call was queued to one skillset, presented to an agent, and subsequently queued to another skillset)

Calls with the greatest age are presented to an agent first.

Example: Call age preference

The following events occur:

11:31:24   Lisa Lanai calls BestAir to book a flight to Switzerland. Her call arrives in the system and is queued to the Bookings skillset. Her call is presented to Rose Chan.

11:31:29   Gerda Spitz calls BestAir for information about British package queues. Her call is queued to the European skillset.

11:31:31   Lisa mentions that she is interested in vacation packages, so Rose transfers Lisa's call to the European skillset.

11:31:37   James Jones, an agent in the European skillset, becomes available, and two calls are in the queue for the European skillset.

The following table summarizes the call ages.

Caller	Time in Bookings queue	Time in European queue	Total call age
Lisa	7 seconds	6 seconds	13 seconds
Gerda	N/A	8 seconds	8 seconds

The following table shows how your call age preference affects call queuing.

IF Idle call age preference is set to	THEN the following call is presented
oldest	Lisa's call
first in queue	Gerda's call

Queuing to a default skillset

You can define one default skillset. Any calls that are not queued by the end of script execution are automatically queued to this skillset. For example, BestAir has defined Bookings as the default skillset. Calls that have not been queued by the end of the script execution are presented to agents assigned to the Bookings skillset.

When skillsets go out of service

Introduction

Skillsets go out of service under the following conditions:

- automatically, when all agents have logged off
- manually, when you change the skillset mode on the Skillset Properties property sheet

Two out of service modes are available: transition mode and night service mode.

Transition mode

Skillsets must be put into transition mode manually, from the Skillset Properties property sheet. For example, you can put a skillset into transition mode if a service interruption occurs during the business day, and you want to answer all calls currently waiting in the queue before putting the skillset out of service.

Example

The computer that stores BestAir's bookings database has gone down. BestAir's information systems staff are attempting to solve the problem, but in the meantime, agents have no information about seats available on any of BestAir's flights. BestAir's call center manager has decided to take manual bookings from all customers who are currently queued for the Bookings skillset. When all waiting calls have been answered, the Bookings skillset will temporarily be put out of service.

To implement this decision, the call center manager puts the Bookings skillset into transition mode.

Night service mode

Skillsets can be put into night service mode automatically—when all agents have logged off—or manually, from the Skillset Properties property sheet.

In your scripts, you define how calls are handled when a skillset is in night service mode.

Example

Bill Bailey calls BestAir at 8:01 p.m. Unfortunately, the office is closed and the Bookings skillset is out of service, in night service mode. Bill hears the following message:

Thank you for calling BestAir. Our office hours are from 8:00 a.m. to 8:00 p.m. Monday to Friday, and 9:00 a.m. to 6:00 p.m. on Saturdays. Please call back during our regular office hours. Thank you.

Tracking call types using activity codes

Introduction

Agents can assign up to three activity (line of business) codes to each call that they answer. The system uses activity codes to track the amount of time that is spent on the various types of incoming calls.

Note: Activity codes can be one to three digits. To use this feature, you must enable the LOB feature on the switch. Then, you must define activity codes at the server to generate reports with meaningful names. To use this feature, you must configure Line of Business codes in the ACDGRP table on the switch.

Example

When James answers Sandra's call, he asks her the question, "How did you hear about us?" She says that she saw a newspaper ad. James presses his LOB key and dials "457."

As the call proceeds, James discovers that it is a "vacation inquiry" call. He enters the activity code for this type of call (440). BestAir has also defined activity codes to be assigned to schedule inquiries, bookings, and vacation package sales.

Note: If the activity codes are defined and named at the server, then the call center supervisor can generate reports on what type of calls are being handled.

Using threshold classes

Introduction

A threshold class is a set of options that you can apply to individual skillsets. Threshold classes specify how statistics are treated in reports and real-time displays. For example, you can create a threshold class for short calls and apply it to particular skillsets. The short call threshold defines the length of a short call for pegging purposes.

Example

BestAir has applied a threshold class to the European skillset that has a short call threshold of ten seconds. This means that if a caller hangs up or is disconnected within ten seconds of speaking to an agent assigned to the European skillset, the call is pegged as a short call. In reports, the short call peg count is incremented by one.

For example, Fred Faraday is inquiring about direct flights to Hamburg. He speaks to Michael Monvale, who tells him that no direct flights are available. Michael adds that BestAir does have flights to Frankfurt and Berlin, and there are frequent shuttles from both of these cities to Hamburg. Fred decides to check around for direct flights, so he thanks Michael and hangs up. The duration of this call was only eight seconds and, therefore, would be pegged as a short call.

Section C: Skillset procedures

In this section

Adding skillsets

Prerequisites

Before you configure a new skillset, do the following tasks:

- Define the ACD-DN number to which calls for this skillset are directed if the system is not available. For information on how to define ACD-DNs on the switch, refer to the *Symposium Call Center Server for DMS/MSL-100 DMS Switch Guide* or *MSL-100 Switch Guide*

- Define the threshold class you want to assign to this skillset if you do not want to use the default threshold class. For information on defining threshold classes, see Chapter 4, "Adding threshold classes."

Limitations

You can define up to 350 skillsets.

To add a skillset

1   From the SMI window, choose Call Flow Administration → Skillsets.

Result: The Skillsets window opens.

2   Choose File → New.

Result: The Skillset Properties property sheet appears.

3   Complete the General property page by entering information into the following fields:

Name: A unique name for the skillset. Skillset names are not case-sensitive.

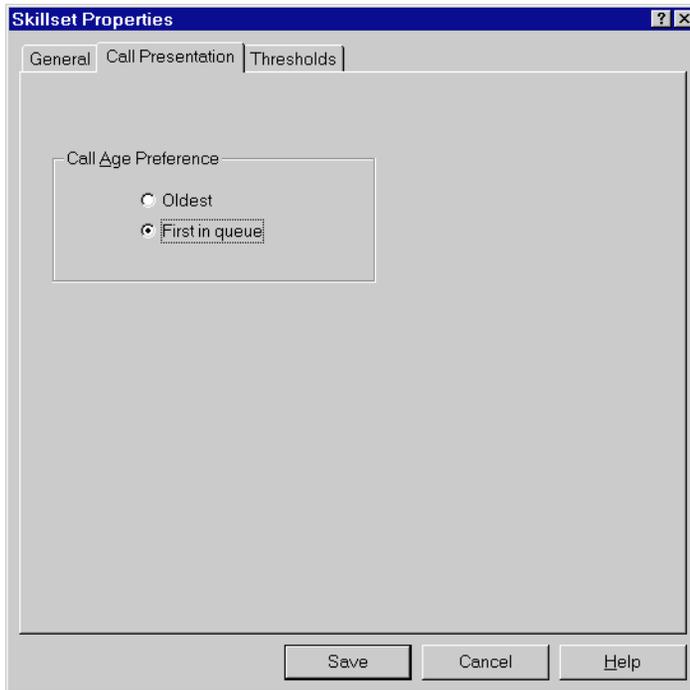**Comment:** Optional. Additional information about the skillset.

Threshold Class: The threshold class to be assigned to this skillset.

Map Skillset to ACD-DN Number: The ACD-DN number for which calls will be pegged to this skillset. If you select this option, you must enter the ACD-DN number as it is defined on the switch.

To put the skillset out of service, see "Putting skillsets out of service" on page 188.

4   Click the Call Presentation tab.

Result: The Call Presentation property page appears.

```
Skillset Properties                                    ? X
┌─────────────────────────────────────────────────┐
│ General │ Call Presentation │ Thresholds │        │
│                                                   │
│   ┌─Call Age Preference──────────────┐            │
│   │                                  │            │
│   │      ○ Oldest                    │            │
│   │      ◉ First in queue            │            │
│   │                                  │            │
│   └──────────────────────────────────┘            │
│                                                   │
│                                                   │
│              Save       Cancel       Help         │
└─────────────────────────────────────────────────┘
```

Note: The Call Source Presentation options are available only for network skillsets.

5   If you want priority to be given to the oldest call in the system, check Oldest. If you want priority to be given to the first call in the queue, check First in queue. For more information on these options, see "Example: Call age preference" on page 174.

6   Click Save.

Result: The skillset is added to the list in the Skillsets window.

7   To return to the SMI window, choose File → Close.

Changing the global skillset properties

Introduction

The following properties apply to all skillsets:

- system default skillset
- the Recorded ANouncement (RAN) for the system default skillset
- the character used to separate fields in caller-entered data
- agent idle time preference
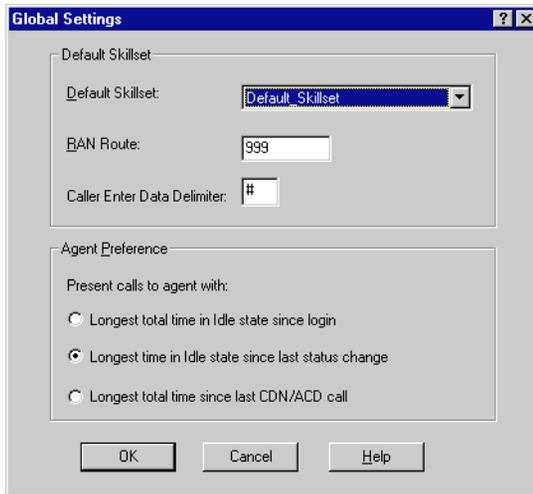
To change global skillset properties

1 From the SMI window, choose Call Flow Administration → Skillsets.

Result: The Skillsets window opens.

2   Choose File → Global Settings.

Result: The Global Settings dialog box opens.

3   Make the desired changes to the following properties:

Default Skillset: The skillset to which calls are queued if they have not been queued to a skillset by the end of script execution.

RAN Route: The number of the recorded announcement (RAN) route for the default skillset, as configured at the switch.

Caller Enter Data Delimiter: Enter the character that separates caller-entered data sequences.

Agent Preference: The method for interpreting agent idle time. Choose one of the following options:

- Idle time since logon—The server presents new calls to the agent who has accumulated the greatest amount of idle time since logging on.

- Idle time since last status change—The server presents new calls to the agent who has been idle longest since his or her last change of state. (The agent idle timer starts when an agent ends a call, or goes out of Not Ready or Walkaway state.)

- Idle time since last Symposium/ACD call—The server presents new calls to the agent who has been idle longest since the end of his or her last Symposium Call Center Server or ACD call.

4   Click Save.

        Result: You are returned to the Skillsets window.

5   To return to the SMI window, choose File → Close.

Putting skillsets out of service

Introduction

You might need to put a skillset out of service for the following reasons:

- a service interruption occurs (for example, the customer database becomes unavailable)

- the skillset is intended for limited-time service (for example, a skillset used to support a marketing campaign)

Note: A skillset goes out of service automatically when

- the last agent serving the skillset logs off

- the last agent serving the skillset is put on standby for the skillset (either manually, from the agent's Skillsets property page, or automatically, with an agent-to-skillset assignment)

To put skillsets out of service

1 From the SMI window, choose Call Flow Administration → Skillsets.

Result: The Skillsets window opens.
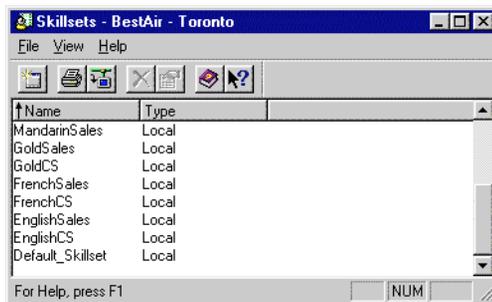
2 Select the skillset you want to put out of service.

3   Choose File → Properties.

Result: The Skillset Properties property sheet opens. The General property page is on top.
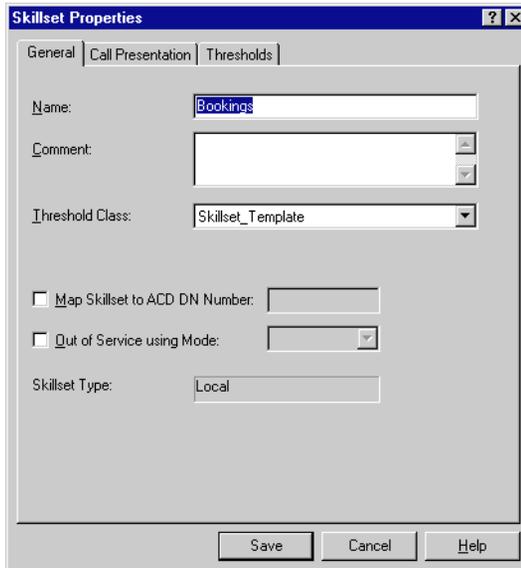
4   Check Out of Service using Mode.

5   Select the out of service mode. If you want all queued calls to be answered before the skillset goes out of service, then select Transition mode. If you want all calls, including waiting calls, to receive night service treatment, then select Night Service mode.

6   Click Save.

Result: You return to the Skillsets window.

7   To return to the SMI window, choose File → Close.

Other procedures for skillsets

Introduction

After you define a skillset, you can change it or delete it. You can also print a list of skillsets.

To change skillset properties

On the Skillsets window, select the skillset you want to change and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

To preview a list of skillsets

From the Skillsets window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To print a list of skillsets

From the Skillsets window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To delete a skillset

Notes:

- Before deleting a skillset, make sure it is not used in an activated script.
- You cannot delete a skillset that is assigned to an agent.

On the Skillsets window, select the skillsets you want to delete, and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Chapter 7

Managing supervisors

In this chapter

Overview

Introduction

When you add an agent, you assign that agent to one or more supervisors. A supervisor is a user who has responsibility for monitoring and supporting their assigned agents.

You must assign each agent a reporting supervisor. You can assign one or more associated supervisors.

Reporting supervisors

Each agent must have one reporting supervisor. The reporting supervisor is the supervisor who

- is notified when the user presses the Emergency key (if the agent has logged on to the phoneset configured for him or her)
- has keys on his or her phoneset that are mapped to the agent keys

Supervisors can view information about their reporting agents on their real-time displays (if the agents have logged in to the ACD subgroup assigned to the supervisor).

Associated supervisors

In addition to the reporting supervisor, an agent may have one or more associated supervisors who provide backup when the reporting supervisor is unavailable. Supervisors can view information about their associated agents in the real-time displays.

Supervisor logon

Supervisors are fixed to a specific phoneset. That is, they must log on at the supervisor phoneset for their ACD subgroup. You configure a phoneset as a supervisor phoneset on the switch, using the SERVORD utility.

Supervisors and real-time displays

When viewing the real-time displays, supervisors can limit the display to

- all agents for whom they are the reporting supervisor

- all agents for whom they are an associated supervisor

- all agents for whom they are the reporting or associated supervisor

- all other agents (that is, agents for whom they are not a reporting or associated supervisor)

- all agents

Supervisors and reports

The agent performance and short calls reports are sorted by supervisor.

Adding or changing supervisors

Before you begin

Make sure the supervisor is defined in the ACDLOGIN table on the switch. For more information, refer to the *Symposium and DMS Switch Guide* or the *Symposium and MSL-100 Switch Guide*.

To add a supervisor

1   From the SMI window, choose User Administration → Users.

Result: The Users window appears.
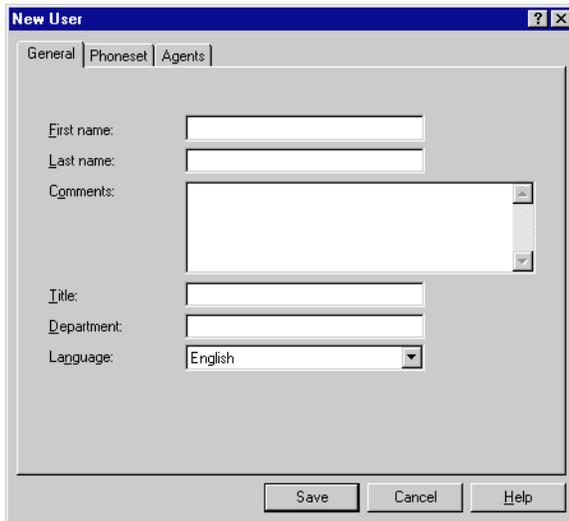
2   Choose File → New.

Result: The User Configuration dialog box appears.

3   Select Call Center Supervisor.

Note: If this user will also have Agent capabilities, click Call Center Agent. (For more information about setting up agents, see Chapter 8, "Managing agents.") If this user will also have Desktop capabilities, click Desktop. (For more information about setting up desktop user accounts, see Chapter 2, "Managing security.")

4   Click OK.

      Result: The New User property sheet appears.

5   Complete the General property page by entering the contact information for the user.

6   Click the Phoneset tab.
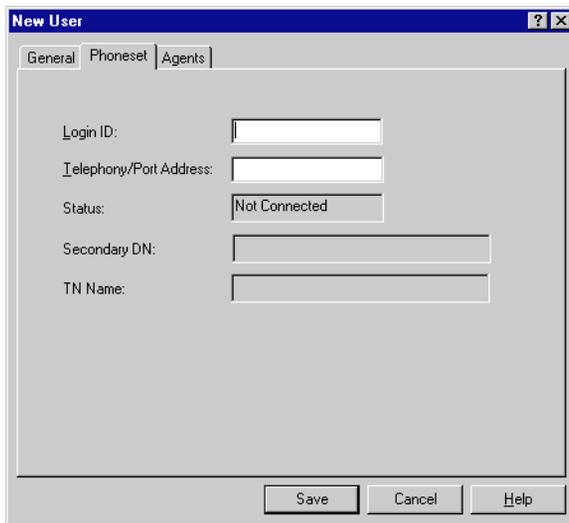
Result: The Phoneset property page appears.

7   Complete the Phoneset property page by entering information into these fields:

Login ID: The number the supervisor uses to log on to the system.

Telephony/Port Address: The position ID of the phoneset at which the supervisor logs on. This is the phoneset on which the switch maps the agent keys for agents reporting to this supervisor.

8   Click Save.

Note: If you click Save before completing the required fields, you are prompted to finish them.

Result: The new supervisor appears in the list in the Users window.

9   To return to the SMI window, choose File → Close.

Viewing the agents assigned to a supervisor

Introduction

You assign agents to supervisors from the agents' Supervisors Property Page. From the supervisor's Agents Property Page, you can view all of the agents assigned to the supervisor.

To view a supervisor's agents

1   From the SMI window, choose User Administration → Users.

Result: The Users window appears.

2   Select the supervisor whose agents you want to view.

3   Choose File → Properties.

Result: The User Properties property sheet appears. The General property page is on top.

4   Click the Agents tab.

Result: The Agents property page appears.

5   Click Save.

Result: You return to the Users window.

6   To return to the SMI window, choose File → Close.

Other procedures for supervisors

Introduction

You can change supervisor capabilities and properties, print or preview the list of users (including supervisors), and delete supervisors.

To change a supervisor's capabilities

From the Users window, select the supervisor you want to change and choose File → Configuration.

For step-by-step instructions, press F1 to access the online Help.

To change a supervisor's properties

ATTENTION

If you change a user's login ID, you must check the user's configuration at the switch. Depending on how the user is configured, you might need to add the new login ID at the switch.

From the Users window, select the supervisor you want to change, and choose File → Properties to change the supervisor's contact information or login ID.

To preview a list of users (including supervisors)

From the Users window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print a list of users

From the Users window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete a supervisor

Note: You cannot delete a supervisor who is assigned to an agent as a reporting supervisor. (You can delete supervisors who are assigned as associated supervisors.) Before you delete a reporting supervisor, reassign all agents who report to that supervisor.

On the Users window, select the supervisor you want to delete and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Chapter 8

Managing agents

In this chapter

Overview

Introduction

Agents are users who can receive incoming call center calls on their phonesets. (The phonesets must have been configured on the switch and acquired on the server.) An agent account has the following properties:

- threshold class
- skillsets
- call presentation class
- supervisor

Before you add an agent, you must define the agent's threshold class, skillsets, call presentation class, and supervisor.

Agent position

In ACD subgroup, one phoneset is configured as a supervisor's set, and the supervisor must log on to this phoneset. Agents, however, can log on at any phoneset that belongs to their ACD subgroup. This ensures that supervisors can view all of their reporting agents.

To ensure that agents have access to all of the phoneset keys (for example, the emergency key that links to their reporting supervisor) set up specifically for them, they should log on at the phoneset ID configured for them at the switch.

Adding agents

Before you begin

Make sure that the agent's phoneset ID (telephony/port address) is defined in the ACDLOGIN table on the switch and is acquired on the server. For more information, refer to the *Symposium and DMS Switch Guide* or the *Symposium and MSL-100 Switch Guide*.
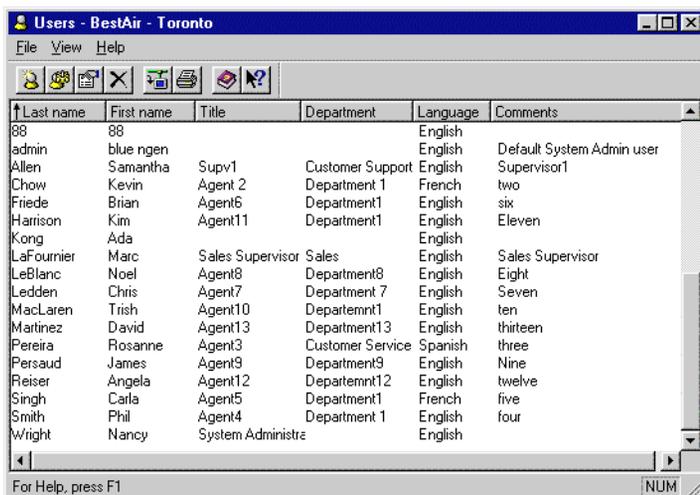
Notes:

1. The number of agents you can add is limited by the keycodes installed on your server.

2. Each agent you add uses resources on the server. Nortel Networks recommends that you only define the number of agents you need.

To add an agent

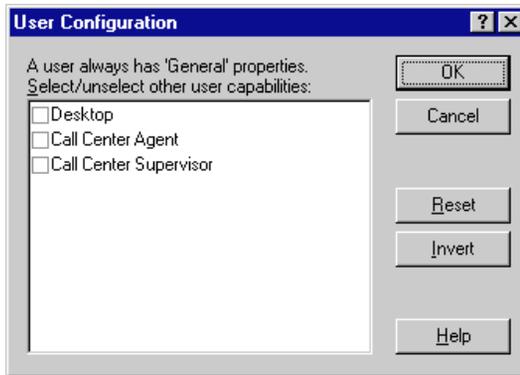**1**   From the SMI window, choose User Administration → Users.

Result: The Users window appears.

2   Choose File → New.

Result: The User Configuration dialog box appears.

3   Select Call Center Agent.

Note: If this user will also have Supervisor capabilities, click Call Center Supervisor. (For more information about setting up agents, see Chapter 7, "Managing supervisors.") If this user will also have Desktop capabilities, click Call Center Supervisor and Desktop. (For more information about setting up desktop user accounts, see Chapter 2, "Managing security.")

4   Click OK.

Result: The New User property sheet appears.

5   Complete the General property page by entering the agent's contact
        information.

6   Click the Phoneset tab.

Result: The Phoneset property page appears.

7   In the Login ID box, enter the number the agent uses to log on to the system.

8   Click the Call Presentation tab.

Result: The Call Presentation property page appears.

9   In the Call Presentation Class for this Agent box, select the call presentation class you want to assign to this agent.

10   Click the Thresholds tab.

Result: The Thresholds property page appears.
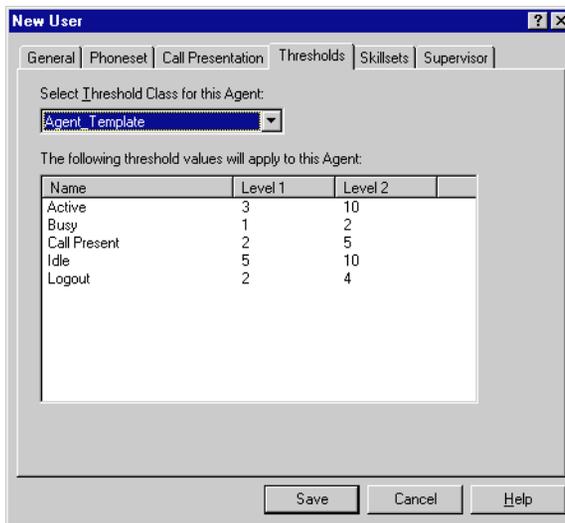
11   In the Select Threshold class for this Agent box, select the threshold class you want to assign to this agent.

12   Continue with the following procedure to assign skillsets to the agent.

To assign skillsets

1   In the New User dialog box, click the Skillsets tab.

Result: The Skillsets property page appears.
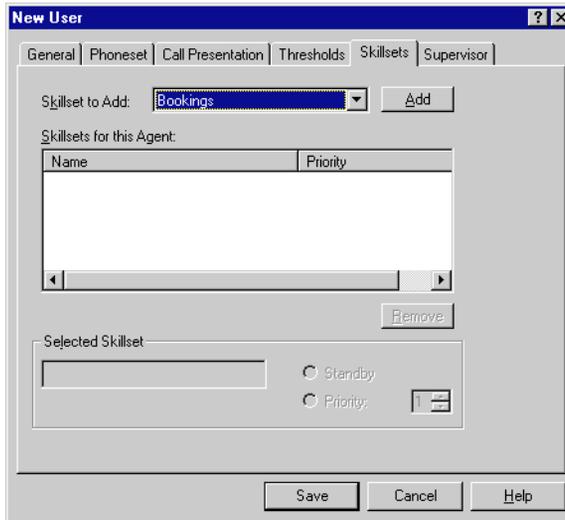
2   In the Skillsets to Add box, select a skillset to be assigned to the agent.

3   Click Add.

4   In the Name column, select the skillset you just added.

5   If you want to put the agent on standby for the skillset, click Standby. If you want to set the agent priority for the skillset, click Priority, and set the priority using a value from 1–48, where 1 is the highest priority and 48 is the lowest priority. For more information on skillset priority, see "Choosing an agent" on page 172.

6   Repeat steps 2 to 5 for each skillset to be assigned to the agent.

7   Continue with the following procedure to assign supervisors to the agent.

To assign supervisors

> **Note:** You must assign at least one agent to a reporting supervisor. Optionally, you can assign one or more associated supervisors.

1   In the New User dialog box, click the Supervisor tab.

Result: The Supervisor property page appears.

2   In the Available Supervisors table, select the supervisor to be assigned as the Reporting Supervisor.

Note: The reporting supervisor must belong to the same ACD subgroup as the agent. This should be the supervisor who monitors the supervisor phoneset for the subgroup.

3   Click Report To.

4   (Optional) You can also select up to five supervisors to be assigned as an associated supervisor. To do so, follow these steps:

    a.   Select the supervisor you want to use as an associated supervisor.

      b. Click Associate.

      Repeat this step for each associated supervisor you want to assign.

5   Click Save.

      Result: The new agent is added to the list in the Users window.

6   To return to the SMI window, choose File → Close.

Other procedures for agents

Introduction

You can change agent capabilities and properties, print or preview the list of users (including agents), and delete agents.

To change an agent's capabilities

Note: You cannot assign an agent desktop capabilities, unless you also give that agent supervisor capabilities.

From the Users window, select the agent you want to change and choose File → Configuration.

For step-by-step instructions, press F1 to access the online Help.

To change an agent properties

You can change an agent's contact information, login ID, call presentation class, threshold class, supervisor assignments, and skillset assignments.

ATTENTION	If you change a user's login ID, you must check the user's configuration at the switch. Depending on how the user is configured, you might need to add the new login ID at the switch.

From the Users window, select the agent you want to change, and choose File → Properties.

Note: When you change an agent's skillset assignments, the server waits for the agent's active calls to end (if any), and then puts the agent into Not Ready state.

To preview a list of users (including agents)

From the Users window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print a list of users (including agents)

From the Users window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete an agent

Note: Before you delete an agent, make sure that

- the agent is not the only agent assigned to active skillsets
- the agent is not specifically referred to in scripts.

On the Users window, select the agent and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Chapter 9

Managing agent to supervisor assignments

In this chapter

Overview

Introduction

Each agent has one reporting supervisor. A reporting supervisor

- is notified when an assigned agent presses the Emergency key (if the agent is logged on to a phoneset configured with his or her reporting supervisor)

- has keys on his or her phoneset that are mapped to the agent keys

Supervisors can view all reporting agents on their real-time displays, and the agent performance and short calls reports are sorted by supervisor.

You assign reporting supervisors to agents on the agents' Supervisors property page. For more information, see "Adding agents" on page 205. You can also assign reporting supervisors with agent to supervisor assignments.

Using agent to supervisor assignments

You might need to temporarily change agents' reporting supervisors for the following reasons:

- for early morning and late evening shifts, when few supervisors are available

- to cover supervisors' coffee and lunch breaks

- when supervisors are sick, on vacation, or on a course

You can manually assign temporary supervisors on the agents' Supervisors property page, and reassign the normal supervisors when they return. You can also set up automatic agent to supervisor assignment, scheduling assignments for known breaks or vacations.

Example 1:
Supervisor is sick

Pat Wilson, one of BestAir's supervisors, calls in sick for the day. The call center manager sets up an agent to supervisor assignment that assigns half of Pat's agents to Chris Konings, and the other half to Cindy Wong. The manager runs the assignment immediately, and all agents are assigned to their temporary supervisors for the day. Another assignment, scheduled for next day, automatically reassigns all agents back to Pat.

Example 2:
Supervisor is on vacation

Pat has booked vacation from the 17th to the 28th of August. BestAir's call center manager has set up an agent to supervisor assignment that reassigns Pat's agents for that period. The manager schedules the assignment to run at 8:30 a.m. on August 17th. Another assignment, which runs at 5:00 p.m. on August 28th, reassigns the agents back to Pat.

Example 3:
Supervisor is on regularly scheduled training

At BestAir, all supervisors are required to participate in regular upgrading. Every four weeks, the supervisor must spend half a day in training. Training sessions are staggered to ensure adequate supervision of the call center. Pat's training occurs every third Thursday of the month. The call center manager has set up an agent to supervisor assignment that automatically reassigns Pat's agents for that time.

Example 4:
Providing supervisory coverage for shifts

At BestAir, agents are usually assigned to supervisors who have experience with the agents' skillsets. However, during the early morning and evening periods, only one supervisor is on duty. The call center manager has set up agent to supervisor assignments to reassign agents for those periods.

For example, from 8:00 a.m. to 9:00 a.m., Cindy Wong is the only supervisor on duty. All agents who start work at 8:00 a.m. are temporarily assigned to her. Other assignments take effect at 9:00 a.m. and 10:00 a.m., as other supervisors arrive.

Example 5:
Providing supervisory coverage for breaks and lunch

As supervisors go on break, their agents must be reassigned. For example, when Cindy goes on break from 10:00 a.m. to 10:15 a.m., all of her agents are temporarily assigned to Pat and Chris in an agent to supervisor assignment.

Adding agent to supervisor assignments

To add an agent to supervisor assignment

Note: Each agent to supervisor assignment uses system resources when it runs. The amount of resources it uses depends on the number of agents reassigned, and how often you run it.

1   Choose Assignments → Agent to Supervisor Assignments.

Result: The Agent to Supervisor Assignments window appears.
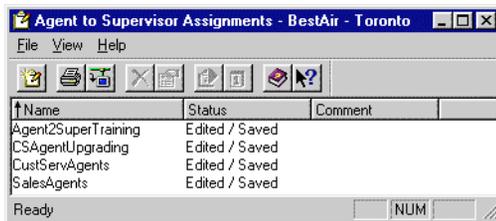
2   Choose File → New.

Result: The Agent-Supervisor Assignments property sheet appears.
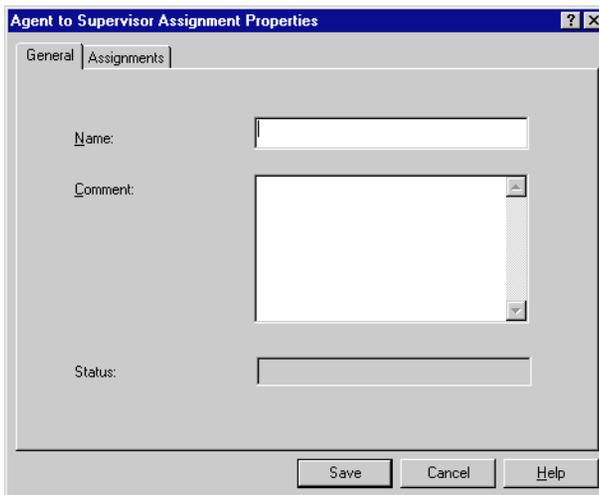
3   Complete the General property page by entering information into these boxes:

Name: The name of the assignment. Use a descriptive name that will help you to identify the purpose of the assignment. For example, "Pats_vacation".

Comments: Optional. Additional information about the assignment.

4   Click the Assignments tab.

Result: The Assignments property page appears.
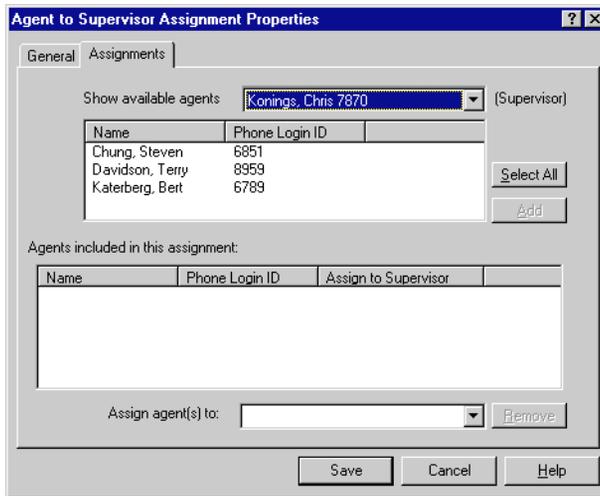
5   In the Show available agents box, select the supervisor whose agents you want to assign.

Result: The agents assigned to that supervisor are displayed in the Show available agents list box.

6   To add an agent to the supervisor assignment, click the agent's name, then click Add. Repeat this step for each agent to be reassigned.

Tip: To add all agents assigned to this supervisor, click Select All, then click Add.

Result: The selected agents are displayed in the Agents included in this assignment list box.

7   Repeat steps 5 and 6 for each supervisor with agents to be added to the supervisor assignment.

8   In the Agents included in this assignment list box, select an agent.

9   In the Assigns Agent(s) to list box, select the supervisor to whom you want to assign the agent.

10   Repeat steps 8 and 9 for each agent you want to assign to another supervisor.

11   Click Save.

     Result: The new assignment is added to the list in the Agent to Supervisor Assignments window.

12   To return to the SMI window, choose File → Close.

After you finish

If you want to schedule the assignment to take effect at a future time, you must schedule it (see "Scheduling agent to supervisor assignments" on page 224).

If you want the agent to supervisor assignment to take effect immediately, you must run it (see "Running agent to supervisor assignments immediately" on page 226).

Scheduling agent to supervisor assignments

Introduction

If you want an agent to supervisor assignment to run at a future date, or if you want it to run regularly, you must schedule it.

To schedule an agent to supervisor assignment

**1**   From the SMI window, choose Assignments → Agent to Supervisor Assignments.

Result: The Agent to Supervisor Assignments window appears.

2   Select the agent to supervisor assignment you want to schedule.

3   Choose File → Edit Schedule.

Result: The Schedule property page appears.

4   Complete the Schedule property page by entering information into these boxes. For example, you might want to apply an assignment at two-hour intervals, starting at 9:00 a.m. and ending at 5:00 pm.

Schedule: The frequency with which you want to run the assignment. When you select a schedule, additional boxes appear.

Day/Date/Month: The day, date, and month (as applicable) you want to run the assignment.

Start: The time on the selected day that you want to run the assignment. For the above example, enter 9:00 a.m. in this field.

End: For assignments run at intervals (specified in the Interval field). The time you want to stop running the assignment. For the above example, enter 5:00 p.m. in this field.

Interval: The frequency, in 15-minute increments, with which the assignment is to be run between the start and end times. For the above example, you would enter 2:00.

Extension: The amount of time the system should wait after a system interruption before abandoning the agent to supervisor assignment schedule.

Note: If system recovery takes place before the Extension time expires, the agent to supervisor assignment schedule runs.

5   Click Save.

Result: You are returned to the Agent to Supervisor Assignments window.

6   To return to the SMI window, choose File → Close.

Running agent to supervisor assignments immediately

When to use

Follow this procedure to make an assignment (either scheduled or unscheduled) effective immediately.

To run an agent to supervisor assignment immediately

1   From the SMI window, choose Assignments → Agent to Supervisor Assignments.

Result: The Agent to Supervisor Assignments window appears.
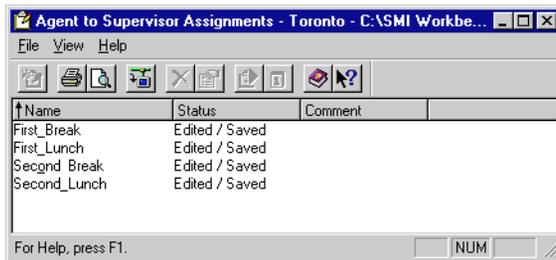
2   Select the agent to supervisor assignment you want to apply.

3   Choose File → Run Now.

4   A message appears asking, "Are you sure you want to run this assignment now?" Click Yes.

5   To return to the SMI window, choose File → Close.

Other procedures for agent to supervisor assignments

Introduction

After you define an agent to supervisor assignment, you can change it or delete it. You can also print a list of agent to supervisor assignments.

To change an agent to supervisor assignment

You can change the properties (the name and comments) of an agent to supervisor assignment, add agents to, or remove agents from, the assignment, and change agents' supervisor assignments.

On the Agent to Supervisor Assignments window, select the assignment and choose File → Properties.

For step-by-step instructions, press F1 to access the online Help.

Note: Changes to an agent to supervisor assignment take effect the next time the agent to supervisor assignment runs.

To preview a list of an agent to supervisor assignments

From the Agent to Supervisor Assignments window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print a list of agent to supervisor assignments

From the Agent to Supervisor Assignments window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete an agent to supervisor assignment

To delete an agent to supervisor assignment, on the Agent to Supervisor Assignments window, select the assignment and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Chapter 10

Managing agent to skillset assignments

In this chapter

Overview

Introduction

A skillset is a group of agents with the expertise necessary to answer a specific type of call. Each agent is assigned to one or more skillsets. Skillsets are used to set up skill-based routing to ensure that callers are matched to the agent best able to meet their needs.

You can make an agent active for a skillset on the agents' Skillsets property page (see "Adding agents" on page 205). You can also use agent to skillset assignments to make agents active for skillsets.

Using agent to skillset assignments

You might need to temporarily assign agents to different skillsets for the following reasons:

- for shifts when fewer agents assigned to a skillset are available

- to cover other agents' breaks

- when agents are sick, on vacation, or on a course

You can manually assign temporary skillsets on the agents' Skillsets property page, or you can use automatic agent to skillset assignments.

To use an automatic agent to skillset assignment, assign agents to skillsets on their Skillsets property page. If you don't want the agent to be active in the skillset immediately, put the agent into standby mode for this skillset. Then, use the agent to skillset assignment to change the agent's priority for the skillset (thus activating the agent for the skillset) at the desired time.

Scenarios to ensure coverage of skillsets

Example 1:
Agents are sick

Mark Schultz, an agent in BestAir's Cargo Tracing skillset is sick and absent
from work today. This has left the Cargo Tracing skillset understaffed,
particularly for the period from 10:00 a.m. to 4:00 p.m., the skillset's busiest
time. The call center manager temporarily assigns Rose Stefanopolis (an agent
who has worked in this skillset before) to the Cargo Tracing skillset for the day.
The manager runs the agent to skillset assignment immediately, and Rose is
automatically reassigned. The manager reassigns Rose to her normal skillset
when Mark returns to work the following day.

Example 2:
Coffee and lunch breaks

As agents go on break, their skillsets become understaffed. To improve skillset
coverage for coffee and lunch breaks, BestAir's call center manager reassigns
agents during these periods.

Example 3:
Shifts

During the early morning and evening periods, few agents are available. As a
result, many skillsets, such as Bookings, are understaffed. Others, such as the
Cargo Tracing skillset, are only in service from 9:00 a.m to 5:00 p.m. BestAir's
call center manager has set up an agent to skillset assignment to automatically
assign members of the Cargo Tracing skillset to Bookings, the busiest skillset,
during early morning and evening periods.

Example 4:
Agents are on vacation

Mark has booked vacation time from the 29th of June to the 10th of July. BestAir's call center manager has set up a scheduled agent to skillset assignment that reassigns Rose to the Cargo Tracing skillset for that period. The manager schedules the assignment to run automatically on June 29th at 8:30 a.m., and schedules another agent to skillset assignment to run on July 10th at 5:00 p.m., restoring Rose's normal skillset assignments.

Example 5:
Agents are on a course

At BestAir, all agents are expected to participate in regular upgrading of their skills, requiring them to be absent while they attend courses. In June, all members of the Europe skillset must attend a one-day course to learn about changes to the company's European vacation packages. To provide adequate coverage while the agents are on course, the call center manager has set up an agent to skillset assignment to assign other qualified staff to the Europe skillset. The manager has scheduled the assignment to run on the day of the course. Another assignment, scheduled to run the next day, restores the agents' normal skillset assignments.

Adding agent to skillset assignments

Introduction

When you use the Agent to Skillset Assignments window, you can add an agent to skillset assignment and change an agent's priority for a currently assigned skillset. You can only change the priority for skillsets that have already been assigned to an agent on the agent's Skillsets property page.

Note: Each agent to skillset assignment uses system resources when it runs. The amount of resources it uses depends on the number of agents reassigned and how often you run it.

To add an agent to skillset assignment

1 Choose Assignments → Agent to Skillset Assignments.

Result: The Agent to Skillset Assignments window appears.
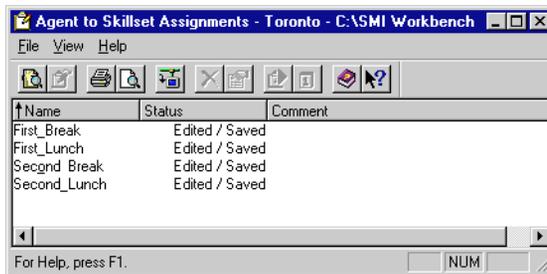
2   Choose File → New.

Result: The Agent to Skillset Assignment Properties property sheet appears.

3   Complete the General property page by entering information into these boxes:

Name: The name of the assignment. Use a descriptive name that allows you to identify the purpose of the assignment, for example, "Early_morning".

Comments: Optional. Additional information about the assignment.

4   Click the Agents tab.

Result: The Agents property page appears.
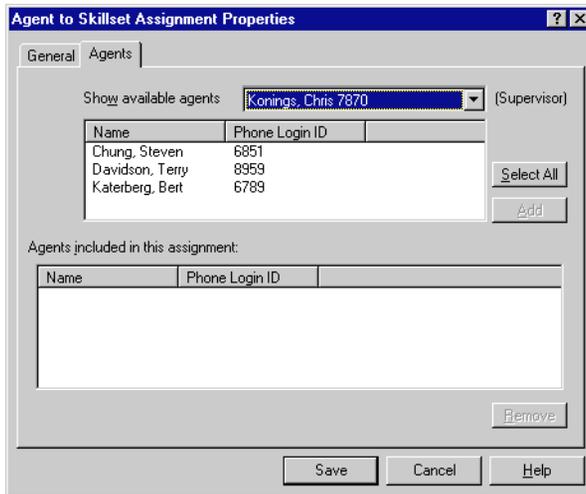
5   From the Show available agents of drop-down list, select the supervisor whose agents you want to assign.

Result: The agents assigned to that supervisor are displayed in the Show available agents list box.

6   To add an agent to the skillset assignment, select the agent's name, then click Add. Repeat this step for each agent to be reassigned.

Hint: To add all agents assigned to this supervisor, click Select All, then click Add.

Result: The selected agents are displayed in the Agents included in this assignment list box.

7   Repeat steps 5 and 6 for each supervisor with agents to be added to the skillset assignment.

8   Click Save.

Result: The new assignment is added to the list in the Agent to Skillset Assignments window.

9   Select the new agent to skillset assignment.

10 Choose File → Open.

Result: The agent to skillset assignment matrix appears. The matrix shows the skillsets to which each agent is assigned, and the agent's priority for each skillset.

11 To change an agent's priority for a skillset, select the priority (the number appearing in the cell opposite the agent's name, and under the desired skillset) and select a new priority from the drop-down list. Repeat this step for each priority you want to change.

12 Choose File → Save.

Result: A confirmation dialog box appears, asking if you want to save the assignment.

13 Click Yes.

14 Choose File → Close.

Result: You return to the Agent to Skillset Assignments window.

15 To return to the SMI window, choose File → Close.

After you finish

If you want to schedule the assignment to take effect at a future time, you must schedule it (see "Scheduling agent to skillset assignments" on page 237).

If you want the agent to skillset assignment to take effect immediately, you must run it (see "Running agent to skillset assignments immediately" on page 239).

Scheduling agent to skillset assignments

When to use

If you want an agent to skillset assignment to take place at a future date, you must schedule it.

Note: When you change an agent's skillset assignments, the server waits for the agent's active calls to end (if any), and then puts the agent into Not Ready state.

To schedule an agent to skillset assignment

1   From the SMI window, choose Assignments → Agent to Skillset Assignments.

Result: The Agent to Skillset Assignments window appears.

2   Select the agent to skillset assignment you want to schedule.

3   Choose File → Edit Schedule.

Result: The Schedule property page appears.

4   Complete the Schedule property page by entering information into these boxes:

Schedule: The frequency with which you want to run the assignment. When you select a schedule, additional boxes appear.

Day/Date/Month: The day, date, and month (as applicable) you want to run the assignment.

Start: The time on the selected day that you want to run the assignment.

End: For assignments run at intervals (specified in the Interval box). The time you want to stop running the assignment.

Interval: The frequency, in 15-minute increments, with which the assignment is to be run between the start and end times.

Extension: The amount of time the system should wait after a system interruption before abandoning the agent to skillset assignment schedule.

Note: If system recovery takes place before the Extension time expires, the agent to skillset assignment schedule runs.

5   Click Save.

Result: You return to the Agent to Skillset Assignments window.

6   To return to the SMI window, choose File → Close.

Running agent to skillset assignments immediately

To run an agent to skillset assignment immediately

> **Note:** When you change an agent's skillset assignments, the server waits for the agent's active calls to end (if any), and then puts the agent into Not Ready state.

1   From the SMI window, choose Assignments → Agent to Skillset Assignments.

   Result: The Agent to Skillset Assignments window appears.

2   Select the agent to skillset assignment you want to apply.

3   Choose File → Run Now.

4   The following message appears: "Are you sure you want to run this assignment now?" Click Yes.

5   To return to the SMI window, choose File → Close.

Other procedures for agent to skillset assignments

Introduction

After you define an agent to skillset assignment, you can change it or delete it. You can also print a list of agent to skillset assignments.

To change an agent to skillset assignment

You can change the properties (the name and comments) of an agent to skillset assignment, add agents to or remove agents from the assignment, and change agents' skillset priorities.

On the Agent to Skillset Assignments window, select the assignment and choose File → Properties.

On the Agent to Skillset Assignments window, select the assignment and choose File → Open.

For step-by-step instructions, press F1 to access the online Help.

Note: Changes to an agent to skillset assignment take effect the next time the agent to skillset assignment runs.

To preview an list of agent to skillset assignments

On the Agent to Skillset Assignments window, choose File → Print Preview.

For step-by-step instructions, press F1 to access the online Help.

To print a list of agent to skillset assignments

On the Agent to Skillset Assignments window, choose File → Print.

To print a list of agent to skillset priorities

On the agent to skillset assignment matrix window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete an agent to skillset assignment

On the Agent to Skillset Assignments window, select it and choose File →
Delete.

For step-by-step instructions, press F1 to access the online Help.

Chapter 11

Working with alarms and events

In this chapter

Overview

Introduction

The Event Browser and Alarms Monitor both show events that occur on the server. These programs provide many common features for viewing events. The table below lists features and which program offers the feature.

Note: To view client events, such as successful log in or log out, or failure to connect, use the PC Events utility on the SMI workbench.

Event Browser

The main advantage for the Event Browser is that you can perform detailed filtering by several categories including severity and event code range. You can also specify a number of latest events to view, so that you see only recent events.

Alarm Monitor

The main advantage for the Alarm Monitor is that it automatically appears in the foreground of the desktop when an event occurs. This immediately alerts you to a problem. You can specify whether the Alarm Monitor will display in the foreground for only critical events, major and critical events, all events, or to stay in the background.

Event Browser versus Alarm Monitor feature matrix

Feature	in Event Browser?	in Alarm Monitor?
view events	Yes	Yes
view online Help for an event	Yes	Yes
sort events by category	Yes	Yes
save a list of events	Yes	**No**

Feature	in Event Browser?	in Alarm Monitor?
print a list of events	Yes	Yes
view minor, major, critical events	Yes	Yes
view information events	Yes	**No**
filter events by code, type, severity, latest events	Yes	**No**
filter events using Event Preferences graphical user interface	Yes	Yes
automatically show the graphical user interface in the foreground when an event occurs	**No**	Yes
clear an event	**No**	Yes

Section A: Viewing events

In this section

Overview of viewing events

Introduction

This section describes how to view and filter events. You can use the Event Browser and the Windows NT Event Viewer to view events. The Symposium Call Center Server also supports Simple Network Management Protocol (SNMP) traps. You can use SNMP to send Symposium Call Center Server events to a Network Management System (NMS) on your network.

This chapter describes procedures for the following tasks:

- viewing, sorting, and printing the event log using the Event Browser on the client
- changing the filtering criteria for the Event Browser
- changing the event log size
- using the event throttling utility to prevent events from repeating in the event log
- using the Windows NT Event Viewer on the server
- configuring SNMP on the server

Events

Events are log entries that record activities on the Symposium Call Center Server, such as

- sending or receiving of messages
- opening or closing of applications
- errors

Some events are for information purposes only, while others can indicate problems. Events are categorized by severity.

Event severity

Events are assigned a default severity of information, minor, major, or critical. The Alarm Monitor does not report Information-level events.

Information

These events indicate that something noteworthy has happened on the system, but do not mean that there is a problem. For example, an information-level event can indicate that a service has started or stopped. These events are displayed in the Event Browser but not in the Alarm Monitor.

Minor

These events indicate that a non-service-affecting fault condition exists, and that you must take corrective action to prevent a more serious fault. For example, a minor event is generated when the file system is 90 percent full.

Major

These events indicate that a service-affecting condition has developed and an urgent corrective action is required. The event condition can cause severe degradation in server performance, and you must restore full capacity. For example, a major event is generated when the file system is 100 percent full.

Critical

These events indicate that a service-affecting condition has occurred and an immediate corrective action is required. Critical events are reported when a component is completely out of service and you must take immediate action to restore it. For example, a critical event is generated when the file system crashes.

Opening the Event Browser

Introduction

The Symposium Call Center Server generates alarms to notify you when minor, major, and critical system events occur. The alarms are shown as events in both the Alarm Monitor and the Event Browser on the client PC.

In the Event Browser, you can filter the list of events, and the Event Browser can also display Information events. (In the Alarm Monitor, you can only filter events by severity. Also, the Alarm Monitor does not display Information events. For more information about the Alarm Monitor, see Section C: "Using the Alarm Monitor," on page 275).

Note: By default, only the latest 100 *critical* events are displayed in the Event Browser. You can configure the filter to display all events. For more information, see "Changing the filtering criteria for events" on page 256.

Follow the procedure in this section to view events in the Event Browser.

To open the Event Browser

From the SMI window, choose Alarms & Events → Event Browser.

Result: The Event Browser window opens.
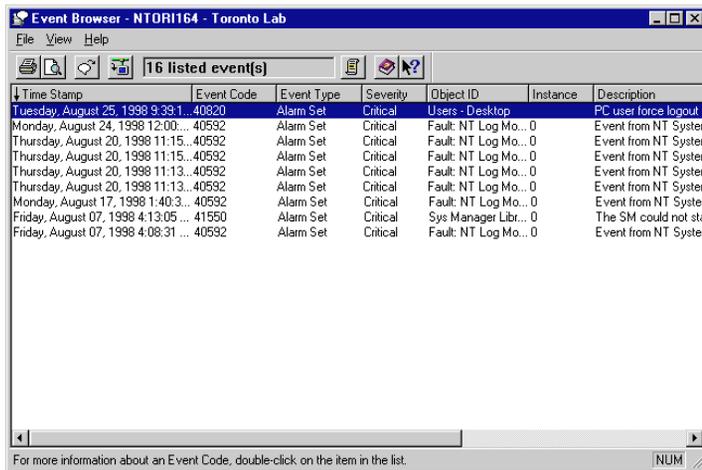
To adjust the column widths, place the cursor on the bar between the column heading names and scroll to the left or right.

To sort events

Click the header of the column by which you want to sort. For example, to sort the events by type, click the Event Type header.

Note: The default order lists the latest event first.

Viewing application, database, and MAS debug events

Application, database, and MAS debug events are logged in the Application log. Application events are accessible through the Event Browser on the client, as well as the Windows NT Event Viewer. MAS debug and MAS database events are accessible only through the Windows NT Event viewer.

For instructions on using the Event Browser, see "Opening the Event Browser" on page 250.

For instructions on using the Windows NT Event Viewer, see "Using the Windows NT Event Viewer" on page 262.

Viewing security events

Security auditing is enabled on the server. Suspicious actions by a user are logged in the Security log. Security events are accessible

■   through the Event Browser on the client

Security events are identified by event code 40593. For instructions on using the Event Browser, see "Opening the Event Browser" on page 250.

■   through the NT Event Viewer on the server

Security events are stored in the Security log. For instructions on using the NT Event Viewer, see "Using the Windows NT Event Viewer" on page 262.

Viewing system events

System events such as Windows NT driver events are logged in the System log. System events are accessible

■   through the Event Browser on the client

System events are identified by event code 40592. For instructions on using the Event Browser, see "Opening the Event Browser" on page 250.

■   through the NT Event Viewer on the server

System events are stored in the System log. For instructions on using the NT Event Viewer, see "Using the Windows NT Event Viewer" on page 262.

Viewing online Help for an event

Introduction

You can view online Help for any selected event. The online Help might provide a recommended action to correct the problem or more information about the event.

To view online Help for an event

1   In the Event Browser or Alarm Monitor, double-click the event that you are investigating.

Result: An Event Details dialog box appears.
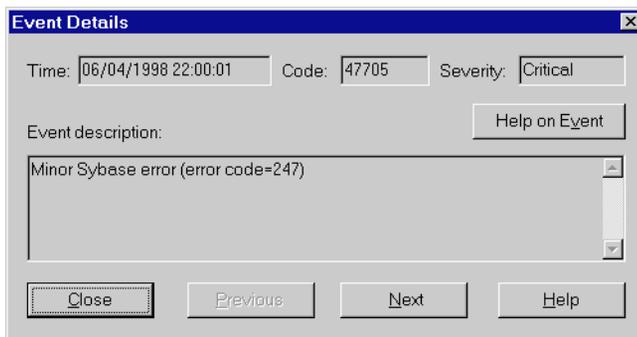
2   Click Help on Event.

Result: The online Help for the selected event appears.
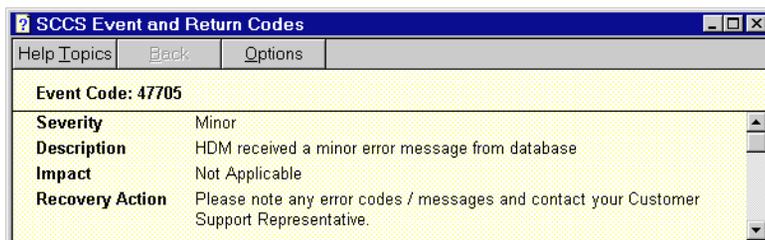
Saving a list of events from the Event Browser

Introduction

Nortel Networks recommends printing or saving relevant sections of the event log in case a problem with your system occurs. The log helps technical support representatives to conduct a thorough analysis of your system.

Before you begin

Make sure that the filter settings are set to show the type and number of events you want to save. For more information, see "Changing the filtering criteria for events" on page 256."

To save events

1 From the SMI window, choose Alarms & Events → Event Browser.

Result: The Event Browser appears.

2 Choose File → Save Event Log.

Result: The Save Event dialog box appears.

3   Choose one of the following options:

- To save all of the events in the Event Browser, check All events.

- To save only the events that are currently selected, check Selected event(s).

4   Click OK.

Result: A dialog box appears for you to provide a file name and select a location.

5   Enter a recognizable file name and location.

6   Click Save.

To print a list of events

From the Event Browser window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

Changing the filtering criteria for events

Introduction

If you want to reduce the number of events shown in the Event Browser at one time, you can screen the log to view a specific number of the most recently filtered events.

Filter settings

You can set the event log filter to display

- a specific number of latest events, or all events (all events available on or retrieved from the system)
- events of a certain severity (critical, major, minor, information)
- a specific event code range, or all event codes
- a specific type of alarm (alarm set, alarm cleared, or message)
- events that occurred during a specific date and time interval

Note: The Set Event Filter Properties tabs work with one another.

Example

At BestAir, system engineer Jane Oliver is testing a new server component. Before she performs the tests, she changes the filtering criteria to display all events, including information events. These events tell her whether system components are starting up. When Jane finishes her tests, she changes the filtering criteria back to the default setting.

To view all events

1   From the SMI window, choose Alarms & Events → Event Browser.

2   Choose File → Change Filter criteria.

Result: The Set Event Filter Properties sheet appears. The Report and Severity page appears first.
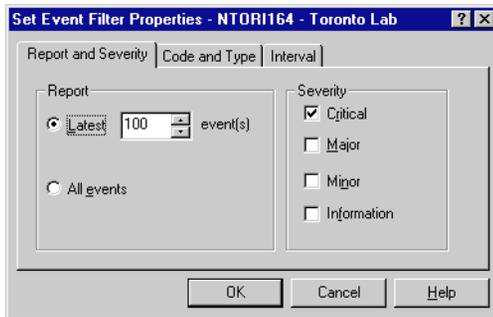
3   Click All Events.

4   Click all the Severity levels.

5   Click the Code and Type tab.

Result: The Code and Type page appears.

6   Select All Codes.

7   Select each box in the Type column.

8   Select the Interval tab.

Result: The Interval page appears.
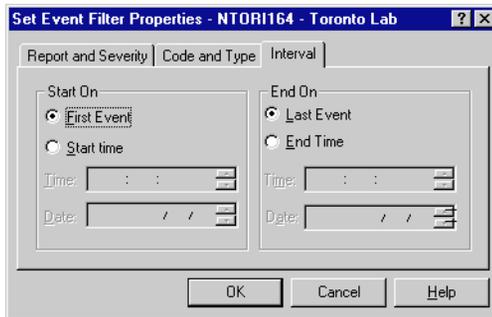
9   To view all events, ensure that the date and time boxes are blank.

10   Click OK to change the filter.

To filter the events

Follow the steps in "To view all events" on page 257, except specify the criteria you are looking for. Events that match the criteria on all tabs in the Set Event Filter Properties sheet are listed in the Event Browser.

Report and Severity tab
On this tab, specify the number of latest events to view, or select all events to view all events that match the other filter criteria. Also specify the severity of events to view.

Code and Type tab
On this tab, specify the range of event codes to view, or select all codes. Also specify the types of alarms to view.

Interval tab
On this tab, you can specify that you want to view events from a specific date and time range. If you do not want to restrict the list of events to a certain date and time range, leave the date and time range blank.

Changing the event log size

Introduction

The event log resides on the server and stores a record of all events that occur on the server. If you change the size settings, the results affect the entire server. You must log on to the server to change the event log size.

Note: Only qualified Nortel Networks technicians should make changes to these settings.

Event wraparound

The event log size is fixed. It does not increase in size as new events are added to the log. When the log is full and a new event is generated, the server removes the *oldest* event report in the log and replaces that report with the newest one.

CAUTION

Risk of data loss
Only qualified Nortel Networks technicians should make changes to these settings.

Log size changes

If you reduce the size of the event log, then the server can store fewer events. If you increase the event log size, you reduce the amount of available disk space on the server, which may slow response times for retrieving events from the Event Browser.

Application events such as Symposium Call Center Server events are stored in the Application log. If you change the Application log size, you also change the number of Symposium Call Center Server events that are stored.

Note: Nortel Networks recommends that you do not change the event log wrapping mechanism and size.

Default event log size

If you change the log size for the Symposium Call Center Server, do not use the Default button. The settings for this button correspond to the Windows NT default settings. During a Symposium Call Center Server installation, the log settings are set to the following defaults:

Log name	Size	Event log wrapping
Application log	8 Mbytes	Overwrite events as needed.
System log	512 kbytes	Overwrite events as needed.
Security log	512 kbytes	Overwrite events as needed.

To change the event log size

1 Choose Start → Programs → Administrative Tools (Common) → Event Viewer.

Result: The Event Viewer appears.
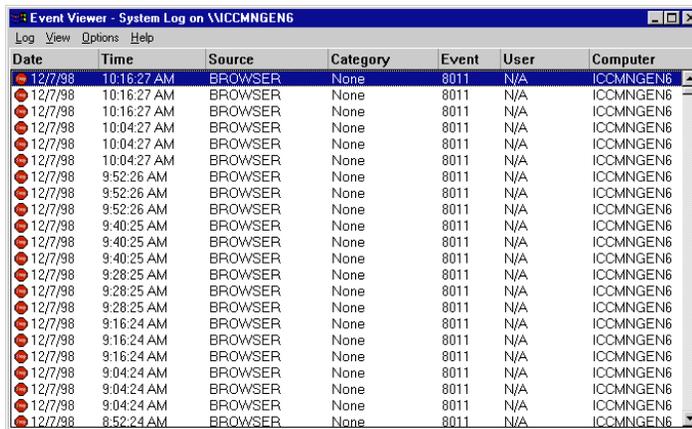
2 Choose Log → Log Settings.

Result: The Log Settings dialog box appears.
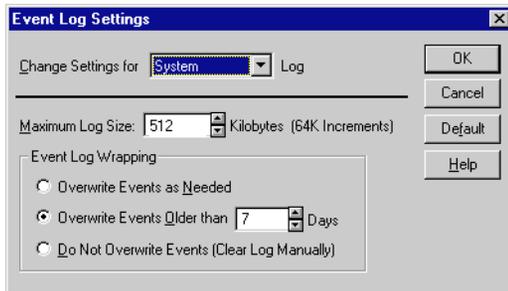
Note: Symposium Call Center Server events are stored in the Application log. Change the Application log size to change the number of Symposium Call Center Server events that are stored.

3 In the Change Settings for box, select the log for which you want to change the size.

4 In the Maximum Log Size box, enter a log size in kbytes.

For the Application log, follow these guidelines:

- For a small call center, set the log size to 512.

- For a medium-sized call center, set the log size to 6015 or greater, depending on the number of days you want to keep the events.

- For a large call center, set the value at 10 000 or greater, depending on the number of days you want to keep events.

5 Click OK to accept the changes.

6 Choose File → Close.

Using the Windows NT Event Viewer

Introduction

Most of the information provided by the Windows NT Event Viewer on the server is also accessible through the Event Browser on the client. The following type of information is not available on the client:

- database events (from the application log)
- MAS debug events (from the application log)

When to use

Use the Windows NT Event Viewer on the server to view information that you cannot view through the Event Browser on the client.

To open the Windows NT Event Viewer

1 From the Windows Start menu, choose Programs → Administrative Tools (Common) → Event Viewer.

Result: The Event Viewer appears.

2 From the Log menu, select one of the following options:

- Click Application to view application, database, and MAS debug events.

- Click Security to view security events.

- Click System to view system events.

Configuring SNMP on the server

Introduction

Windows NT provides a Simple Network Management Protocol (SNMP)
version 1.0 agent, which runs as a service on the Symposium Call Center Server.
You can use this service to direct the SNMP traps generated by the server to a
Network Management System (NMS) on your network. To do so, you must

■   configure the Windows NT SNMP service on the server

■   configure the NMS

To configure the Windows NT SNMP service to forward traps to an NMS

1   For the Windows Start menu, choose Settings → Control Panel.

2   Double-click the Network icon.

    Result: The Network property sheet opens.

3   Click the Services tab.

4   In the list of Network Services, select SNMP Service.

5   Click Properties.

    Result: The SNMP Properties property sheet appears.

6   Click the Traps tab.
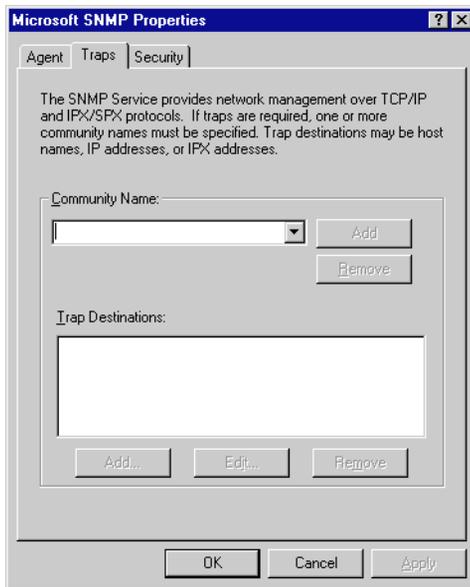
7   If no community name is defined, type **public** and click Add.

8   Add a trap IP destination by clicking Add and typing the IP address of the
          NMS.

9   Click OK.

          Result: The SNMP Properties property sheet closes.

10   Click Close.

          Result: The Network property sheet closes.

11   In the Control Panel window, double-click the Services icon.

          Result: The Services dialog appears.

12   Select the SNMP Trap Service.

13   Click Start.

          Result: The SNMP Trap Service starts.

14   Click Close.

Configuring the NMS

After you configure the server, you must configure the NMS to receive and interpret traps. To do so, you need the Memory Information Block (MIB) files, which describe the format of the traps generated by the server. There files are installed in the Nortel\data directory. They are also located on the installation CD, in the path *platform*\default\nortel\data.

For more information about configuring your NMS, refer to your NMS documentation.

Section B: Managing event preferences

In this section

Overview

Introduction

This chapter describes how to change the classification of particular events. For example, you can choose to treat a major event as a minor event if you are aware it exists and the situation is being resolved.

You can create an event preference to override the default severity or throttling parameters of any event code. You might want to change the preferences of an event for the following reasons:

- to increase the severity of an event (for example, from information to minor). By increasing an event's severity, you ensure that the event displays in the Alarm Monitor when it occurs.

- to reduce the severity of a recurring alarm to information. By reducing an event's severity, you prevent it from appearing in the Alarm Monitor.

- to set the throttling parameters to reduce the frequency an event is generated

Previous occurrences of the event are not affected. You can revert to the default event definition at any time by deleting the event preference for that event code.

Example

At BestAir, the Symposium Call Center Server is generating a critical alarm because of a database error. The system engineer, Jane Oliver, has ordered a replacement for the malfunctioning disk drive that is causing the problem. Since she is aware of the problem, Jane does not want to see an alarm on her console every time the error occurs.

Jane can use the event preferences to reduce the severity of the error from Critical to Information. After the new disk is installed, she can delete the event preference to restore the severity to critical.

Adding event preferences

Introduction

To create an event preference for an event, follow the procedure in this section. If an event preference has already been defined for the event, you can change the event severity. See "To change an event preference" on page 273.

To add an event preference

1 From the SMI window, choose System Administration → Alarms & Events → Event Preferences.

Result: The Event Preferences window appears.
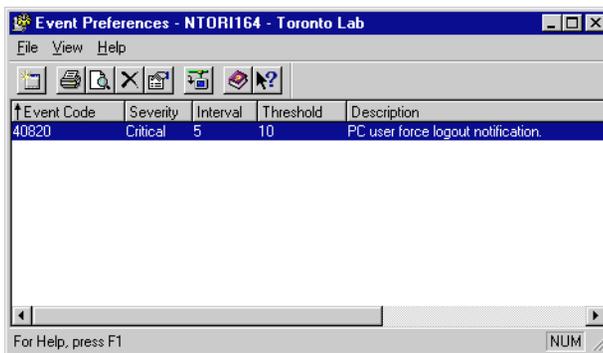
2 Choose File → New.

Result: The New Event Preferences Properties sheet appears.
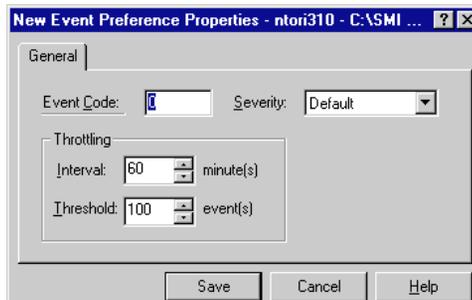
3   In the Event Code box, type the event code number for the event you want to add.

Note: The Symposium Call Center Server does not accept unrecognized event codes. For a complete list of valid event codes, go to the Event Browser and select Event Code Reference from the Help menu.

4   From the Severity drop-down list box, select the severity you want to assign to the event.

5   In the Interval box, type the throttling interval (the time interval during which the event can be logged a specified number of times).

Example: In 30 minutes (the interval), allow the event to be logged a maximum of 10 times (the number).

6   In the Threshold box, type the number of instances of the event that can be logged during the specified interval.

7   Click Save to return to the Event Preferences window.

Result: The new event is added to the list of events.

8   To return to the SMI window, choose File → Close.

Throttling all events

Introduction

Event throttling lets you control the frequency with which events are recorded by the server log. You can throttle all events to prevent the log from becoming overcrowded. If too many instances of each event are recorded, there may not be enough space in the log to record more important events. Too many instances of the same event can distract users, causing them to overlook other important events.

Note: To set throttling on specific event codes, see "Adding event preferences" on page 269.

To throttle all events

1   From the SMI window, choose Alarms & Events → Event Preferences.

Result: The Event Preferences window appears.
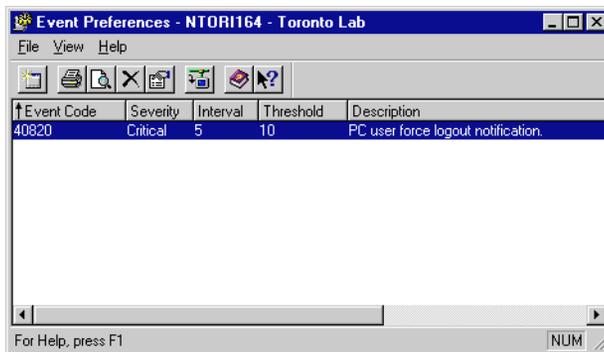
2 Choose File → Default Throttling.

Result: The Set Default Throttling Properties sheet appears.
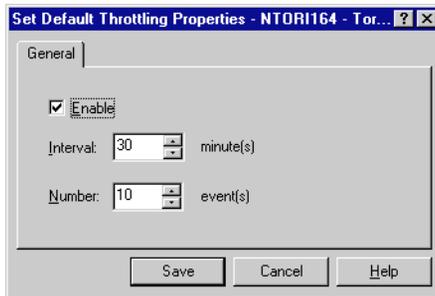
3 Select Enable.

4 In the Interval box, type the interval for which you want events logged.

5 In the Number box, type the number of instances of each event that you want logged.

6 Click Save to return to the Event Preferences window.

7 To return to the SMI window, choose File → Close.

Other procedures for event preferences

To change an event preference

On the Event Preferences window, select the event preference you want to change and choose File → Properties.

Note: If the event code that you want does not appear in the list, define an event preference first. For information about creating a new event preference, see "Adding event preferences" on page 269.

For step-by-step instructions, press F1 to access the online Help.

To print the list of event preferences

On the Event Preferences window, choose File → Print.

For step-by-step instructions, press F1 to access the online Help.

To delete an event preference

When you delete an event preference, the event settings for severity and throttling revert to their default values.

From the Event Preferences window, select the event preference you want to delete and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

Section C: Using the Alarm Monitor

In this section

Overview

When to use

This section describes how to view and manage alarms. The Symposium Call Center Server generates alarms to notify you when minor, major, and critical system events occur.

You can configure the Alarm Monitor to appear either

■   in the foreground

■   in the background

when a new alarm is registered.

In the Alarm Monitor, you can access, clear, and print system alarm information.

Preventing recurring alarms

You can prevent an alarm from recurring in the following ways:

■   Change the throttling parameters for all events (see "Throttling all events" on page 271).

■   Change the throttling parameters for a specific event (see "Adding event preferences" on page 269).

■   Override the default severity of the event so it no longer appears in the Alarm Monitor. For more information, see "Adding event preferences" on page 269.

Viewing events in the Alarm Monitor

When to use

By default, the Alarm Monitor appears in the foreground when an event occurs. If you cannot see the Alarm Monitor or if it has been closed, follow the steps in this section to open it.

To open the Alarm Monitor

1 On the client PC, log on to the server.

2 From the SMI window, choose System Administration → Alarms & Events → Alarm Monitor.

Result: The Alarm Monitor window appears.
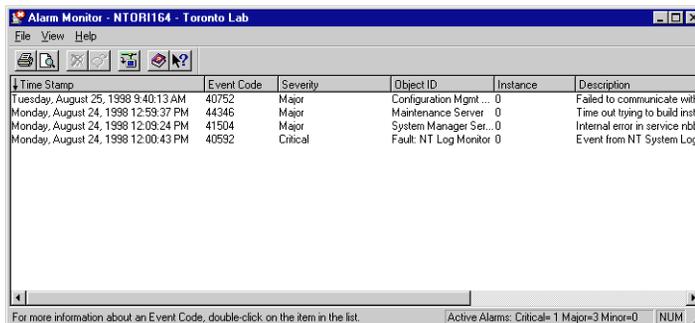
To adjust the column widths, click the cursor on the bar between the column heading names and drag the cursor to the left or right.

To refresh the Alarm Monitor

From the Alarm Monitor window, choose View → Refresh.

Note: After you refresh the Alarm Monitor, the number of alarms might decrease. Any alarms that have been cleared by other processes are removed from the Alarm Monitor.

To sort events

On the Alarm Monitor window, click the header of the column by which you want to sort. For example, to sort the events by type, click the Event Type header.

Note: By default, events are sorted on Timestamp, in reverse chronological order.

To specify when the Alarm Monitor appears in the foreground

By default, the Alarm Monitor appears in the foreground when any event occurs. (That is, it takes the focus from the currently active window.) You can configure the severity of alarm that will force the Alarm Monitor to appear in the foreground.

From the SMI window, on the Utilities menu, click one of the following options.

- Alert All Alarms - This option shows the Alarm Monitor window every time an alarm is registered or updated.

- Alert Major and Critical Only - This option shows the Alarm Monitor window every time a Major or Critical alarm is registered or updated.

- Alert Critical Only - This option shows the Alarm Monitor window every time a Critical alarm is registered or updated.

To configure the Alarm Monitor to appear in the background

If you do not want to see the Alarm Monitor every time it receives and updates a new alarm, you can force it to appear in the background of your display.

1   From the SMI window, choose System Administration → Alarms & Events
→ Alarm Monitor.

Result: The Alarm Monitor window opens.
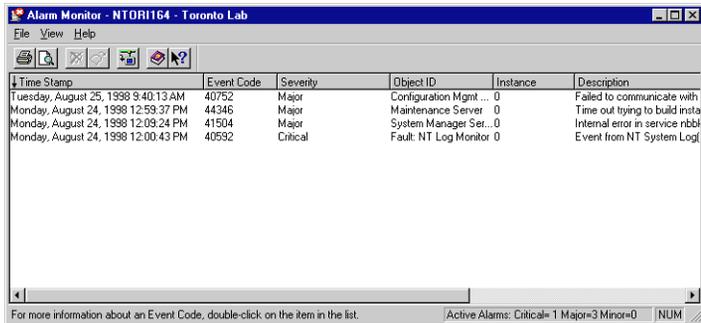
2   From the SMI window Utilities menu, click Alerting Off.

Result: The Alarm Monitor is moved to the background. When a critical alarm is registered, the Alarm Monitor window taskbar flashes until the Alarm Monitor window is brought to the foreground.

Note: If you select Alerting Off and then minimize the Alarm Monitor, the minimized Alarm Monitor flashes when a critical alarm is registered until the Alarm Monitor window is restored.

To obtain more information about an alarm

1   Double-click its entry in the Alarm Monitor.

2   The Event Details dialog box appears.

3   Click Help on Event.

Clearing active alarms

When to use

Alarms are cleared from the Alarm Monitor in one of two ways:

■   The Symposium Call Center Server automatically clears alarms when the
      alarm condition changes.

■   You can clear alarms manually.

When you clear an alarm, you remove the selected alarm (but not the event that
raised it) from the event log. The action also removes the selected alarm from the
list shown in the Alarm Monitor. If the event occurs again, however, the alarm
reappears in the Alarm Monitor.

Example

At BestAir, an alarm appears with the description "Disk is 90% full." Mark
Brown, the system administrator, checks the system disk space, removes
temporary files, and may even decide to order a larger hard drive. Only after he
has resolved the problem does he clear the alarm from the Alarm Monitor.

To clear an alarm

1   From the SMI window, choose System Administration → Alarms & Events
     → Alarm Monitor.

     Result: The Alarm Monitor window opens.
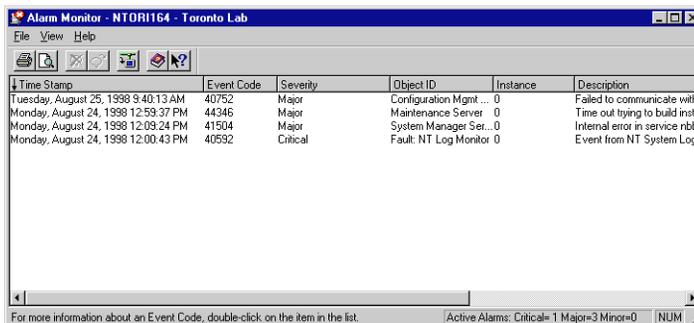
2   Select the alarm you want to clear.

3   Choose File → Clear Alarm.

Result: A dialog box asks you to confirm that you would like to clear the selected alarm.

```
┌─────────────────────────────────────────────┐
│ Clear Alarm                              ☒   │
├─────────────────────────────────────────────┤
│    ⚠    Alarm Code <41248> is selected to be CLEARED. │
│   /!\   Are you sure?                        │
│                                              │
│         ┌──────────┐   ┌──────────┐          │
│         │   Yes    │   │    No    │          │
│         └──────────┘   └──────────┘          │
└─────────────────────────────────────────────┘
```
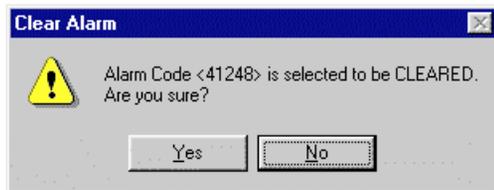
4   Click Yes.

Result: The alarm entry is removed from the Alarm Monitor.

Chapter 12

Backing up data

In this chapter

Overview of backing up data

Introduction

The Symposium Call Center Server backup utility backs up the data on the server. It enables you to recover from a catastrophic failure in the storage subsystem of the server. (The backup utility is not intended to restore individual pieces of information or files that were deleted by accident.)

Note: To back up data on the client, you must provide separate software and hardware.

Checklist for performing backups

Step	✔
After installing your server, or after making changes to your server configuration (for example, IP addresses), create a Platform Recovery disk using the migration.exe utility. For more information, see "To create a Platform Recovery disk" on page 286.	
Ensure that you have enough backup tapes to rotate them. See page 287.	
Ensure that you have a head-cleaning kit and that you clean the tape drive regularly. See page 288.	
Schedule a daily database backup from the client PC. Also schedule a full backup if you do not have a current full backup tape. See page 291.	

CAUTION

Risk of data loss
The server does not contain a default backup schedule. Perform a full backup after all system hardware and software are installed and also before and after any upgrade. Schedule a daily database backup with tape rotation.

Backup types and backup speeds

The following table provides a summary description of the types of backups.

Backup type	Definition	Result	Approximate speed of backup
Full backup	Backs up all files, including the operating system, Symposium Call Center Server software, and the database.	*Offline* operation: All Symposium Call Center Server services are disabled while the backup executes.	■ 3.0 Gbytes/hour with a 4 mm DAT drive ■ 6.0 Gbytes/hour with a Tandberg MLR1 QIC drive
Database backup	Backs up to tape all information stored in the Symposium Call Center Server database.	*Online* operation: Call processing continues as the backup executes. No Symposium Call Center Server services are stopped.	■ 3.0 Gbytes/hour with a 4 mm DAT drive ■ 6 Gbytes/hour with a Tandberg MLR1 QIC drive
RAID drive backup	Backs up drives to a spare drive pack.	*Offline* operation: Fast system backup and simple restore.	■ 6 Gbytes/hour on a 702t ■ 13.5 Gbytes/hour on a 1003t

Note: The approximate speed of the backup depends on the load on the system. These speeds are guidelines only.

When to use a full backup

The full backup allows you to restore a full working version of the system without reinstalling and reconfiguring the server. A full backup can be done while the server is still offline after an installation, upgrade, or major modification. Used in conjunction with a database backup, a full backup allows you to restore your system to its condition preceding a crash.

Note: Nortel Networks recommends that you use a database backup and Platform Recovery disk for system recovery.

When to use a database backup

Nortel Networks recommends performing a daily database backup. A database backup allows you to restore all system data (scripts and statistics) after a crash.

Note: If your server is equipped with a mirrored Redundant Array of Inexpensive Disks (RAID) system, recovery from a single drive failure does not require a tape backup. However, you should still continue to perform daily backups.

To perform a full system recovery using a database backup, you must create a platform recovery disk. Nortel Networks recommends you create a platform recovery disk after installation, upgrade, or major modifications to the system.

To create a Platform Recovery disk

1   Insert a disk into the floppy drive.

2   From the Windows Start menu, choose Programs → Symposium Call Center Server → Migration.

3   Select Dump system information to floppy disk and click Continue.

    Result: The program prompts you to insert a disk.

4   Click OK.

    Result: The program saves the configuration to the disk, and displays messages telling you that the save is complete.

5   Click OK in response to these messages.

    Result: The program prompts you to remove the disk.

6   Click OK.

7   Label the disk with "Platform Recovery Disk" and the current date, and store it in a safe place.

When to use a RAID backup

RAID backups are recommended for platforms with hot-swap disk configurations. They provide a fast mechanism for backing up and restoring your system. Used in conjunction with a database backup, a RAID backup allows you to restore your system to its condition preceding a crash.

ATTENTION RAID backups do not replace full and database backups. Make sure you have a full backup available before you perform a RAID backup. Perform a daily database backup unless you perform daily RAID backups.

Daily maintenance and database backups

The daily maintenance process consolidates statistics. It runs on the server at midnight, and takes several hours, depending on the system configuration. Frequent delays occur if you schedule a database backup at the same time as the daily maintenance process. The server puts the database backup on hold until the maintenance process is completed. The delay is logged in the backup log file, and it has no impact on the system or backup.

Backup tape maintenance

Dedicated tapes for backup types
Use one backup tape for each database or full backup, regardless of whether extra space is available on the tape. Make sure you have enough backup tapes on hand so that you can save backups for a safe period of time before you have to overwrite an old backup. Dedicate separate tapes for full backups and database backups.

CAUTION

Risk of overwriting data
After a database backup, the tape is not ejected from the tape drive. Rotate tapes after *each* backup to avoid overwriting data.

Tape size

Ensure the backup tape is large enough to store the data you are backing up. You cannot use multiple backup tapes for a single backup.

Tape rotation

Rotate tapes daily and store them at an off-site location. Do not keep a tape in the tape drive for more than one or two days for the following reasons:

- The next backup might overwrite existing data on the tape. If the same tape is used for several consecutive nightly backups and the tape becomes damaged, no other backup is available to restore lost data.

- Consistent reuse of the same tape accelerates wear on the tape. Tapes might need replacement earlier than their normal life span of 2000 uses.

Nortel Networks recommends storing backup tapes off-site for as long as possible before reusing them. Store tapes for at least two weeks.

Tape drives

Backups can be performed on the following tape drives:

- Tandberg MLR1 QIC
- 4 mm DAT drive

Head-cleaning kit

Nortel Networks recommends purchasing a head-cleaning tape to prolong the life of your tape heads and ensure the quality of your backups. Clean tape drives based on how often you use them.

Tape cartridges used per day	1	2	3	4 or more
Cleaning interval	Weekly	Every other day	Every other day	Daily

Most cleaning kits suggest how often heads should be cleaned.

Section A: Scheduling backups

In this section

Overview

Introduction

Use the Backup Scheduler on the client PC to schedule backups for the server. There are no predefined backup schedules.

Note: You can initiate backups immediately using the Backup and restore command-line utility. See "Initiating and canceling backups" on page 305.

Administrative privileges required

To schedule backups, you must log on to the server from the client PC as sysadmin.

Scheduling a backup

Introduction

To ensure that your system information can be restored after a hardware failure or data corruption, schedule full backups and database backups. For scheduling suggestions, see "When to use a full backup" on page 285 and "When to use a database backup" on page 286.

ATTENTION	Ensure that you select PrimaryServerTape as the backup device in the following procedure. This represents the local tape drive.

Notes:

1. If your scheduled backups are not running, you can initiate a backup manually. For more information, see "Running the backup utility" on page 300.

2. To recover your system using a database backup, you must have a Platform Recovery disk. See "To create a Platform Recovery disk" on page 286.

Overwriting unusable data

When you schedule a backup, the overwrite option is selected automatically. This option overwrites any data on the tape. In addition, be aware of the following events that occur when a backup is canceled:

- For DAT drives, the software searches for the "end of tape" marker and rewinds to the spot where the tape was stopped. Data for the next backup is appended immediately after the last usable data from the previous backup, overwriting the unusable data.

  Note: If the tape has been ejected, the tape cannot be rewound in this way.

- QIC drives do not use an "end of tape" marker. The unusable data from the previous backup remains on the tape, and the data for the new backup is recorded following the unusable data.

To schedule a backup

1   Remove the write-protect tabs from the backup tapes.

2   Label your backup tapes with the following information:

- backup date and time

- backup type

- backup files

- name of person who is performing the backup

3   Insert the tape properly into the tape drive on the server.

CAUTION

Risk of equipment damage

If you insert the tape incorrectly, you run the risk of damaging your system.

4   At the client PC, log on to the server as sysadmin.

5   From the SMI window, choose System Administration → Server Backup → Backup Scheduler.

Result: The Backup Scheduler window appears.
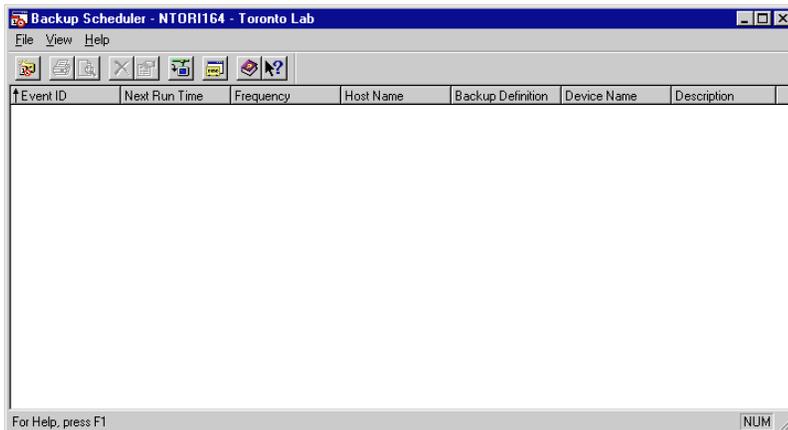
6   In the Backup Scheduler window, choose File → New Schedule.

Result: The Event Properties window appears.

7   Select PrimaryServerTape in the Device Name box. This represents the local tape drive.

8   Select the type of backup in the Backup Definition box. This can be

-   SCCS_Database for a database backup

-   SCCS_Full for a full system backup

9   Click the Schedule tab.

         Result: The Schedule property page appears.

10   Select the type of schedule (daily, weekly, monthly, yearly, or specific date).

11   Select the month, day, or date, on which the backup should run. (The options available depend on the type of schedule selected.)
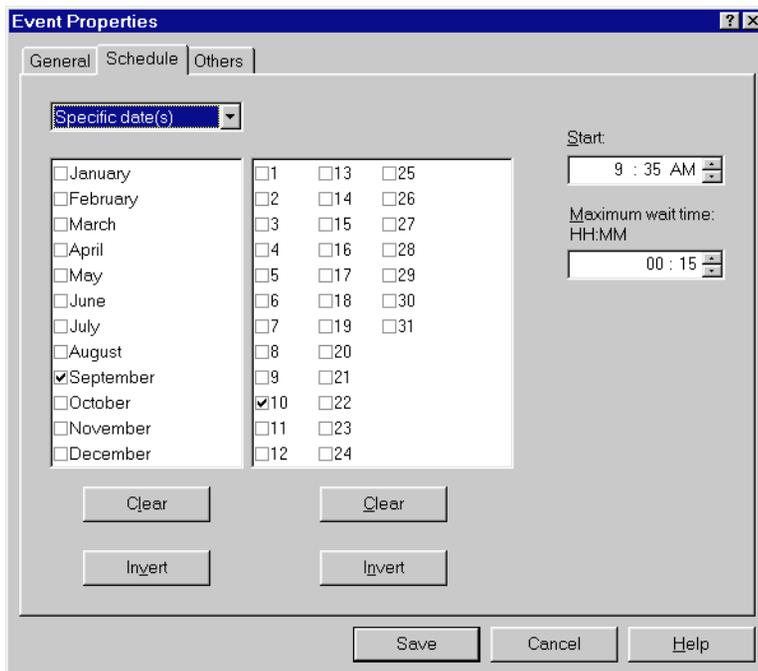
12   In the Start box, select the time to start the backup.

         Note: The backup is scheduled according to the server time, which is not necessarily the same as the client PC time.

13   In the Maximum wait Interval box, enter the length of time the backup can wait before starting the backup. This time is required in case a scheduling conflict with other tasks forces the backup to wait. If the wait time expires before the backup is able to start, then the backup is skipped. For example, you can schedule a backup for a non-peak period, but in three hours the morning shift arrives. In this case, you can enter 03:00 as the interval time. This ensures that the backup does not take place when the morning shift arrives.

14   Click the Others tab.

Result: The Others property page appears.
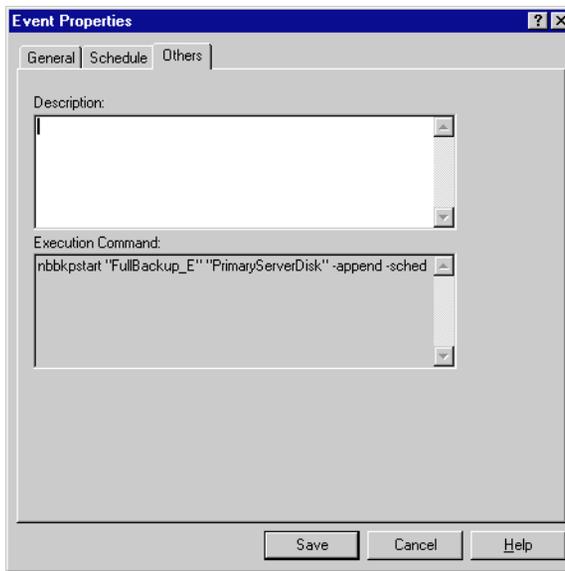
15   In the Description box, type the description or the purpose of the backup.

16   Click Save.

Result: The backup is scheduled.

Monitoring backups

Introduction

You can monitor the status of a running backup as follows:

- database—Use the Backup Status window on the client PC. This window opens when a SCCS_Database backup is running.

- full—Use the nbbkp_ci.exe utility on the server.

You can also use view backup status in the log file.

Backup Status window

The Backup Status window shows whether any files were skipped or copied in error during an SCCS_Database backup.

If any files are not copied successfully, a minor alarm is generated. Obtain the Event ID from the alarm in the Alarms Monitor for more information.

nbbkp_ci.exe

Use the status command to show the status of the SCCS_Full backup. The utility shows the progress of the backup. For detailed instructions for using this utility, see "To monitor the status of a backup" on page 305.

Using log files

To verify that a backup was successful, use a text editor (such as Notepad or WordPad) to check the backup log. The backup log is generated at the end of the backup, and it is stored on the server in the following directory:

d:\nortel\iccm\data\backup\BackupLogs

Database backup

The file name for a database backup is SCCS_Database yymmdd hhmm.LOG, where yymmdd hhmm are the date and time of the backup. For example, 990817 1415 represents 2.15 p.m. on August 17 1999.

If a database backup was successful, the backup log contains all of the following messages:

```
Starting backup of 'SCCS_Database' to device
'PrimaryServerTape'
The backup of 'SCCS_Database' was completed successfully.
```

If these messages are not present, the backup was unsuccessful.

Full backup

The file name for a full backup is SCCS_Full yymmdd hhmm.LOG, where yymmdd hhmm are the date and time of the backup. For example, 990817 1415 represents 2.15 p.m. on August 17 1999.

An error message, `Error reading from tape, win32 rc=1104, MAS rc=41831`, appears at the top of the log. Ignore this message.

If a full backup was successful, the backup log does *not* contain messages about skipped files. Search through the backup file for the word "skipped." If you find messages similar to the following, the backup was *not* successful:

```
FILE C:\IO.SYS was skipped
```

Other procedures for backups

Introduction

You can change any detail of a scheduled backup using the Event Properties window. You can also delete backups from this window.

To change a scheduled backup

On the Backup Scheduler window, double-click the scheduled backup you want to change.

For step-by-step instructions, press F1 to access the online Help.

To delete a scheduled backup

On the Backup Scheduler window, select the scheduled backup you want to delete and choose File → Delete.

For step-by-step instructions, press F1 to access the online Help.

To cancel a running backup

Click Cancel in the Backup Status window.

Note: If you cancel the backup, any data that was written to the backup device is unusable.

Section B: Working with the backup command-line utility

In this section

Running the backup utility

Introduction

The backup command-line utility includes options to initiate or cancel a backup, and other actions related to backup. To restore data from a backup, see Section A: "Restoring the database," on page 337 or Section B: "Restoring the complete system (non-RAID)," on page 343.

To run the backup utility

1   Log on to the server as Administrator.

2   From the installation CD-ROM, locate the MAS subdirectory, and then double-click the file **nbbkp_ci.exe**.

    Result: The CI> prompt appears.

3   At the CI> prompt, type the appropriate command to view information or initiate a process, and then press Enter. The following table lists some of the available actions; however, refer to the appropriate procedure for detailed instructions and commands:

Action	See page
To display a list of all objects	301
To display a particular object	302
To view the contents of a tape or disk backup directory	304
To format a backup tape	304
To start a backup	305
To monitor the status of a backup	305
To cancel a running backup	306

Displaying objects

Introduction

You can display an individual or a full list of backup and restore objects. Types of objects include the following:

- backup definitions (scheduled backups)
- backup devices
- remote servers
- backup logs
- restore logs
- applications

To display a list of all objects

1   Type **listobject** in the command line.

Example: CI>listobject

Result: The system responds with the message Object type:.

2   Type the name of the object type to be listed, as shown on the following chart, and then press Enter:

Object type	Displays a list of the following objects
definitions	backup definitions (scheduled backups)
devices	backup devices
RemoteServers	remote servers
blog	backup logs
rlog	restore logs
applications	server applications

Result: A full list of the names of all server backup and restore objects of the requested type appears.

```
CI>listobjects
Object type: (Max Leng. = 15): devices
Backup devices:
    PrimaryServerDisk      (Disk)
    PrimaryServerTape     (Local Tape)
```

To display a particular object

1   Type **displayobject** in the command line, followed by the object type. For a complete list of object types, refer to the chart in the procedure, "To display a list of all objects" on page 301.

Example: CI>**displayobject**

2   Type the object type when this prompt appears.

Example: Object type: **devices**

3   Type the object name when this prompt appears.

Example: Object name: **PrimaryServerTape**

Result: The system displays a detailed description of the requested object, such as the Primary Server Tape.

Example:

```
CI>displayobject
Object type: (Max Leng. = 15) : device
Object name: (Max Len. = 100) : primaryservertape
Backup device 'primaryservertape' :
   path:        \\.\TAPE0
   type:         Local Tape
```

Working with backup tapes

Introduction

You can view the contents of a backup tape using the List Tape command. You can also format a backup tape using the Format tape command. You must format tapes before using them for backups.

Before you begin

To format a tape, you must know the name of the device. To obtain the name of the device, see "Displaying objects" on page 301.

To view the contents of a tape or disk backup directory

1   Type **listtape** in the command line.

    Example: CI>**listtape**

2   Type the name of the device that contains the backup you want to view.

    Result: A list of all backups stored on the specified device appears. This can take some time.

    Note: If the tape is not a formatted backup tape, the following message appears:

    ```
    NBbkp_eFOREIGN_MEDIA
    ```

To format a backup tape

Note: This process erases all existing data on the tape.

1   Type **format** in the command line.

    Example: CI>**format**

2   Type the name of the device that contains the tape to be formatted.

    Result: The system formats the tape in the specified device.

Initiating and canceling backups

Introduction

You can initiate a backup immediately using the startbackup command, and check its status using the status command. You can also cancel a running backup using the cancel command.

ATTENTION	Do not log off your Windows NT session until the backup is complete. If you log off early, the backup will not complete properly.

Before you begin

You must know the names of the destination backup device, and the backup definition (type of predefined backup).

If you do not know the names of the backup device or the backup definition, see "Displaying objects" on page 301.

To start a backup

1   Type **startbackup** in the command line.

2   Type the name of the backup device.

3   Type the name of the backup definition.

4   Select Y to overwrite the contents of the tape.

5   Select Y to automatically format the tape.

To monitor the status of a backup

1   Type **status** in the command line.

   Result: The progress of the backup displays and refreshes every few seconds.

2   Press any key to stop the display and return to the CI> prompt.

To cancel a running backup

1 Type **cancel** in the command line.

Example: Cl>**cancel**

Result: The system displays the following message: "Are you sure?"

2 Type **Y** to confirm the cancellation.

Result: The system cancels the running backup.

Section C: Performing RAID procedures on a 702t

In this section

Overview of RAID procedures on a 702t

Introduction

If your server is equipped with RAID, you can use the RAID subsystem and a spare disk set to create a complete system backup. RAID backups provide a mechanism for fast backup and simple restore.

Splitting and rebuilding the RAID drives

When you are making significant changes to your server (for example, during application of PEPs), you can split the RAID drives. This ensures that only one set of drives is affected by the changes. If you have any problems, you can easily back out of the changes by using the other set of drives.

When you are satisfied that your system is running properly, you can rebuild the RAID drives.

Note: The procedures for splitting and rebuilding the RAID drives are different for different platforms. Make sure you follow the proper procedure for your platform.

RAID backups and tape backups

RAID backups do not replace tape backups. Even if you are using RAID backups, create a full tape backup after installation, upgrade, or major modifications to the system. Unless you are performing daily RAID backups, you should continue to perform daily database backups.

Note: The procedure for RAID backups is different for different platforms. Make sure you follow the proper procedure for your platform.

Nortel Networks recommends performing a RAID backup procedure for platforms equipped with hot-swap disk configurations.

Performing a consistency check on a 702t

Introduction

Perform regular consistency checks prior to backing up or splitting a RAID drive. The consistency check is time-consuming, so you might prefer to perform it a few days before splitting or backing up your RAID drives.

Note: A consistency check is not necessary every time you split the RAID drives.

You can perform the consistency check while the server is online, but it degrades server performance. Therefore, Nortel Networks recommends that you perform the operation during non-peak times. A consistency check of a 4-Gbyte volume takes approximately 45 minutes.

To perform a consistency check

1   On the server, log on to Windows NT as NGenSys.

2   Start the dac960 Administration utility by running dacadm.exe from a command line.

Result: The dac960 Administration utility main window appears.
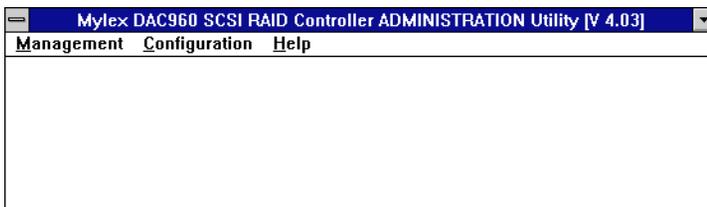
3   Perform a consistency check of the RAID system packs by choosing Management → Consistency Check.

Result: The Consistency Check dialog box appears.

4   Select the first system drive to check, and click OK.

Result: The following message appears: `Restore consistency check in case of error?`

5   Click No.

6   Repeat steps 4 and 5 for the remaining system drives. (Check drives B-1 and C-1.)

7   Click OK to close the Consistency Check dialog box.

8   Exit from the dac960 Configuration utility.

Splitting the RAID drives on a 702t

Introduction

Split the RAID drives when you are upgrading the server or applying PEPs or service update packs.

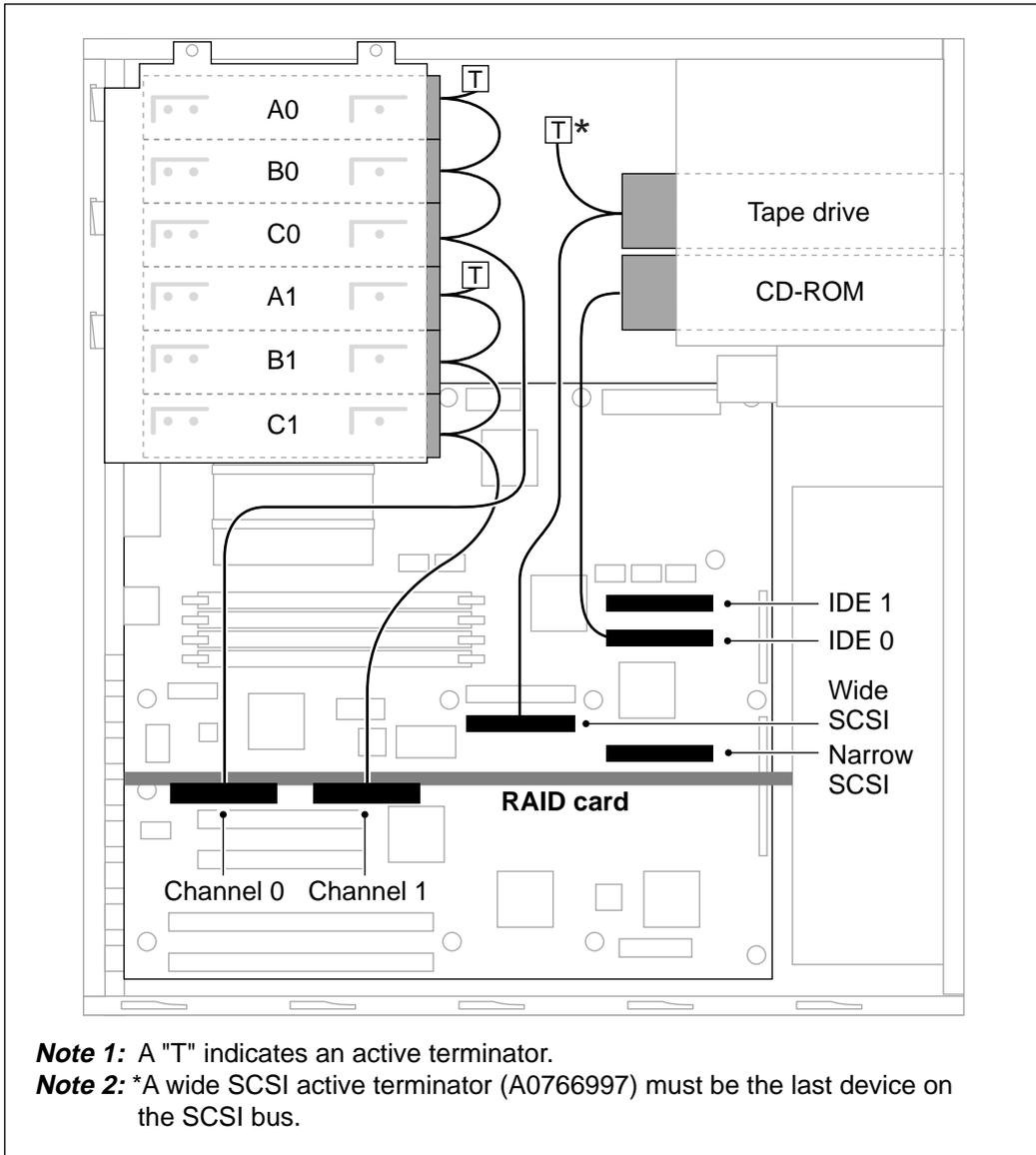### About splitting the RAID drives

When you split the RAID drives, you are breaking the mirrored image of the RAID hard drives (channels 0 and 1) and disabling the channel 1 hard drives. Any software activity that is performed on the system affects only the channel 0 hard drives. The channel 1 hard drives continue to have the current system configuration, and you can use them to rebuild the RAID hard drives if a problem occurs during conversion.

Splitting the RAID drives is supported for 702t platforms with the following:

- a Mylex RAID controller (dac960PL, with firmware revision 3.x, or dac960PG, with any firmware revision)
- RAID 1
- Platform Upgrade Kit

Platform configurations

A 702t system has three system drives set up in a RAID configuration. These drives should be labeled A-0, A-1, B-0, B-1, C-0, and C-1, where 0 and 1 are the channel numbers. The following diagram shows the SCSI cable connections for the two channels to the RAID controller card.

A0	T
B0	T *
C0	Tape drive
A1	CD-ROM
B1	
C1	

IDE 1

IDE 0

Wide
SCSI

Narrow
SCSI

RAID card

Channel 0   Channel 1

Note 1: A "T" indicates an active terminator.
Note 2: *A wide SCSI active terminator (A0766997) must be the last device on
the SCSI bus.

G100812

Before you begin

- Make sure that the RAID subsystem is cabled as specified in the *Meridian Application Server Installation Guide* for your hardware platform.

  Note: Ensure that the SCSI cable is correctly installed. Reversed cables increase the risk of data loss.

- Back up the RAID Controller configuration to a disk.

- Make sure you have a full or database tape backup available.

- Make sure that the Windows NT Repair disk is up to date.

- Make sure that you have the dac960 Configuration Disk 1/2 (NTRH8003 Release 3.0).

- Nortel Networks recommends that you perform a consistency check (see "Performing a consistency check on a 702t" on page 309).

  Note: A consistency check is not necessary every time you split the RAID drives.

Understanding the dac960 Configuration Utility

The dac960 Configuration Utility is a DOS-based utility. It has a status bar at the bottom of the screen, which indicates the action that is taking place. Check the status bar frequently while you are using this utility.

To split the RAID drives

1   On the server, log on to Windows NT as Administrator.

2   Insert the bootable dac960 Configuration disk in the floppy disk drive.

     Note: If the dac960 disk is not bootable, insert a bootable disk to start the system until the DOS prompt appears, and then insert the dac960 Configuration disk.

3   Shut down and restart the server.

     a.   From the Start menu, choose Shutdown.

     b.   Click Restart the computer, and click Yes.

4   If you are prompted for the date and time, make sure the displayed date and time are correct. If they are, press Enter. If they are not, enter the correct date and time.

Result: The A:\> prompt appears.

5   Type **CD \daccfg** and press Enter.

Result: The A:\DACCFG\> prompt appears.

6   Type **daccf** and press Enter.

Result: The daccf utility starts and scans the SCSI buses. The main menu appears.

7   If you do not have a current backup of your RAID controller configuration, make one before you proceed. To do so, follow these steps:

   a.   From the dac960 utility main menu, choose Tools and press Enter.

      Result: The Tools menu appears. On the left side of the window is a list of the drives and their current states. All drives (both channel 0 and 1) should be ONL (online).

   b.   Choose Backup/Restore Conf and press Enter.

   c.   Choose Backup configuration and press Enter.

   d.   Remove the dac960 utility disk and insert a new formatted disk in floppy drive A.

   e.   Type **A:\raidcfg** and press Enter.

      Result: The following message appears: `Existing files if any will be overwritten.`

   f.   Select Yes and press Enter.

   g.   When the status bar indicates that the configuration has been successfully saved, remove the disk and label it RAID controller configuration backup.

   h.   Insert the dac960 Configuration disk and press Enter to continue.

   i.   Press Esc to return to the main menu.

8   From the main menu, select Tools and press Enter.

9   Select Kill Drive and press Enter.

Result: The utility shows the system drives and their current statuses. The drive status can be ONL (online) or DED (dead).

10   Select drive A-1 and press Enter twice.

11   When prompted to confirm your action, select Yes and press Enter.

          Result: Drive A-1 is marked as DED (dead).

12   Record the SCSI channel and ID of the drive.

13   Repeat steps 9 to 12 for the remaining system packs. (Kill drives B-1 and C-1.)

14   Exit from the dac960 Configuration utility by pressing Esc and selecting Yes when prompted to exit.

15   Power down the server.

16   Disconnect the disks marked DED by disconnecting the SCSI cables for channel 1 (see the preceding illustration). For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

          Note: If you decide to remove the drives, be sure to label them with their SCSI channel and ID and store them in antistatic bags and suitable foam material.

          CAUTION

          Risk of data loss

          If you label drives incorrectly, you might not be able to recover your system using these drives.

17   Remove the dac960 Configuration utility disk.

18   Power up the server.

          Result: When the server boots, you see errors indicating that the system has found several dead drives. The list of drives should include all of the channel 1 drives that you killed in this procedure.

          When you log on to Windows NT, the dac960 RAID Control Monitor window appears. It reports the statuses of the dead drives. You can minimize this window.

Rebuilding the RAID drives on a 702t

Introduction

Use this procedure after you have split the RAID drives and you are confident with the operation of your system.

Assumptions

This procedure assumes that you are rebuilding the RAID drives using the drives that were split previously. If you are using new drives, make sure you do the following tasks:

- Use the jumpers on the drives to set the SCSI IDs correctly. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

- Format the new drives.

To rebuild the RAID drives

1   Shut down the server.

   a.   From the Start menu, choose Shutdown.

   b.   Click Shut down the computer, and click Yes.

2   Power down the server.

3   Connect the SCSI cables for channel 1. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

4   Insert the dac960 Configuration disk in the floppy disk drive.

5   Power on the server.

   Result: POST messages from the RAID controller warn you that the system is operating in critical mode (that is, with some drives offline). The A:\> prompt appears.

6   Type **CD \daccfg** and press Enter.

   Result: The A:\DACCFG\> prompt appears.

7 Type **daccf** and press Enter.

Result: The daccf utility starts, and might display the current SCSI buses. Drives A-0, B-0, C-0, and so on are ONL (online), and drives A-1, B-1, C-1, and so on are DED (dead).

8 If the utility prompts you to save the current state of the RAID controller, type **S**.

9 If you are prompted to restart, do so, and repeat steps 6 and 7.

Result: The main menu of the dac960 Configuration utility appears.

10 Choose Rebuild and press Enter.

Result: The utility shows a list of the hard drives.

11 Select A-1 and press Enter.

Result: The utility prompts you to format before rebuilding.

12 Select No and press Enter.

Result: The utility begins rebuilding the drive. Rebuilding a 4 Gbytes volume takes approximately 45 minutes.

13 When prompted to continue, press Enter.

14 Repeat steps 10 to 13 for each drive to be rebuilt. (Rebuild drives B-1 and C-1.)

15 When all drives are rebuilt, press Esc to exit the dac960 Configuration utility.

Result: The A:\DACCFG\> prompt appears.

16 Remove the dac960 Configuration disk from the floppy drive.

17 Press Ctrl-Alt-Del to restart the server.

Performing a RAID backup on a 702t

Introduction

Full backup with RAID drives is supported for 702t platforms with the following components:

■ a Mylex RAID controller (dac960PL with firmware revision 3.x, or dac960PG with any firmware revision)

■ RAID 1

■ a Platform Upgrade Kit

Before you begin

■ Make sure that the RAID subsystem is cabled as specified in the *Meridian Application Server Installation Guide* for your hardware platform.

  Note: Ensure that the SCSI cable is correctly installed. Reversed cables increase the risk of data loss.

■ Back up the RAID Controller configuration to a disk.

■ Make sure you have a full or database tape backup available.

■ Make sure that the Windows NT Repair disk is up to date.

■ Make sure that the following components are available:

  ■ dac960 Configuration Disk 1/2 (NTRH8003 Release 3.0)

  ■ a new or blank formatted disk for each RAID system pack

■ Nortel Networks recommends that you perform a consistency check (see "Performing a consistency check on a 702t" on page 309).

  Note: A consistency check is not necessary every time you split the RAID drives.

To perform a RAID backup

1   Split the RAID drives, following steps 1 to 15 in "Splitting the RAID drives on a 702t" on page 311.

Note: Remove the hard drives marked DED, and label them with their SCSI channel and ID. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

CAUTION

Risk of data loss

If you label drives incorrectly, you might not be able to recover your system using these drives.

2   Store the hard drives in anti static bags and suitable foam material. (Use the original packaging, if it is available.)

3   Use the jumpers on the drives to set the SCSI IDs. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

4   Replace the drives. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

5   Rebuild the RAID drives, following steps 5 to 17 in "Rebuilding the RAID drives on a 702t" on page 316.

Section D: Performing RAID procedures on a 1003t

In this section

Overview of RAID procedures on a 1003t

Introduction

If your server is equipped with RAID, you can use the RAID subsystem and a spare disk set to create a complete system backup. RAID backups provide a mechanism for fast backup and simple restore.

Splitting and rebuilding the RAID drives

When you are making significant changes to your server—for example, during application of PEPs, you can split the RAID drives. This ensures that only one set of hard drive is affected by the changes. If you have any problems, you can easily back out of the changes by using the other set of hard drives.

When you are satisfied that your system is running properly, you can rebuild the RAID drives.

Note: The procedures for splitting and rebuilding the RAID drives are different for different platforms. Make sure you follow the proper procedure for your platform.

RAID backups and tape backups

RAID backups do not replace tape backups. Even if you are using RAID backups, create a full tape backup after installation, upgrade, or major modifications to the system. Unless you are performing daily RAID backups, you should continue to perform daily database backups.

Note: The procedure for RAID backups is different for different platforms. Make sure you follow the proper procedure for your platform.

Nortel Networks recommends performing a RAID backup procedure for platforms equipped with hot-swap disk configurations.

Performing a consistency check on a 1003t

Introduction

Perform regular consistency checks prior to backing up or splitting a RAID drive. The consistency check is time-consuming, so you might prefer to perform it a few days before splitting or backing up your RAID drives.

Note: A consistency check is not necessary every time you split the RAID drives.

You can perform the consistency check while the server is online, but it degrades server performance. Therefore, Nortel Networks recommends that you perform the operation during non-peak times. A consistency check of a 9-Gbyte volume takes approximately 45 minutes.

To perform a consistency check

1   On the server, log on to Windows NT as NGenSys.

2   Start the NetRAID Assistant utility.

    Result: The Server Selection dialog box appears.

3   Select the local server, and make sure access mode is set to Full Access.

    Result: The NetRAID Assistant window appears.

4   Select the drive you want to check in the Logical Devices list.

5   Choose Logical Drv → Check Consistency.

6   A message appears, asking if you want to parity check selected devices. Click OK.

7   Click OK to close the Consistency Check dialog box.

8   Exit from the NetRAID Express Tools utility.

Splitting the RAID drives on a 1003t

Introduction

Split the RAID drives when you are upgrading the server or applying PEPs or service update packs.

When you split the RAID drives, you are breaking the mirrored image of the RAID hard drives (channels 0 and 1) and disabling the channel 1 hard drives. Any software activity that is performed on the system affects only the channel 0 hard drives. The channel 1 hard drives continue to have the current system configuration, and you can use them to rebuild the RAID hard drives if a problem occurs during conversion.

Full backup with RAID drives is supported for 1003t platforms with the following components:

- a NetRAID controller
- RAID 1
- the NetRAID Assistant utility

Before you begin

- Make sure that the NetRAID subsystem is cabled as specified in the *Meridian Application Server Installation and Maintenance Guide* for your platform.

    Note: Ensure that the SCSI cable is correctly installed. Reversed cables increase the risk of data loss.

- Back up the NetRAID Controller configuration to a disk.
- Make sure you have a full or database tape backup available.
- Make sure that the Windows NT Repair disk is up to date.
- Nortel Networks recommends that you perform a consistency check (see "Performing a consistency check on a 1003t" on page 323).

    Note: A consistency check is not necessary every time you split the RAID drives.

To split the RAID drives

1   On the server, log on to Windows NT as NGenSys.

If you do not have a current backup of your RAID controller configuration, continue with the following steps. If you have a current backup, skip to step 10.

2   Shut down all Symposium Call Center Server services by choosing, from the Windows Start menu, Programs → Symposium Call Center Server → Shutdown.

3   Shut down all Sybase services.

    a.   From the Windows Start menu, choose Programs → Sybase SQL Server Professional → Services Manager.

    Note: If you cannot select Sybase SQL Server Professional, select Sybase for Windows NT.

    b.   Select SQL Server and double-click Stop.

    c.   Select Backup Server and double-click Stop.

    d.   Close the Services Manager window.

4   Start the NetRAID Assistant utility.

Result: The Server Selection dialog box appears.

5   Select the local server, and make sure access mode is set to Full Access.

Result: The NetRAID Assistant window appears.

6   Insert a blank formatted disk.

7   Choose Configuration → Save.

8   Select drive A, type a filename, and click Save to store the configuration.

9   Remove the RAID controller configuration backup disk and close the NetRAID Assistant Utility.

10   Shut down and restart the server.

    a.   From the Start menu, choose Shutdown.

    b.   Click Restart the computer, and click Yes.

Result: During restart, the following message appears: `Option: Experienced User may press <CTRL><M> for NP NetRAID Express Tools Now.`

11 Press Ctrl+M.

Result: The Management menu appears.

12 Select Object and press Enter.

Result: The Object menu appears.

13 Select Physical Drive and press Enter.

Result: The Physical Drive menu appears, displaying a list of drivers, appears.

14 Select drive A0-1 and press Enter.

Result: The Physical Drive menu appears.

15 Select Fail Drive and press Enter.

16 A prompt appears, asking you to confirm your action. Select Yes and press Enter.

Result: The is marked FAIL and is offline.

17 Record the SCSI channel and ID of the drive.

Note: Physical drive locations do not correspond to locations shown on the table in NetRAID Express Tools. Refer to the following tables for correct identification of the drives:

NetRAID Express Tools drive locations

SCSI ID	Channel 0	Channel 1
0	A0-0	A0-1
1	A1-0	A1-1
2	A2-0	A2-1

1003t physical drive locations

SCSI ID	Channel 1	Channel 0
2	A2-1	A2-0
1	A1-1	A1-0
0	A0-1	A0-0

18   Repeat steps 14 to 17 for the remaining system packs (A1-1, A2-1).

19   Exit from the NetRAID Express Tools utility by pressing Esc three times.

20   When you are prompted to confirm your action, select Yes and press Enter.

21   Power down the server.

22   Unseat the drives marked FAIL from their slots, but do not remove them.

Note: If you decide to remove the drives, be sure to label them with their SCSI channel and ID and store them in antistatic bags and suitable foam material.

CAUTION

Risk of data loss

If you label drives incorrectly, you might not be able to recover your system using these drives.

23   Power up the server.

Rebuilding the RAID drives on a 1003t

Introduction

Use this procedure after you have split the RAID drives and you are confident about the operation of your system.

Assumptions

This procedure assumes that you are rebuilding the RAID drives using the drives that were split previously. If you are using new drives, make sure you do the following tasks:

- Set the SCSI IDs for the new drives to 0.

- Format the new drives (see "Formatting drives on a 1003t" on page 332).

To rebuild the RAID drives

1   Shut down the server.

   a.   From the Start menu, choose Shutdown.

   b.   Click Shut down the computer, and click Yes.

2   Power down the server.

3   Install the drives. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

4   Power on the server.

   Result: POST messages from the RAID controller warn you that the system is operating in critical mode (that is, with some drives offline). The following message appears: `Option: Experienced User may press <CTRL><M> for HP NetRAID Express Tools Now.`

5   Press Ctrl+M.

   Result: The Management menu appears.

   Note: Because the NetRAID controller is in critical state, the utility may display a list of the current SCSI buses, in which the channel 0 drives are ONL and the channel 1 drives are FAIL.

6   Select Rebuild and press Enter.

   Result: A list of drives appears.

7   Highlight each new drive, and press Space.

8   Press F10.

   Result: The utility begins rebuilding the drive. The process of rebuilding a 9-Gbyte volume takes approximately 45 minutes.

9   Exit from the NetRAID Express Tools utility.

Performing a RAID backup on a 1003t

Introduction

Full backup with RAID drives is supported for 1003t platforms with the following components:

- a NetRAID controller
- RAID 1
- the NetRAID Assistant utility

Before you begin

- Make sure that the NetRAID subsystem is cabled as specified in the *Meridian Application Server Installation and Maintenance Guide* for your platform.
  Note: Ensure that the SCSI cable is correctly installed. Reversed cables increase the risk of data loss.
- Back up the NetRAID Controller configuration to a disk.
- Make sure you have a full or database tape backup available.
- Make sure that the Windows NT Repair disk is up to date.
- Make sure that you have a new or blank hard drive for each RAID system pack. If the drive is not new, it must be formatted (see "Formatting drives on a 1003t" on page 332).
- Nortel Networks recommends that you perform a consistency check (see "Performing a consistency check on a 1003t" on page 323).
  Note: A consistency check is not necessary every time you split the RAID drives.

To perform a RAID backup

1   Split the RAID drives, following steps 1 to 21 in "Splitting the RAID drives on a 1003t" on page 324.

2   Remove the hard drives marked FAIL, and label them with their SCSI channel and ID. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

CAUTION

Risk of data loss

If you label drives incorrectly, you might not be able to recover your system using these drives.

3   Store the hard drives in antistatic bags and suitable foam material. (Use the original packaging, if it is available.)

4   Make sure that the SCSI IDs are set to 0 on the new or blank formatted hard drives. (If a drive is not new, you must format it. See "Formatting drives on a 1003t" on page 332.)

5   Insert the hard drive. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

6   Rebuild the RAID drives, following steps 4 to 8 in "Rebuilding the RAID drives on a 1003t" on page 328.

Formatting drives on a 1003t

Introduction

Use either the NetRAID Express Tools or the NetRAID Assistant procedure to format the drives on a 1003t. The NetRAID Express Tools method requires the server to be offline. The NetRAID Assistant method enables you to keep the server online.

Note: Formatting destroys all the data on the drive. Make sure that you select the correct drive.

To format drives

Using NetRAID Express Tools

1   Shut down the server.

    a.   From the Start menu, choose Shutdown.

    b.   Click Shut down the computer, and click Yes.

2   Power down the server.

3   Make sure that the SCSI IDs are set to 0 on the hard drives. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

4   Insert the drives. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

5   Power on the server.

    Result: POST messages from the RAID controller warn you that the system is operating in critical mode (that is, with some drives offline). The following message appears: `Option: Experienced User may press <CTRL><M> for NP NetRAID Express Tools Now.`

6   Press Ctrl+M.

    Result: The Management menu appears.

7   Select Object and press Enter.

    Result: The Object menu appears.

8   Select Physical Drive and press Enter.

Result: A list of drives appears.

9   Select the drive that you want to format. Ensure that you do not select the existing drive that contains your data. Press Enter.

Result: The Physical Drive menu appears.

10   Select Fail Drive.

11   Select Format and press Enter.

Result: The utility formats the drive. The process of formatting of a 9-Gbyte volume takes approximately 45 minutes.

Using NetRAID Assistant

1   Shut down the server.

    a. From the Start menu, choose Shutdown.

    b. Click Shut down the computer, and click Yes.

2   Power down the server.

3   Make sure that the SCSI IDs are set to 0 on the hard drives. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

4   Insert the drives. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

5   Power on the server.

Result: POST messages from the RAID controller warn you that the system is operating in critical mode (that is, with some drives offline). The following message appears: `Option: Experienced User may press <CTRL><M> for NP NetRAID Express Tools Now.`

6   Log on to Windows NT as Administrator.

7   Start the NetRAID Assistant utility.

Result: The Server Selection dialog box appears.

8   Select the local server, and make sure access mode is set to Full Access.

Result: The NetRAID Assistant window appears.

9   In the Physical Devices list, select the drive that you want to format. Ensure that you do not select the existing drive that contains your data.

10 Select Fail Drive.

11 Choose Physical Drv → Format.

> **Result:** The utility formats the hard drive. The process of formatting of a 9-Gbyte volume takes approximately 45 minutes.

Chapter 13

Restoring data

In this chapter

Overview of recovery procedures

Which procedures to use

The following tables outline the types of failures and the procedures you must follow to recover the system.

Systems without RAID controllers

If you experience the following type of failure	Then refer to this section
Primary or secondary hard drive fails or File system (NTFS) corruption	Section B: "Restoring the complete system (non-RAID)" on page 343
Database is corrupted	Section A: "Restoring the database" on page 337

Systems with RAID controllers

If you experience the following type of failure	Then refer to this section
Primary or secondary hard drive fails or File system (NTFS) corruption	Section C: "Recovering a 702t RAID system" on page 385 or Section D: "Recovering a 1003t RAID system" on page 397
Database is corrupted	Section A: "Restoring the database" on page 337

Section A: Restoring the database

In this section

Restoring the Symposium Call Center Server database

Introduction

Use the Symposium Call Center Server database restore utility to restore the database.

The restore process causes the connection between the client PC and server to be lost, and the services on the server to be shut down. After the restore process is finished, restart the server, and reconnect the client PC.

As the restore progresses, the status information is displayed in the Status group box.

ATTENTION   After a major system failure, you must recover the system using one of the methods described in Section B: "Restoring the complete system (non-RAID)" on page 343. After the system is recovered, you can restore the database using the steps described below.

To restore the Symposium Call Center Server database

1   Log on to Windows NT as NGenSys.

2   Insert the database backup tape.

3   From the Windows Start menu, choose Programs → Symposium Call
        Center Server → Database Restore.

        Result: The Database Restore window appears.
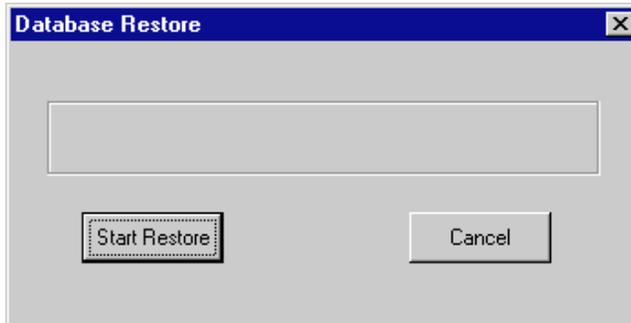
4   Click Start Restore to begin the database restore process.

        Result: The message `Please ensure the database backup tape`
        `is in the tape drive` appears.

5   Click OK to continue.

        Note: The database takes one to three hours to restore, depending on the
        amount of data, and the following dialog box appears.
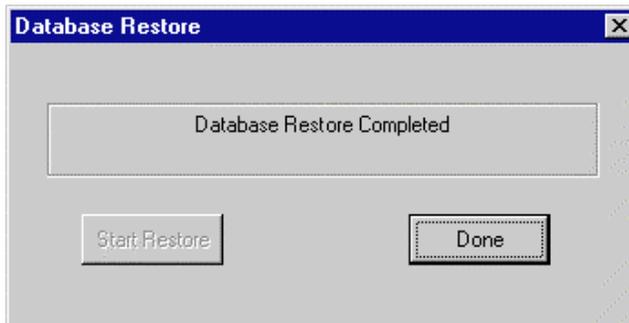
        A log file is created with the following pathname after the database restore
        is completed: D:\Nortel\data\backup\RestoreLogs\restore.log.

6 Click Done.

Result: The following dialog box appears.

7 Eject the backup tape from the tape drive and then click OK to exit the Database Restore utility. Do not restart the server.

8 From the Windows Start menu, choose Programs → Symposium Call Center Server → Migration.

Result: The Platform Migration Utility dialog box appears.
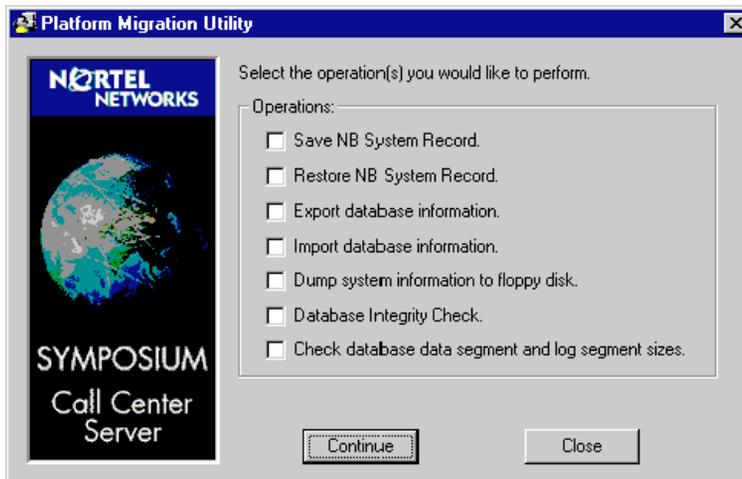
9   Select the Database Integrity Check option. Click Continue.

   Result: The following dialog box appears:
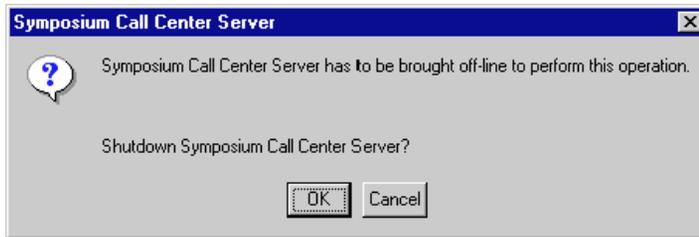
10   Click OK.

   Result: The following dialog box appears:

11   Click OK to start the database integrity check.

   Note: Since the database integrity check takes some time to complete, you might not see any active activity on the screen. However, you should notice continuous disk activity. Wait until the following dialog box appears:

12   Click OK to exit the utility.

13   Check the log file (C:\DbChk.log) for errors. To do so, open the log file in a text editor (such as NotePad), and search for the text ERROR or MSG.

14   Restart the server.

Section B: Restoring the complete system (non-RAID)

In this section

Overview

Introduction

The procedures in this section provide instructions for recovering a system from

- a hardware failure (for example, a hard drive failure)

    or

- file corruption that affects more than the Symposium Call Center Server database or DMI database

ATTENTION	You cannot simply reinstall the Symposium Call Center Server and then do a database restore. You must recover the system, using one of the methods described in this section.

Types of recovery

Two methods are available for full system recovery:

- using the Platform Recovery disk
- using a full system backup

Note: When you restore from a full backup, details such as network addresses, drivers, and services are reset during the full restore.

Recovering with a Platform Recovery disk

Introduction

If you have a current Platform Recovery disk and recent database backup, you can use the this recovery method.

Note: Before using this method, check the Nortel Networks web site, www.nortel-sccs.com, for updated Installation Addendums.

Requirements

Step	✔
Two blank formatted disks	
Installation media for MS-DOS v6.20 (three disks)	
Symposium Call Center Server Operating System CD	
Symposium Call Center Server Application CD	
Latest database backup tape of the server	
Platform Recovery disk	
Printout of the Miginfo.txt file, located on the Platform Recovery disk This file contains the setup information for the system you are recovering, and is used during installation and configuration of Windows NT and the Symposium Call Center Server.	
Head-cleaning kit	

Checklist for recovering with a Platform Recovery disk

Description	✔
Replace the faulty hard drive if the hard drive is not usable. For instructions, refer to the *Maintenance Guide* for your hardware platform.	
Partition the hard drive. For instructions, refer to the *Meridian Application Server Maintenance Guide* for your hardware platform.	
Install MS-DOS. For instructions, refer to the *Meridian Application Server Guide* for your hardware platform.	
Install Windows NT 4.0 Server. Make sure that the computer name matches the original computer name assigned to the server being recovered. For instructions, refer to the *Meridian Application Server Guide* for your hardware platform. **Note:** Install Windows NT in the WIN NT directory on drive D.	
Install the tape device driver. For instructions, refer to the *Meridian Application Server Maintenance Guide* for your hardware platform.	
Install Windows NT 4.0 Server Service Pack 3. See page 373.	
Apply the Microsoft hot fix. See page 348.	
Format optional hard drives, if applicable. Refer to the *Software Installation and Upgrade Guide.*	
Check and correct drive letter mapping. See page 349.	
Install the Symposium Call Center Server software. See page 352.	
Clean the tape drive using the appropriate head-cleaning kit. Follow the instructions provided with the head-cleaning kit.	
Restore the database. See page 364.	

To install Windows NT 4.0 Server Service Pack 3

1 Log on to the server as Administrator.

2 Insert the Symposium Call Center Server Operating System CD in the CD-ROM drive.

Result: The Windows NT Setup Splash screen appears.

3 Click Close to close the screen.

4 From the Start menu, choose Programs → Windows NT Explorer.

Result: The Windows NT Explorer screen appears.

5 Click the plus sign (+) next to the CD-ROM drive to display its subdirectories.

6 Select the directory named sp3.

7 Locate the file Update.exe, and double-click to run it.

Result: A welcome screen appears.

8 Click Next.

9 Click Yes to accept the license agreement.

10 Click Next to Install the service pack.

11 Select Yes, I want to create an uninstall directory, and click Next to continue.

12 Click Finish to finish installing the service pack.

Result: The program examines the system, selects the files to copy and then copies them. If messages display, refer to the next three steps for the action to take in response.

Note: As the files are installed, the following message might appear: `The target file exists and is newer than the source. Overwrite the newer file?` Click No.

The following screen might also display:

Click No.

13 When the following message appears, remove the CD from the CD-ROM drive and click OK:

To apply the Microsoft hot fix

1 Make sure that hidden files are visible. To do so, follow these steps:

a. In Windows NT Explorer, choose View → Options.

b. Select Show all files.

c. Click Apply, and then click OK.

2 Copy the folder Hotfixes\Microsoft\q178741 on the CD to the root of drive D.

3 In Windows NT Explorer, click the D:\Hotfixes\Microsoft\q178741 folder.

4 Double-click the file hfx.exe, located in this folder.

Result: The Hotfix Manager window opens.

5 Click InstallNewFix.

Result: The Install Path dialog box opens.

6   Make sure that the path specified is
d:\Hotfixes\Microsoft\q178741\hotfix.inf. If it is not correct, browse to this
path.

7   Click OK.

Result: The program installs the hot fix on the server. When the installation
is complete, the program notifies you that Windows NT has been updated.

8   Click OK.

Result: The system prompts you to restart. Do not click OK yet.

9   When the HotFix Manager appears, click Done.

10   Restore the settings for hidden files. To do so, follow these steps:

   a.   In Windows NT Explorer, choose View → Options.

   b.   Select Hide files of these types.

   c.   Click Apply, and then click OK.

11   Click OK to restart the server.

Result: The server restarts.

Note: If the server hangs during the restart, restart it manually.

Formatting optional hard drives

If the system contains optional hard drives, you must format them. For detailed
instructions, see the *Software Installation and Upgrade Guide.*

Checking and correcting the drive letter assignments

Use this procedure if the drive letter assignments do not match the original
assignments on the server.

To check the drive letter assignment

1   From the Windows Start menu, choose Programs → Administrative Tools
→ Disk Administrator.

2   If the Disk Administrator has never been run before, it must update the
system configuration. Click OK to let it do so.

3 For any new disks in the system, the Disk Administrator warns you that there is no signature on the disk. Click OK to allow the signature to be written to disk. You must repeat this step for each new disk in the system.

4 Check whether the hard drives have the same drive letter assignments as before.

5 If the drive letter assignments match, exit the Disk Administrator by selecting Partition → Exit from the Disk Administrator window.

6 If the drive letter assignments do *not* match, use the following steps to reassign the drive letters on the new server to the drive letter assignments of the original server.

To change the drive letter assignment

Note: Disk Administrator does not let you reassign a hard drive to a drive letter that is currently in use by another drive. You must first assign each hard drive to a temporary drive letter and restart the server before the drive letters can be reset to the correct order.

1 Assign the CD-ROM drive to the last available drive letter as follows:

a. From the Disk Administrator window, select Tools → Assign CD-ROM Drive Letters.

b. In the CD-ROM Drive Letters dialog box, change the drive letter to the last available letter, and then click Change.

c. In the confirmation window, confirm that the drive letter should be changed immediately by clicking Yes.

2 For each hard drive partition (excluding the C: partition), change the drive letter to the last available drive letter:

a. Start with the second partition on drive 0, and click the partition to select it.

b. From the Disk Administrator window, select Tools → Drive Letter.

c. In the Assign Drive Letter dialog box, change the drive letter to the last available drive letter and then click OK.The Disk Administrator warns you that the drive cannot be locked for exclusive use (so the drive letter cannot be changed immediately).

d. Click OK to continue.

e. In the confirmation dialog box, click Yes to change the drive letter when the system is next restarted.

f. Repeat step 2 for each remaining hard drive partition in the system.

Note: When you change the drive letters on the remaining partitions, you are informed that the drive letters can be changed immediately (click Yes to do so). This is because the partitions are not the primary partition (the one with the operating system installed on it).

3 From the Disk Administrator window, select Partition → Commit Changes Now to save the drive letter assignment.

Result: A message appears warning you that you should update the emergency repair disk.

4 Click OK to continue.

Result: The system alerts you that the server must now be restarted to allow the drive letters to be changed.

5 Click OK to shut down and restart the server.

6 After the server restarts, log on to the server as the Administrator. After you log in, a message appears in the System dialog box.

7 Click Cancel to exit.

8 Assign the CD-ROM drive to the correct drive letter:

a. From the Disk Administrator window, select Tools → Assign CD-ROM Drive Letters.

b. In the CD-ROM Drive Letters dialog box, change the drive letter to the correct letter and then click Change.

c. In the confirmation window, confirm that the drive letter should be changed immediately by clicking Yes.

9 For each hard drive partition (excluding the C: partition), change the drive letter to the correct drive letter:

a. Start with the extended partition on drive 0, and click the partition to select it.

b. From the Disk Administrator window, select Tools → Drive Letter.

c. In the Assign Drive Letter dialog box, change the drive letter to the correct drive letter, and then click OK. The Disk Administrator warns you that the drive cannot be locked for exclusive use (so the drive letter cannot be changed immediately).

d. Click OK to continue.

      e. In the confirmation dialog box, click Yes to change the drive letter when the system is next restarted.

      f. Repeat step 8 for each remaining hard drive partition in the system.

      Note: When you change the drive letters on the remaining partitions, you are informed that the drive letters can be changed immediately (click Yes to do so). This is because the partitions are not the primary partition (the one with the operating system installed on it).

10 From the Disk Administrator window, select Partition $\rightarrow$ Commit Changes Now. to save the drive letter assignment.

      Result: A message appears warning you that you should update the emergency repair disk, click OK to continue.

      Result: The system alerts you that the server must now be restarted to allow the drive letters to be changed.

11 Click OK to shut down and restart the server.

12 After the server restarts, log on to the server as the Administrator.

To install the Symposium Call Center Server software

You must install the Symposium Call Center Server software version and PEPs originally installed on the server.

1 Log on to the Windows NT as Administrator.

2 Insert the Platform Recovery Disk into drive A of the new server.

3 Open a command prompt and type the following commands:

A: <Enter>
sysrecres.exe <Enter>

Result: The Platform Migration Utility window appears.
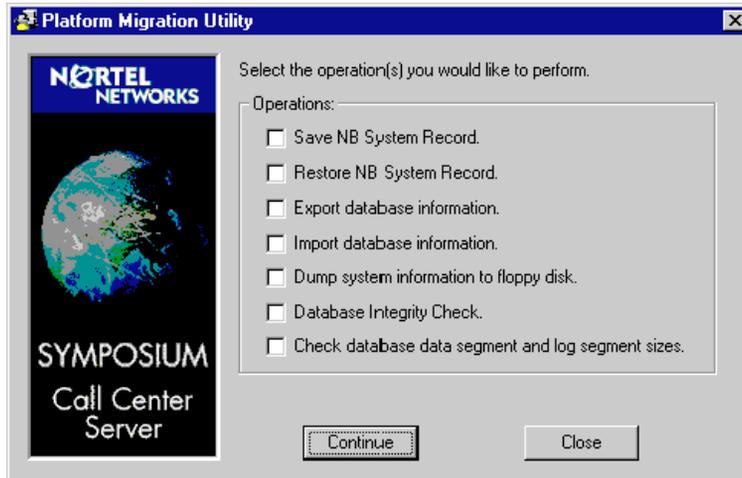
4 Select Import database information from the selection dialog box. Click Continue.

Result: The following dialog box appears:
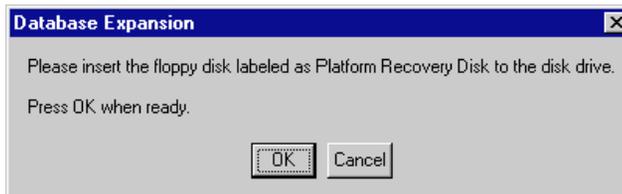
5 Make sure the Platform Recovery disk is in drive A and that it is not write-protected. Click OK to continue.

Result: The database information is imported to the new server.

> **ATTENTION**
>
> If you see the message `Please eject the floppy disk from the drives and start the Symposium Call Center Server installation`, click OK and then proceed with steps 6 through 14. If you see the message `This platform cannot support platform migration. There is not enough disk space`, click OK, proceed with steps 6 and 7, and then follow the procedure "To adjust the swap file" on page 356. You will be asked to perform steps 8 through 14 after you complete the procedure "To adjust the swap file" on page 356.

6 Remove the disk from Drive A and click OK.

Result: The sysrecres.exe utility is terminated.

Note: It is important that you import the platform database configuration be imported before you install the Symposium Call Center Server software. Failure to do so can cause a database restoration error.

7 Close the command prompt window.

> **ATTENTION**
>
> If you saw the message in step 5 `This platform cannot support platform migration. There is not enough disk space`, follow the procedure "To adjust the swap file" on page 356 now. You will be asked to perform steps 8 through 14 after you complete the procedure "To adjust the swap file" on page 356.

8 Install the Symposium Call Center Server software using the same options as for the original installation. Refer to the MigInfo.txt file on the Platform

Recovery disk for server details. For details about installing Symposium Call Center Server, see the *Software Installation and Upgrade Guide*.

ATTENTION

During the third phase of the installation (that is, after all the Symposium Call Center Server-specific information has been entered),

- if you see the message `The database will take between 1 to 3 hours to create...`, then the platform migration is proceeding and should complete successfully.

- if you see the message `This platform cannot support platform migration. There is not enough disk space`, click OK. If the following two error messages appear, click OK to abort the migration procedure. Then, check whether the swap file on drive D is reduced to 32 Mbytes or not. If it is not reduced to 32 Mbytes, go to the procedure "To adjust the swap file" on page 356. If it is reduced to 32 Mbytes already, contact your Nortel Networks customer support representative.

Error ✕

An ERROR occured while executing.
Please check the D:\Nortel\iccm\dbinst\sysmig.txt logfile for details

[OK]

Symposium Call Centre Server ✕

Could not create the database

[OK]
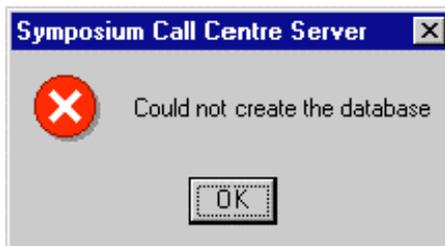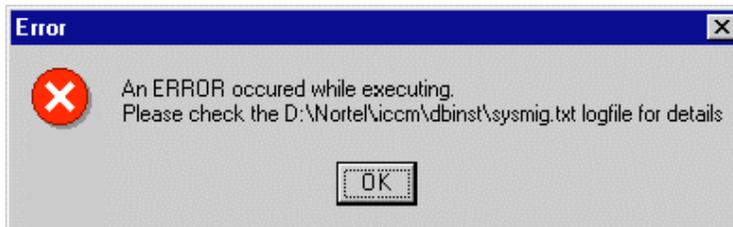
Notes:

- It is very important that you install the new server with the same Symposium Call Center Server software version as the original server.

- It is not necessary to configure the new server in Configuration Mode during installation of the Symposium Call Center Server software.

- If the server is a DMS/MSL server type, the Symposium Call Center Server installation does not need the Nortel Networks software feature key adapter (dongle) to be connected to the LPT1 parallel port of the new server during the installation procedures.

9   After installation of the Symposium Call Center Server software, restart the new server.

10 Log on to Windows NT as NGenSys.

11 If the swap file was reduced to 32 Mbytes during step 5 or 8 and the swap file should remain on drive D (since it was on drive D on the original server), follow the procedure "To move the swap file from drive D for Windows NT 4.0" on page 360. This moves the swap file to the next available drive, as the D drive would not have sufficient free drive space if the swap file was extended to the required 268 Mbytes.

12 If the swap file was on a drive other than D and the new server has the same size D drive partition as the original server, follow the procedure "To move the swap file from drive D for Windows NT 4.0" on page 360.

13 Apply the same Performance Enhancement Packages (PEP) level to the new server as in the original server.

    Note: It is very important that the new server be installed with the platform migration support PEP and the minimum backup and restore PEP level for the corresponding version. PEPs are available at the Nortel Networks web site www.nortel-sccs.com.

14 With the Symposium Call Center Server software successfully installed, continue with "To restore the database" on page 364.

To adjust the swap file

If the physical disk space on drive D cannot accommodate the old database size, an error message appears stating `This platform cannot support platform migration. There is not enough disk space.`

■   If this message appears when the database information is being imported (steps 1 to 5 in "To install the Symposium Call Center Server software" section), skip the first nine steps and perform steps 10 and 11 as follows.

■   If this message appears during installation of the Symposium Call Center Server software (step 8 in the "To install the Symposium Call Center Server software" section), proceed with steps 1 to 11 as follows.

1   Click OK to abort the migration procedure.

2   Check the log file D:\Nortel\iccm\dbinst\sysmig.txt to determine how much more space is required.

3   If the log file indicates that the required disk space is greater than 268 Mbytes, then the new server does not have sufficient disk space on drive D. For assistance, contact your Nortel Networks customer support representative.

4   If the required disk space is less than 268 Mbytes, clean the Symposium Call Center Server installation by running uninstall. From the Windows Start menu, choose Programs → Symposium Call Center Server → Uninstall.

5   Click Select All to uninstall all the components for both MAS and Symposium Call Center Server.

6   Follow the on-screen instructions to complete the uninstall process. See the *Software Installation and Upgrade Guide.*

7   When prompted to restart the system, click No.

8   Run uninstall one more time. From the Windows Start menu, choose Programs → Symposium Call Center Server to remove DMI. Follow the on-screen instructions.

9   When prompted to restart the system, click OK.

10   Once the system has restarted, reduce the swap file size on drive D, setting both minimum and maximum values to 32 Mbytes using the procedure "To reduce the swap file size on drive D" on page 358.

11   Perform steps 8 to 14 in the procedure "To install the Symposium Call Center Server software" on page 352 to install Symposium Call Center Server software. If you do not see the message `The database will take between 1 to 3 hours to create...`, contact your Nortel networks customer support representative.

To reduce the swap file size on drive D

Use this procedure only if instructed from the procedure "To adjust the swap file" on page 356.

1   From the Windows Start menu, choose Settings → Control Panel, and then double-click the System icon.

Result: The System Properties window appears.
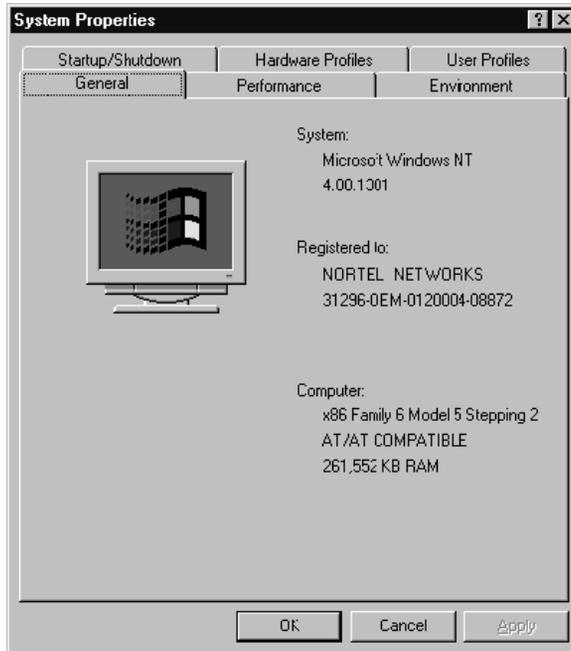
2 Click the Performance tab.

Result: The Performance tab appears.
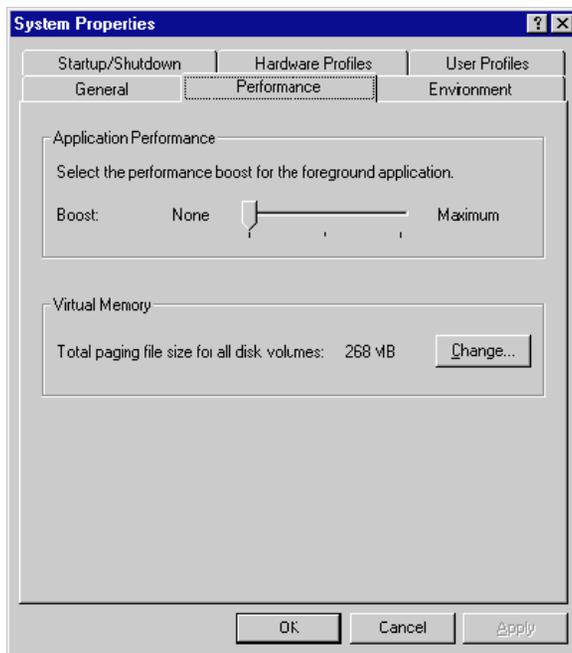
3   Click the Change button in the Virtual memory section.

Result: The Virtual Memory settings appear.
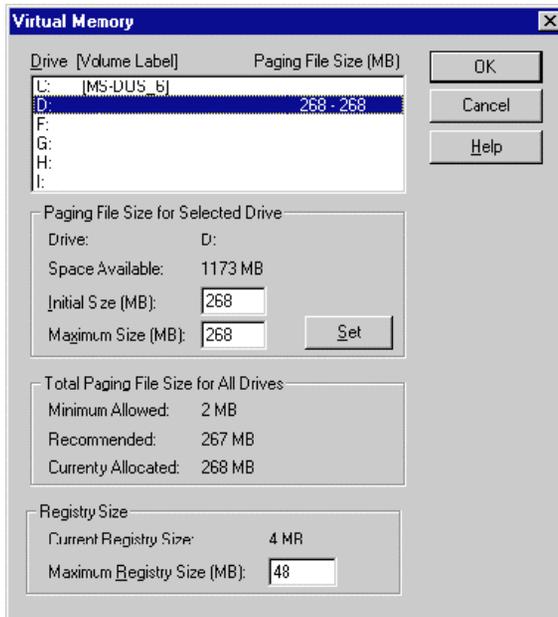
4   Highlight drive D.

5   Type **32** for both Initial Size (MB) and Maximum Size (MB).

6   Click Set and accept any warnings presented.

7   Click OK.

8   Restart the server when prompted.

To move the swap file from drive D for Windows NT 4.0

Use this procedure only if instructed from the procedure "To adjust the swap file" on page 356, or "To install the Symposium Call Center Server software" on page 352.

1   From the Windows Start menu, choose Settings → Control Panel, and then double-click the System icon.

Result: The System Properties window appears.
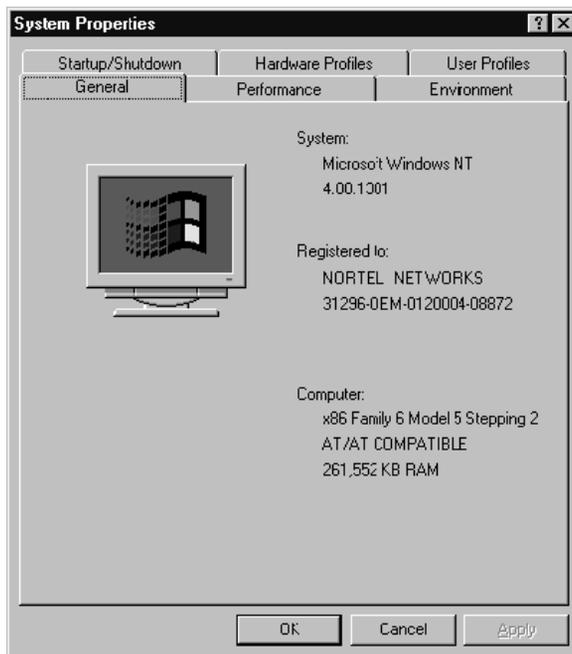
2   Click the Performance tab.

Result: The Performance tab appears.
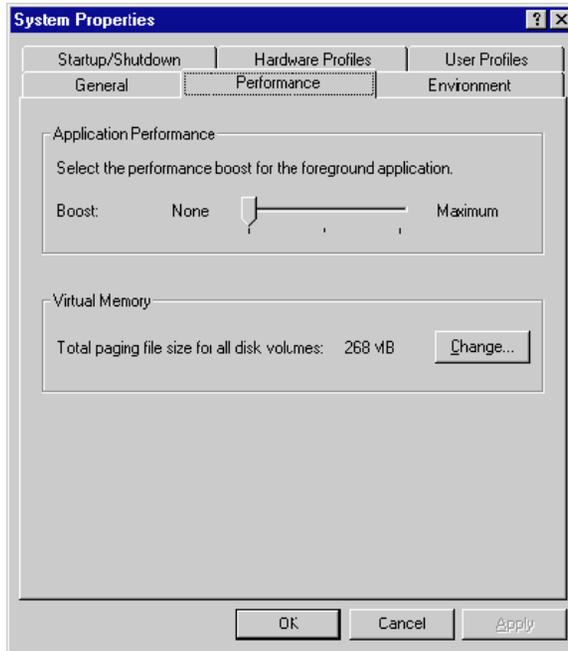
3   Click Change in the Virtual memory section.

       Result: The Virtual Memory settings appear.
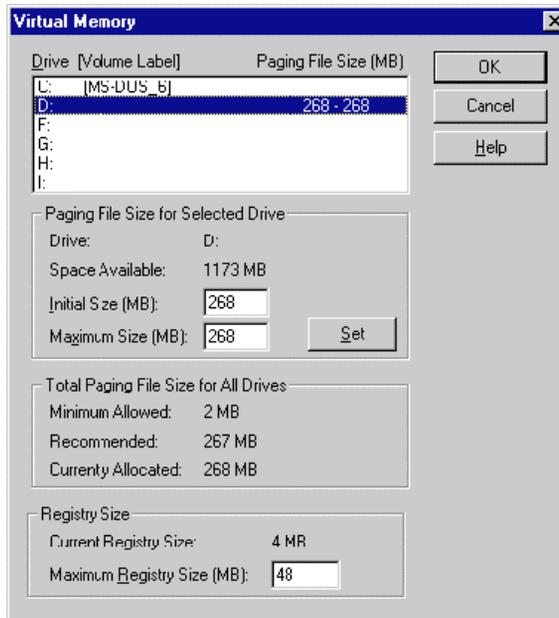
4   Highlight drive F, or the first drive letter that appears after the D drive.

5   Ensure that there are at least 288 Mbytes of available space.

6   If there is not enough available space, select the next available drive and repeat steps 4 and 5. If you check all drives and none have 288 Mbytes of available space, contact your Nortel Networks customer support representative for assistance.

7   Highlight drive D to display the existing swap file Initial Size (MB) and Maximum Size (MB).

8   Type **0** for both Initial Size (MB) and Maximum Size (MB).

9   Click Set and accept any warnings presented.

10   Select the drive identified in steps 4 through 6.

11   Type **268** for both Initial Size (MB) and Maximum Size (MB), and click Set.

12   Click OK to apply the changes.

13 Click Close in the System Properties window.

Result: The system indicates that a restart is required.

14 Click Yes to restart the system now.

To restore the database

The final part of the recovery procedure involves restoring the database backup. The new server need not be connected to the network or the M1 or DMS switch.

1 From the Windows Start menu, choose Programs → Symposium Call Center Server → Migration.

Result: The Platform Migration Utility dialog box appears.
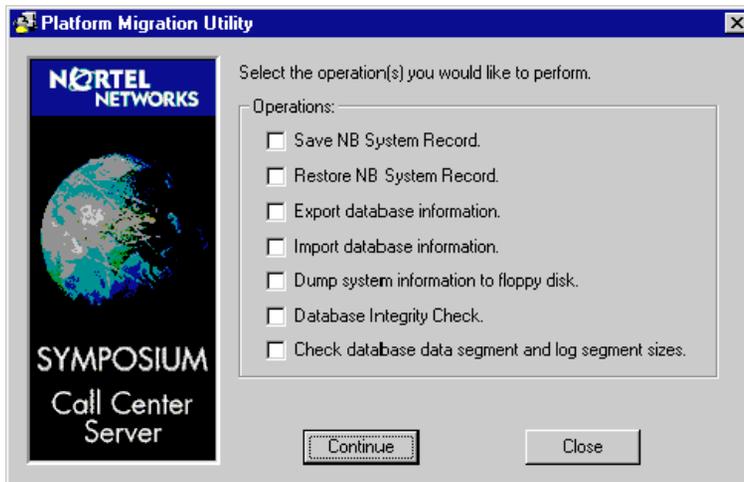
2 Choose the Save NB System Record option. Click Continue.

Result: The following dialog box appears:
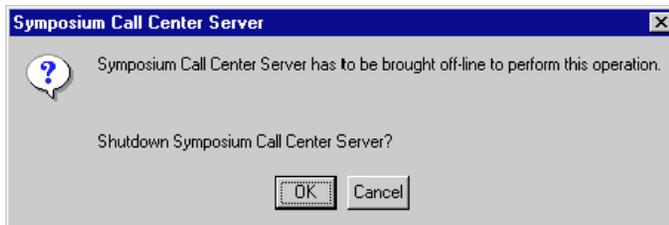
3   Click OK to shut down the Symposium Call Center Server.

Result: When the Symposium Call Center Server shuts down, the following dialog box appears:

4   Insert a blank preformatted disk into the floppy disk drive, and click OK to continue after the disk is inserted.

Result: The following dialog box appears:

5   Eject the disk and label it as instructed. Click OK to terminate the utility (the utility closes automatically after you click OK). Save the NBSystemRecord backup disk for step 17.

6   Insert the database backup tape from the original platform into the tape drive of the new platform.

Note: The new platform must have a tape drive and driver software compatible with the original platform. The new platform must be installed with the minimal backup and restore PEP level before you can proceed to the next step. The computer name of the new server must be the same as that of the original server.

7   On the new server, from the Windows Start menu, choose Programs →
Symposium Call Center Server → Database Restore to migrate the original
platform database to the new platform.

Result: The Database Restore window appears.
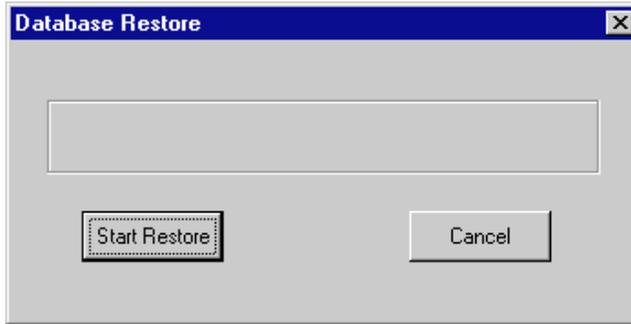
8   Click Start Restore to begin the database restore process.

Result: The message `Please ensure the database backup tape`
`is in the tape drive appears.`

9   Click OK to continue.

Note: The database takes one to three hours to restore, depending on the
amount of data. The following dialog box appears:
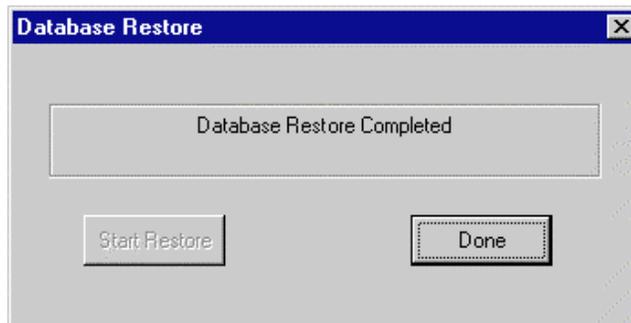
10   Click Done.

   Result: The following dialog box appears:

11   Eject the backup tape from the tape drive, and then click OK to exit the
        Database Restore utility. *Do not* restart the server.

12   From the Windows Start menu, choose Programs → Symposium Call
        Center Server → Migration.

   Result: The Platform Migration Utility dialog box appears.
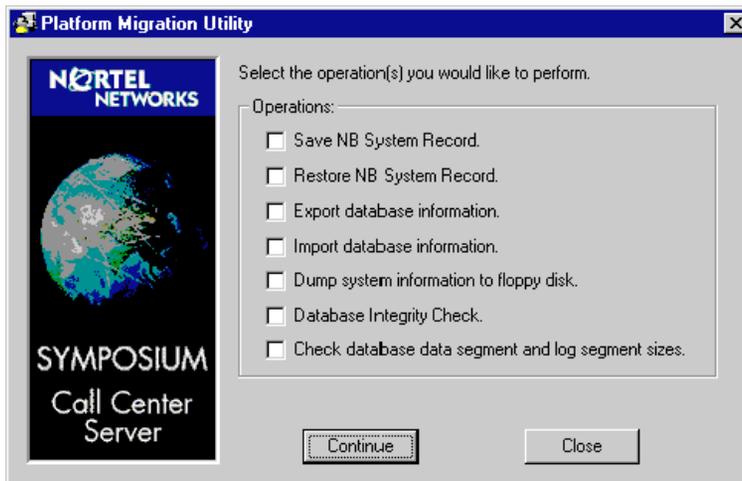
13   Select the Restore NB System Record option. Click Continue.

Result: The following dialog box appears:
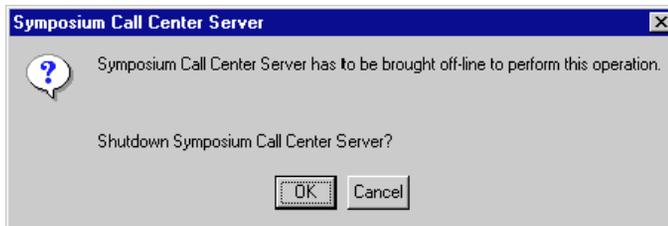
14   Click OK to shut down the Symposium Call Center Server.

Result: When the Symposium Call Center Server shuts down, the following dialog box appears:
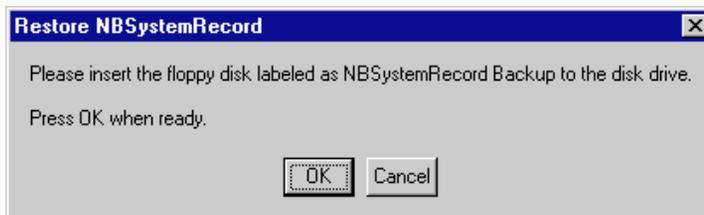
15   Insert the NBSystemRecord Backup disk created in steps 4 to 6 into the drive, and click OK to continue.

Note: It takes some time for the database server to recover from the database restore and can take several minutes for the SQL database server to start up properly. The utility waits until the SQL server is completed before restoring the NBSystemRecord table. Wait until the following dialog box appears:

16 Eject the NBSystemRecord Backup disk from the drive, and then click OK to continue.

Result: The selection dialog box appears.
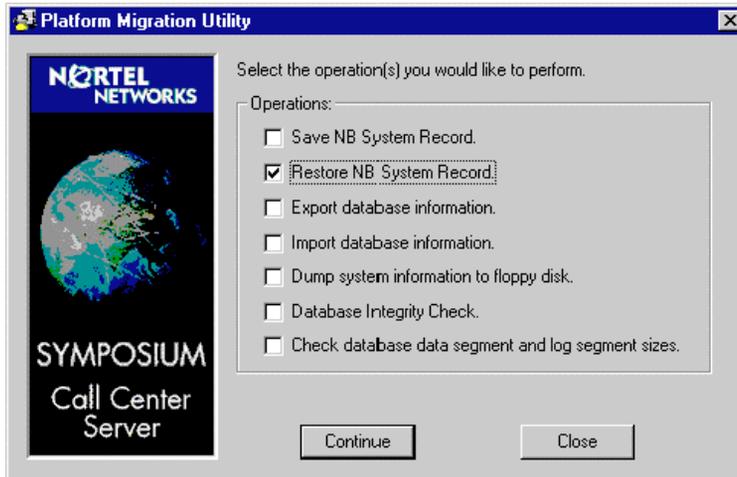
17 Select the Database Integrity Check option. Click Continue.

Result: The following dialog box appears:
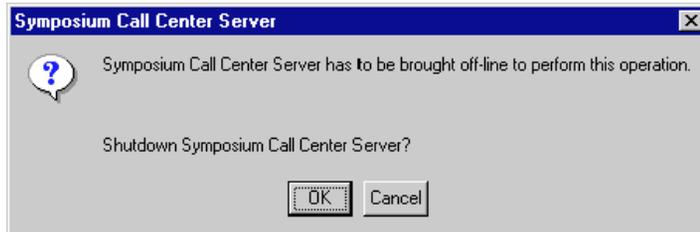
18 Click OK.

Result: The following dialog box appears:
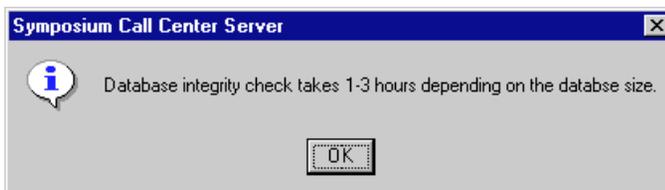
19 Click OK to start the database integrity check.

Note: The database integrity check takes a while to complete, and you might not see any activity on the screen, but you should notice continuous disk activity. Wait until the following dialog box appears:

20 Click OK to terminate the utility (the utility closes automatically when you click OK).

21 View the database check log (C:\DbChk.log) for any possible database errors.

Note: Contact your Nortel Networks customer support representative for any detected database errors. *Do not* put the server into service with any detected database error, even though it might seem to be functioning normally. When checking the log file, search for key words such as ERROR or MSG.

22 Restart the server.

Recovering with a full backup tape

Introduction

If you do not have a current Platform Recovery disk and recent database backup, but you have a full system backup, use the full backup recovery method.

Requirements

Step	✔
Advanced technical knowledge in Windows NT	
Replacement hard drive with a capacity that is the same as or greater than that of the drive being replaced	
Recovery disks to install the restore service and utility (three)	
Installation media for MS-DOS v6.20 (three disks)	
Installation media for Windows NT Server 4.0 (three disks)	
Installation media for the Symposium Call Center Server Operating System (CD-ROM)	
Full backup tape of the server	
Latest database backup tape of the server	
Head-cleaning kit	

Checklist for recovering with a full backup tape

Step	✔
Replace the faulty hard drive if the hard drive is not usable. For instructions, refer to the *Meridian Application Server Guide* for your hardware platform.	

Step	✔
Partition the hard drive. For instructions, refer to the *Meridian Application Server Maintenance Guide* for your hardware platform.	
Install MS-DOS. For instructions, refer to the *Maintenance Guide* for your hardware platform. (This is a temporary copy, and it will be replaced by the copy on the full system backup.)	
Install Windows NT 4.0 Server. For instructions, refer to the *Meridian Application Server Maintenance Guide* for your hardware platform. (This is a temporary copy, and it will be replaced by the copy on the full system backup.) **Note:** Install Windows NT to the WIN_TMP directory on drive D. Also ensure that networking is installed.	
Install the tape device driver. For instructions, refer to the *Maintenance Guide* for your hardware platform.	
Install Windows NT 4.0 Server Service Pack 3. See page 373.	
Reduce the size of the swap file. See page 376.	
Format optional hard drives, if applicable. Refer to the *Software Installation and Upgrade Guide.*	
Clean the tape drive using the appropriate head-cleaning kit. Follow the instructions provided with the head-cleaning kit.	
Restore the full backup. See page 379.	
Reassign drive letters. See page 380.	

Step	✔
Rebuild the system from the state of the last full backup to the state it was in when the hardware failure or data corruption occurred. To do this, follow the steps below in the order they occurred since the last full backup: ■ Perform any software upgrades that occurred since the last full backup. ■ Reinstall PEPs that were installed since the last full backup. ■ Restore the database backup if it is more up to date than the last full backup.	
Bring up the restored server. Make sure all services come up, and log on from a client PC. Monitor the Event Log for problems.	
After confirming that the restore was successful, delete the following directories: ■ the temporary Windows NT directory (d:\win_tmp) ■ d:\nortel_temp	

To install Windows NT 4.0 Server Service Pack 3

1   Insert the Symposium Call Center Server CD-ROM in the CD-ROM drive.

   Result: The Windows NT Setup Splash screen appears.

2   Click Close to close the screen.

3   From the Start menu, choose Programs → Windows NT Explorer.

   Result: The Windows NT Explorer screen appears.

4   Click the plus sign (+) next to the CD-ROM drive to display its subdirectories.

5   Select the directory named sp3.

6   Locate the file Update.exe, and double-click to run it.

   Result: A welcome screen appears.

7   Click Next.

8   Click Yes to accept the license agreement.

9 Click Next to Install the service pack.

10 Select Yes, I want to create an uninstall directory, and click Next to continue.

11 Click Finish to finish installing the service pack.

Result: The program examines the system, selects the files to copy, and then copies them. If messages display, refer to the next three steps for the action to take in response.

Note: As the files are installed, the following message might appear: `The target file exists and is newer than the source. Overwrite the newer file?` Click No in response.

The following screen also might appear:

Click No.

12 When the following message appears, remove the CD-ROM from the CD-ROM drive and click OK.

To apply the Microsoft hot fix

1 Log on to the server as Administrator.

2 Insert the Symposium Call Center Server Release 3.0 Operating System CD Version 1.0 into the CD-ROM drive.

3   Make sure that hidden files are visible. To do so, follow these steps:

     a.   In Windows NT Explorer, choose View → Options.

     b.   Select Show all files.

     c.   Click Apply and then OK.

4   Copy the folder Hotfixes\Microsoft\q178741 on the CD to the root of drive D.

5   In Windows NT Explorer, click the D:\Hotfixes\Microsoft\q178741 folder.

6   Double-click the file hfx.exe, located in this folder.

     Result: The Hotfix Manager window opens.

7   Click InstallNewFix.

     Result: The Install Path dialog box opens.

8   Make sure that the path specified is d:\Hotfixes\Microsoft\q178741\hotfix.inf. If it is not correct, browse to this path.

9   Click OK.

     Result: The program installs the hot fix on the server. When the installation is complete, the program notifies you that Windows NT has been updated.

10   Click OK.

     Result: The system prompts you to restart. Do not click OK yet.

11   When the HotFix Manager appears, click Done.

12   Restore the settings for hidden files. To do so, follow these steps:

     a.   In Windows NT Explorer, choose View → Options.

     b.   Select Hide files of these types.

     c.   Click Apply, and then click OK.

13   Click OK to restart the server.

     Result: The server restarts.

     Note: If the server hangs during the restart, restart it manually.

To reduce the swap file size

During installation of the temporary Windows NT, a swap file of 267 Mbytes is created on drive D. As a result, insufficient space is available for the restore. To allow the restore to proceed, reduce the size of this swap file.

1   Log on to the server as Administrator.

2   From the Windows Start menu, choose Settings → Control Panel, and then double-click the System icon.

Result: The System Properties window appears.
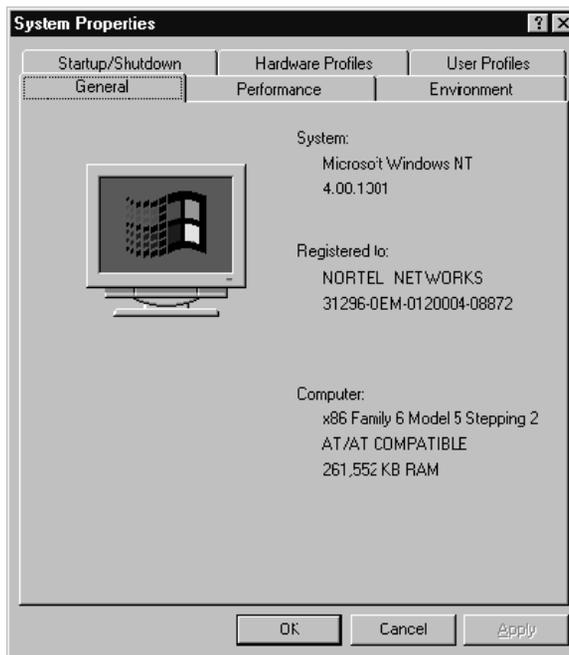
3   Click the Performance tab.

Result: The Performance tab appears.
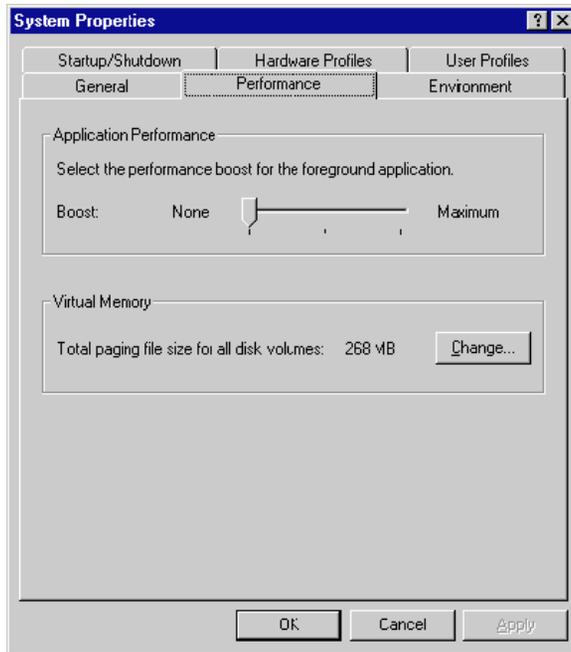
4   Click Change in the Virtual Memory section.

       Result: The Virtual Memory settings appear.
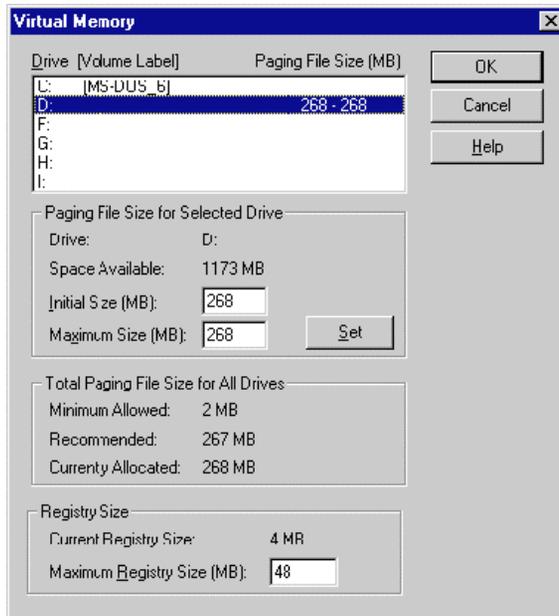
5   Highlight drive D.

6   Type **32** for both Initial Size (MB) and Maximum Size (MB).

7   Click Set and accept any warnings presented.

8   Click OK.

9   When prompted, restart the server.

To restore data from a full backup

CAUTION

Risk of system failure

The process of restoring from the full backup tape overwrites every file on the server, including all DOS and Windows NT operating system files. If the server you are restoring to does not have the same hardware configuration as the original server (for example, if you are restoring to a different server, or if the hardware configuration of the original server changed after the backup was made), you must back up the file C:\bootsect.dos. To do so, follow these steps:

1 Insert a formatted disk into drive A.

2 Open a DOS window, type the command **COPY C:\bootsect.dos A:\,** and press Enter.

3 Remove the disk.

When the restore is complete, follow these steps:

1 Insert the disk into drive A.

2 Open a DOS window, type the command **COPY A:\bootsect.dos C:\,** and press Enter.

3 Remove the disk.

1   Log on to the server as Administrator.

2   Insert the Symposium Call Center Server installation CD-ROM into the CD-ROM drive.

3   Locate the MAS subdirectory on the CD-ROM and double-click the file nbrestore.exe.

Result: The nbrestore program installs all necessary files in the d:\Nortel_temp directory and starts the restore service and utility. The NBCLI (library Test Shell) window will automatically display with a CI> prompt.

4   At the CI> prompt, Type **listtape PrimaryServerTape** and press Enter.

Result: The backup file name is displayed, which includes the type of backup and the time stamp for the backup (for example, SCCS_FULL 990528 1315).

5   Type **StartRestore**, followed by the backup device name followed by the backup file name.

Example:
StartRestore PrimaryServerTape "SCCS_FULL 990528 1315"

6   At the CI> prompt, type **status**, and then press Enter.

Result: The system displays the progress of the restore process, including the number of items, file size restored, and time to completion.

7   When the status shows as "Completed", press Enter to return to the CI> prompt.

Result: When the backup is finished, a restore log file is created with the following pathname:

d:\Nortel_temp\data\backup\RestoreLogs\SCCS_Full yymmdd hhmm yymmdd hhmm.Log

where the first date and time is the backup time and the second date and time is for the restore.

8   If you have restored data to a replacement server, then copy the backup version of c:\bootsect.dos from the floppy disk to c:\ directory on the server.

9   Restart the server.

To check drive letter assignments

Depending on which disk was changed in the system, the drive letter assignments might be incorrect after the restore. Check the drive letter assignments to see if they are correct. If they are not correct, assign temporary drive letters and then reassign the correct drive letters.

1   Log on to Windows NT as Administrator, or use another account that has administrative privileges.

2   Choose Start → Programs → Administrative Tools (Common) → Disk Administrator.

3   If the Disk Administrator has never been run before, a message appears asking you to update the system configuration. Click OK.

4   When prompted, click OK to allow the signature to be written to disk. Repeat this step for each new disk in the system.

Check if the hard drive letter assignments on your server match the illustration below. The hard drive sizes might be different on your server.
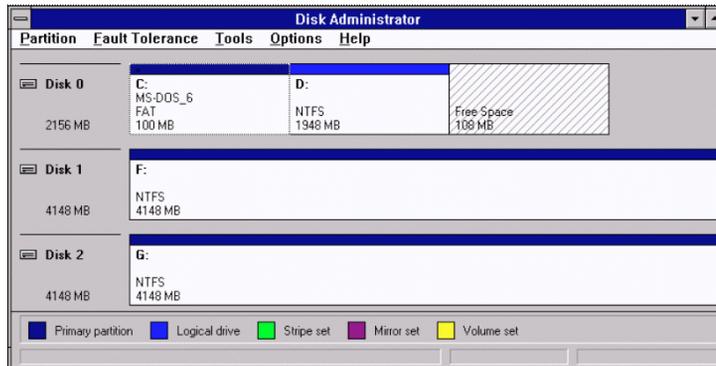
Note: Assign drive letter E to the CD-ROM drive.

5   If the drive letter assignments match the illustration, you do not need to continue with the next procedures. Choose Partition → Exit to close the Disk Administrator.

If the drive letter assignments do not match, continue with the following procedures.

To assign temporary drive letters

You cannot assign a drive letter to a hard drive if that letter is already in use. First, you must assign each hard drive a temporary drive letter. To do so, follow these steps:

1   Choose Start → Programs → Administrative Tools (Common) → Disk Administrator.

2   Choose Tools → Assign CD-ROM Drive Letters.

3   In the CD-ROM Drive Letters dialog box, change the drive letter to the last available drive letter.

Example: If Z is unused, assign the letter Z.

4   Click Change.

5   Click Yes to confirm that the drive letter should be changed immediately.

6 Select the first partition to which you want to assign a temporary drive letter. (Start with the second partition on drive 0.)

Note: Do not change the primary partition (C:\) drive letter.

7 Choose Tools → Drive Letter.

8 In the Assign Drive Letter dialog box, change the drive letter to the last available drive letter, and click OK.

Result: The Disk Administrator warns you that the drive cannot be locked for exclusive use (therefore, the drive letter cannot be changed immediately).

9 Click OK to continue.

10 Click Yes to change the drive letter when the system is next restarted.

11 Repeat steps 6 to 10 for each remaining hard drive in the system.

12 When you change the drive letters on the remaining partitions, you are informed that the drive letters can be changed immediately. Click Yes to do so. This is because the partitions are not the primary partition (the one with the operating system installed on it).

13 The drive letters should now be similar to this illustration.
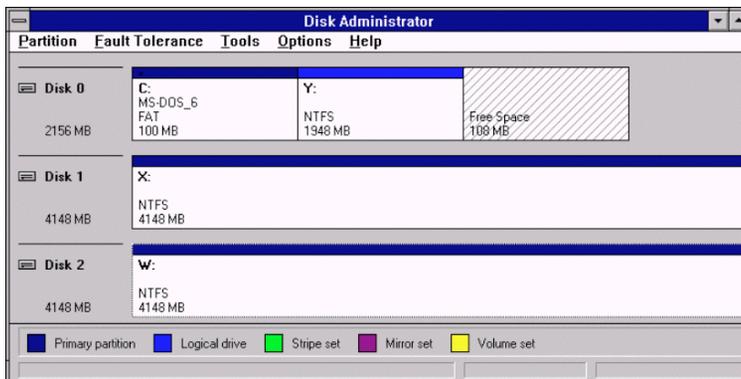
14 Choose Partition → Commit Changes Now... to save the drive letter assignments.

Result: A message appears warning you that you should update the emergency repair disk.

15 Click OK to continue.

   Result: The system alerts you that the server must now be restarted for the drive letters to be changed.

16 Click OK to shut down and restart the server. Then continue with the following procedure.

To reassign the original drive letters

1 Log on to Windows NT as Administrator.

   Note: The system might be slow to respond as the Symposium Call Center Server services attempt to start (for approximately ten minutes).

   Result: A message displays warning you that the server is running with limited virtual memory (because no paging file exists).

2 Click OK.

   Result: The System dialog box appears.

3 Click Cancel to exit.

4 Remap the drive letters to their original assignments. To do so, repeat steps 2 to 12 in "To assign temporary drive letters" on page 381.

   Assign the drive letters as instructed in the following table:

Drive	Assign letter
CD-ROM	E
Disk 1	F
Disk 2	G

5   When you are done, the drive letters should match the following illustration:
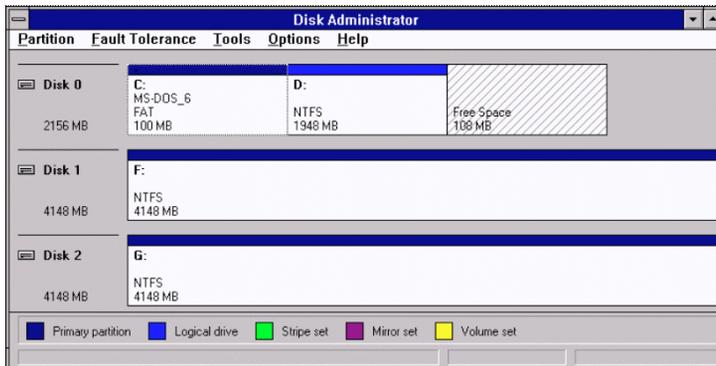
6   Choose Partition → Commit Changes Now to save the drive letter assignments.

Result: A message appears warning you that you should update the emergency repair disk.

7   Click OK to continue.

Result: The system alerts you that the server must now be restarted for the drive letters to be changed.

8   Click OK to shut down and restart the server.

Section C: Recovering a 702t RAID system

In this section

Recovering a drive on a 702t

Introduction

Follow the procedures in this section to recover a hard drive on a server that has a RAID controller.

Note: The server must be offline when you recover the drive.

> **CAUTION**
>
> **Risk of data loss**
> Before you begin this procedure, make sure that the backup drives you are using are properly labelled.

RAID utilities

Two utilities are used in the recovery process:

- dac960 Monitor utility (dacmon.exe)

  By default, this utility is always running on a Windows NT system that has the dac960 RAID controller. This utility displays the status of the RAID controller, its hard drives, and the progress of any hard drive rebuild operation.

  When a hard drive fails, the dac960 Monitor utility window appears on the screen and reports the event. The fault is also logged to the Windows NT event log under the application events. The server continues to function using the mirrored pair of the faulty hard drive until the faulty hard drive is replaced.

- dac960 Administration utility (dacadm.exe)

  This utility enables you to determine which hard drive has failed and to rebuild the replacement hard drive.

Requirements

- Check that the dac960 Monitor utility (d:\winnt\system32\dacmon.exe) is running when you perform these procedures.
- If the faulty hard drive is being replaced, do the following:
    - Ensure that the replacement hard drive is the same size as or a greater size than the faulty hard drive.
    - Ensure that the replacement hard drive has the same SCSI ID as the faulty hard drive.
    - Insert the new hard drive into the drive array in the slot that held the old hard drive.

To determine which hard drive had a failure

1 Log on to Windows NT as NGenSys.

2 Run dacadm.exe from a command line or through Windows NT Explorer (d:\winnt\system32\dacadm.exe).

Result: The dac960 Administration utility main window appears.
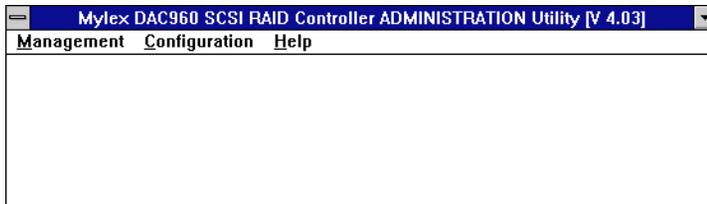
3   From the Configuration menu, select Drive Information.

Result: The Device Selection window appears. This window displays all SCSI buses and hard drives in the system. The status of each hard drive is identified by a label.
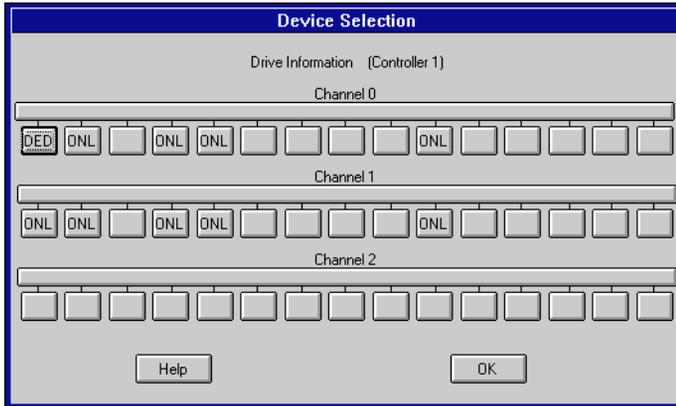
The hard drive status labels have the following definitions:

Label	Definition
ONL	working, online hard drive
DED	dead (failed) hard drive
SBY	Standby (this only appears if you make a hard drive Standby using the dac960 Administration utility)

4 Click the hard drive marked DED.

Result: The Drive Information window appears.

```
┌─────────────────────────────────────┐
│ ▬           Drive Information        │
├─────────────────────────────────────┤
│              Ch-0 : Id-0             │
│                                      │
│   Soft Error(s)         :    0       │
│                                      │
│   Hard Error(s)         :    0       │
│                                      │
│   Parity Error(s)       :    0       │
│                                      │
│   Miscellaneous Error(s) :   0       │
│                                      │
│                                      │
│          SEAGATE ST32155W            │
│                                      │
│                                      │
│                 [OK]                 │
└─────────────────────────────────────┘
```
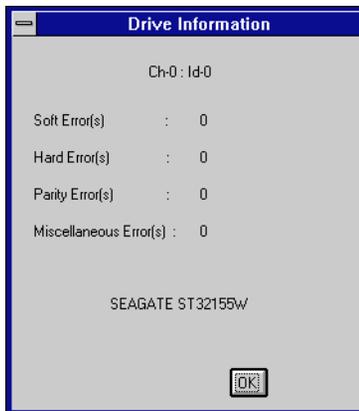
5 Record the SCSI bus and SCSI ID of the hard drive.

Example: Ch-0:Id-0 in the Drive Information window refers to a hard drive on SCSI channel 0 with SCSI ID 0.

6 Click OK to exit the Drive Information window.

7 Click OK to exit the Device Selection window.

8 Replace the faulty hard drive with the backup drive. Replace the other drive in the system pack with a blank formatted disk. Refer to the *Meridian Application Server Installation and Maintenance Guide* for your platform for instructions.

To rebuild the new hard drive

1 Log on to Windows NT as NGenSys.

2 Shut down all Symposium Call Center Server services by choosing, from the Windows Start menu, Programs → Symposium Call Center Server → Shutdown.

3 If you are not already running the dac960 Administration utility, then run dacadm.exe from a command line or through Windows NT Explorer (d:\winnt\system32\dacadm.exe).

Result: The dac960 Administration utility main window appears.

4   From the Management menu, select Rebuild Drive.

Result: The Device Selection window appears. This window displays all SCSI buses and hard drives in the system. The status of each hard drive is identified by a label.

5   Click the hard drive marked DED.

Result: The Rebuild Progress window appears.
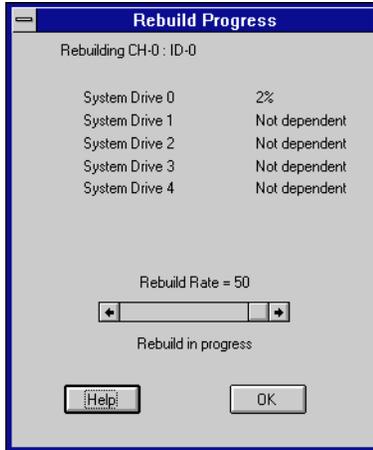
The Rebuild Progress window displays the rebuild progress in percentage form beside the relevant System Drive.

The dac960 Monitor utility comes to the foreground and displays the rebuild progress in percentage form.

The following table provides approximate times for a rebuild to complete.

Hard drive size	Approximate time to rebuild
2 Gbyte	15 minutes
4 Gbyte	30 minutes
9 Gbyte	1 hour

6   Once the rebuild is complete, a dialog box titled Rebuild Drive appears and contains the message `Rebuild over`.

         Note: If this dialog box is hidden by the dac960 Monitor utility window, then click on the Rebuild Progress window to bring it and the Rebuild Drive dialog box to the front.

7   Click OK on the Rebuild Drive dialog box.

8   Click OK on the Rebuild Progress window.

9   Check the Drive Selection window. The label on the replacement hard drive will read ONL to indicate that the new hard drive is working and online.

10   Click OK on the Drive Selection window.

11   In the dac960 Administration utility main window, click the hyphen in the top left corner to access a menu. From this menu, select Close to stop the dac960 Administration utility.

         Result: The server is fully operational.

Recovering a 702t

Introduction

Nortel Networks recommends that you split your RAID drives before making major changes to you server, such as upgrading the server software or applying PEPs. If the process fails, you can use this procedure to restore you system to its former.

To recover a system running in split mode

1 Shut down the server.

    a. From the Start menu, choose Shutdown.

    b. Click Shutdown the computer, and click Yes.

2 Power down the server.

3 Disconnect the channel 0 SCSI cable and reconnect the channel 1 SCSI cable. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

4 Insert the bootable dac960 Configuration disk in the floppy disk drive.

    Note: If the dac960 disk is not bootable, insert a bootable disk to start the system until the DOS prompt appears, and then insert the dac960 Configuration disk.

5 Power up the server.

    Result: During startup, POST messages from the RAID controller warn that the system is having problems recognizing the system drives (some drives are offline). The channel 0 drives should be listed as dead.

    The A:\> prompt appears.

6 If you are prompted for the date and time, make sure the displayed date and time are correct. If they are, press Enter. If they are not, enter the correct date and time.

7 Type **cd daccfg** and press Enter.

    Result: The A:\daccfg\> prompt appears.

8   Type **daccf** and press Enter to start the dac960 Configuration utility.

        Result: The daccf Configuration utility starts and scans the drives on both channels. It displays the drive statuses. Drives on channel 0 have on original state of ONLINE and a current state of DEAD.

9   Press Enter to continue.

10   If prompted to save the configuration, press **S**.

        Result: The utility scans the drives again.

11   From the main menu, select Tools and type Enter.

12   From the Tools menu, select Make Online and press Enter.

13   Select A-1 and press Enter twice.

14   Select Yes to confirm.

15   Repeat steps 12 to 14 for each drive to be brought online. (For a 701t or 702t, bring drives B-1 and C-1 online. For a 1001t, bring drives B-1, C-1, D-1, and E-1 online.)

16   Press Esc to exit.

        Result: A prompt appears asking if you want to save the configuration.

17   Select **Yes** and press Enter.

        Result: The A:\DACCFG\> prompt appears.

18   Press Ctrl-Alt-Del to restart the server.

        Result: Symposium Call Centre Server Release 1.1 or 1.5 is now restored.

When you are ready to rebuild the RAID system, follow the steps outlined in "Rebuilding the RAID drives on a 702t" on page 316.

Note: The server must be offline when you rebuild the drives.

Recovering a 702t system from a backup

Introduction

Follow this procedure to restore an entire system from a backup.

> ⚠️ **CAUTION**
>
> **Risk of data loss**
> Before you begin this procedure, make sure that the backup drives you are using are properly labelled.

To recover an entire system

1 Shut down the server.

    a. From the Start menu, choose Shutdown.

    b. Click Shutdown the computer, and click Yes.

2 Power down the server.

3 Disconnect the SCSI cable for both channel 0 and channel 1. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

4 Insert the bootable dac960 Configuration disk in the floppy disk drive.

Note: If the dac960 disk is not bootable, insert a bootable disk to start the system until the DOS prompt appears and then insert the dac960 Configuration disk.

5 Power up the server.

Result: During startup, POST messages from the RAID controller warn that the system is having problems recognizing the system drives (some drives are off-line). The channel 0 drives should be listed as dead.

The A:\> prompt appears.

6 Type **cd daccfg** and press Enter.

Result: The A:\daccfg\> prompt appears.

7   Type **daccf -o** and press Enter to start the dac960 Configuration utility.

        Result: The daccf Configuration utility starts.

8   From the main menu, select Tools and press Enter.

9   From the Tools menu, select Clear Configuration and press Enter.

10   Select Yes to confirm.

11   Exit from the dac960 Configuration utility by pressing Esc and selecting Yes
        when prompted to exit.

        Result: The A:\DACCFG\> prompt appears.

12   Power down the server.

13   Remove the set of drives that you will be replacing with the backup drives.
        (For example, if the backup was created on the channel 1 drives, remove
        the channel 1 drives.)

14   Connect the SCSI cables for the hard drive. For detailed instructions, see
        the *Meridian Application Server Installation and Maintenance Guide* for
        your platform.

15   Make sure that the bootable dac960 Configuration disk is still in the floppy
        disk drive.

16   Power up the server.

        Result: During startup, POST messages from the RAID controller warn
        that the system is having problems recognizing the system drives (some
        drives are offline). The channel 0 drives should be listed as dead.

        The A:\> prompt appears.

17   Type **cd daccfg** and press Enter.

        Result: The A:\daccfg\> prompt appears.

18   Type **daccf** and press Enter to start the dac960 Configuration utility.

        Result: The daccf Configuration utility starts and scans the drives on both
        channels. It displays the drive statuses. The backup drives should have a
        status of ONL, and the other drives should be DED.

19   If prompted to save the configuration, type **S**.

20   Exit from the dac960 Configuration utility by pressing Esc and selecting Yes
        when prompted to exit.

        Result: The A:\DACCFG\> prompt appears.

21 Remove the dac960 Configuration disk from the floppy drive.

22 Press Ctrl-Alt-Del to restart the sever.

Result: During boot-up, POST messages from the RAID controller warn that some drives are dead. The server should start normally.

23 When you log on to Windows NT, the dac960 RAID Control Monitor window appears. It reports the statuses of the dead drives. You can minimize this window.

When you are confident of system operation, proceed to rebuild the drives. (See "Rebuilding the RAID drives on a 702t" on page 316.)

Section D: Recovering a 1003t RAID system

In this section

Recovering a drive on a 1003t

Introduction

Follow the procedures in this section to recover a hard drive on a server that has a RAID controller.

Note: The server must be offline when you recover the drive.

Before you begin

Make sure you have the backup disk, and a new or blank formatted disk. (To find out how to format a disk, see "To format drives" on page 332.)

> **CAUTION**
> _____
> **Risk of data loss**
> Before you begin this procedure, make sure that the backup drives you are using are properly labelled.

To determine which hard drive had a failure

1   Log on to Windows NT as Administrator.

2   Start the NetRAID Assistant utility.

    Result: The Server Selection dialog box appears.

3   Select the local server, and make sure access mode is set to Full Access.

    Result: The NetRAID Assistant window appears.

4   Check which drive is in FAIL state.

5   Replace the faulty hard drive with the backup drive. Replace the other drive in the system pack with a blank formatted disk. Refer to the *Meridian Application Server Installation and Maintenance Guide* for your platform for instructions.

To rebuild the new hard drive

1   Power on the server.

Result: POST messages from the RAID controller warn you that the system is operating in critical mode (that is, with some drives offline). The following message appears: `Option: Experienced User may press <CTRL><M> for NP NetRAID Express Tools Now.`

2   Press Ctrl+M.

Result: The Management menu appears.

3   Select Rebuild and press Enter.

Result: A list of drives appears.

4   Highlight each new drive, and press Space.

5   Press F10.

Result: The utility begins rebuilding the drive. To rebuild a 9-Gbyte volume takes approximately 45 minutes.

Recovering an entire system on a 1003t

Introduction

Follow this procedure to restore an entire system, either while it is running in split mode, or from a backup.

Nortel Networks recommends that you split your RAID drives before making major changes to your server, such as upgrading the server software or applying PEPs. If the process fails, you can easily restore your system to its former state by following this procedure.

> **CAUTION**
>
> **Risk of data loss**
> Before you begin this procedure, make sure that the backup drives you are using are properly labelled.

To recover an entire system

1   Power down the server.

2   Remove all hard disks, for both channel 0 and channel 1. For detailed instructions, see the *Meridian Application Server Installation and Maintenance Guide* for your platform.

3   Install the backup drives into the their original location. (For example, if the backup was created on the channel 1 drives, insert them in channel 1.)

4   Insert new, blank formatted disks (see the *Administrator's Guide*, backup procedures) in the proper locations on Channel 0.

5   Restart the system.

    Result: POST warning messages from the RAID controller state that the system is having problems recognizing the system drives (configuration mismatch between the drives and the NVRAM). The system prompts you to go to NetRAID Express.

6   Press Ctrl+M to go to the NetRAID Express Tool utility.

7   Under the main menu, choose Rebuild for those drives on Channel 0 that are formatted. Note that a drive has to be marked FAILED in order to be rebuilt.

8   When the Rebuild operation is complete, exit the NetRAID Express utility.

9   Restart the server to full service.

Chapter 14

Controlling the server from a client PC

In this chapter

Overview

Introduction

This chapter describes how to establish a dial-up connection to the server, and also how to control the server from a remote or local client PC. pcANYWHERE32 is used to enable a remote or local PC to control the server.

In this chapter, a remote support PC or a local PC that is used to administer or access the server is referred to as a client PC.

ATTENTION   Do not perform intensive remote tasks during peak call traffic hours as this can adversely affect the server's call processing capabilities.

Establishing a network connection with the server from a remote PC

Client PCs that are not on the same LAN as the server must use Dial-Up Networking to connect to the server. Remote Access Service (RAS) must be installed and configured on the server.

Dial-Up Networking software is usually installed during the Windows NT 4.0, Windows 95, or Windows 98 initial installation. If the Dial-Up Networking folder does not appear in My Computer, it is not installed. Refer to your Windows documentation for a Dial-Up Networking installation procedure.

RAS is installed on the server at the factory. RAS is configured during Windows NT configuration.

A dial-up connection enables the remote client PC to appear as if it is on the same LAN as the server, and allows you to

- perform limited file transfers to the server
- perform administration using an SMI system on the client PC
- attempt to establish a pcANYWHERE32 remote control session over a modem link

Section A: Installing and configuring pcANYWHERE32

In this section

Overview of pcANYWHERE32

Introduction

With pcANYWHERE32, you can perform advanced administrative tasks on the server and control the server as though you were directly connected to it.

One licensed copy of pcANYWHERE32 Version 8.0 is provided for the server on the Meridian Application Server Operation System CD. pcANYWHERE32 is installed at the factory.

To install pcANYWHERE32 Version 8.0 on the client PC, you must purchase a separate license for the client PC.

When to use pcANYWHERE32

Remote control (using pcANYWHERE32) allows administrators and Nortel Networks product support representatives to perform advanced administrative actions such as

- query the server event logs
- shut down or restart the server
- use server-only support tools
- apply PEPs and other advanced administration activities

System requirements for the client PC

- Windows NT 4.0, Windows 95, or Windows 98 operating system
- Dial-Up Networking (DUN) if connecting over the Public Switch Telephone Network (PSTN); DUN is normally included on Windows PCs
- pcANYWHERE32 (must be purchased for the client)

System requirements for the server

- RAS must be installed and properly configured if connecting over the PSTN.

RAS is installed on the server at the factory and configured on-site as part of the Windows NT configuration procedures. For details, refer to the *Software Installation and Upgrade Guide*.

■   pcANYWHERE32 must be installed and properly configured on the server. It is installed on the server at the factory. The configuration is verified as part of the on-site installation procedures. For details, refer to the *Software Installation and Upgrade Guide*.

Maintaining system security

For information and recommendations on passwords, see "Changing pcANYWHERE32 passwords" on page 69.

Installing pcANYWHERE32 on the client PC

Introduction

A copy of pcANYWHERE32 for the client PC is not provided. To install pcANYWHERE32 on the client PC, you must have a separate licence for the client PC.

The steps for installing pcANYWHERE32

Installation and initial setup of pcANYWHERE32 on the client PC involves these tasks:

1. Install the pcANYWHERE32 application.

2. Start pcANYWHERE32 for the first time. During this task, you identify the network protocol.

3. Set the video mode. This task synchronizes the video card settings of the client PC with that of the server to ensure the remote user can see the graphical user interfaces properly.

To install pcANYWHERE32 on the client PC

1   Log on to the client PC.

   Note: If the client PC is running Windows NT Workstation, log on as Administrator.

2   Insert the MAS Operating System CD-ROM in the CD-ROM drive.

3   Run the cdinst.exe program on the CD-ROM to start the installation.

4   Click the Install Software button.

   Result: The Welcome window appears.

5   Click Next.

   Result: The User Information window appears.

6   Enter both the user and the company names, then click Next.

   Result: The Online License Agreement window appears.

7   Click Yes to accept the software license agreement.

Result: The Choose Destination window appears.

8   Click Next until you get to the Registration Wizard screen.

9   Click Skip.

Result: The pcANYWHERE32 Setup window appears. The system asks whether you want to view the readme file.

10   Click No.

11   Select Yes to restart the computer, then click Finish.

To start pcANYWHERE32 for the first time

1   From the Windows Start menu, choose Programs → pcANYWHERE32 → pcANYWHERE.

Result: The Smart Setup Wizard window appears.

2   Click Next.

Result: The Network Device window appears.

3   Ensure only TCP/IP is selected, then click Next.

4   Select Finish.

To set the video mode

1   In pcANYWHERE32, select Application Options from the File menu.

2   Select the Host Operation tab.

3   Make sure that the Video mode is set to Default.

4   Click Apply.

5   Click OK to exit.

Configuring pcANYWHERE32 on the client PC

Introduction

You must create a remote control connection icon in pcANYWHERE32 that allows you to connect to the server. Configure other options on pcANYWHERE32 as required by the customer.

To create a remote control connection icon

1   From the Windows Start menu, choose Programs → pcANYWHERE32 → pcANYWHERE.

    Result: The pcANYWHERE32 window appears.

2   Click Remote Control.

3   Double-click Add Remote Control Item.

    Result: The Remote Control Wizard appears.

4   Create a new pcANYWHERE32 connection profile using the following parameters:

    a.   Assign a profile name.

    b.   For the connection device, select TCP/IP.

        Note: Do not select a modem.

    c.   For the Host PC Name, enter the LAN IP address.

    d.   Clear the check box for Automatically begin remote control session upon wizard completion field, then click Finish.

5   Right-click the new remote control connection icon, then select Properties.

6   Under the Setting tab, increase the Number of connection attempts to a value higher than zero.

7   Under the Security Options tab, ensure that pcANYWHERE encryption is selected (this is the default).

8   All other fields are optional. Set as required for the customer, or leave at default values.

9   Click OK.

What's next?

If you are using pcANYWHERE32 on a remote client PC, then continue with "Creating a Dial-Up Networking connection profile" on page 412.

Creating a Dial-Up Networking connection profile

Introduction

If the client PC is not on the same LAN as the server, you must create a Dial-Up Networking connection profile. The Dial-Up Networking software enables the client PC to connect to the server over the public switch telephone network (PSTN). When you create a connection profile, an icon representing the connection profile appears in the Dial-Up Networking folder.

Before you begin

Dial-Up Networking must be installed
Dial-Up Networking software is installed during the Windows NT 4.0, Windows 95, or Windows 98 setup and is usually present on PCs that have a standard setup.

If the Dial-Up Networking folder does not appear in My Computer, it is not installed. Refer to your Windows documentation to find out how to install Dial-Up Networking.

What you need
To create a server Dial-Up Networking connection profile, you must have the following information:

- the server telephone number
- the server IP address

If you do not know this information, contact the system administrator.

To create a server connection profile (for Windows 95 or 98 client PC)

1   From the Windows Start menu, choose Programs → Accessories → Dial-Up Networking or Programs → Accessories → Communication → Dial-Up Networking.

   Result: If no connections have been defined on this PC, the Make New Connection wizard appears.

   If one or more connections has been created on this PC, click the Make New Connection icon in the Dial-Up Networking window to display the wizard.

2   Enter a name for the connection and select a modem.

3   Click Next.

4   Enter the server telephone number, then click Next.

5   Click Finish.

6   Continue with the following procedure.

To configure a connection profile

1   Right-click on the server connection profile icon, then select Properties.

2   Verify the information on the General property page, and correct it if necessary.

3   Click Configure.

   Result: The Modem Properties property sheet appears.

4   Update the tabs as required, then click OK.

   Result: You return to the connection property sheet.

5   Click Server Types.

6   For Dial-Up Server, select PPP:Windows NT.

7   For the network protocols, select only TCP/IP and NETBEUI.

8   Click TCP/IP settings.

   Result: The TCP/IP Settings property sheet appears.

9   Select Specify an IP address, and enter the server IP address.

10 Select Use default gateway on remote network.

11 The remaining fields are optional. Fill them in as required for the customer's network.

12 Click OK.

Result: You return to the connection property sheet.

13 Click OK.

Section B: Performing remote tasks using pcANYWHERE32

In this section

Overview

Introduction

This section describes how to log on to the server using pcANYWHERE32. Once you have logged on to the server using pcANYWHERE32, you can control the server as though you were sitting at a keyboard connected directly to the server.

If the server is powered off, you cannot establish a connection with the server. Someone at the server's location must turn on the server.

If the client PC is not on the same LAN as the server, then you must establish a dial-up connection. To find out whether the client PC is on the server's LAN, use the ping command. Ping the CLAN or ELAN depending on whether the client PC is connecting to the server over the CLAN or ELAN.

To test the connection if the client PC is on the server's LAN

1 Open up a DOS prompt and type ping "XX.XX.XX.XX" where XX.XX.XX.XX is the IP address of the CLAN or ELAN card on the server.

2 If it is successful, then a connection has been established. Otherwise, check the cabling and the client PC's TCP/IP configuration information.

Establishing a connection using Dial-Up Networking

Introduction

If the client PC is not on the same LAN as the server, you must establish a dial-up networking connection to the server. After the connection is established, the client PC can behave as though it is on the same LAN as the server. You can launch an SMI system or use pcANYWHERE32 to control the server.

Before you begin

- Ensure that you have created a server connection profile. See "Creating a Dial-Up Networking connection profile" on page 412.

- Contact the LAN administrator to find out whether you need a user ID and password to connect to the LAN.

- If you are using pcANYWHERE32, contact the LAN administrator for the remote access user account and password and the pcANYWHERE32 caller account on the server (for example, the NGenDist user account and pcANYWHERE32 NGenDist caller account).

To establish a connection to the server

1 Log on to the client PC.

2 From the Windows Start menu, choose Programs → Accessories → Dial-Up Networking or Programs → Accessories → Communication → Dial-Up Networking.

3 Double-click the server connection profile icon.

Note: If the icon is unavailable, you have not created a server connection profile. See "Creating a Dial-Up Networking connection profile" on page 412.

4 If you are prompted for a user ID and password, enter the user ID and password to log on to the customer's network.

5 Wait until the connection is established.

To disconnect a dial-up connection

1   Right-click the icon on the toolbar

2   Click Disconnect.

What's next?

After the connection has been made, you can do the following tasks:

- Launch an SMI system to access the SMI window. See "Logging on to the server" on page 21.

- Use pcANYWHERE32 to control the server to perform any administrative task. See "Controlling the server using pcANYWHERE32" on page 419.

- Restart the server. See "Restarting the server remotely" on page 421.

Controlling the server using pcANYWHERE32

Introduction

You can use pcANYWHERE32 to operate the server as if you were directly connected to it.

Before you begin

- If the server is not on the same LAN as the client PC, then establish a dial-up connection. See "Establishing a connection using Dial-Up Networking" on page 417.

- Contact the LAN administrator for the remote access user account and password and the pcANYWHERE32 caller account on the server (for example, the NGenDist user account and pcANYWHERE32 NGenDist caller account).

Remote tasks

Once a pcANYWHERE32 session is successfully established, you can take direct control of the server to

- query the server event logs

- shut down or restart the server

- use server-only support tools

- apply PEPs

- perform other advanced administration activities

To control the server using pcANYWHERE32

1   If you are dialing in over the PSTN, then establish a dial-up connection (see "To establish a connection to the server" on page 417).

2   On the client PC, from the Windows Start menu, choose Programs → pcANYWHERE32 → pcANYWHERE.

3   Double-click the remote control icon for the server.

        Note: If the icon is unavailable, see "To create a remote control connection icon" on page 410.

4   When prompted, enter the pcANYWHERE32 login ID and password.

To end a pcANYWHERE32 remote control session

1   To log off the server, press Ctrl+Alt+Del on the client PC and select Logout.

2   Disconnect the pcANYWHERE32 connection.

3   If applicable, disconnect the Dial-Up Networking connection.

        a.   Right-click the icon on the toolbar.

        b.   Click Disconnect.

Restarting the server remotely

Introduction

You might need to restart the server from a remote location if the system goes down or if you need to run startup diagnostic tests.

Restarting the server using pcANYWHERE32

If pcANYWHERE32 is installed, then establish a remote control session and restart the server using the Start → Shut Down option. See "Controlling the server using pcANYWHERE32" on page 419.

Restarting the server when pcANYWHERE32 is not available

See "Restarting the server remotely without using pcANYWHERE32" on page 422.

Restarting the server remotely without using pcANYWHERE32

Introduction

This section describes how to restart the server *without* using pcANYWHERE32 if pcANYWHERE32 is not installed or not available. If pcANYWHERE32 is installed, then establish a remote control session and restart the server using the Start → Shut Down option. See "Restarting the server remotely" on page 421.

What restarting the server remotely involves

Restarting the server remotely involves the following steps:

- configuring the Hyperterminal connection
- configuring the ports
- editing the Host file to establish a connection with the server

HyperTerminal

HyperTerminal (with a modem) enables you to connect to a remote computer, even if it is not running Windows. You must configure a HyperTerminal connection from the server.

After a HyperTerminal connection is configured, it appears as a submenu in Accessories in the Programs menu.

To configure HyperTerminal

1   From the Windows Start menu, choose Programs → Accessories → HyperTerminal or Programs → Accessories → Communications → HyperTerminal.

2   Double-click Hypertrm.exe.

    Result: The Connection Description window appears.

3   Enter a name that describes the connection, then select an icon (optional).

4   Click OK.

    Result: The Connect to dialog box appears.

5   Select the port to which the modem is attached.

    Result: The Properties window appears.

6   Select 19200 Bits per second.

7   Click OK.

To configure the modem port

1   From the Windows Start menu, choose Settings → Control Panel.

2   Double-click System.

3   Click the Device Manager tab.

4   Select View the devices by type.

5   Double-click Ports (COM & LPT).

6   Click the Communications Port used by the modem, either COM1 or COM2.

7   Click the Port Settings tab.

8   Select 19200 in the Bits per second tab.

To restart the server remotely

1   Open Notepad or a similar application.

2   Add the server IP address to the end of the following file: WinNT/System32/Drivers/etc/host.

    Example: 127.0.0.1 <name>

3   Establish a connection to the server using Dial-Up Networking (DUN).

4   Type the following in the host file:

    shutdown -n <number> and -r

    Example: shutdown -h myhostname -n 4165971111

5   Disconnect the DUN connection:

    a.   Right-click the icon on the toolbar

    b.   Click Disconnect.

Result: The connection to the server is broken and the system calls back to the client PC at the number entered in step 4. When the connection is reestablished, the server restarts and restart information is displayed in the HyperTerminal window, which appears onscreen.

Note: This process takes approximately five minutes.

6   Type the following in the HyperTerminal window:

ATS0=1

7   Press Enter.

8   After restart is complete, close the HyperTerminal window.

Section C: Reinstalling pcANYWHERE32 on the server

In this section

Overview

Introduction

This section provides procedures for reinstalling pcANYWHERE32 on the server.

Remote Access Service

Remote Access Service (RAS) enables you to establish a connection between the server and client PC over a public switch telephone network (PSTN) using a modem.

RAS is installed during the initial installation of the operating system on the server. RAS is configured as part of the Configuring Windows NT procedures.

pcANYWHERE32

pcANYWHERE32 enables a user to administer the server from

- a client PC that is on the server's LAN
- a client PC that has a modem and has successfully established a dial-up connection

One licensed copy of pcANYWHERE32 Version 8.0 is provided with the Meridian Application Server Operation System CD.

Maintaining system security

For information and recommendations on passwords, see Chapter 2, "Managing security."

Reinstalling pcANYWHERE32 on the server

Introduction

This section describes how to reinstall pcANYWHERE32. Reinstallation may be required if you have to recover from a hard drive failure.

The steps for installing pcANYWHERE32

The following procedures must be followed to complete the installation and initial setup of pcANYWHERE32 on the server.

Install the pcANYWHERE32 application
This procedure installs pcANYWHERE32 on the server.

Start pcANYWHERE32 for the first time
This procedure allows you to set the network device.

Set the video mode
This procedure synchronizes the video card settings of the server with that of the client PC to ensure the remote user can see the graphical user interfaces properly.

Set the pcANYWHERE32 service to Automatic
This procedure enables the pcANYWHERE32 service to start automatically after restart.

To install pcANYWHERE32 on the server

1   Log on as Administrator.

2   Insert the MAS Operating System CD-ROM in the CD-ROM drive.

3   Run the cdinst.exe program on the CD-ROM to start the installation.

4   Click the Install Software button.

      Result: The Welcome window appears.

5   Click Next.

   Result: The User Information window appears.

6   Enter both the user and the company names, then click Next.

   Result: The Online License Agreement window appears.

7   Click Yes to accept the software license agreement.

   Result: The Choose Destination window appears.

8   Click Next until you get to the Registration Wizard screen.

9   Click Skip.

   Result: The pcANYWHERE32 Setup window appears. The system asks whether you want to view the readme file.

10   Click No.

11   Select Yes to restart the computer, then click Finish.

To start pcANYWHERE32 for the first time

1   From the Windows Start menu, choose Programs → pcANYWHERE32 → pcANYWHERE.

   Result: The Smart Setup Wizard window appears.

2   Click Next.

   Result: The system prompts you to select the network device.

3   Ensure that only TCP/IP is selected, then click Next.

   Result: The system prompts you to select a port.

4   Click Finish to accept the default port.

To set the video mode

1   From the Windows Start menu, choose Programs → pcANYWHERE32 → pcANYWHERE.

2   From the File menu, select Application Options.

3   Select the Host Operation tab.

4   Make sure that the Video mode is set to Default.

5   Click Apply.

6   Click OK to exit.

To set the pcANYWHERE32 service to Automatic

1   From the Windows Start menu, choose Settings → Control Panel.

2   Double-click Services.

3   Scroll to pcANYWHERE and highlight the service.

4   Click Startup.

5   Select Automatic.

6   Click OK.

What's next?

Configure pcANYWHERE32. Refer to the *Software Installation and Upgrade Guide*.

Appendix A

Troubleshooting

In this appendix

Overview

Introduction

This section provides troubleshooting checklists and procedures in case you experience any problems with the application software or with connecting to the network or server.

Problems with application software

Checklist

If you have problems with the application software, perform the following tasks:

- Ensure that all cables are installed correctly. See *Meridian Application Server Installation and Maintenance Guide* for your server for detailed information.

- Verify that the system board jumpers are set correctly. See *Meridian Application Server Installation and Maintenance Guide* for your hardware platform for detailed information.

- Verify that the Windows NT is properly configured for the system. See *Symposium Call Center Server Software Installation Guide* for instructions on configuring Windows NT.

If the problem persists, contact your Nortel Networks customer support representative for assistance and more information.

Cannot connect to the server

Checklist

If you cannot connect to the server, perform the following tasks:

■   Ensure that you are using the drivers that are shipped on the system configuration software CD for the CLAN/ELAN network controller.

■   Ensure that the driver is loaded and the protocols are bound.

■   Ensure that the network cable is securely attached to the connector at the system back panel and that the network controller link LED is on and visible at the back panel. If the cable is attached but the problem persists, try a different cable.

■   Ensure that the hub port is configured for the same duplex mode as the network controller.

■   Check with your LAN administrator about the correct networking software that needs to be installed.

■   If you are directly connecting two servers, some hubs might also require a crossover cable. Check your hub documentation for more information on crossover cables.

■   Check the visible network controller LEDs through an opening at the system back panel.

Problems with the network

Checklist

If you are having network problems, check the following list for possible solutions.

The network driver fails to start, or hangs the server on starting

- Use the SCU software to verify interrupt and other system resource settings. For more information, refer to the *Software Installation and Upgrade Guide*.
- Verify that the proper Windows NT Service Pack is loaded.
- Verify that diagnostics on the card pass.

Diagnostics pass, but the connection fails

- Ensure the network cable is securely attached.
- Ensure you specify the correct frame type in your net.cfg file.

The Link LED does not light

- Ensure you have loaded the network drivers.
- Check all cable connections.
- Try another port on the hub.
- Ensure you have the correct type of cable between the adapter and the hub. Some hubs require a crossover cable, while others require a straight-through cable. For more information about crossover cabling, see the manufacturer's hub directions.

The Activity LED does not light

- Ensure you have loaded the correct network drivers.
- The network may be idle. Try to access a server.

The controller stopped working when an add-in adapter was installed

- Ensure the cable is connected to the port from the onboard network controller.

- Ensure your PCI BIOS is current. Try the "PCI installation tips" on page 437.

- Ensure that the adapter is not attempting to share interrupts, since Windows NT does not support shared interrupts. See the "PCI installation tips" on page 437.

- With the system powered down, try reseating the add-in adapter.

The add-in adapter stopped working without apparent cause

- With the system powered down, try reseating the adapter first. If the problem persists, try installing the card in a different slot. This helps you identify whether the problem is with the adapter or with the slot.

- The network driver files may be corrupt or deleted. Delete and then reinstall the drivers.

- Run the diagnostics.

PCI installation tips

Checklist

Here are two useful PCI tips:

- Reserve interrupts (IRQs) and memory addresses specifically for ISA adapters. This prevents PCI cards from trying to use the same settings that ISA cards are using. Use the SCU to keep track of the ISA adapter resources.

- Certain drivers might require interrupts that are not shared with other PCI drivers. The SCU can be used to adjust the interrupt numbers for PCI devices. For certain drivers, you might have to alter settings so that interrupts are not shared. Interrupt sharing is not supported on this platform.

Glossary

A   **accelerator key**

A key on a phoneset that an agent can use to place a call quickly. When an agent presses an accelerator key, the system places the call to the configured number associated with the key. For example, if an agent presses the Emergency key, the system places a call to the agent's supervisor.

access class

A collection of access levels that defines the actions a member of the access class can perform within the system. For example, a member of the Administrator access class might be given a collection of Read/Write access levels.

access level

A level of access or permission given to a particular user for a particular application or function. For example, a user might be given View Only access to historical reports.

ACD call

See Automatic call distribution call.

ACD-DN

See Automatic call distribution directory number.

ACD group

See Automatic call distribution group.

ACD routing table

See Automatic call distribution routing table.

ACD subgroup

See Automatic call distribution subgroup.

acquired resource
A resource configured on the switch that is under the control of the Symposium Call Center Server. Resources must be configured with matching values on both the switch and the Symposium Call Center Server.

activated script
A script that is processing calls or is ready to process calls. Before you can activate a script, you must first validate it.

activity code
A number that an agent enters on his or her phoneset during a call. Activity codes provide a way of tracking the time agents spend on various types of incoming calls.They are also known as Line of Business (LOB) codes. For example, the activity code 720 might be used to track sales calls. Agents can then enter 720 on their phonesets during sales calls, and this information can be generated in an Activity Code report.

administrator
A user who is responsible for maintaining the Symposium Call Center Server.

agent
A user who is responsible for handling customer calls.

agent login ID
A unique identification number assigned to a particular agent. The agent uses this number when logging in. The agent ID is not associated with any particular phoneset.

agent to skillset assignment
A matrix that, when you run it, sets the priority of one or more agents for a skillset. Agent to skillset assignments can be scheduled.

agent to supervisor assignment
A definition that, when you run it, assigns one or more agents to specific supervisors. Agent to supervisor assignments can be scheduled.

application

1. A logical entity that represents a Symposium Call Center Server script for reporting purposes. The master script and each primary script have an associated application.The application has the same name as the script it represents. 2. A program that runs on a computer.

application program interface

A set of routines, protocols, and tools that programmers use to develop software applications. APIs simplify the development process by providing commonly used programming procedures.

associated supervisor

A supervisor who is available for an agent if the agent's reporting supervisor is unavailable. *See also* reporting supervisor.

Automatic call distribution call

A call to an ACD-DN. ACD calls are distributed to agents in an ACD group based on the ACD routing table on the switch.

Automatic call distribution directory number

Primary and supplementary DNs associated with an ACD group. Calls made to these DNs are distributed to agents belonging to the group, based on the ACD routing table on the switch.

Automatic call distribution group

An entity defined on the switch for the purpose of call distribution. When a customer dials an ACD group, the call is routed to any agent who is a member of that group.

Automatic call distribution routing table

A table configured on the switch that contains a list of ACD-DNs used to define routes for incoming calls. This ensures that incoming calls not processed by Symposium Call Center Server will be queued to ACD groups and handled by available agents.

Automatic call distribution subgroup

An entity defined on the switch to assign supervisory responsibilities. Each subgroup has one supervisor phoneset and a number of agent phonesets associated with it. Agents can log on to any phoneset within their ACD subgroup. The supervisor must log on to the supervisor phoneset to monitor his or her assigned agents.

C

call age

The amount of time a call was waiting in the system before being answered by an agent.

call intrinsic

A script element that stores call-related information assigned when a call enters the Symposium Call Center Server. *See also* intrinsic, skillset intrinsic, time intrinsic, and traffic intrinsic.

call presentation class

A collection of preferences that determines how calls are presented to an agent.

call priority

A numerical value assigned in a script that defines the relative importance of a call. If two calls are in the queue when an agent becomes available, and one call is queued with a higher priority than the other, the agent receives the higher priority call first. *See also* skillset priority.

call treatment

A script element that enables you to provide handling to a call while it is waiting to be answered by a call center agent. For example, a caller can hear a recorded announcement or music while waiting for an agent.

call variable

A script variable that applies to a specific call. A call variable follows the call through the system and is passed from one script to another with the call. *See also* global variable, variable.

Calling Line Identification

This is an optional service that identifies the telephone number of the caller. This information can then be used to route the call to the appropriate agent or skillset. The CLID can also be displayed on an agent's phoneset.

CDN

See controlled directory number.

CLAN

See Customer local area network.

CLID

See Calling Line Identification.

client

The part of Symposium Call Center Server that runs on a personal computer or workstation and relies on the server to perform some operations. *See also* server.

command

A building block used with expressions, variables, and intrinsics to create scripts. Commands perform distinct functions, such as routing a call to a specific destination, playing music to a caller, or disconnecting a caller.

controlled directory number

A special directory number that allows calls arriving at the switch to be queued when the CDN is controlled by an application such as Symposium Call Center Server. When a call arrives at this number, the switch notifies the application and waits for routing instructions, which are performed by scripts in Symposium Call Center Server.

Customer local area network

The LAN to which your corporate services and resources connect. The Symposium Call Center Server and client both connect to the CLAN. Third-party applications that interface with the server also connect to this LAN.

D   **DBMS**

Database Management System

deactivated script
A script that does not process any new calls. If a script is in use when it is deactivated, calls continue to be processed by the script until they are completed.

default activity code
The activity code that is assigned to a call if an agent does not enter an activity code manually, or when an agent presses the activity code button twice on his or her phoneset.

default skillset
The skillset to which calls are queued if they have not been queued to a skillset or a specific agent by the end of a script.

desktop user
A configured user who can log on to the Symposium Call Center Server from a client PC.

DHCP
See dynamic host configuration protocol.

Dial-Up Networking
See Remote Access Services.

Dialed Number Identification Service
An optional service that allows Symposium Call Center Server to identify the phone number dialed by the incoming caller.

directory number
The number that identifies a phoneset on a switch. The directory number (DN) can be a local extension (local DN), a public network telephone number, or an automatic call distribution directory number (ACD-DN).

directory number call
A call that is presented to the DN key on an agent's phoneset.

display threshold
A threshold used in real-time displays to highlight a value below or above the normal range.

DMS
Digital Multiplex Switch.

DN
See directory number.

DN call
See directory number call.

DNIS
See Dialed Number Identification Service.

dongle
The attachment plugged into the parallel port of a server connected to a DMS/
MSL-100 switch that authenticates the serial number required at the time of
server installation.

dynamic host configuration protocol
A protocol for dynamically assigning IP addresses to devices on a network.

dynamic link library
A library of executable functions or data that can be used by a Windows
application. Typically, a DLL provides one or more particular functions and a
program accesses the functions by creating either a static or dynamic link to the
DLL. A DLL can be used by several applications at the same time.

E

ELAN
See embedded local area network.

embedded local area network
A dedicated Ethernet TCP/IP LAN that connects the Symposium Call Center
Server and the switch.

Emergency key
A key on an agent's phoneset that, when pressed by an agent, automatically calls
his or her supervisor to notify the supervisor of a problem with a caller.

event

1. An occurrence or action on the Symposium Call Center Server, such as the sending or receiving of a message, the opening or closing of an application, or the reporting of an error. Some events are for information only, while others can indicate a problem. Events are categorized by severity: information, minor, major, and critical. 2. An action generated by a script command, such as queuing a call to a skillset or playing music.

expression

A building block used in scripts to test for conditions, perform calculations, or compare values within scripts. *See also* logical expression, mathematical expression, and relational expression.

F   **first-level threshold**

The value that represents the lowest value of the normal range for a statistic in a threshold class. The system tracks how often the value for the statistic falls outside this value.

G   **global settings**

Settings that apply to all skillsets that are configured on your system.

global variable

A variable that contains values that can be used by any script on the system. The value of a global variable can only be changed in the Script Variable Properties sheet. It cannot be changed in a script. *See also* call variable, variable.

I   **ICM**

See Intelligent Call Manager.

Incalls key

The key on an agent phoneset to which incoming ACD and Symposium Call Center Server calls are presented.

Intelligent Call Manager

A high capacity call center TCP/IP interface to the switch that enables the exchange of messages between the switch and a remote host computer.

Internet Protocol address

An identifier for a computer or device on a TCP/IP network. Networks use the TCP/IP protocol to route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four values separated by periods. Each value can be 0 to 255. For example, 1.160.10.240 could be an IP address.

intrinsic

A word or phrase used in a script to gain access to system information about skillsets, agents, time, and call traffic that can then be used in formulas and decision-making statements. *See also* call intrinsic, skillset intrinsic, time intrinsic, and traffic intrinsic.

IP address

See Internet Protocol address.

L

LAN

See Local area network.

Line of Business code

See activity code.

LOB code

See activity code.

Local area network

A computer network that spans a relatively small area. Most LANs connect workstations and personal computers and are confined to a single building or group of buildings.

logical expression

A symbol used in scripts to test for different conditions. Logical expressions are AND, OR, and NOT. *See also* expression, mathematical expression, and relational expression.

M   master script

The first script executed when a call arrives at the Symposium Call Center Server. A default master script is provided with Symposium Call Center Server, but it can be customized by an authorized user. It can be deactivated but not deleted. *See also* primary script, script, and secondary script.

mathematical expression

An expression used in scripts to add, subtract, multiply, and divide values. Mathematical expressions are addition (+), subtraction (-), division (/), and multiplication (*). *See also* expression, logical expression, and relational expression.

music route

A resource installed on the switch that provides music to callers while they wait for an agent.

N   night mode

A skillset state in which the server does not queue incoming calls to the skillset, and in which all queued calls are given night treatment. A skillset goes into night mode automatically when the last agent logs off, or the administrator can put it into night mode manually. *See also* out-of-service mode, transition mode.

NPA

See Number Plan Area.

Number Plan Area

Area code

O object linking and embedding

A compound document standard that enables you to create objects with one application and then link or embed them in a second application.

ODBC

See Open Database Connectivity.

OEM

Original equipment manufacturer

OLE

See object linking and embedding.

Open Database Connectivity

A Microsoft-defined database application program interface (API) standard.

out-of-service mode

A skillset state in which the skillset does not take calls. A skillset is out of service if there are no agents logged on or if the supervisor puts the skillset into out-of-service mode manually. *See also* night mode, transition mode.

out-of-service skillset

A skillset that is not taking any new calls. While a skillset is out of service, incoming calls cannot be queued to the skillset. *See also* skillset.

P pegging

The action of incrementing statistical counters to track and report on system events.

pegging threshold

A threshold used to define a cut-off value for statistics such as short call and service level. Pegging thresholds are used in reports.

PEP

See Performance Enhancement Package.

Performance Enhancement Package
A Symposium Call Center Server supplementary software application that enhances the functionality of previously released software by improving performance, adding functionality, or correcting a problem discovered since the original release.

phoneset
The physical device, connected to the switch, to which calls are presented. Each agent and supervisor must have a phoneset.

phoneset display
The display area on an agent's phoneset where information about incoming calls can be communicated.

Position ID
1. A unique identifier for a phoneset, used by the switch to route calls to the phoneset. 2. Referred to as Telephony/Port Address in Symposium Call Center Server.

primary ACD-DN
A directory number that callers can dial to reach an ACD group.

primary script
A script that is executed or referenced by the master script. A primary script can route calls to skillsets, or it can transfer routing control to a secondary script. *See also* master script, script, and secondary script.

R   RAN
recorded announcement

RAN route
See recorded announcement route.

RAS
See Remote Access Services.

recorded announcement route

A resource installed on the switch that offers a recorded announcement to callers.

relational expression

An expression used in scripts to test for different conditions. Relational expressions are less than ($<$), greater than ($>$), less than or equal to ($<=$), greater than or equal to ($>=$), and not equal to ($<>$). *See also* expression, logical expression, and mathematical expression.

Remote Access Services

A feature built into Windows NT and Windows 95 that enables users to log on to an NT-based LAN using a modem, X.25 connection, or WAN link. This feature is also known as Dial-Up Networking.

reporting supervisor

The supervisor who has primary responsibility for an agent. When an agent presses the Emergency key on the phoneset, the emergency call is presented to the agent's reporting supervisor. *See also* associated supervisor.

S

sample script

A script that is installed with the Symposium Call Center Server client. Sample scripts are stored as text files in a special folder on the client. The contents of these scripts can be imported or copied into user scripts to create scripts for typical call center scenarios.

SCM

See Service Control Manager.

script

A set of instructions that relates to a particular type of call, caller, or set of conditions, such as time of day or day of week. *See also* master script, primary script, and secondary script.

script variable

See variable.

second-level threshold
The value used in display thresholds that represents the highest value of the normal range for a given statistic. The system tracks how often the value for the statistic falls outside this value.

secondary directory number
A DN defined on the agent's phoneset as a Centrex line for incoming and outgoing non-ACD calls.

secondary script
Any script (other than a master or primary script) that is referenced from a primary script or any other secondary script. There is no pegging of statistics for actions occurring during a secondary script. *See also* master script, primary script, and script.

server
A computer or device on a network that manages network resources. Examples of servers include file servers, print servers, network servers, and database servers. The Symposium Call Center Server is used to configure the operations of the call center. *See also* client.

service
A process that adheres to a Windows NT structure and requirements. A service provides system functionality.

Service Control Manager
A Windows NT process that manages the different services on the PC.

service level
The percentage of incoming calls answered within a configured number of seconds.

service level threshold
A parameter that defines the number of seconds within which incoming calls should be answered.

Simple Network Management Protocol
A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network and then analyzing the responses.

site
A system using Symposium Call Center Server that can be accessed using SMI.

skillset
A group of capabilities or knowledge required to answer a specific type of call.

skillset intrinsic
A script element that inserts information about a skillset in a script. Skillset intrinsics return values such as skillsets, integers, and agent IDs. These values are then used in queuing commands. *See also* call intrinsic, intrinsic, time intrinsic, and traffic intrinsic.

skillset priority
An attribute of a skillset assignment that determines the order in which calls from different skillsets are presented to an agent. When an agent becomes available, calls might be waiting for several of the skillsets to which the agent belongs. The server presents the call queued for the skillset for which the agent has the highest priority.

standby
In skillset assignments, a property that grants an agent membership in a skillset, but makes the agent inactive for that skillset.

supervisor
A user who manages a group of agents. *See also* associated supervisor, reporting supervisor.

supplementary ACD-DN
A DN associated with a primary DN. Any calls to the supplementary DN are automatically routed to the primary DN. A supplementary DN can be a toll-free (1-800) number.

switch

The hardware that receives incoming calls and routes them to their destination.

switch resource

A device that is configured on the switch. For example, a CDN is configured on the switch, and then is used as a resource with Symposium Call Center Server. *See also* acquired resource.

Symposium Call Center Server call

A call to a CDN that is controlled by the Symposium Call Center Server. The call is presented to the Incalls key on an agent's phoneset.

system-defined script

The Master_Script. This script can be customized or deactivated by a user, but cannot be deleted. This script is the first script executed for every call arriving at the call center.

T

TCP/IP

See Transport Control Protocol/Internet Protocol.

telephony

The science of translating sound into electrical signals, transmitting them, and then converting them back to sound. The term is used frequently to refer to computer hardware and software that perform functions traditionally performed by telephone equipment.

threshold

A value for a statistic at which system handling of the statistic changes.

threshold class

A set of options that specifies how statistics are treated in reports and real-time displays. *See also* display threshold, pegging threshold.

time intrinsic

A script element that stores information about system time, including time of day, day of week, and week of year. *See also* call intrinsic, intrinsic, skillset intrinsic, and traffic intrinsic.

Token Ring
A PC network protocol developed by IBM. A Token Ring network is a type of computer network in which all the computers are arranged schematically in a circle.

traffic intrinsic
An intrinsic that inserts information about system-level traffic in a script. *See also* call intrinsic, intrinsic, skillset intrinsic, and time intrinsic.

transition mode
A skillset state in which the server presents already queued calls to a skillset. New calls queued to the skillset are given out-of-service treatment. *See also* night mode, out-of-service mode.

Transport Control Protocol/Internet Protocol
The communication protocol used to connect devices on the Internet. TCP/IP is the standard protocol for transmitting data over networks.

treatment
See call treatment.

U

user-created script
A script that is created by an authorized user on the Symposium Call Center Server system. Primary and secondary scripts are user-created scripts.

user-defined script
A script that is modified by an authorized user on the Symposium Call Center Server system.

utility
A program that performs a specific task, usually related to managing system resources. Operating systems contain a number of utilities for managing disk drives, printers, and other devices.

V   validation

The process of checking a script to ensure that all the syntax and semantics are correct. A script must be validated before it can be activated.

variable

A placeholder for values calculated within a script, such as CLID. Variables are defined in the Script Variable Properties sheet and can be used in multiple scripts to determine treatment and routing of calls entering the Symposium Call Center Server. *See also* call variable, global variable.

W   WAN

See Wide area network.

Wide area network

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs). The largest WAN in existence is the Internet.

workload scenarios

Sets of configuration values defined for typical patterns of system operations. Five typical workload scenarios (entry, small, medium, large, and upper end) are used in the Capacity Assessment Tool for capacity analysis for the Symposium Call Center Server.

Index

Symbols

%_Calls_Abandoned threshold, 127
%Abandoned_Aft_Threshold threshold, 127
%Service Level for Ans Calls threshold, 130
%Service Level threshold, 128

Numerics

1003t
    formatting the RAID drives on, 332–334
    performing a consistency check on, 323
    performing a RAID backup on, 330–331
    rebuilding RAID drives on, 328
    recovering an entire system, 400–401
    restoring a RAID backup, 385–399
    splitting the RAID drives on, 324–327
4 mm DAT tape drive, 288
40593 error code, 252
40593 event code, 71
702t
    performing a consistency check on, 309–310
    performing a RAID backup on, 318–319
    rebuilding the RAID drives on, 316–317
    recovering an entire system, 392–393, 394–396
    restoring a RAID backup, 386–391
    splitting the RAID drives on, 311–315

A

Access Class box, 49
access classes, 27–34
    adding, 29–31
    changing, 34
    deleting, 34
    previewing list of, 34
    printing list of, 34
Access Classes function, 35

access privileges, 35–44
access to server, controlling, 51–53
ACD subgroup, 92, 192
ACD-DNs, 114
ACDLOGIN table, 205
acquiring
    CDNs, 82
    phonesets, 95
    resources, 74–75
    voice ports, 104
Active Agents parameter, 156
Active threshold, 126
Activity Code box, 154
Activity Code Name box, 110
Activity Code Number box, 110
activity codes, 107–111, 178
    adding, 109–110
    changing, 111
    deleting, 111
    previewing list of, 111
    printing list of, 111
Activity Codes function, 35
Activity Codes parameter, 156
Activity LED, 435
    troubleshooting, 435
Add Voice Port box, 94
add-in adapter, problems with, 436
adding
    access classes, 29–31
    activity codes, 109–110
    agent to skillset assignments, 233–236
    agent to supervisor assignments, 221–223
    agents, 205–213
    call presentation classes, 165–166
    CDNs, 79–81
    connection profile, 413
    desktop users, 47–50
    Dial-Up Networking connection profile, 412–414
    DNISs, 115–116

I

Idle threshold, 126
idle time preference, 172, 173
    configuring, 185–187
Information event severity level, 249
installation tips, PCI, 437
installing
    Dial-Up Networking, 404, 412
    pcANYWHERE32 on the client, 408–409
    pcANYWHERE32 on the server, 406, 427–429
    Remote Access Service, 404
Interval box, 157, 225, 238, 270, 272
interval-to-date mode, 141
IRQs, installation tips, 437
IVR ports parameter, 157
IVR Voice Port box, 158

L

Length of business day box, 158
Let Call Ring at Phoneset option, 166
Level 1 box, 123
Level 2 box, 123
lights, troubleshooting, 435
line of business codes. *See* activity codes
Link LED, 435
    troubleshooting, 435
LOB codes. *See* activity codes
local calls, collection of call-by-call statistics
        for, 159
location, grouping servers by, 20
locking out desktop users, 51–52
lockout, 25
logged-on desktop users
    printing list of, 60
    viewing list of, 60
logging desktop users off, 61
logging on
    to the server, 21
Login ID box, 197, 208
Login/Logout box, 154
Logout threshold, 127
Longest Wait Since Last Call threshold, 133

Longest Wait Since Login threshold, 133

M

maintaining Symposium Call Center Server, 9–10
Maintenance function, 40
Major event severity level, 249
managing Symposium Call Center Server, 9–10
Map Skillset to ACD-DN Number box, 183
MAS database events, 251
MAS debug events, 251, 262
MAT systems, 18
Max Wait Time threshold, 133
Max Waiting Time threshold, 129
Maximum Log Size box, 261
Maximum wait Interval box, 294
Measured Value box, 155
members of access classes, viewing, 32–33
Meridian Application Tool, 18
Microsoft hot fix, 348, 374
Minimum refresh rate for Agent Real-time
        Displays box, 144
Minimum refresh rate for other Real-time
        Displays box, 144
Minor event severity level, 249
modem port, configuring, 423
modifying. *See* changing
Month box, 225, 238
Monthly box, 157
moving window mode, 141
MSL-100 switch. *See* switch
music routes, 85–89
    adding, 87–88
    changing, 89
    deleting, 89
    previewing list of, 89
    printing list of, 89
Music Routes parameter, 156
Music/RAN Route box, 154
Music/RAN Route Name box, 88
Music/RAN Route Number box, 88
Music/RAN Routes function, 40

N

O

P

U

V

W

Reader Response Form

**Nortel Networks Symposium Call Center
Server Product release 3.0
Administrator's Guide
P0911818**

Tell us about yourself:

Name: _____

Company: _____

Address: _____

_____

Occupation: _____ Phone: _____

1. What is your level of experience with this product?

   ☐ New user   ☐ Intermediate   ☐ Experienced   ☐ Programmer

2. How do you use this book?

   ☐ Learning   ☐ Procedural   ☐ Reference   ☐ Problem solving

3. Did this book meet your needs?

   ☐ Yes   ☐ No

   If you answered No to this question, please answer the following questions.

4. What chapters, sections, or procedures did you find hard to understand?

   _____

   _____

   _____

5. What information (if any) was missing from this book?

   _____

   _____

   _____

6. How could we improve this book?

   _____

   _____

   _____

Please return your comments by fax to (416) 597-7104, or mail your comments to
Toronto Information Products, Nortel Networks, 522 University Avenue, 14th Floor, Toronto, ON,
Canada, M5G 1W7.

NORTEL NETWORKS™

How the world shares ideas.

Reader Response Form

Nortel Networks Symposium Call Center Server

for DMS/MSL-100
Administrator's Guide

NORTEL NETWORKS™

How the world shares ideas.