Optivity Telephony Manager

Installation and Engineering

Guide

Document Number: P0910102
Document Release: Standard 1.0
Date: July 2000

Printed in the United States of America

Revision history

Date	Document Version	Product Release
July 2000	Standard	1.0

Contents

Glossary . . . . . **xix**

Initial Installation Tasks **21**

OTM requirements 22
- Meridian 1 X11 release and package requirements 22
- OTM Server hardware requirements 23
- OTM Server software requirements 24
- PC Client requirements 24

OTM Server software installation 25
- Software License Agreement 28
- Welcome 29
- Identification 30
- Setup Choices 31
- Serial Number and Keycode 33
- Destination for Application Files 34
- Destination for Common Data Files 35
- Destination for Local Data 35
- Installation options 36
- Applications to Install 37
- Copy files 38
- Database Rebuild 38
- Read Me File 39
- Java Runtime Environment (JRE) 40
- System Restart 41

OTM Client software installation 43

OTM upgrades 49

Upgrade the OTM Server to the same release of OTM 49
Upgrade to new release of OTM 49
Web Help and Documentation Installation 53
Migration from MAT to OTM 54
MAT/OTM Migration 57
Uninstall OTM 59
License Management 64
TN license 64
Client license 65
Security device (dongle) 65

Initial configuration tasks 67

Log in and change the default password 68
Test the connection 69
Set up communications information 69
Set up customer information 73
Set up OTM applications 74
Set up system data 75
Add sites and systems via the OTM Windows Navigator 76
Adding a site 76
Adding a Meridian 1 system 77
Adding a Generic system or device 91
Add OTM Windows users via the OTM Windows Navigator 93
Create a user template 93
Adding a user 96
Adding web users 97
Web Navigator users 97
Desktop Services Users 98
Set Up Meridian 1 98
Determine the OTM PC IP address 108
Enable alarms with Overlay 117 109
Set Up the Virtual Terminal Service 110
Virtual Ports 110
Set Up the Data Buffering and Access Application 116

Set Up the LDAP Server 117
Set Up Alarm Management 118
Perform an OTM backup 118
OTM Web Browser Client installation 120
Accessing the OTM Server Web Navigator via the PC Client 120

Appendix A: Windows NT installation example 121

Hardware Compatibility Check 122
Running the Windows NT Setup Program 122
Installing Windows NT components 124
Network Adapter Software Installation 124
TCP/IP Configuration 126
Initial Workgroup Configuration 128
Configuring system settings 128
Creating an Emergency Repair Disk 128
Completing the Windows NT Installation 129
Remote Access Service Installation 129
RAS with TCP/IP 130
Grant Permission 130
Call back 131
Encrypted Passwords and Data Encryption 131
Multilink 132
RAS Client 133
Testing Network Cards 134
Internet Explorer Installation 134
Windows NT Service Pack 5 installation 135
Windows NT 4.0 Option Pack installation 135
Reinstall Service Pack 5 136
Setting up a separate Windows NT account 137

Appendix B: Configuring a Windows NT Server or Workstation as an IP router 139

Requirements 139

Setup 140
Windows NT Workstation/Server 4.0 Network Configuration . . . 141
Windows 95 TCP/IP Configuration 143
Meridian 1 switch TCP/IP Configuration 144
Troubleshooting 145

Appendix C: Windows NT Security Guidelines 149

Installation 150
General Policies 151
Secure the User Accounts on the Windows NT System 151
Passwords 153
Audit Trail and Security Log 154
System Services 154
Network Sharing 155
Networking 155
Remote Access 156
NT Option Pack 4—IIS 156

Appendix D: Modem Configuration for OTM Applications in Microsoft Windows 161

High-speed smart modem configuration consideration 163
Troubleshooting modem connections 165

Appendix E: Integrating OTM with Optivity NMS 169

How the OTM with Optivity NMS Integration Works 170
Integration Requirements 171
What Happens During the OTM Installation 172
Checklist for Installing the OTM Integration 172
About oitInstall 173
Alarm Integration 174
Using Optivity NMS InfoCenter 174
Creating an OTM Server Object In Optivity NMS InfoCenter . . . 174
Viewing OTM Server Object Properties 175

Modifying OTM Server Object Properties 176
Starting OTM Web Applications 176
Java Runtime Environment 176
Web Server 176
Removing an OTM Server 177

Appendix F: OTM Engineering Guidelines 179

Capacity Factors 179
Sample walk-through of computations 181
Sample configurations based on application usage and features . . . 181
Sample PC and Meridian 1 configurations 181
Operational constraints 182
Configuration Calculations 184
Software Limits 189
Hard-coded Limits 189
Operational Limits 190
PC Hardware 192
OTM Server Minimum Hardware Requirements 193
Physical Memory 195
Hard Disk 196
Processor Speed 197
Windows NT Server and Windows NT Workstation Differences . 198
Network Bandwidth 199
Typical Configurations 199
Bandwidth Utilization 205

List of figures

Figure 1
High level outline 25

Figure 2
Software Installation Wizard 26

Figure 3
Software Selection 27

Figure 4
Software License Agreement 28

Figure 5
Welcome 29

Figure 6
Identification 30

Figure 7
Setup Choices 31

Figure 8
Enter Keycodes 33

Figure 9
Destination for Application Files 34

Figure 10
Select Components 36

Figure 11
Applications to Install 37

Figure 12
Copy files 38

Figure 13
Station Database Rebuild 38

Figure 14
JRE Installation 40

Figure 15
CLI configuration window 41

Figure 16
Source for Application Executables dialog box 44

Figure 17
Source for Common Data Files dialog box 45

Figure 18
Destination for Local Data Files dialog box 46

Figure 19
Enter Keycodes dialog box 47

Figure 20 48

Figure 21
Applications to Install 50

Figure 22
Applications to Upgrade 51

Figure 23
Applications to Remove 52

Figure 24
Software Selection: Web Help 53

Figure 25
MAT Migration: OTM Setup dialog box 55

Figure 26
MAT Backup Database: Choose Destination Location 56

Figure 27
Uninstall dialog box 60

Figure 28
Uninstall Confirmation dialog box 61

Figure 29
Uninstall status box 61

Figure 30
Uninstall Common Services dialog box 62

Figure 31
Uninstall confirmation question box 63

Figure 32
Uninstall complete information box 63

Figure 33
TN license warning dialog box 64

Figure 34
TN license error dialog box 64

Figure 35
Client removed dialog box 65

Figure 36
Change Password dialog box 68

Figure 37
Add Communications Profile dialog box 69

Figure 38
System property sheet, Communications tab, Ethernet profile 70

Figure 39
System property sheet, Communications tab, PPP Profile 71

Figure 40
System property sheet, Communications tab, Serial Profile 72

Figure 41
Customer property sheet, General tab 73

Figure 42
System property sheet, Applications tab 74

Figure 43
New Site Properties sheet 76

Figure 44
Add System dialog box 78

Figure 45
System Properties—General tab 79

Figure 46
Add Communications Profile dialog box 80

Figure 47
System Properties—Communications tab—Ethernet Profile 81

Figure 48
System Properties—Communications tab—PPP Profile 82

Figure 49
System Properties—Communications tab—Serial Profile 83

Figure 50
System Properties—System Data tab 84

Figure 51
System Properties—Applications tab 86

Figure 52
System Properties—Customers tab 87

Figure 53
Customer property sheet, General tab 88

Figure 54
Customer property sheet, Features tab 89

Figure 55
Customer property sheet, Numbering Plans tab 90

Figure 56
Configure non-Meridian 1 devices 92

Figure 57
OTM Users window 93

Figure 58
User Templates Window 94

Figure 59
New Template property sheet 94

Figure 60
New User property sheet 96

Figure 61
Configuring Virtual Ports (serial, logging disabled) 111

Figure 62
Configuring Virtual Ports (Meridian 1 system, logging enabled) 112

Figure 63
Configuring Virtual Ports (Telnet system, logging enabled) 113

Figure 64
Terminal Properties dialog box 115

Figure 65
OTM Backup Information dialog box 119

Figure 66
JRE Plug-in download prompt 120

Figure 67
Microsoft TCP/IP Properties window 127

Figure 68
RAS Server TCP/IP Configuration window 131

Figure 69
Network Configuration window 133

Figure F-1
Connecting OTM to legacy Meridian systems (pre-Ethernet) 199

Figure F-2
Connecting OTM to ELAN connected Meridian Systems 201

Figure F-3
Connecting OTM to CWAN connected Meridian systems 202

Figure F-4
Networking OTM Servers, External to Customer WAN 203

Figure F-5
Networking OTM Servers, Internal to Customer WAN 204

List of tables

Table 1
Meridian 1 X11 release and packages 22

Table 2
Migration for OTM Windows NT server mode 58

Table 3
Migration for OTM standalone mode 59

Table 4
SDI Port settings for OTM applications 101

Table 5
Directory Permissions 157

Table 6
Services that can Run on a Secure IIS Server 158

Table F-1
Maximum configuration for an Option 11C network averaging 400 lines per switch 183

Table F-2
Maximum configuration for an Option 81 network averaging 2000 lines per switch 184

Table F-3
PC Performance by Application 191

Table F-4
Differences Between Windows NT Server and Windows NT Workstation 198

Table F-5
Network Bandwidth Usage Per Meridian 1 System 205

Glossary

ASP

Active Server Page.

CLI

Command Line Interface.

DBA

Data Buffering and Access.

GUI

Graphical User Interface.

IP

Internet Protocol.

LAN

Local Area Network. Generally, a LAN is a group of computers connected in a geographically close network.

LDAP

Light-weight Directory Access Protocol.

MAT

Meridian Administration Tools.

NMS

Network Management System.

OTM

Optivity Telephony Manager.

PTY

Pseudo-TTY (network port).

RAS

Remote Access Server.

TBS

Telecom Billing System. OTM replacement for MAT Call Accounting application.

TTY

TeleType (serial port).

uid

Unique Identifier in LDAP synchronization.

Initial Installation Tasks

This section contains:

- Optivity Telephony Manager (OTM) installation requirements
- Procedures to install the OTM server software, validate the installation, and configure OTM features

OTM server software installation begins on page 25.

Appendix A provides a Microsoft® Windows NT® installation example to help the new Windows NT and OTM administrator get started. OTM is designed for use in either Windows NT, Windows 95® or Windows 98® operating environments. Only the Windows NT environment supports the server/client and web interface features of OTM.

OTM combines with Optivity Network Management System (NMS) 9.0.1 and above to give an integrated data, voice and video network, as part of the Nortel Networks Unified Networking system. The resulting integration provides converged LAN, WAN and voice management, and the capacity to monitor OTM server activity through Optivity NMS. See *Appendix E: Integrating OTM with Optivity NMS* on page 169 for more information on OTM/Optivity NMS integration procedures and requirements.

For information on how to set up a Microsoft NT Server or Workstation as an alternative IP router on the LAN, refer to *Appendix B: Configuring a Windows NT Server or Workstation as an IP router* on page 139.

For installation recommendations that will help to create a secure environment for your OTM data and users, refer to *Appendix C: Windows NT Security Guidelines* on page 149.

To configure modems for use with OTM, refer to *Appendix D: Modem Configuration for OTM Applications in Microsoft Windows* on page 161.

For detailed hardware and software guidelines to consider when planning OTM installations, refer to *Appendix F: OTM Engineering Guidelines* on page 179.

OTM requirements

OTM requirements include:

- "Meridian 1 X11 release and package requirements" on page 22
- "OTM Server hardware requirements" on page 23
- "OTM Server software requirements" on page 24
- "PC Client requirements" on page 24.

Meridian 1 X11 release and package requirements

In general, OTM 1.0 requires no special X11 release to run.
Table 1 is a list of X11 releases and packages required based on the OTM applications.

Table 1
Meridian 1 X11 release and packages

OTM Application	Minimum X11 Release Required	X11 Pkg Required
Alarm Notification	X11 R22 or later	Pkg 296, 315
Data Buffering and Access-Ethernet	X11 R24 or later	Pkg 296, 351
Data Buffering and Access - Serial	N/A	N/A
M1 Database Disaster Recovery	X11 R24 or later	Pkg 296, 351
Virtual Terminal	X11 R22 or later for access over IP	

OTM Server hardware requirements

The OTM Server must meet the following minimum hardware requirements. Refer to *Appendix F: OTM Engineering Guidelines* on page 179 for more information on OTM Server hardware requirements.

Note: This information is subject to change. For the latest system requirements, see the OTM General Release Bulletin.

- Intel Pentium II Processor 400MHz or faster CPU
- 2 GB hard drive or greater (1000 MB free space plus customer data storage requirements)
- 256 MB of RAM (Minimum)
- CD-ROM Drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA Color Monitor and interface card (800 X 600 resolution for graphics)
- Two Ethernet Network Interface cards are required to support connection with the Meridian 1 via Ethernet and Customer LAN
- Hayes-compatible modem is optional for connection to remote systems, required for polling configurations (56K BPS or better recommended)
- PC COM port with 16550 UART
- Printer port required for dongle
- Dongle (for server only)
- Windows-compatible mouse or pointing device (PS/2 mouse preferred to free up a PC serial port)

OTM Server software requirements

OTM requires a Windows NT 4.0 Server or Windows NT Workstation with the following software:

- TCP/IP Protocol
- Remote Access Service
- NT Server 4.0 and Service Pack 5
- Windows NT Option Pack 4
- Network card drivers

Note 1: Optivity Telephony Manager is not supported in a Novell® Netware® network environment.

Note 2: Ask the network card manufacturer about the type of network card and the availability of the required software driver.

PC Client requirements

A PC Client (a computer that accesses the OTM Server) requires the following:

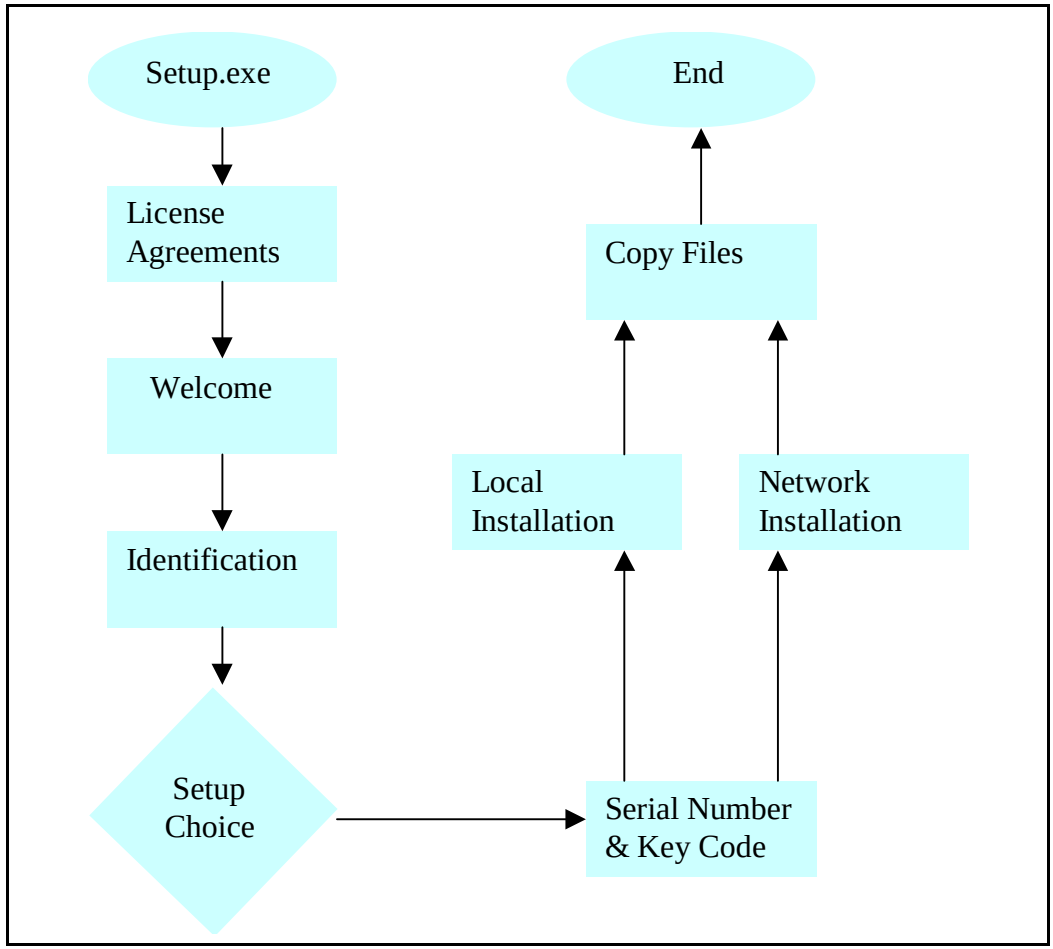
- Intel Pentium 200MHz or faster CPU (Pentium II 300MHz for running Telecom Billing System)
- 2 GB hard drive with 500 MB of free space 64 MB of RAM (Minimum)
- CD-ROM Drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA Color Monitor and interface card (800 X 600 resolution for graphics)
- Ethernet Network Interface
- Windows-compatible mouse or pointing device
- Windows 95, Windows 98 and Windows NT Workstation 4.0 or Server
- The correct Java Runtime Environment (currently version 1.21) installed on the client machine.
- A Microsoft Active Server Page (ASP) and HTML-compliant Web browser

OTM Server software installation

This section describes the OTM Server software installation. The OTM software installation program uses a standard Windows “Wizard” method of user interaction. Before installing OTM, you must log into Windows NT as an Administrator.

The following figure is an high level outline of the installation screens.

Figure 1
High level outline



Note: At the beginning of OTM software installation, the setup program checks for various prerequisites, and displays appropriate messages if one or more required components are not present. Additionally, a log records all errors. During installation, the log resides in the following directory path: **C:\NortelLog\log.txt.** After installation, the log resides in the local directory path where you installed the application. For each error or event, the log lists an "Event type" (Info, Warning, Critical, or Major), and "Message" (e.g., Service Pack 5 is not installed.").

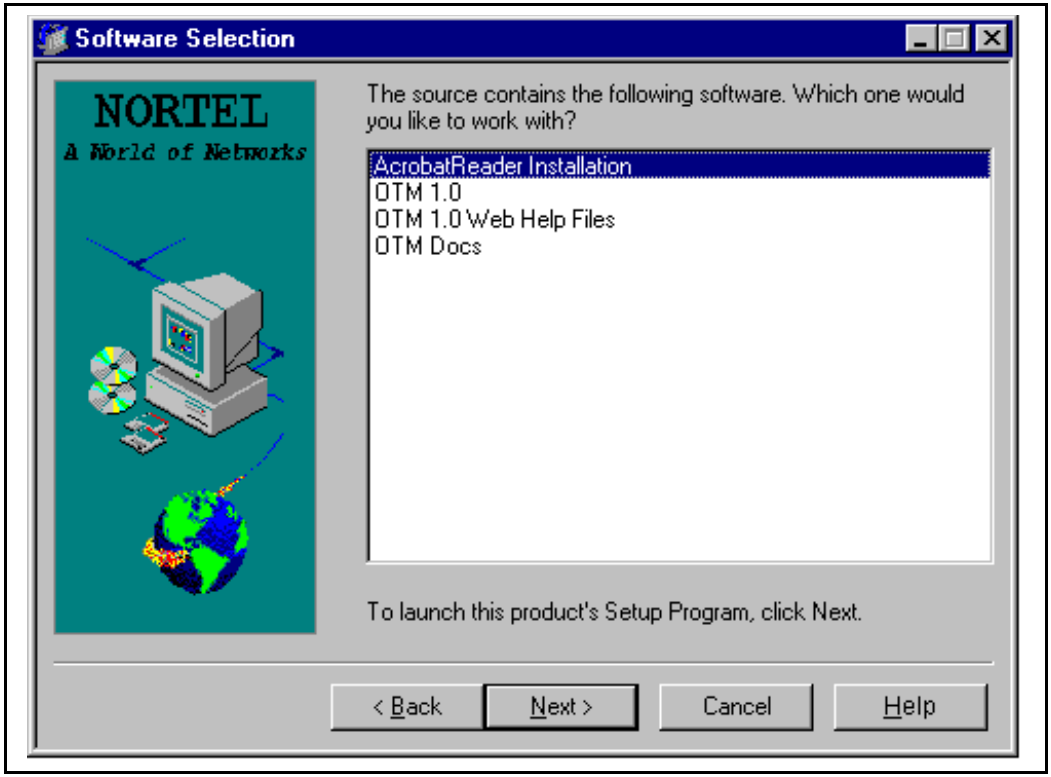
1 Before installation, make sure that you remove the **MAT.exe** shortcut file in the **Start up** folder, if present.

2 Double-click the **Setup.exe** file on the OTM CD-ROM. The welcome screen is displayed (Figure 2). Click **Next** to continue.

Figure 2
Software Installation Wizard

3 Select **OTM 1.0**. The other options are **OTM Documentation**, OTM Web Help files, and Adobe® Acrobat® Reader (Figure 3). These applications can be installed once the OTM Application installation is complete.

Figure 3
Software Selection

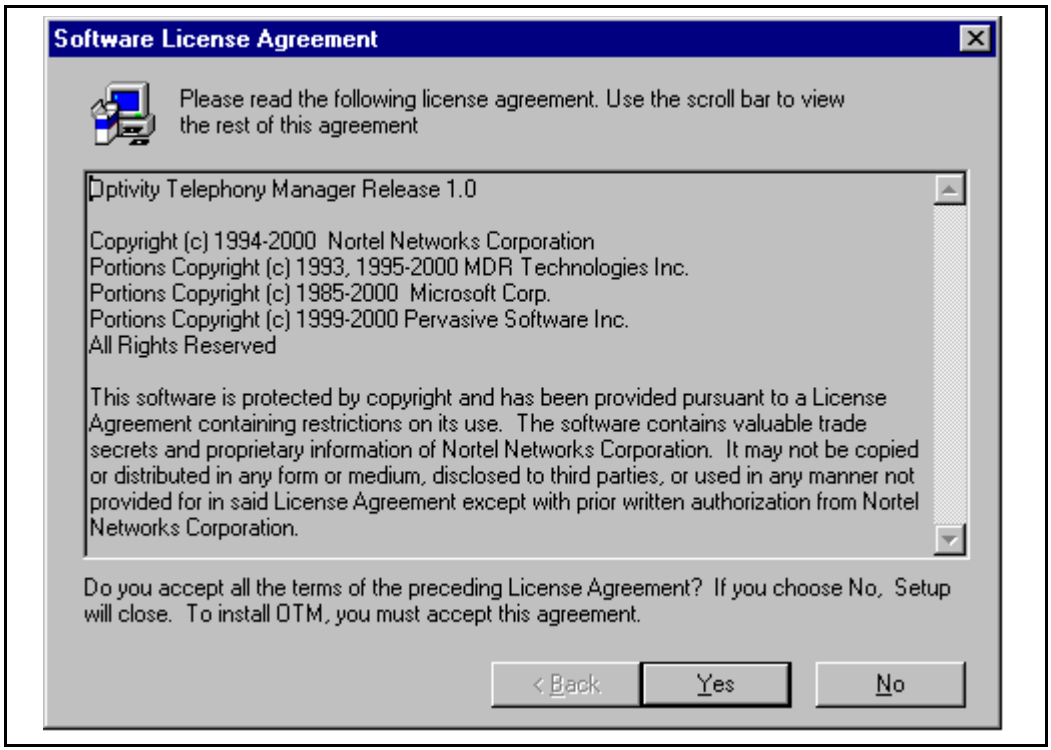


The system then prompts you to install Java Runtime Environment (JRE) and the Windows NT Service Pack 5 if you have not already done so. You may install these options now or later. If you choose to install them now, follow the instructions on screen. reboot your PC when finished, if prompted to do so, and run the OTM Application Setup again.

Software License Agreement

4 The “Software License Agreement” is the first dialog displayed when you launch the OTM installation program (Figure 4). Click **Yes** to accept the agreement.

Figure 4
Software License Agreement

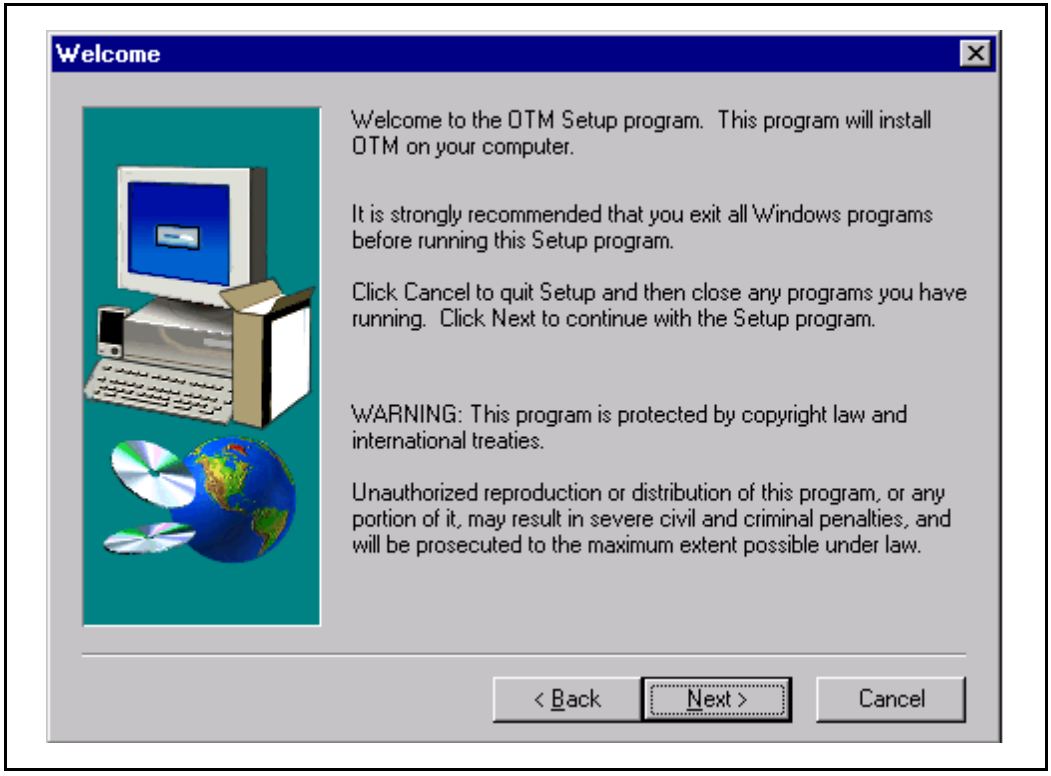


Welcome

The “Welcome” screen (Figure 5) welcomes you to the OTM installation program.

5 Click **Next** to continue.

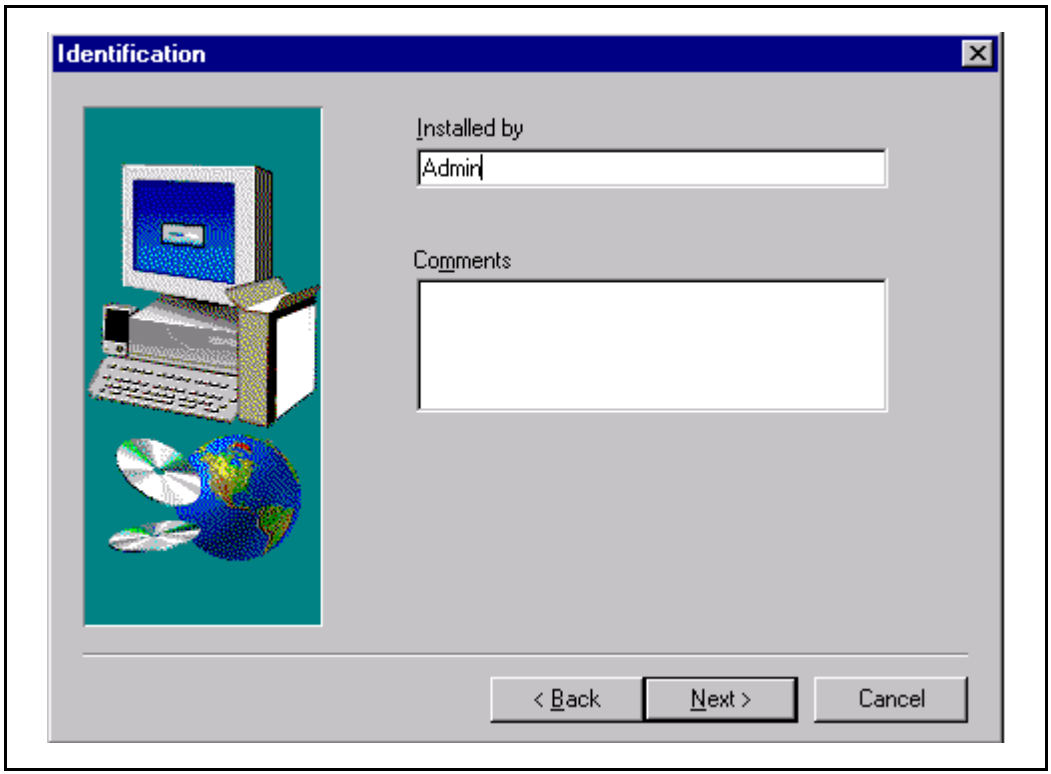
Figure 5
Welcome



Identification

6 Specify the name of the person performing the installation and, optionally, a comment about the installation (Figure 6). Click **Next** to continue.

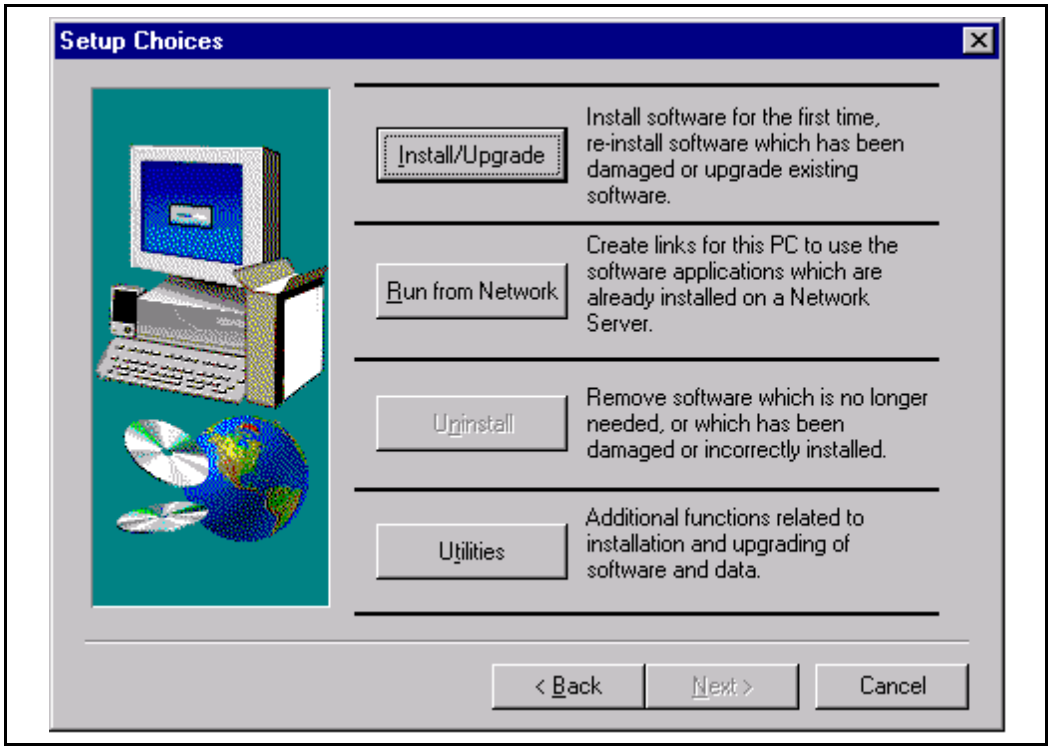
Figure 6
Identification



Setup Choices

7 For installation on an OTM Server, select **Install/Upgrade** (Figure 7). For installation on a Client PC, select **Run from Network** and see "OTM Client software installation" on page 43.

Figure 7
Setup Choices



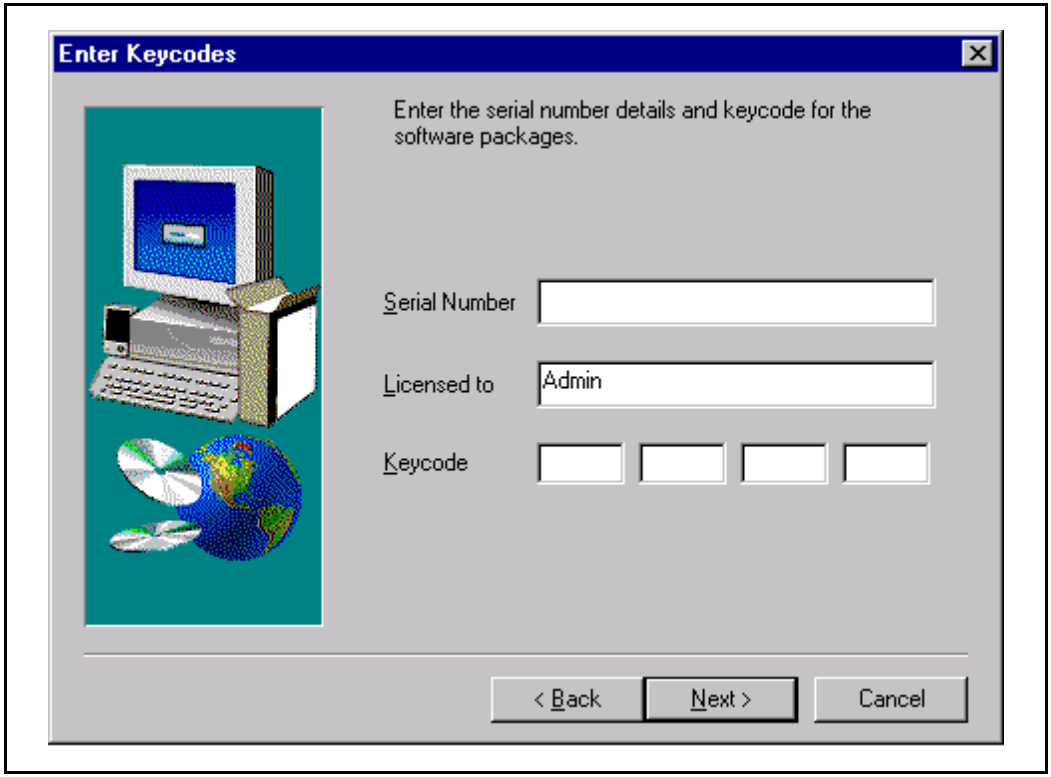
Note 1: Install/Upgrade will not resolve problems with damaged software. To resolve a damaged software problem, backup your data files and perform an Uninstall. Next, perform an Install/Upgrade and then restore your data. See “Table 3 summarizes the migration steps to use OTM in standalone mode.” on page 59.

Note 2: Run from Network is used to install an OTM client. The client has applications/executables, but uses the common data from the OTM server. You must have the OTM Server software installed prior to installing the client software.

Serial Number and Keycode

8 Enter the serial number and keycode which you received with your OTM software package in the Enter Keycodes dialog box (Figure 8). The serial number and keycode determine which applications are installed during the software installation process. The serial number and keycode also determine the maximum number of terminal numbers (TNs), or telephones, and OTM Clients that can be configured in your OTM system. To purchase licensing for additional TNs or Clients, please contact your OTM vendor. Click **Next** to continue.

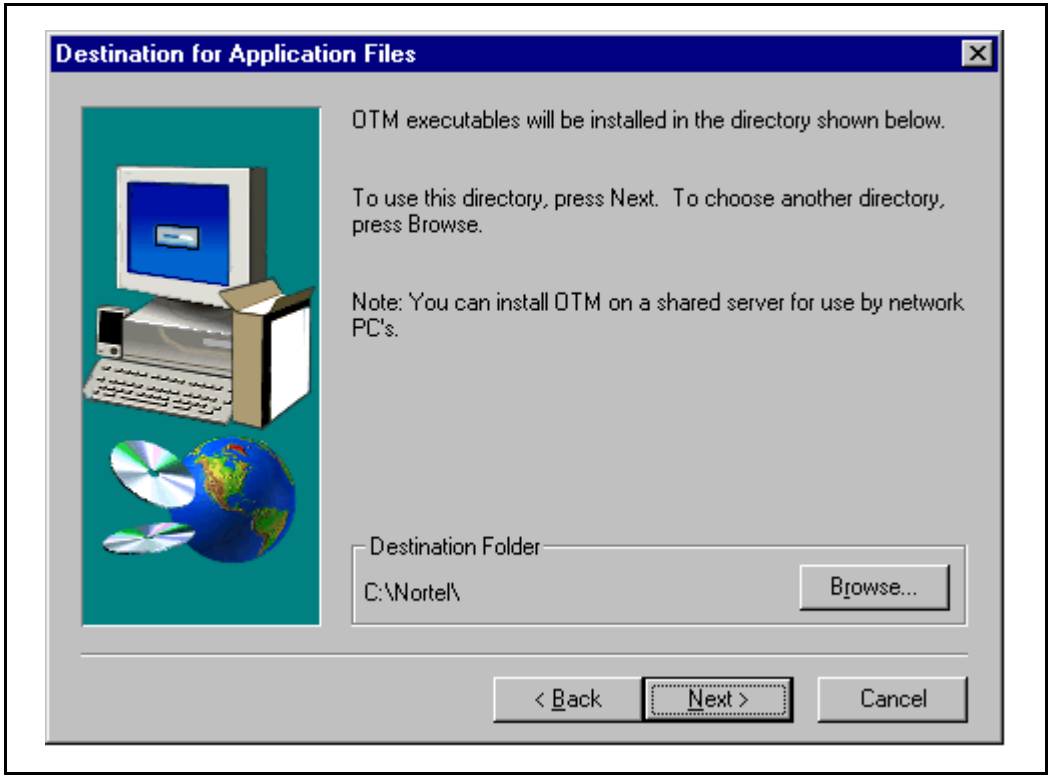
Figure 8
Enter Keycodes



Destination for Application Files

9 Specify the root directory for installing OTM Application files. Use the default directory or browse to specify a different location, as shown in Figure 9. Click **Next** to continue.

Figure 9
Destination for Application Files



Destination for Common Data Files

10 Specify the root directory for installing OTM Common Data files. Use the default directory or browse to specify a different location. The directory defaults to the path defined in step 9. Click **Next** to continue.

> **CAUTION**
> You must specify a local drive for Common Data files storage, to avoid the access problems that can arise with networked drives. The installation process will check your system and prevent you from specifying a networked drive.

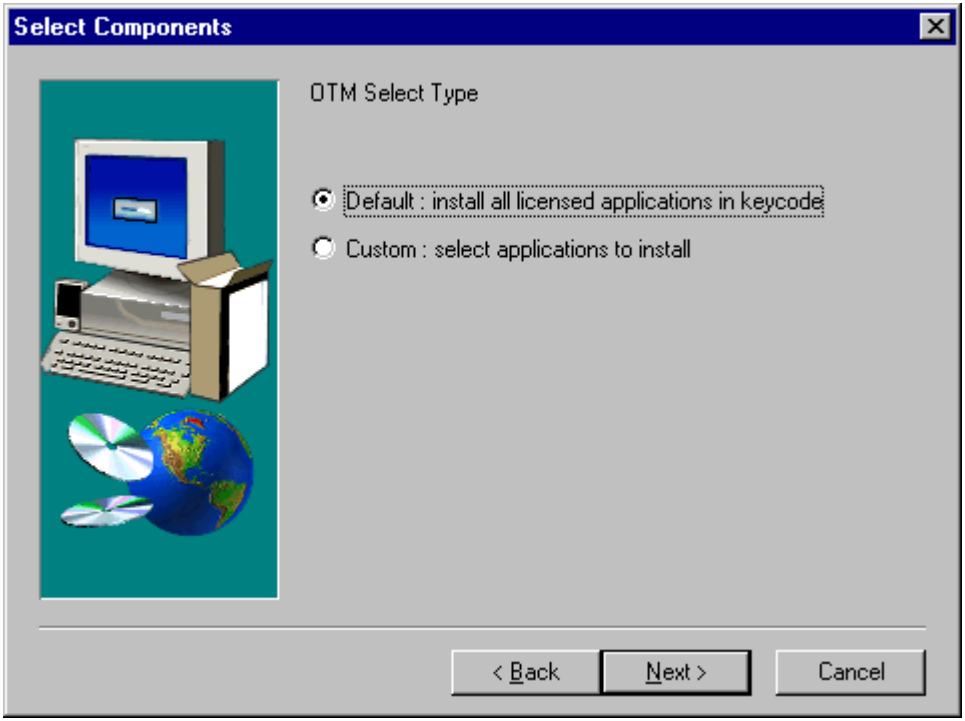
Destination for Local Data

11 Specify the root directory for installing OTM Local Data files. Use the default directory or browse to specify a different location. The directory defaults to the path defined in step 9. Click **Next** to continue.

Installation options

12 Specify Custom or Default installation. Select **Default** to install all purchased applications, select **Custom** to select the OTM applications that you want Setup to install (Figure 10).

Figure 10
Select Components



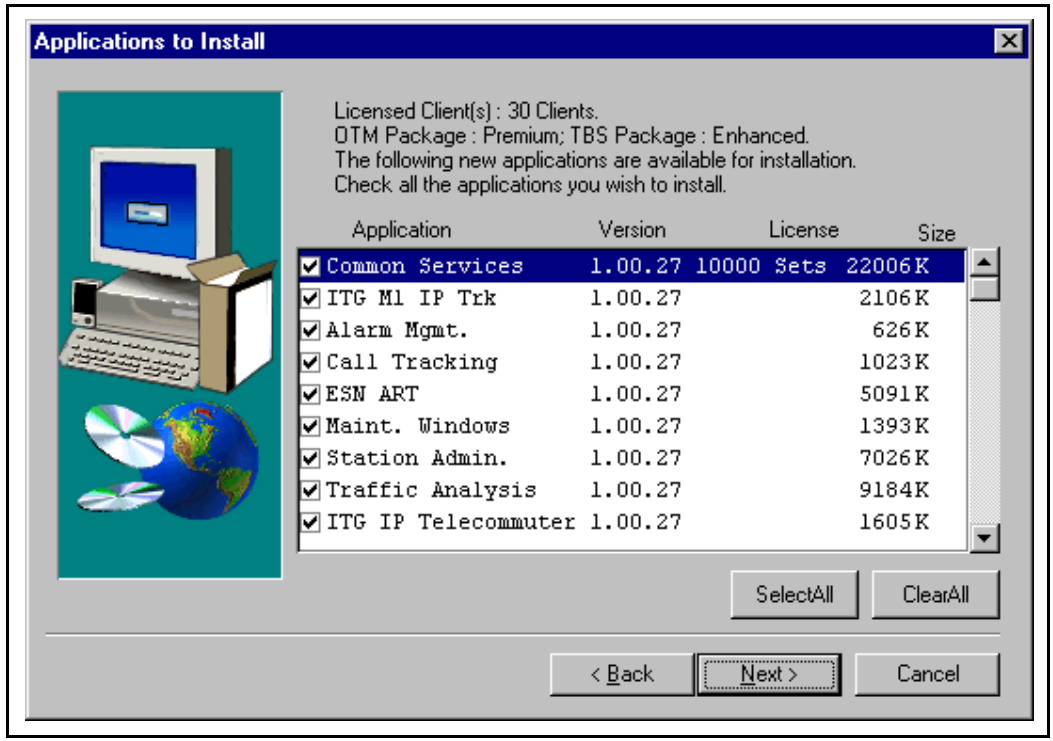
If you select Default, a summary of default applications is displayed.

Note: This summary is displayed for premium OTM installation only. Lesser or customized installations do not install all of these options and will not include these in the summary.

Applications to Install

13 If you selected Custom Install, you are given a list of applications to install (Figure 11). Check the appropriate applications.

Figure 11
Applications to Install

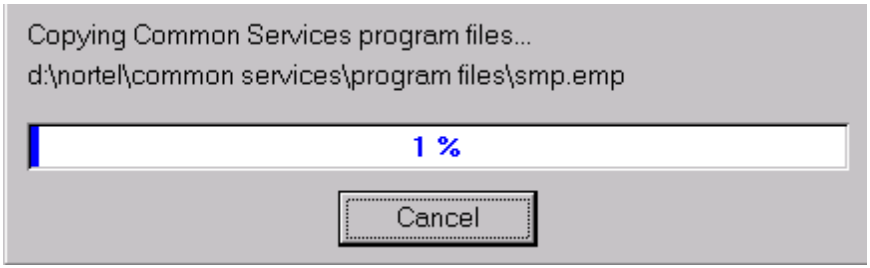


14 Click **Next** to continue.

Copy files

This dialog box displays the percentage status of OTM installation, which application files are being copied and their locations (Figure 12).

Figure 12
Copy files



Database Rebuild

15 Before the Setup program has finished copying program files to your hard drive, you will be prompted to rebuild your Station Database files. The dialog has four buttons (as shown in Figure 13):

- **Rebuild:** To rebuild the current site and system
- **Skip:** To skip the rebuild process for this site
- **Rebuild All:** Rebuild all sites and systems
- **Cancel:** To cancel the rebuild process

Figure 13
Station Database Rebuild

This option allows you to rebuild the Station database of a previous MAT or OTM installation for use with the current OTM version.

You may decide to rebuild specific sites and systems only, using the Skip button. When installing for the first time, it is sufficient to click on the Rebuild button.

Read Me File

This dialog prompts you to read the readme.txt file.

16 Click **Yes** to view the Read Me file or **No** to skip the Read Me file.

Java Runtime Environment (JRE)

If Alarm Notification is installed, you will then be prompted to install Java Runtime Environment (JRE) at this point.

17 Click **Yes** to install JRE.

Figure 14
JRE Installation

You may decide to install JRE at a later time. The JRE install program is located in the OTM directory (e.g., Nortel) at:

- For Windows: **C:\Nortel\OMServices\Jre\Windows\jre1_2_1-win.exe**
- For other operating systems: Support for Java Plug-in Software on other operating systems is provided by the operating system vendor. For more information on Java Plug-in documentation and FAQ, please refer to **http://java.sun.com/**

Note: JRE is required for the Alarm Script Wizard and also for the Web Client. JRE is installed automatically when the client connects to the server for the first time, but must be installed specifically for the Alarm Script Wizard to function.

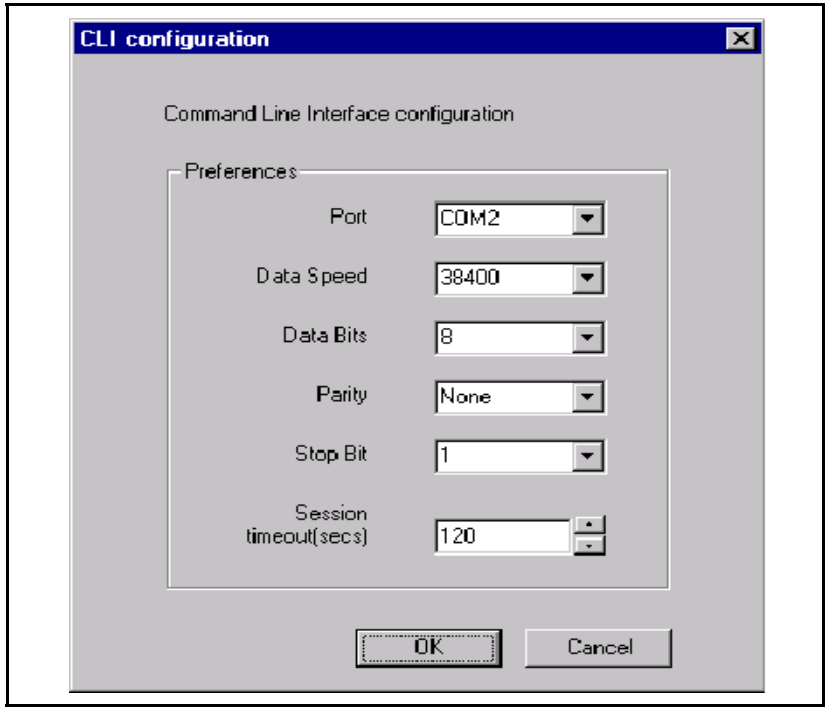
System Restart

This dialog box asks you to restart the computer or end the installation without restarting the computer.

18 Select **Yes, I want to restart my computer now** and click **OK**.

After restarting, the Command Line Interface (CLI) Configuration window appears. See Figure 15.

Figure 15
CLI configuration window



The CLI launches at OTM Server startup. The status window displays CLI status messages. For more information on CLI, see the chapter "Access Server" in the *Optivity Telephony Manager Common Services User Guide*.

19 The CLI configuration window is used to define the following OTM Server COM port settings:

Port - list of COM ports on the OTM Server
Data Speed of COM port - 4800, 9600, 19200, 38400
Data Bits - 5, 6, 7, 8 bits
Parity - None, Odd, Even Mark, Space
Stop Bits - 1, 1.2, 2 bits
Session timeout (secs): if current session is idle for the specified time, CLI disconnects the call

20 Check the installation log to make sure you installed OTM software correctly, and that prerequisites have been met.
During installation, the log resides in the following directory path: **C:\NortelLog\log.txt**. After installation, the log resides in the LocalData directory where you installed the application.

The OTM software installation is complete. The remaining sections in this chapter are:

- *OTM Client software installation* on page 43
- *OTM upgrades* on page 49
- *Web Help and Documentation Installation* on page 53
- *Table 3 summarizes the migration steps to use OTM in standalone mode.* on page 59
- *Table 3 summarizes the migration steps to use OTM in standalone mode.* on page 59

Note: You are required to run **Setup.exe** from your installation CD-ROM each time for the separate OTM install components: OTM, OTM Web Help and OTM Docs.

OTM Client software installation

This section describes the OTM Client software installation. The installation steps are similar to the OTM Server installation. The steps are summarized below. See “OTM Server software installation”, beginning on page 25, to view the installation screens that are common to both procedures.

1 Before installation:

- **a** Remove the **MAT.exe** shortcut file in the **Start up** folder, if present.
- **b** On the OTM server, share the Nortel directory.
- **c** On the Client PC, map the Nortel directory located on the OTM Server.

2 Double-click the **Setup.exe** file on the OTM CD-ROM.

3 Navigate through the OTM installation wizard. The following screens are displayed (see Server installation for examples).

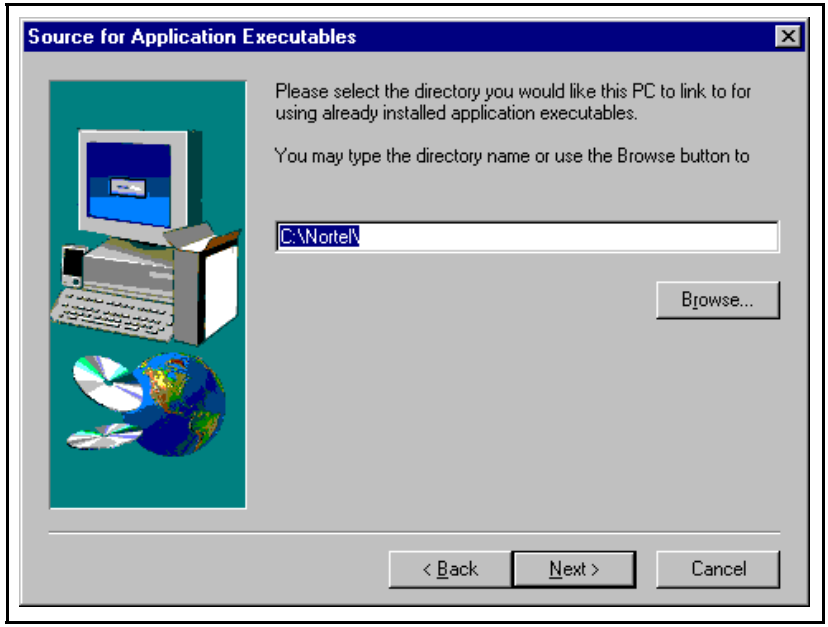
- **a** Software Licences Agreement
- **b** Welcome
- **c** Identification

Note: If required, the setup program installs DCOM at this point if it is not present on the PC. Once installed, the PC must be rebooted. After you reboot and log in, the OTM software installation continues.

4 In the Setup Choices dialog box, select **Run from Network**.

5 Select the directory for the installation of the application executables as shown in Figure 16. Click **Next** to continue.

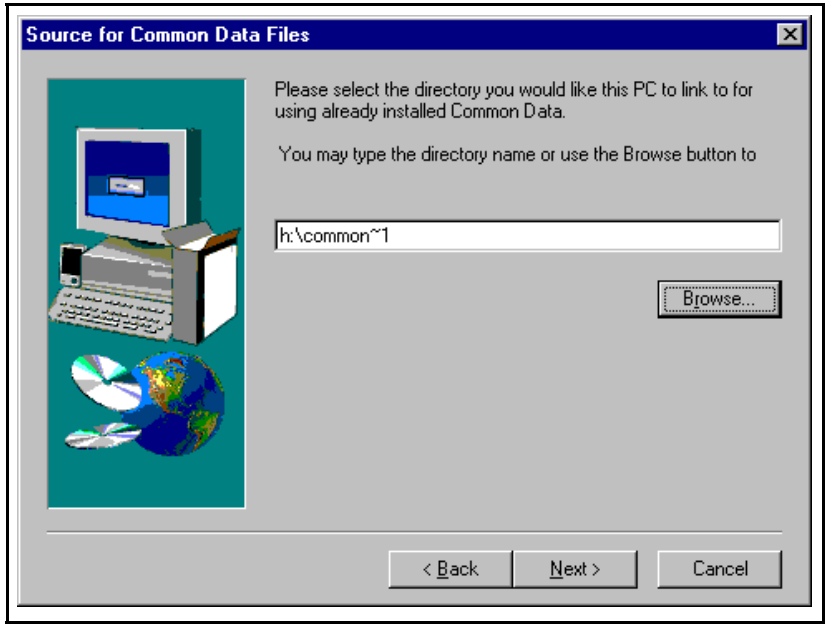
Figure 16
Source for Application Executables dialog box



Note: You may browse and select a local directory on the Client PC, or you may browse and select the mapped OTM Server directory.

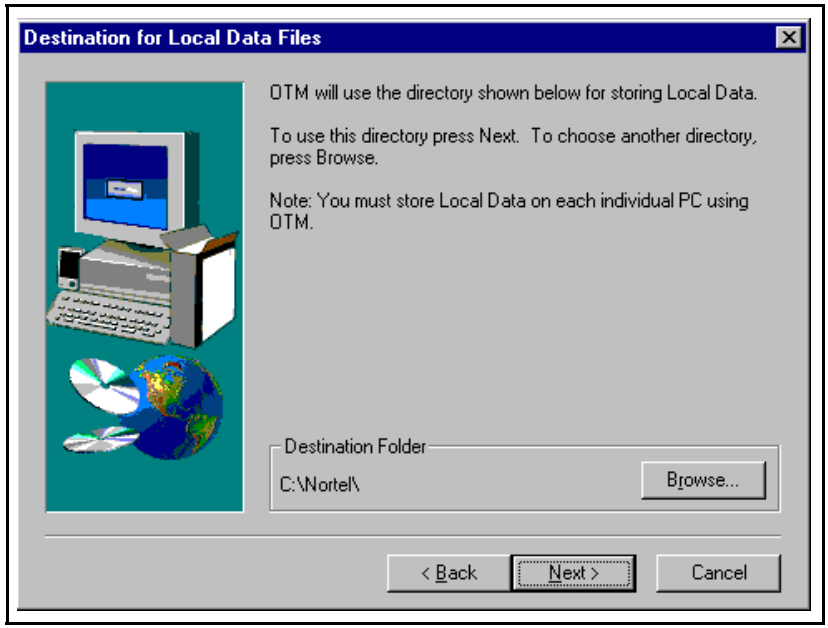
6 Select the directory, on the OTM Server, where the common data files are stored as shown in Figure 17. Click **Next** to continue.

Figure 17
Source for Common Data Files dialog box



7 Select the destination on the Client PC for the local data files. See Figure 18. You must select a directory on the Client PC. Click **Next** to continue.

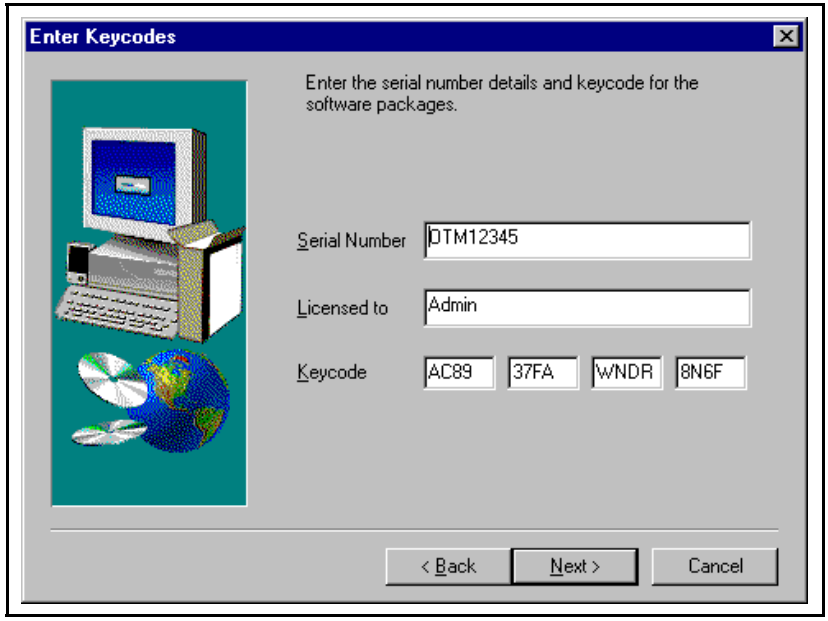
Figure 18
Destination for Local Data Files dialog box



Note: The setup program installs Microsoft Data Access Components (MDAC) at this point if it is not present on the PC. Once installed, the PC must be rebooted (Windows 95/98 only).

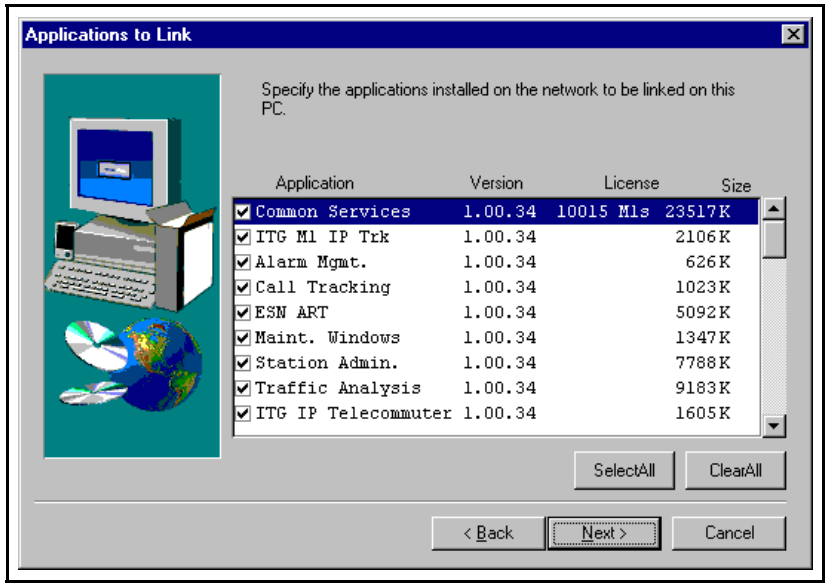
8 The Enter Keycodes dialog box appears. See Figure 19. The fields contain the data stored on the OTM Server. Click **Next** to continue.

Figure 19
Enter Keycodes dialog box



9 Select the applications to be installed if you chose to have the application executables installed on the Client PC, or select the applications to be linked if you chose to use the applications installed on the OTM Server. See Figure 20. Click **Next** to continue.

Figure 20



10 The following screens are displayed (see “OTM Server software installation” to view the screens).

a Applications to install.

b After the installation is complete you are given the option to view the Read Me file

c Reboot the PC.

OTM upgrades

This section describes the various upgrade paths for OTM software.

Upgrade the OTM Server to the same release of OTM

You can upgrade the OTM Server for the following reasons:

- to install OTM applications not previously installed
- to upgrade to another OTM package (i.e., from Basic to Premium)
- to increase the maximum number of OTM clients or the maximum number of telephones supported by OTM.

The upgrade installation is very similar to the initial installation. You need a new keycode to upgrade to another OTM package or to increase the maximum number of OTM clients and telephones.

Upgrade to new release of OTM

This upgrade is performed when installing a new release of OTM. Upgrade the OTM Server before performing client upgrades.

1 Double-click the “Setup.exe” file on the OTM CD-ROM.

2 Navigate through the OTM installation wizard. The following screens are displayed (see Server installation for examples).

3 Software Licences Agreement

4 Welcome

5 Identification

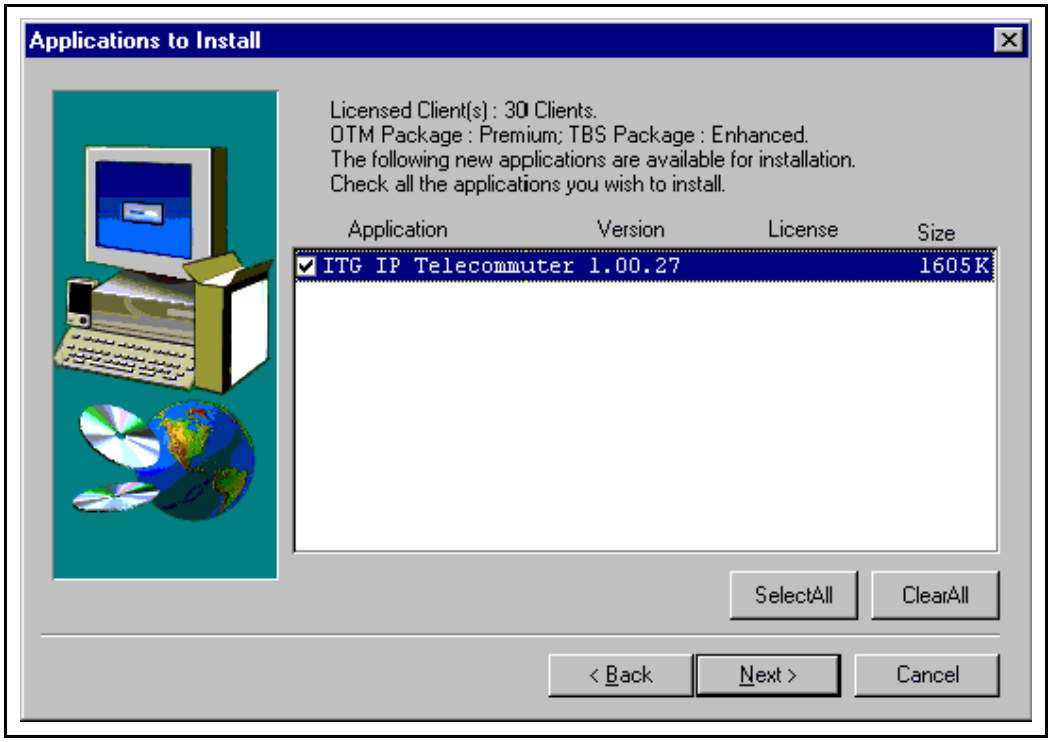
6 Setup Choices. Select “Install/Upgrade” to upgrade the OTM Server, or select “Run from Network” to upgrade an OTM Client.

7 Serial Number and keycode.

8 Destination for files.

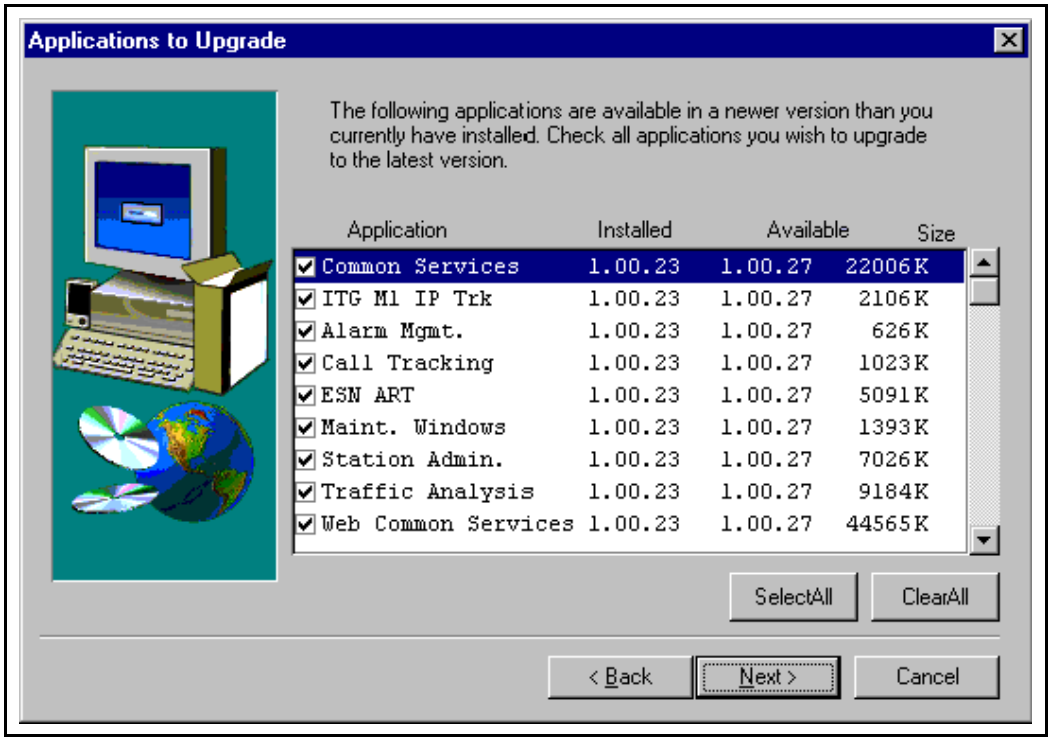
9 New applications to install. See Figure 21.

Figure 21
Applications to Install



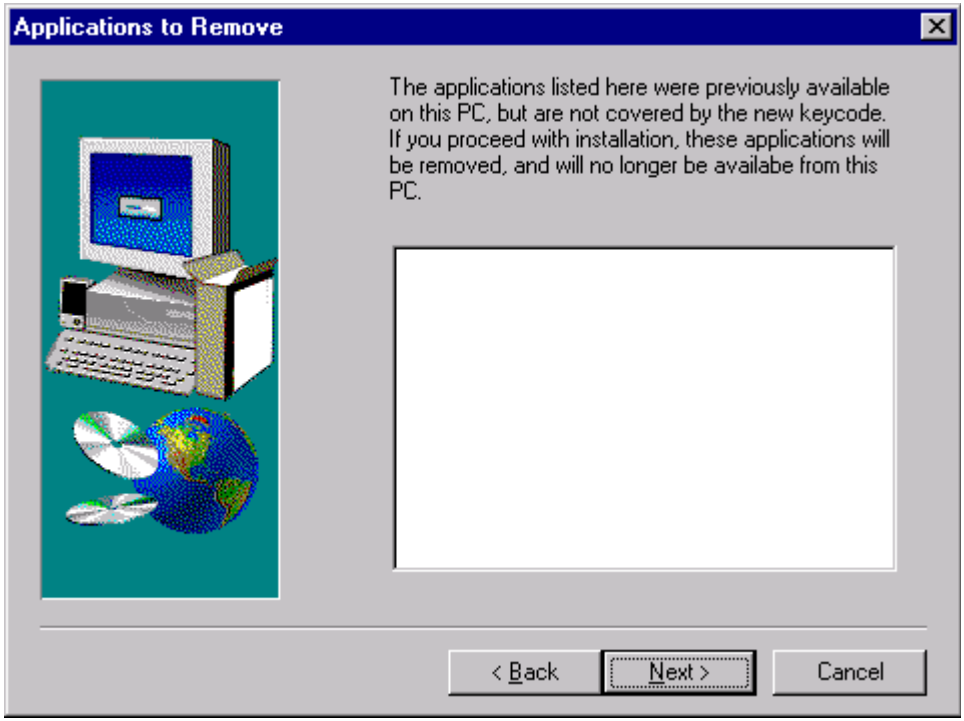
10 Applications to upgrade. See Figure 22.

Figure 22
Applications to Upgrade



11 Applications to remove. These are applications available in the old keycode, but not available in the new keycode. See Figure 23.

Figure 23
Applications to Remove



12 Copying files.

13 After the installation is complete you are given the option to view the Read Me file

14 Install JRE if required.

15 Install Web based help if required.

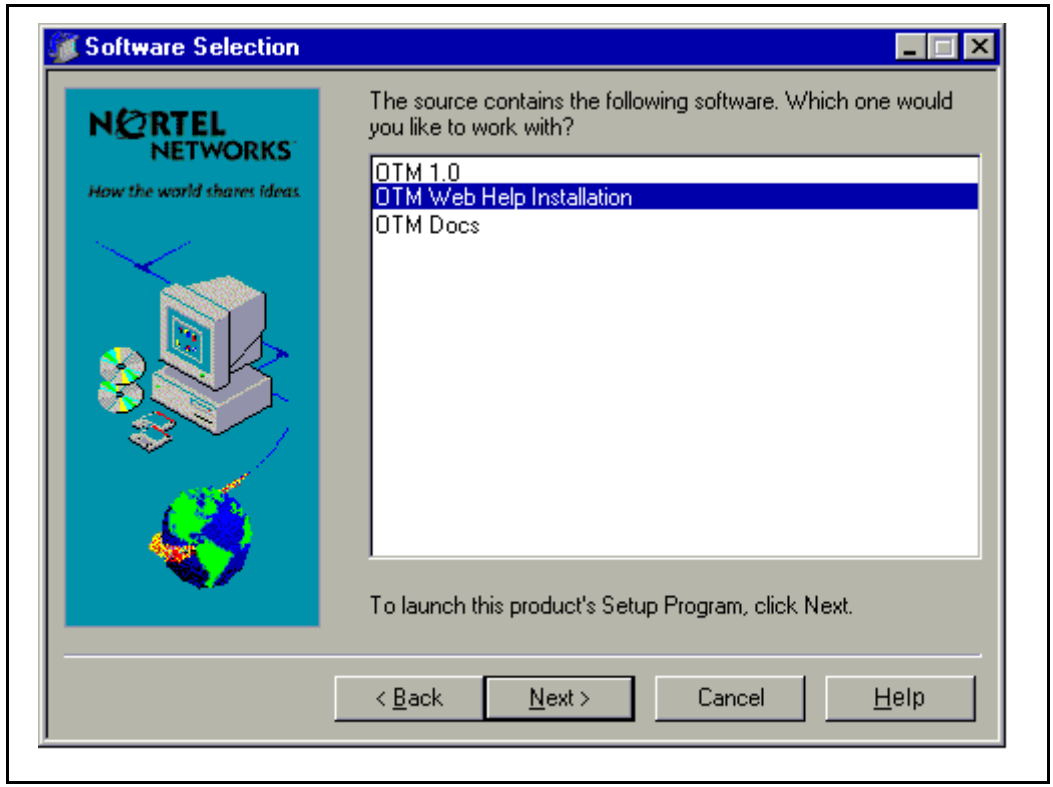
16 Reboot the PC.

Web Help and Documentation Installation

If you will be using OTM Web Services, install the Web based help files by selecting the option in the Software Selection dialog (Figure 24).

1 Double click the **Setup.exe** file and select the **OTM Web Help Installation** option.

Figure 24
Software Selection: Web Help



This will copy the OTM Web Help files to your hard drive.

To copy OTM Documentation in PDF file format, select the **OTM Docs** option. This creates the folder **C:/OTM Documents**.

You will need Adobe Acrobat Reader to read the PDF files. If you do not have Acrobat Reader installed on your PC already, an Acrobat Setup file is contained in the folder **C:/OTM Documents/32-bit**.

Migration from MAT to OTM

This upgrade is performed when upgrading from MAT 5.7.02 or later to OTM. The migration copies and converts exiting MAT data to the OTM PC. This data includes:

- MAT Site and System data
- MAT Users and Templates
- Application data (Station, ESN, etc.)

WARNING

Do NOT manually delete all the existing OTM program files when upgrading your system. If no OTM program files exist when you begin the Upgrade process, the system will attempt to migrate your data from MAT to OTM. This will cause a loss of data.

There are three scenarios:

1 Installing OTM on a Windows 95/98/NT Workstation on which MAT has been previously installed.

2 Installing OTM on a Windows NT server being used as a MAT file server.

3 Installing OTM on a clean Windows NT server and migrating the MAT data from another PC. See “Migrating data from MAT on one PC to OTM on another PC” on page 57.

Migrating data from MAT to OTM on the same PC

The migration is automatic if the setup program knows where MAT is installed (e.g., install OTM on MAT PC) . See Figure 25.

Figure 25
MAT Migration: OTM Setup dialog box

On the next reboot, run the MAT to OTM Migration tool to complete the migration process.

Note: Once the installation is complete and successful you can delete the **Nortel.MAT** directory.

Installing OTM on a Windows NT server being used as a MAT file server.

1 Back up the Common Data directory of MAT to a temporary directory

- **a** Create a new directory such as **C:\Backup**
- **b** Copy the whole Common Data directory into **C:\Backup**. The backup data path will be **C:\Backup\Common Data.**

CAUTION
To avoid loss of data, complete Step 1 first.

2 Install OTM

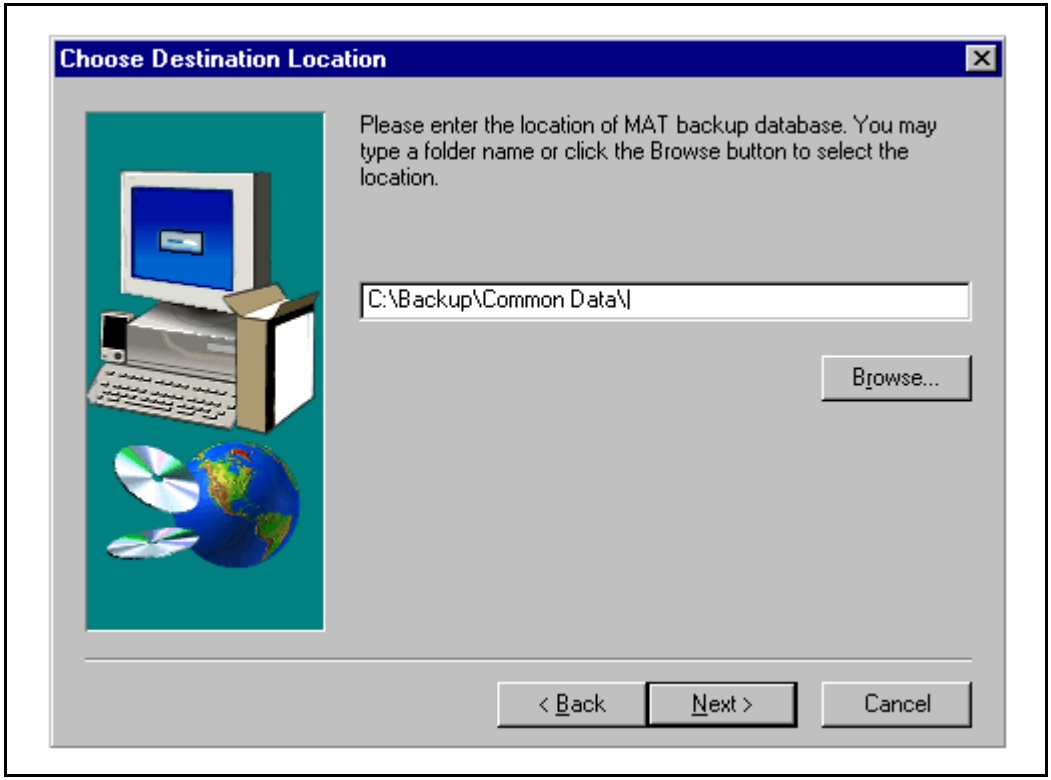
3 Restart the PC

4 In the **Start** menu, select **Program Files**, then select **Optivity Telephony Manager**, then select **Database Migration Utility**

5 Run the utility

6 When asked for the path to Common Data (to migrate), enter: **C:\Backup\Common Data** or click on the **Browse** button and locate the backup directory. See Figure 26.

Figure 26
MAT Backup Database: Choose Destination Location



7 When asked to make a selection to rebuild data, choose **Rebuild All.**

Migrating data from MAT on one PC to OTM on another PC

1. Install OTM on the new PC
2. Create a temporary directory on the OTM PC such as **C:\Backup**
3. Copy the Common Data directory on the MAT PC (typically located in: **C:\Nortel\Common Data**) to the temporary directory on the OTM PC (**C:\Backup\Common Data**)

Note: You can also copy the Common Data directory indirectly to the OTM PC by copying the Common Data Directory to a file server first

4. On the OTM PC: In the **Start** menu, select **Program Files**, then select **Optivity Telephony Manager**, then select **Database Migration Utility**
5. Run the utility
6. When asked for the path to Common Data (to migrate), enter: **C:\Backup\Common Data**
7. When asked to make a selection to rebuild data, choose **Rebuild All.**

MAT/OTM Migration

Tables 2 and 3 summarize the procedures for migrating data (from MAT to OTM). The migration procedures apply to the MAT version and OTM mode (such as Windows NT server or standalone) shown in each table.

Table 2 summarizes the migration steps to use OTM in Windows NT server mode. It also lists the MAT versions, by target directory on the Windows NT system.

Table 2
Migration for OTM Windows NT server mode

	MAT data migration for OTM Windows NT server mode:	
	Migrate data from MAT to OTM using same directory	**Migrate data from MAT to OTM using different directory**
Migration procedure on server	1. Move 'Common Data' folder to c:/backup 2. Run setup.exe on NT	1. Run setup.exe on NT 2. Run migration tool on NT
Migration procedure on client	3. Run upgrade on client	3. Run upgrade on client
MAT Version to migrate		
5.71.02	95/98/WS/server	95/98/WS/server
6.1	95/98/WS/server	95/98/WS/server
6.53.06	95/98/WS/server	95/98/WS/server
6.67.04.1	95/98/WS/server	95/98/WS/server

Table 3 summarizes the migration steps to use OTM in standalone mode.

Table 3
Migration for OTM standalone mode

	MAT data migration for OTM standalone mode:	
	Migrate data from MAT to OTM on same machine	**Migrate data from MAT to OTM on different machine**
Summary of steps	Run setup.exe	1. Run setup.exe 2. Copy 'Common Data' directory to c:/Backup 3. Run migration tool
MAT version to migrate	95	95
5.71.02	95	95
6.1	95/98/WS/server	95/98/WS/server
6.53.07	95/98/WS/server	95/98/WS/server

Uninstall OTM

Use Uninstall to remove software that is no longer needed, or that has become damaged or was incorrectly installed.

1 Use one of the following two methods to access Uninstall:

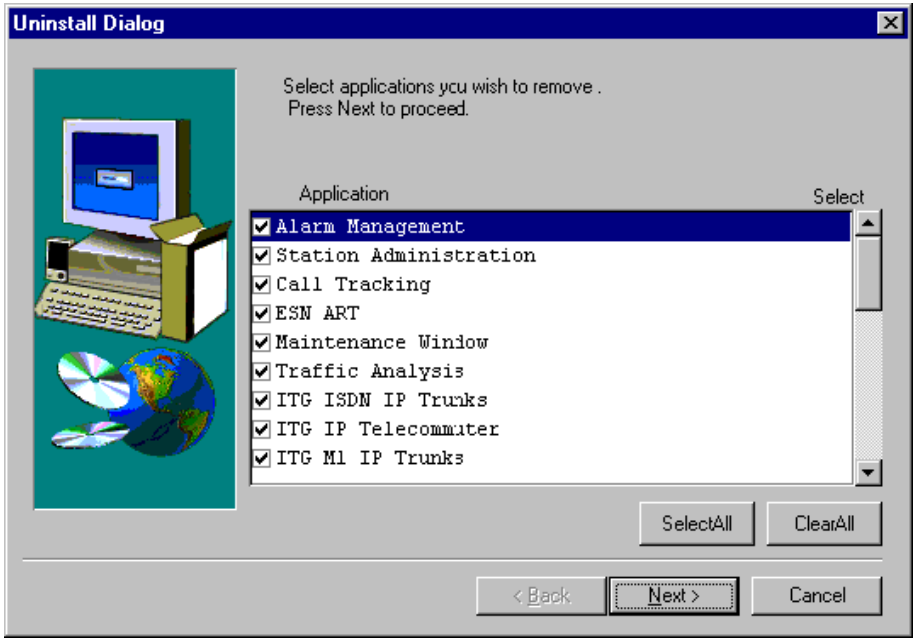
a From the **Start** menu, select **Programs**, then select **Optivity Telephony Manager**, then select **Uninstall OTM 1.0**.

or

b In the Software Installation Wizard, select **Uninstall** in the Setup Choices dialog box. See "Setup Choices" on page 31.

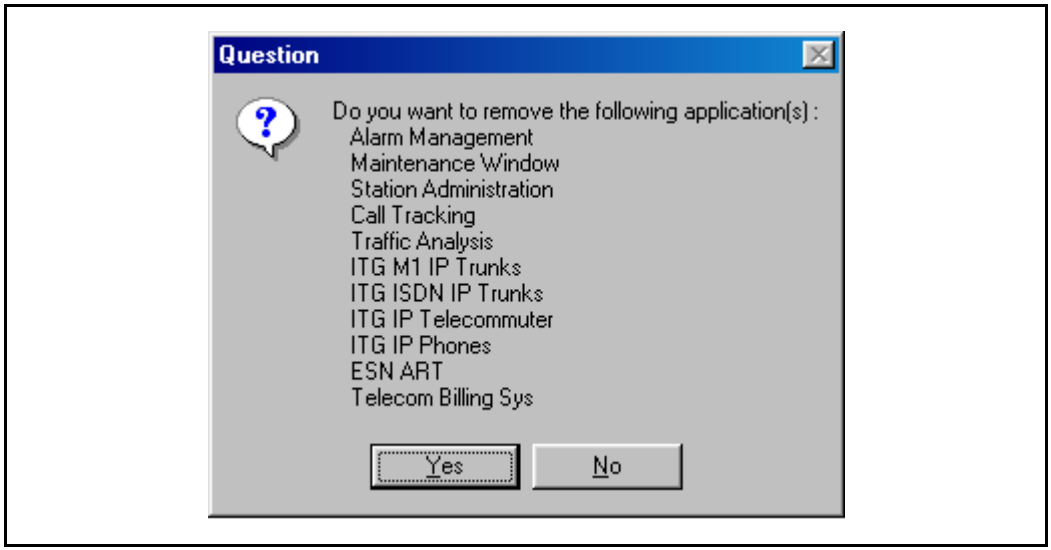
2 The Uninstall dialog box displays a list of OTM applications which are currently installed. See Figure 27. Use the check boxes to select the applications you want to remove. Click **Next** to continue the uninstall process.

Figure 27
Uninstall dialog box



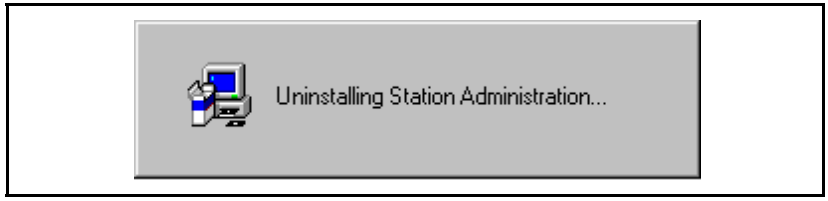
3 The dialog box shown in Figure 28 appears asking for confirmation that you want to delete the applications that you selected in the previous step. Click **Yes** to continue.

Figure 28
Uninstall Confirmation dialog box



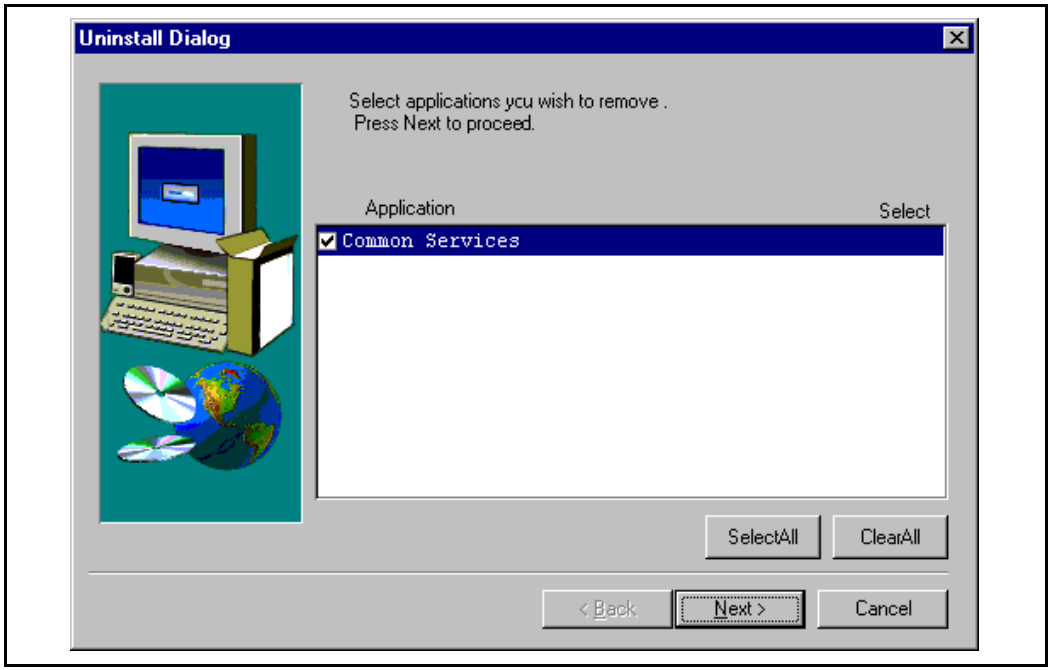
4 The status box, shown in Figure 29, provides a visual indicator of the progress of the uninstall process.

Figure 29
Uninstall status box



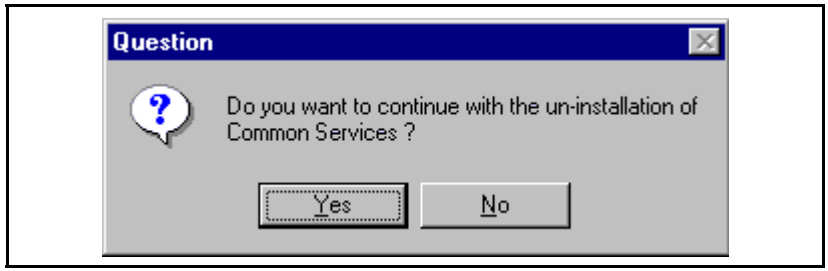
5 Common Services is always the last application to be uninstalled. After all other applications have been uninstalled, select Common Services from the Uninstall Dialog box as shown in Figure 30. Click on Next.

Figure 30
Uninstall Common Services dialog box



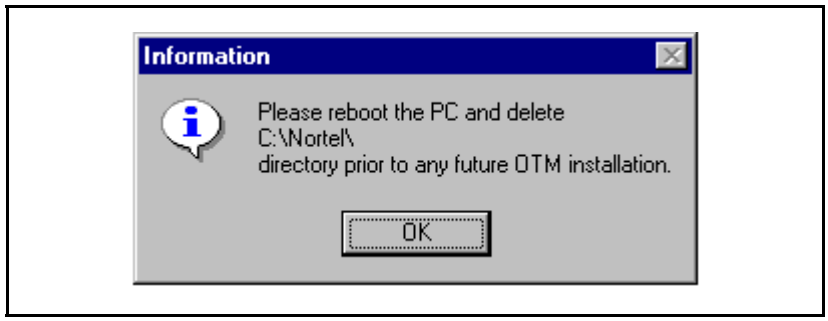
6 The dialog box shown in Figure 31 appears asking for confirmation that you want to continue with the uninstall. Click **Yes** to confirm that you want to remove Common Services.

Figure 31
Uninstall confirmation question box



7 The dialog box shown in Figure 32 appears requesting that you reboot the PC and reminding you to delete the OTM directory. Click **OK**.

Figure 32
Uninstall complete information box



8 Reboot the PC and remove the directory where the OTM software was installed.

License Management

The serial number and keycode which you received with your OTM software package determine the maximum number of terminal numbers (TNs), or telephones, and OTM Clients that can be configured in your OTM system. To purchase licensing for additional TNs or Clients, please contact your OTM vendor.

TN license

Each time you log in to OTM, your TN license is checked. If the number of TNs configured in your system is approaching the maximum for your license, the dialog box shown in Figure 33 will appear.

Figure 33
TN license warning dialog box

If your TN license has been exceeded, the error message shown in Figure 34 will appear. This message will appear every 15 minutes. Contact your vendor to obtain a license for additional TNs.

Figure 34
TN license error dialog box

Client license

When you install an OTM Client, the hostname of the OTM Client is registered on the OTM Server database. Each time a user attempts to log in to the OTM Client, the OTM software will check the OTM database. If the OTM Client is not located in the database the dialog box shown in Figure 35 will appear.

Figure 35
Client removed dialog box

This message will appear if the OTM Client machine's hostname has been changed or if the OTM Client has been removed from the OTM database.

If the hostname of an OTM Client machine is changed, the OTM Administrator can use the Client Utility to update the hostname in the OTM database. For information on the Client Utility, please refer to the *Optivity Telephony Manager Common Services User Guide* (P0910103).

Security device (dongle)

The process for checking the security device, commonly referred to as the "dongle", is different in OTM when compared to MAT. In MAT, every Client is required to have a dongle. In OTM, the dongle attached to the OTM Server allows access for all of the OTM Clients configured on the server.

When OTM is launched from an OTM Client, the OTM Server's dongle is checked. The OTM Client cannot launch the OTM System Window if the OTM Server's dongle is missing.

If the dongle has been removed from the OTM Server, it takes approximately five minutes, once it has been reattached, for the OTM Client to recognize the dongle.

Initial configuration tasks

After installing the OTM Server Software, follow the steps under “Log in and change the default password” to connect to the Meridian 1 switch and change the default OTM password.

Test the connection using the sample site and system configuration. See “Test the connection” on page 69.

After connecting successfully, refer to “Add sites and systems via the OTM Windows Navigator” on page 76 to configure your own sites and systems.

The complete list of OTM configuration procedures includes:

- “Log in and change the default password” on page 68
- “Test the connection” on page 69
- “Add sites and systems via the OTM Windows Navigator” on page 76
- “Add OTM Windows users via the OTM Windows Navigator” on page 93
- “Set Up the Virtual Terminal Service” on page 110
- “Set Up the LDAP Server” on page 117
- “Set Up Alarm Management” on page 118
- “Perform an OTM backup” on page 118

Log in and change the default password

1 Select **Optivity Telephony Manager** then **Navigator** in the Windows Programs list in the **Start** menu.

In later sessions, OTM will automatically begin as part of the Windows start-up routine.

2 Enter the default user ID and password shown below, then click **OK**.

User ID: **Admin**
Password: **Admin**

Note: For security purposes, the password does not appear as you type in the Password field.

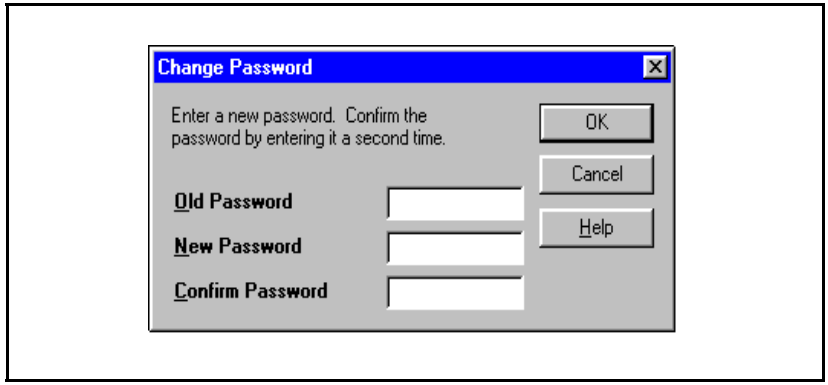
3 Click **OK**.

After OTM accepts your ID and password, the OTM Windows Navigator opens.

4 Change the default password to ensure security:

- In the Navigator window, choose **Change Password** from the **Security** menu to open the **Change Password** dialog box (see Figure 36)..

Figure 36
Change Password dialog box



— Enter the old password in the Old Password field.

— Type a new password in the New Password field.

— Retype the new password in the Confirm Password field.

— Click **OK**.

- A message box informs you that the password was successfully changed. Click **OK**.

Note: You need to use this password next time you start OTM

When exiting from OTM, the administrator will be prompted to either log out of OTM or terminate OTM. If OTM is scheduled to complete any other tasks, such as Station Administration Synchronization, ESN or Traffic, you should log out of the system but not terminate, as OTM will continue to run in the background and complete the scheduled tasks.

Test the connection

Use the following procedures to test the connection between OTM and your equipment.

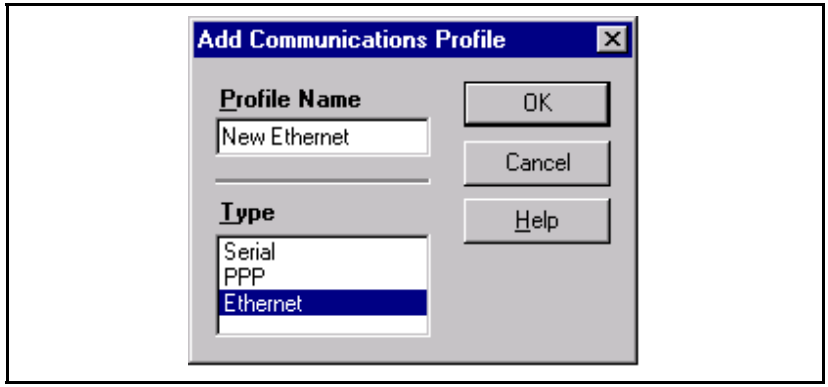
Set up communications information

1 In the Navigator window, double-click **Sample Site**.

2 Select Sample System and choose **Properties** from the **File** menu.

3 Click the **Communications** tab and click **Add**.

Figure 37
Add Communications Profile dialog box

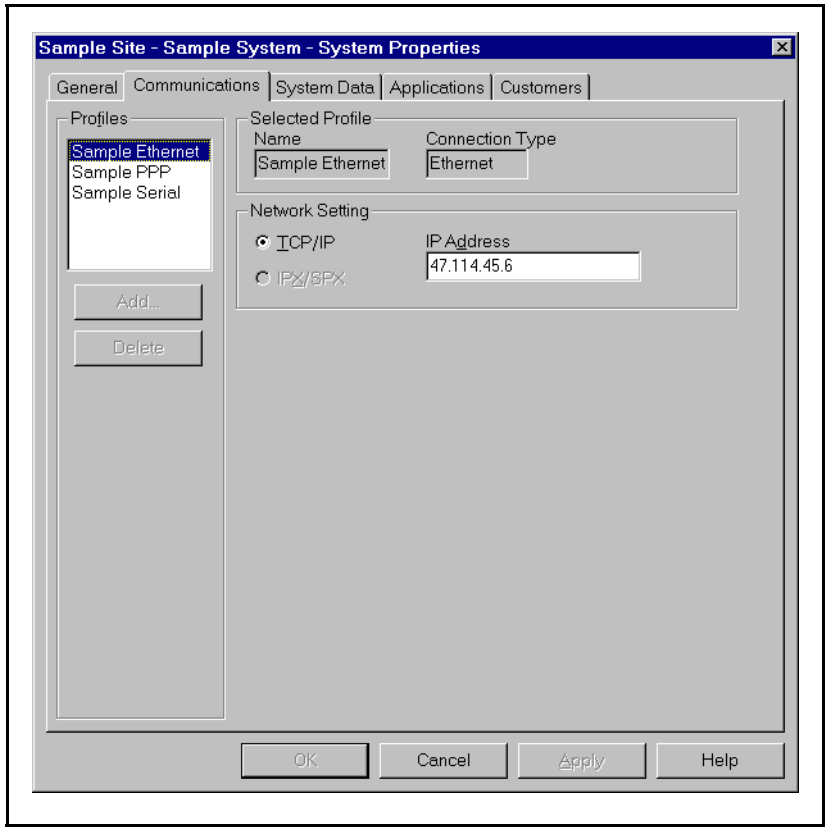


4 From the Type box, select a communications type that will be used by OTM, then enter a Profile Name and click **OK**.

5 Fill in the communications information:

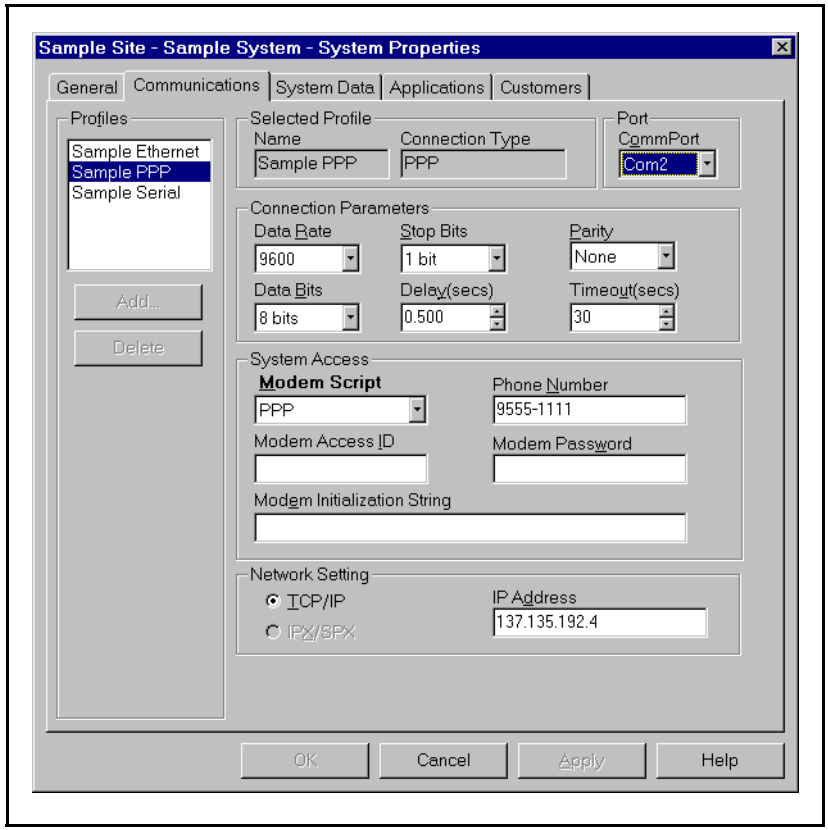
For Ethernet: Enter the IP address that you configured on the Meridian 1. Click **Apply**.

Figure 38
System property sheet, Communications tab, Ethernet profile



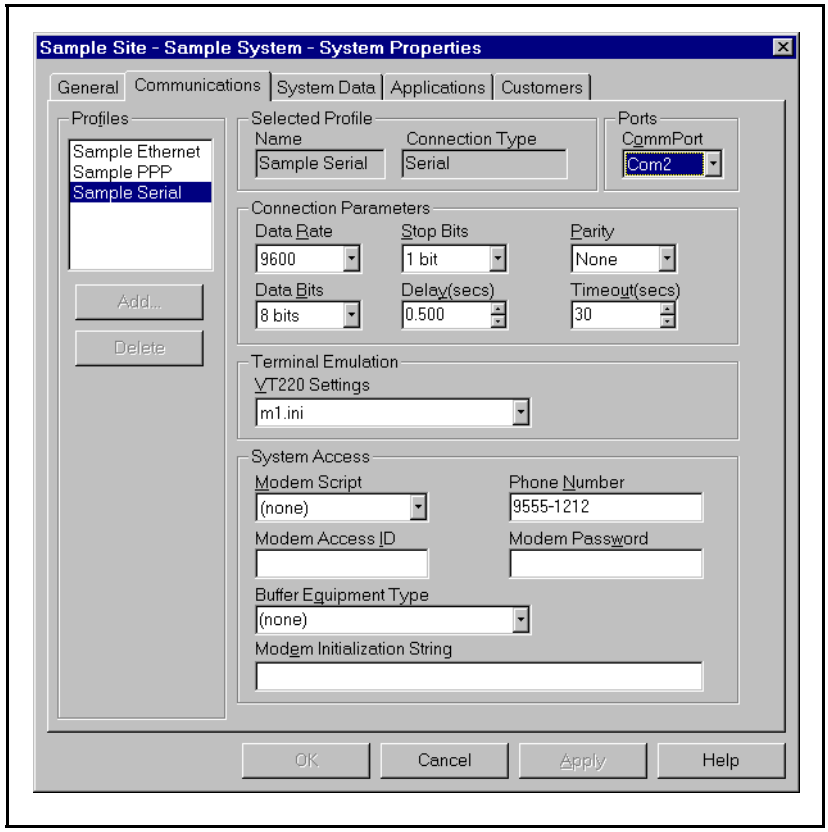
For PPP: Enter all modem parameters and dialup information. Select **PPP** in the **Modem Script** text box. Set the IP address to the local IP address, as configured on the Meridian 1. Click **Apply.**

Figure 39
System property sheet, Communications tab, PPP Profile



For Serial: Enter all modem parameters and dialup information. Select the appropriate value in the **Modem Script** text box. This will commonly be "None" unless a specific value is defined for your system. Click **Apply**.

Figure 40
System property sheet, Communications tab, Serial Profile



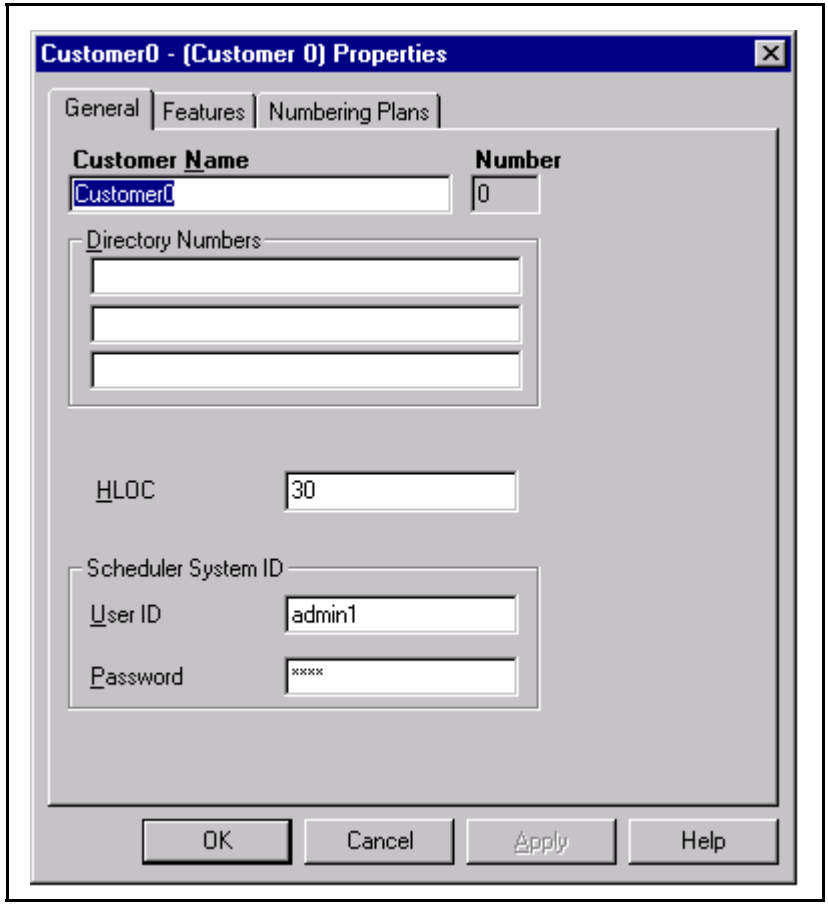
Set up customer information

1 Click the **Customers** tab and click **Properties**.

2 Click the **General** tab. In the Scheduler System ID box, change the User ID and Password to one that is valid for logging onto the Meridian 1, then click **OK**.

Note: HLOC displays the home location code (ESN) defined in LD90.

Figure 41
Customer property sheet, General tab

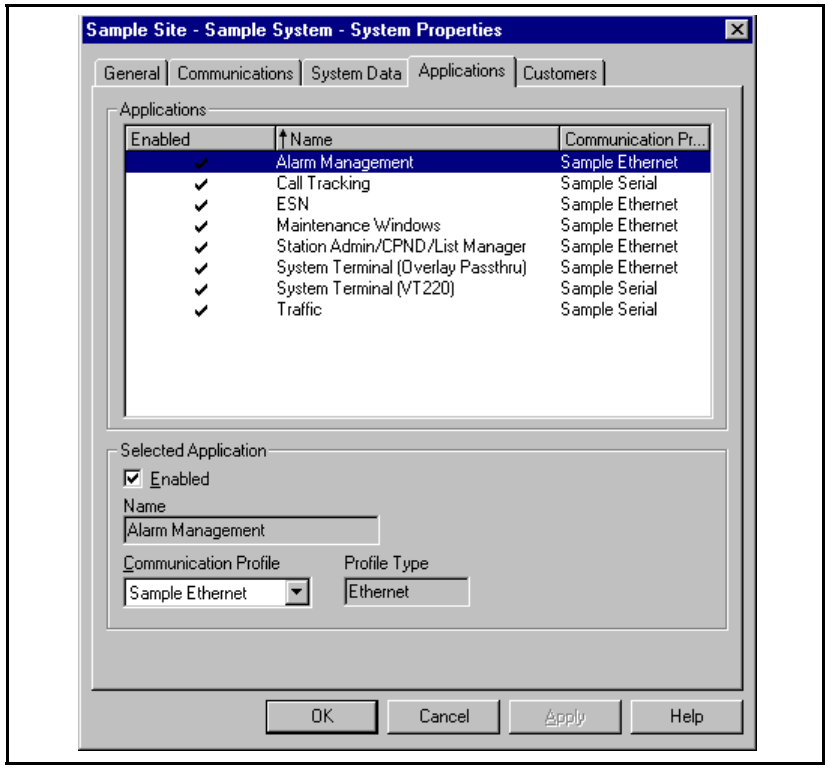


Set up OTM applications

Applications must be enabled to make them available in the System window.

1 Click the **Applications** tab.

Figure 42
System property sheet, Applications tab



2 Enable each OTM Windows application:

— Select the application.

— Select a Communications Profile from the drop-down list box.

A checkmark appears in the Enabled checkbox and next to the application name.

3 Click **OK** to close System Properties.

Set up system data

1 Double-click the **Sample System** icon to open the System window.

2 Choose **Update System Data** from the **File** menu.

3 Select the options "Update Data Stored in the PC" and "Do it Now," then click **OK**.

The system data (such as the machine type and M1 packages) is copied into OTM directly from the Meridian 1.

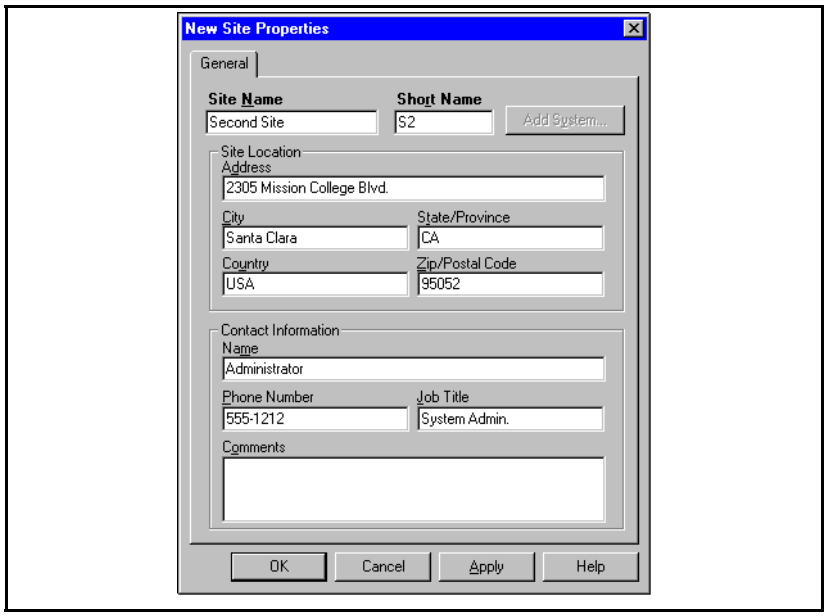
Add sites and systems via the OTM Windows Navigator

Adding a site

You can add any number of sites to the Navigator window.

1 In the Navigator window, choose **Add Site** from the **Configuration** menu. The **Site Properties** window appears (Figure 43).

Figure 43
New Site Properties sheet



2 Fill in the **Site Name** and **Short Name** fields (these are required fields).

The **Site Name** appears in the Navigator tree. The Short Name is an abbreviated site name that displays in the Alarm Banner.

3 In the **Site Location** box, fill in the site address information.

4 In the **Contact Information** box, fill in the contact name and related information. Click **Apply**.

5 To add a new system to this site:

— Click **Add System**.

— Follow the instructions for "Adding a Meridian 1 system" on page 77 or "Adding a Generic system or device" on page 91"

6 When you have finished entering Site information, click one of the following buttons to add the site to the Navigator tree:

— **OK** adds the site and closes the property sheet

— **Apply** adds the site and leaves the property sheet open allowing you to add another system to this site (you may repeat step 5 to add another system)

— **Cancel** closes the dialog box without adding the site.

Adding a Meridian 1 system

You can add as many systems (including non-Meridian 1 systems) to a site as your license permits. You must have administrator privileges to add a system.

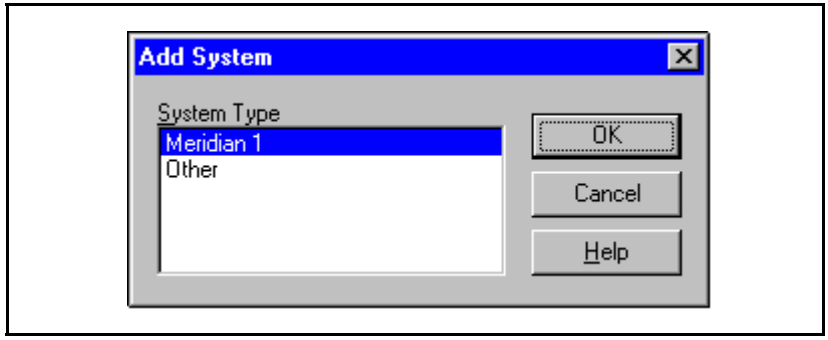
1 In the Navigator window, select the desired site.

Note: If you are adding a new system from within the New Site Properties window, skip to step 3 in this procedure.

2 Choose **Add System** from the **Configuration** menu or the right mouse button pop-up menu.

3 In the Add System dialog box, select the type of system you want to add. Then click **OK**.

Figure 44
Add System dialog box



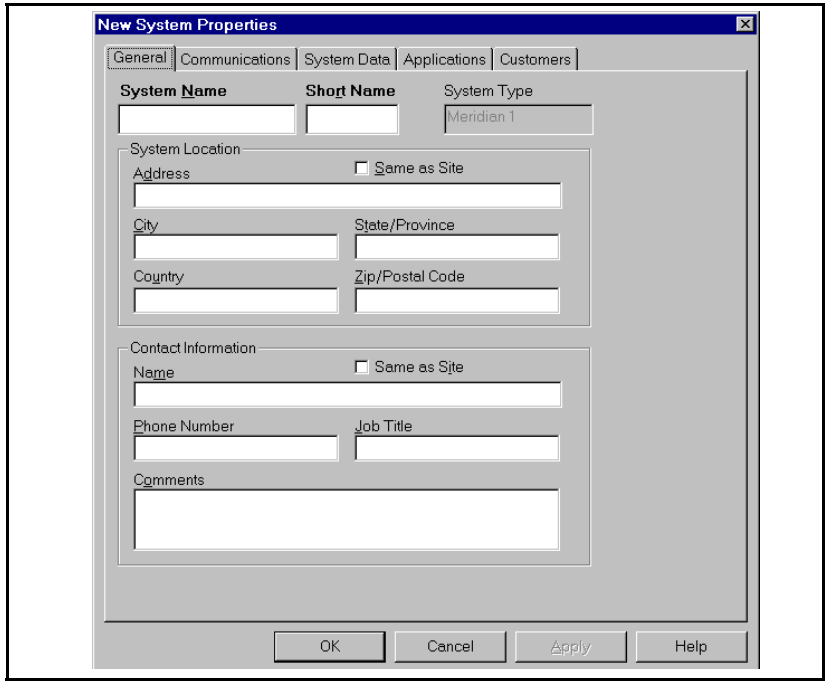
Note: You may need to install additional software to enable other system types not listed here. Follow the installation instructions included with your order.

4 Click the **System Properties—General tab** (Figure 45) enter the System Name and **Short Name** (required fields) and other information as needed. Click **Apply**.

You can make system location and contact information the same as site information by clicking the **Same as Site** checkbox.

Note: Bolded fields indicate required information. To change a value, edit the field. Some fields may have a list of predefined choices. An arrow within a field indicates a drop-down list of choices. Press the arrow to select from the list. For more detailed information, refer to the online help.

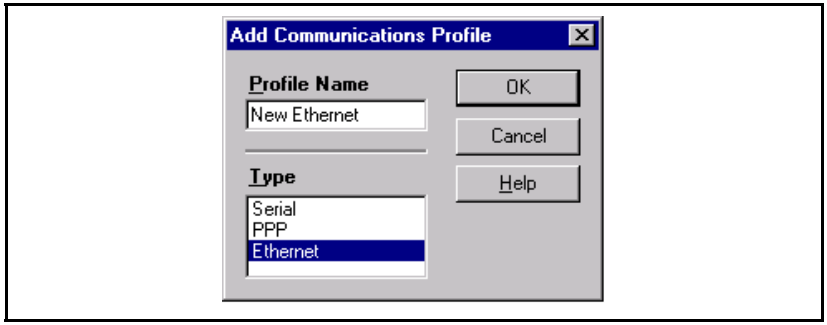
Figure 45
System Properties—General tab



5 To add a new communications profile, use the **System Properties—Communications** tab. This tab defines the types of communications profiles that may be applied to system applications (one profile may be used for multiple applications).

Click **Add**. The "Add Communications Profile" dialog box appears. See Figure 46.

Figure 46
Add Communications Profile dialog box

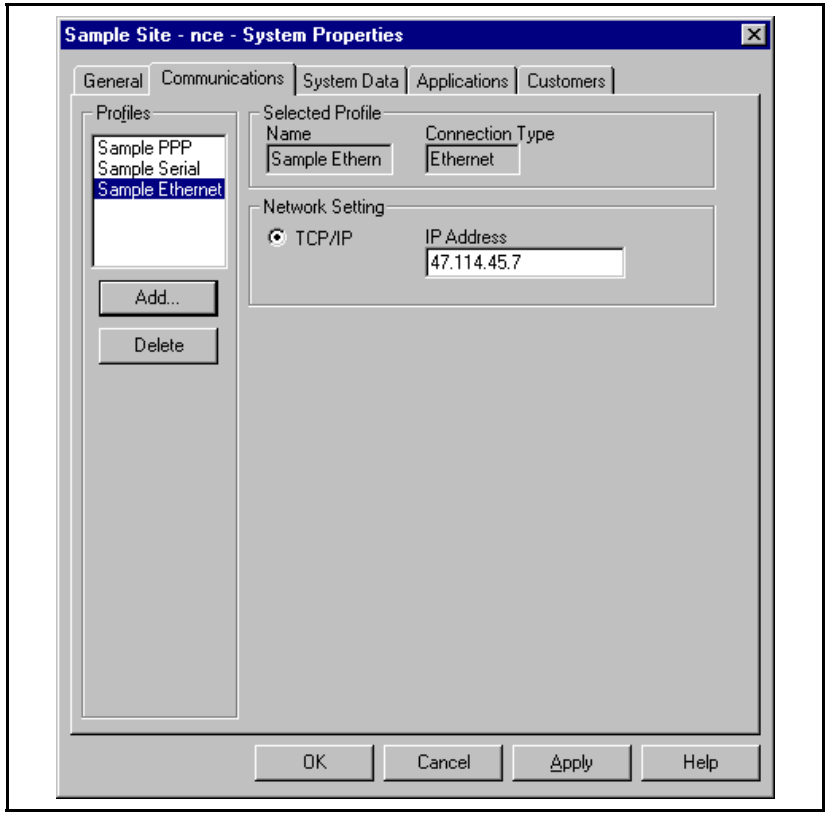


Select a communications type from the "Type" box and enter a Profile Name, then click **OK** to go back to the "Communications" tab. See Figure 47.

6 Fill in the communications information for the new profile:

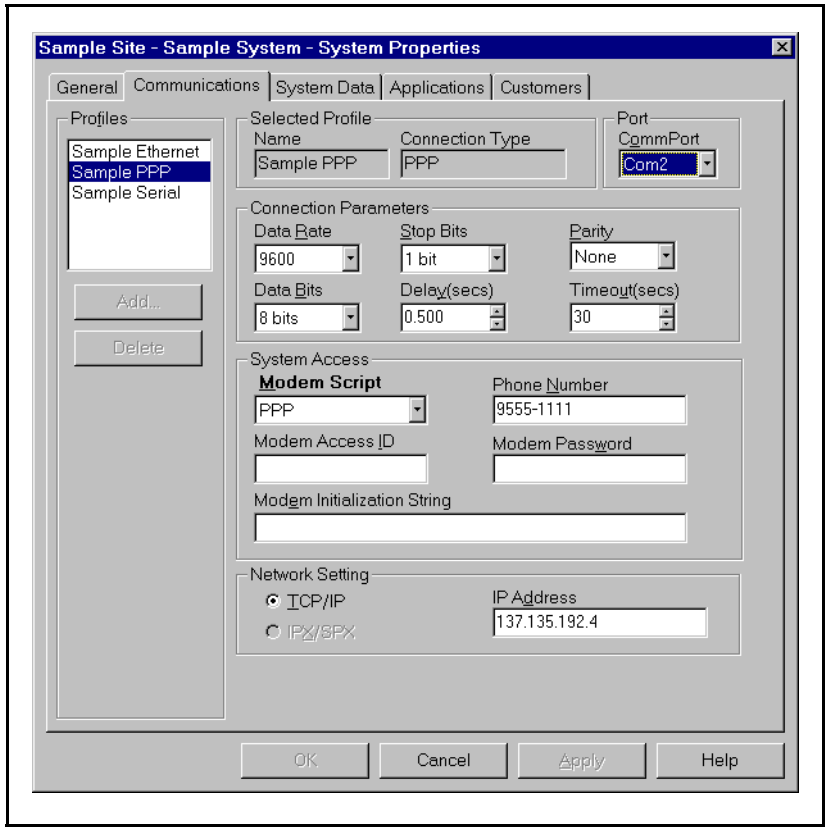
For Ethernet: Enter the IP address that you configured on the Meridian 1. Click **Apply**.

Figure 47
System Properties—Communications tab—Ethernet Profile



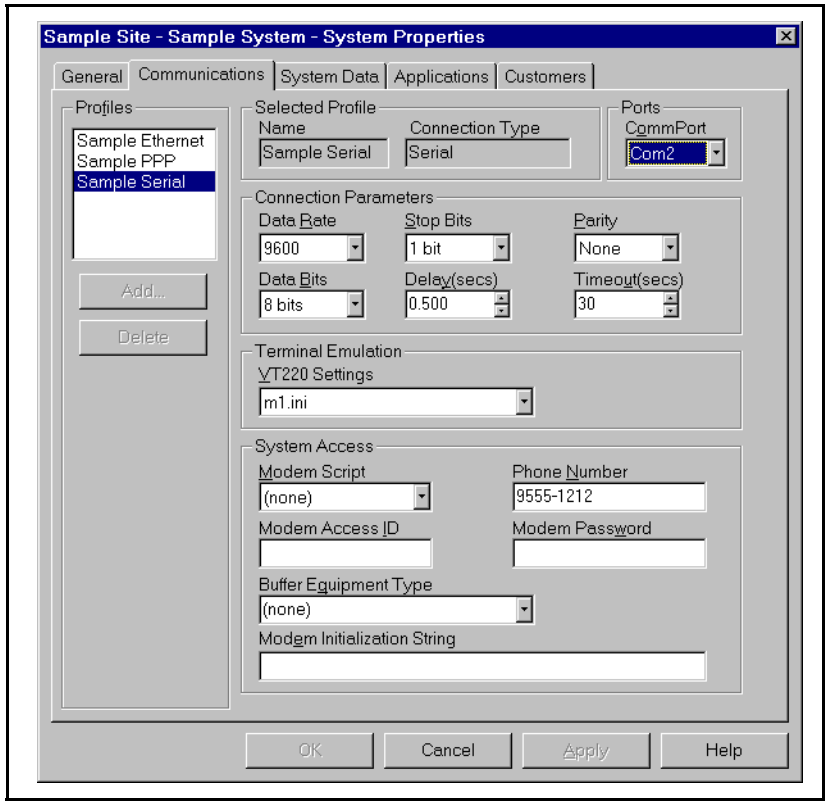
For PPP: Enter all modem parameters and dialup information. Select PPP in the Modem Script text box. Set the IP address to the local IP address, as configured on the Meridian 1. Click **Apply**.

Figure 48
System Properties—Communications tab—PPP Profile



For Serial: Enter all modem parameters and dialup information. Select the appropriate value in the Modem Script text box. This will usually be "None" unless a specific value is defined for your system. Click **Apply**.

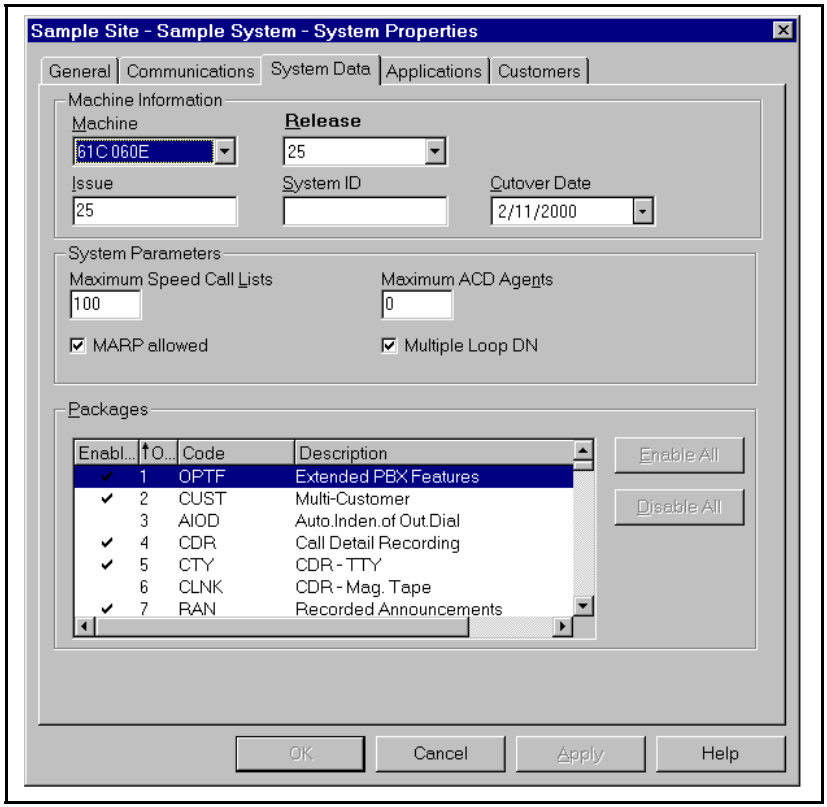
Figure 49
System Properties—Communications tab—Serial Profile



7 Click the **System Properties—System Data** tab (Figure 50). Enter the machine/system type and release version for the system and enable or disable M1 packages. For example, if your Meridian 1 is an Option 61C running X11 Release 22 software, enter **61C** in the Machine field and use the drop down box to select **22** in the Release field.

Note: You can copy this data directly from an installed switch by scheduling an upload with the **File** menu **Update System Data** command in the System window. **Update System Data** uses the communication profile for Station Administration. However, configure the Release number here first to allow available applications to show up properly in the Applications Tab.

Figure 50
System Properties—System Data tab



8 Click the **System Properties— Applications** tab (Figure 51).

This tab defines the OTM applications that will appear in the System window and the communications profile to be used with each application. *You must enable an application for it to be available in the System window.*

To enable an application:

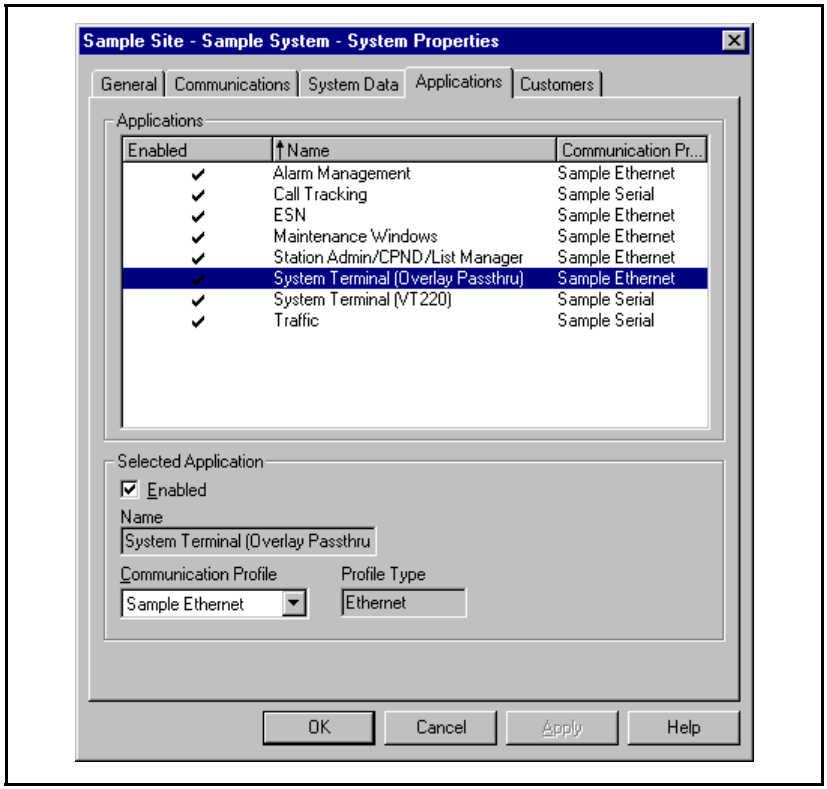
- Select the application in the Applications box.
- Select a Communications Profile from the drop-down list in the Selected Application box.

A checkmark appears next to the application and the Enabled box is also checked.

To disable an application:

- Select the application in the Applications box.
- In the Selected Application box, click the **Enabled** checkbox to remove the checkmark.

Figure 51
System Properties—Applications tab

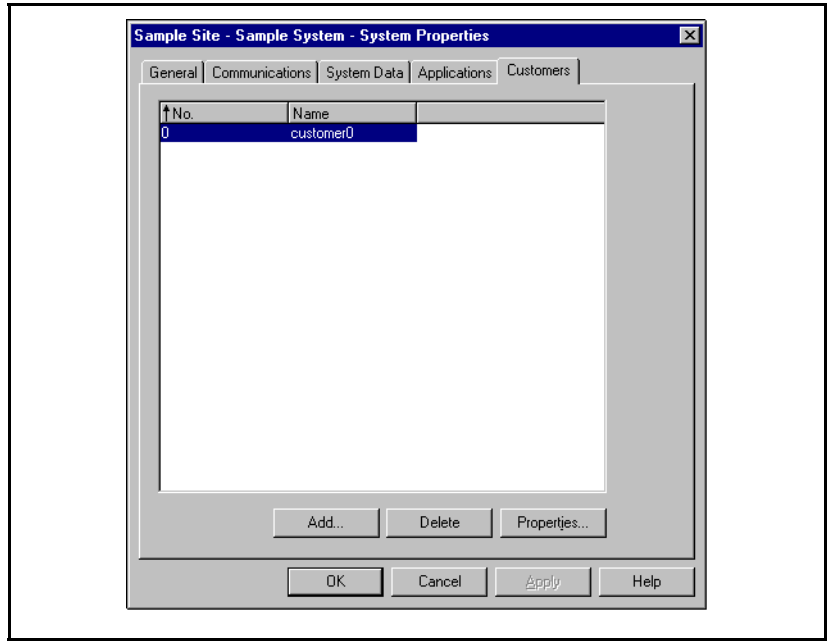


9 Click the **System Properties—Customers** tab (Figure 52).

This tab lists the customers currently defined for this Meridian 1 system. You may add new customers, delete customers, or review the properties of a selected customer. When you add a new customer, you configure the Meridian 1 features and numbering plans that are available to the customer. This information it is not automatically updated on the Meridian 1 and must be updated by using LD15 customer data block.

Note: Customer information is required for System Administration/CPND and ESN applications.

Figure 52
System Properties—Customers tab



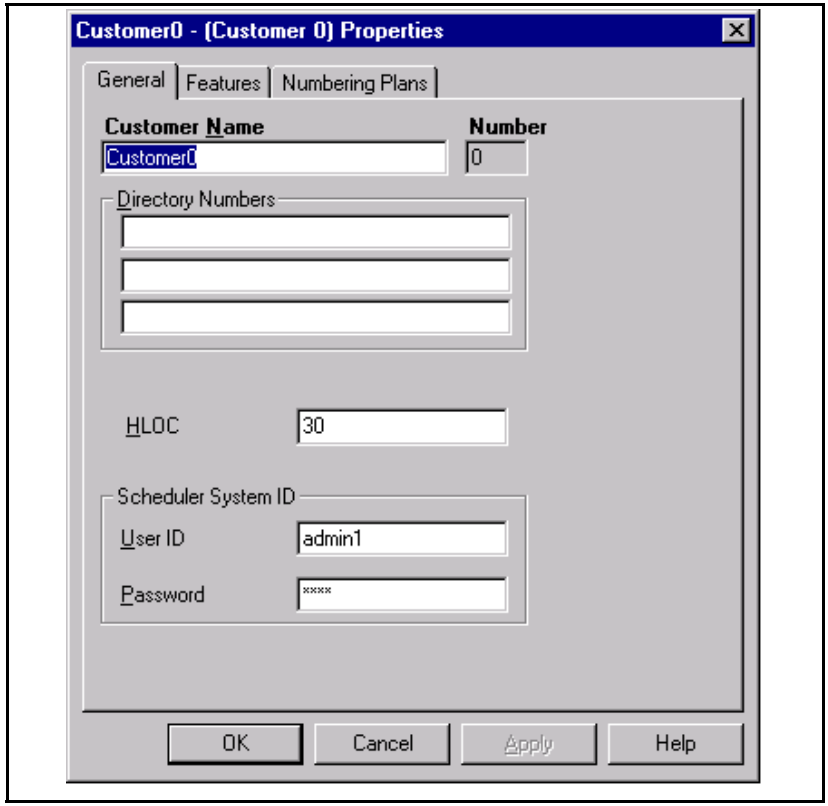
10 To add a customer:

- Click **Add** in the System Properties—Customers tab.
- Select a Customer number. Click **OK**.
- Select the **General** tab, in the Customer Property sheet (Figure 53) and fill in the customer information.

Note 1: HLOC displays the home location code defined in LD 90.

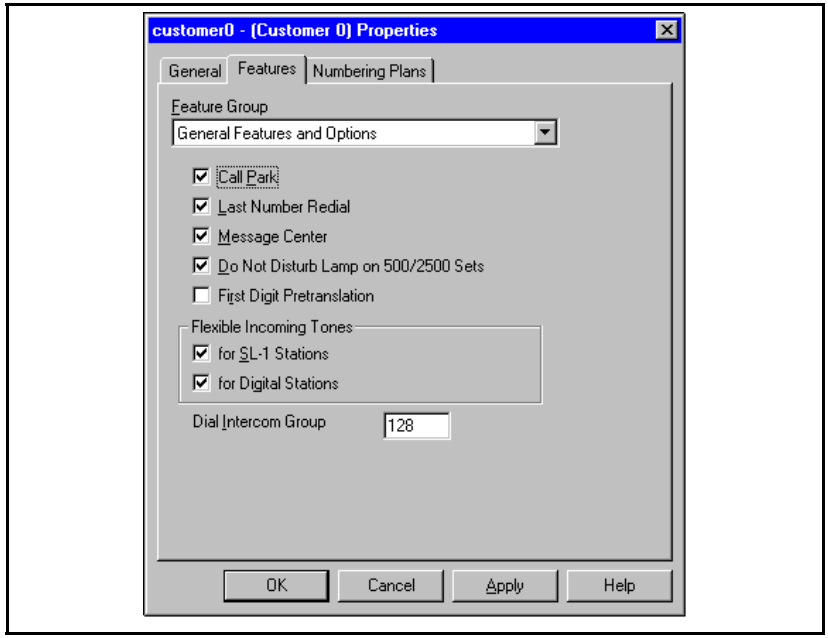
Note 2: Enter User information in the **Scheduler System ID** text box if you are using applications with scheduled activities, such as Station Administration/CPND, ESN, and Traffic.

Figure 53
Customer property sheet, General tab



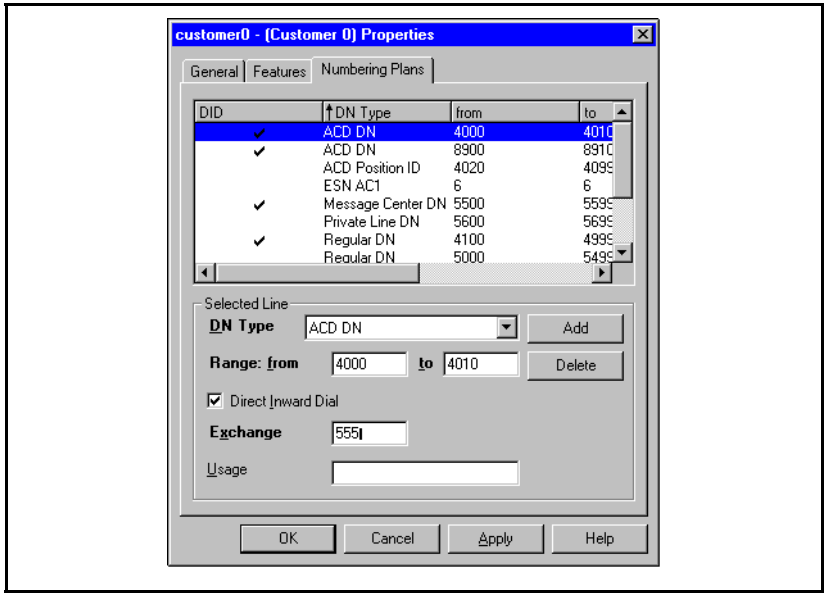
- Select the **Features** tab (Figure 54), and fill in the customer information.

Figure 54
Customer property sheet, Features tab



- Select the **Numbering Plans** tab (Figure 55), and fill in the customer information.

Figure 55
Customer property sheet, Numbering Plans tab



- When you have finished entering customer information, click one of the following buttons to save the information:
  - **OK** adds the customer and return to the System properties sheet.
  - **Apply** adds the customer and leaves the Customer properties open so that you may add other information for this customer.
  - **Cancel** closes the dialog box without adding the customer.

11 To delete a customer, click **Delete** in the System Properties—Customers tab. A delete confirmation box opens. Click **OK**.

12 To modify customer information, click **Properties** in the System Properties—Customers tab. The Customer property sheet opens. Modify information in the appropriate tabs and click **OK**.

13 In the System properties sheet, click one of the following buttons:

- **Apply** adds the system and leaves the dialog box open.
- **OK** adds the system and closes the dialog box.
- **Cancel** closes the dialog box without adding the system.
- **Help** provides online help.

Adding a Generic system or device

You can add as many systems (including non-Meridian 1 systems) to a site as your license permits. You must have administrator privileges to add a system.

1 In the Navigator window, select the desired site.

2 For non-Meridian 1 devices, configure a "Generic System."

3 Complete the General and Communications tabs as you would for a Meridian 1.

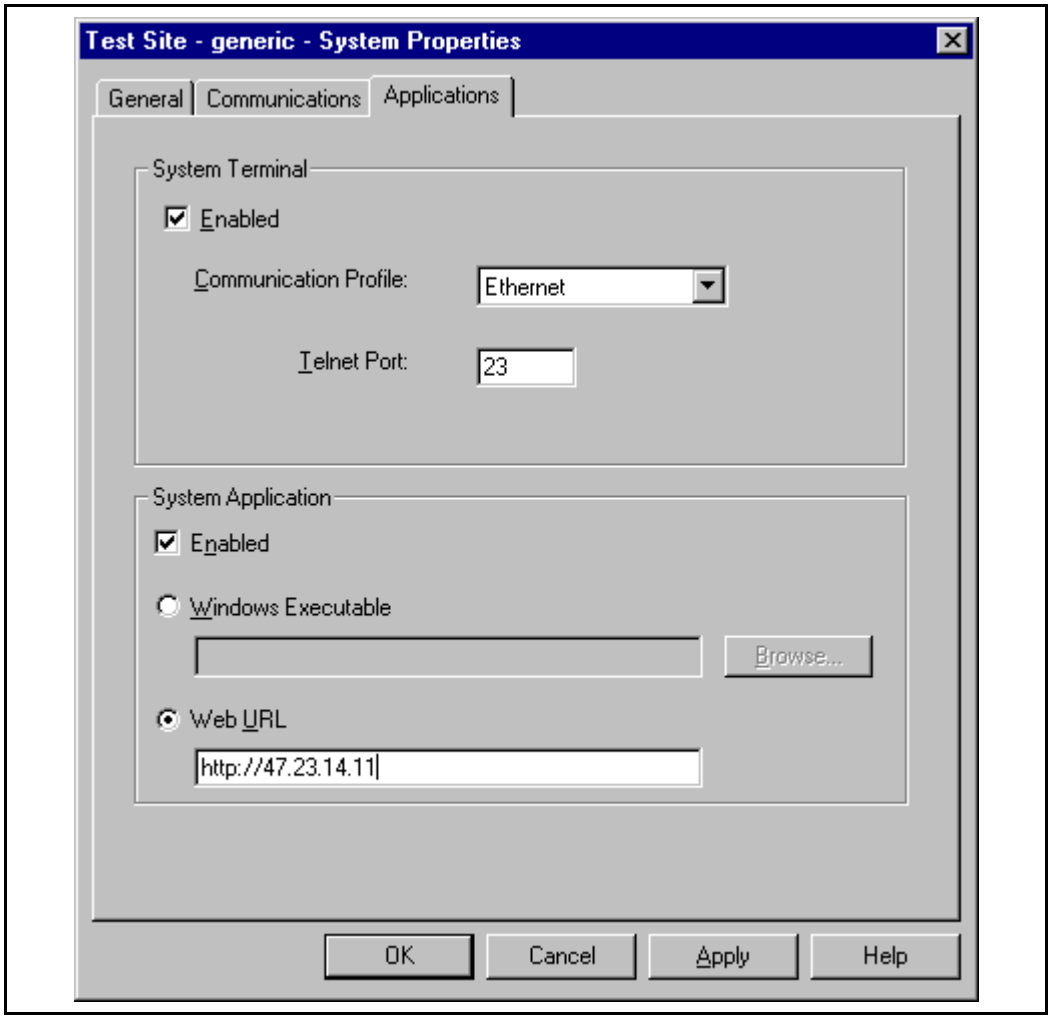
4 On the Application tab define the applications available for the device as follows:

- In System Terminal section, select the communications profile. Typically, this will be an Ethernet profile. Once defined, the user can double click on the system in the Windows Navigator to launch the Windows System Terminal, and/or open a web based terminal window from the OTM Web Navigator Systems page.
- In the System Application section you have the option of launching a Windows executable or Web browser page for managing the device.

If a Windows executable is selected, it can only be accessed from the Windows Navigator. If a URL selected, the web site can be accessed from either the Windows or Web Navigators.

The availability of an terminal connection, executable and/or web site depends on the device.

Figure 56
Configure non-Meridian 1 devices



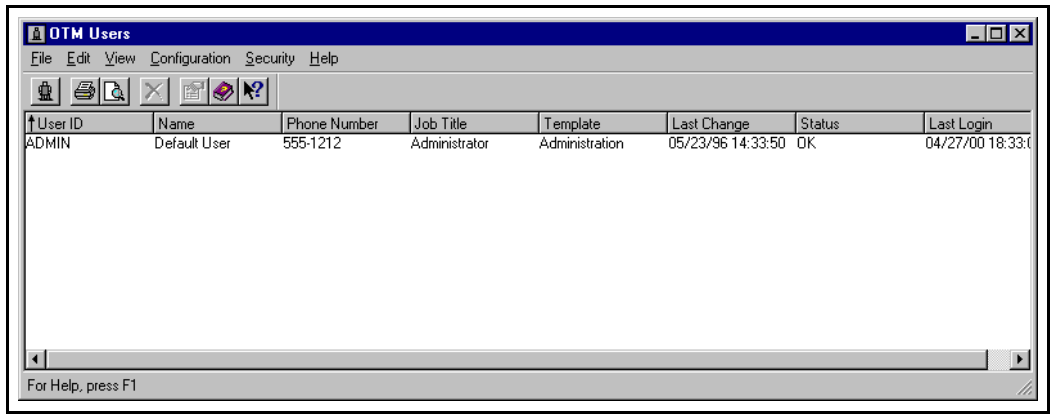
Add OTM Windows users via the OTM Windows Navigator

OTM allows you to create User Templates to speed the process of adding users. A template is a form that you fill in to define most aspects of a certain kind of user, such as their level of access to sites and systems and automatic connection to particular systems. You can create as many user templates as you need. You will assign a template to individual users when you add users to the OTM database.

Create a user template

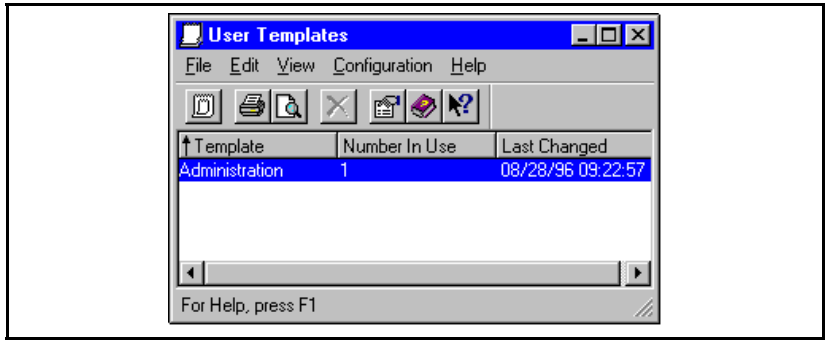
1 In the Navigator window, choose **OTM Users** from the **Security** menu to display the OTM Users window (Figure 57).

Figure 57
OTM Users window



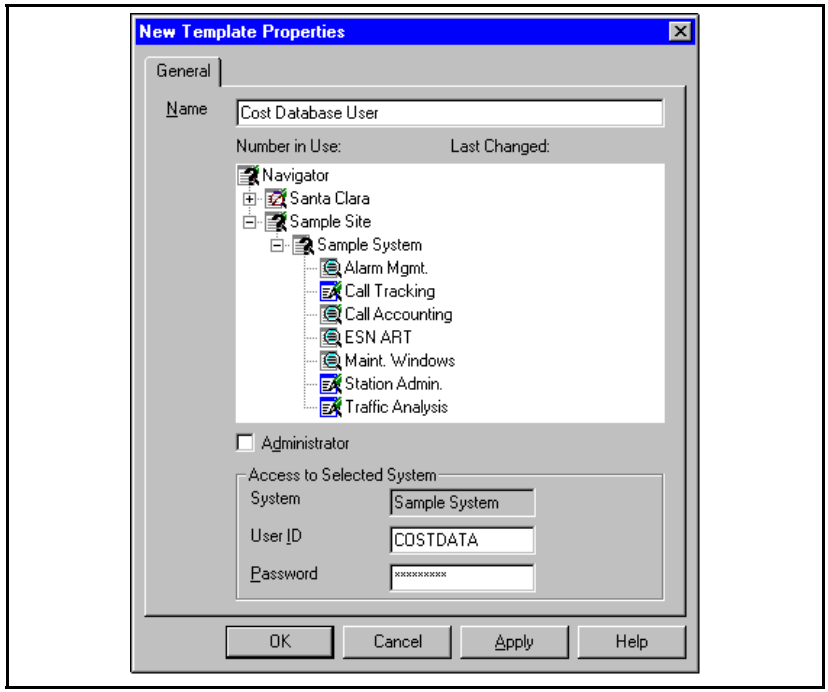
2 Choose **User Templates** from the **Configuration** menu. The User Templates window appears (Figure 58).

Figure 58
User Templates Window



3 Choose **Add Template** from the **Configuration** menu. The New Template property sheet appears (Figure 59).

Figure 59
New Template property sheet



4 Enter a name for this class of user.

For each site, system, and application in the tree, use the right mouse button popup menu to assign user privileges (**Read-write**, **Read-only**, **or No Access**). Select the **Administrator** box, if appropriate. The site and system icons change to reflect the access level.

Note: Access privileges defined for sites or systems at higher levels in the tree structure are applied to all subordinate items.

5 Enter values in the User ID and Password text boxes to allow this class of user to connect to this system without having to enter a User ID and Password each time you want to connect.

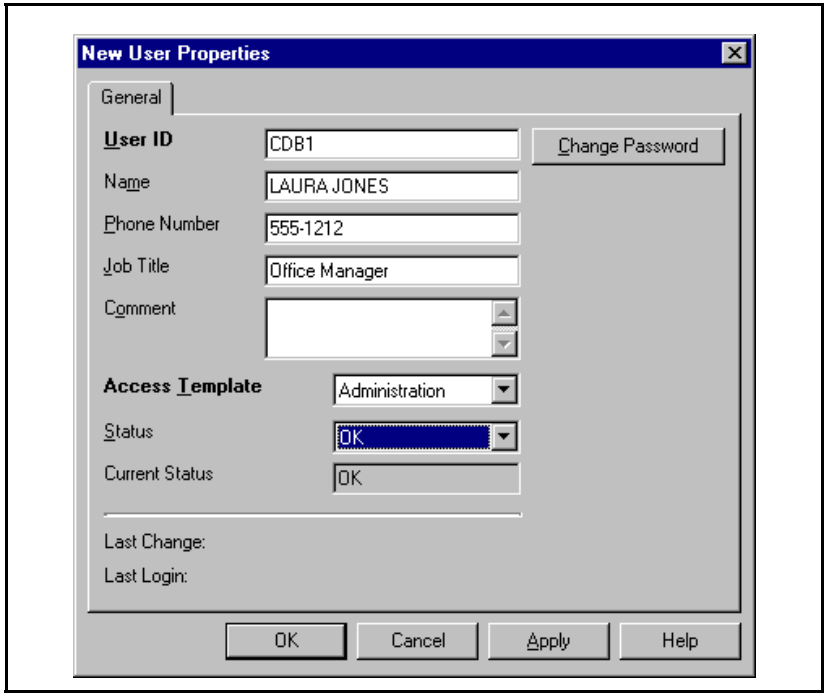
6 Click **OK**. Close the User Template window.

Adding a user

1 In the OTM Users window, choose **Add User** from the **Configuration** menu.

The New User property sheet appears (Figure 60).

Figure 60
New User property sheet



2 Enter a **User ID**, and from **the Access Template** drop-down list, select the template that you will use as the basis for this user definition.

3 Fill in other data as required. The window prompts you to enter a password and confirm it after clicking **OK** or **Apply**.

4 Click the **Change Password** button to change the OTM login password for this user only.

5 Click **OK**. The new user appears in the OTM User window. Close the OTM User window.

Refer to the *Optivity Telephony Manager Common Services User Guide* for detailed information.

Adding web users

There are two types of web users:

- Web Navigator users
- Desktop Users

Web Navigator users

The OTM Web Navigator allows users to access Maintenance Pages for performing maintenance operations on Meridian 1 hardware. They can also view alarms and events from multiple systems and devices using the Alarm browser. Web Navigator users can use the web interface to locate Meridian telephones and view configuration data.

Web Navigator Users users are authenticated via Windows NT user accounts.

1 Create Windows NT user groups on the OTM Server.

2 Assign individual users to the user groups.

3 Go to the Web Navigator Access page in the OTM Web Navigator and set access privileges for each group.

Note: These privileges determine which Web Navigator pages are visible to user in the selected group. For example, Meridian 1 technicians will typically only have access to the Equipment and Telephones pages.

Desktop Services Users

Desktop Services provides end-users with web pages that display the configuration of the user's telephone as well as information on features and telephone troubleshooting. Desktop Services users are authenticated via Windows NT or LDAP Directory Server user accounts.

1 Go to the Desktop User Access page in the OTM Web Navigator and set the user authentication method.

a For Windows NT enter the domain name. Typically, this will be an existing domain in the customer's network. If you leave this blank, it defaults to the local OTM domain.

b For LDAP select the field used for the login name.

2 Go to the Desktop User Groups page in the OTM Web Navigator and set restrictions for each features to Read Only or Hidden for EndUser and Administrator. This determines which features are visible on the Features tab in the Desktop Services.

3 Go to the OTM Directory and fill in the Desktop User Group and Login Name fields for the users you wish to have access to Desktop Services.

Note 1: For Desktop User Groups, you can use the Directory Global Change page in the OTM Web Navigator to simplify this process. See "Web Services" in the *Optivity Telephony Manager Common Services User Guide* (P0910103).

Note 2: If you have access to the Login Names in another database, consider using the Import/Export utility in the OTM System Window to simply this process.

Set Up Meridian 1

1 Verify that the Meridian 1 system has the following system configuration:

- The appropriate X11 release, configured with the appropriate packages.
- 48MB or greater of memory on the Meridian 1
- For Ethernet communications and Release 22 or Release 23:

— IOP cards (Part number NT6D63BA or later), IOP/CMDU cards (Part number NT5D20BA or later)—not applicable to Option 11C systems, Release 22, or IODU/C cards (Part number NT5D61AB or later)

— One or two Ethernet AUI cables (Part number NT7D90DA or later). You will attach one cable to each IOP, IOP/CMDU, or IODU/C.

— For Option 11C, an NTDK27AA Ethernet cable

2 **For Ethernet networks**, you will need the following:

- One or two Ethernet transceivers (different types for 10BaseT and 10Base2 cabling)—attach one transceiver to each AUI cable

  — Ethernet communications cable: 10BaseT cabling requires Category 5 cable with RJ45 connectors

  Note: Although normal phone cable and Category 5 cable are similar in appearance, phone cable is not acceptable for network applications.

  — 10Base2 cabling requires RG58 cable with BNC connectors.

  Note: Although normal television video coaxial cable and RG58 cable are similar in appearance, video coaxial cable is not acceptable for network applications.

- If you are using the 10BaseT interface, an Ethernet hub is required.

CAUTION

If you plan to connect the Meridian 1 switch to a corporate network, an Ethernet gateway or router is required to separate the Meridian 1 from the corporate network. Connecting the Meridian 1 without a gateway or router will adversely affect the Meridian 1 system's call handling ability.

3 **For PPP networks**, you will need the following:

- Hayes command compatible modem
- modem cables
- M1 SDI ports will require user type MTC and SCH be set in LD17

4 **For serial communications**, you will need the following:

- Hayes command compatible modem only for remote dial-up
- Modem cables
- Direct serial cable connection between the PC and the SDI port on the switch
- M1 SDI ports will require the appropriate user type be set in LD17 for each OTM application (see Table 4)

Table 4
SDI Port settings for OTM applications

OTM Application	SDI Port Setting
Station Administration	SCH
ESN	SCH
Telecom Billing System	CTY
Traffic Analysis	TRF if information is output to a buffer box SCH if information is collected hourly from the Meridian 1 switch

5 Configure OTM users on the Meridian 1:

User input is shown in bold following the ">" prompt. For example, > **LD 17**.

- Install the appropriate release (minimum is Release 22) of X11 software.
- Perform an INIT.

  Note: The OTM application will not function properly if an INIT has not been performed.

- Configure LAPW. OTM communicates with the Meridian 1 through LAPW IDs and passwords configured on the Meridian 1.

>**logi (ID) (enter the login ID)**

Note: When a Limited Access Password (LAPW) is defined to collect traffic data from Overlay 2, configure the password to have access to all customers by setting the CUST prompt to ALL. For more information about Limited Access to Overlays, see the X11 Software Features Guide.

PASS?> **(enter the level 1 or level 2 password)**

```
WARNING: THE PROGRAMS AND DATA STORED ON THIS
SYSTEM ARE LICENSED TO OR ARE THE PROPERTY OF
NT/BNR AND ARE LAWFULLY AVAILABLE ONLY TO
AUTHORIZED USERS FOR APPROVED PURPOSES.
UNAUTHORIZED ACCESS TO ANY PROGRAM OR DATA ON
SYSTEM IS NOT PERMITTED. THIS SYSTEM MAY BE
MONITORED AT ANY TIME FOR OPERATIONAL REASONS.
THEREFORE, IF YOU ARE NOT AN AUTHORIZED USER, DO
NOT ATTEMPT TO LOGIN.

TTY #00 LOGGED IN 15:02   9/7/1996
```

Note: The following section is only required if login names are not configured.

>**ld 17**
CFN000
MEM AVAIL: (U/P): 3352174 USED: 203153 TOT: 3555327
DISK RECS AVAIL: 2764
DCH AVAIL: 15 USED: 1 TOT: 16
AML AVAIL: 10 USED: 0 TOT: 10
REQ> **chg**
TYPE> **pwd**
PWD2 **(your level 2 password)**
LNAME_OPTION> **yes**

MEM AVAIL: (U/P): 3352174 USED: 203153 TOT: 3555327
DISK RECS AVAIL: 2764
DCH AVAIL: 15 USED: 1 TOT: 16
AML AVAIL: 10 USED: 0 TOT: 10

DEFAULT LOGIN NAMES SAVED

Note: At this point, your old passwords will work with either the newly assigned user IDs or with the default user ID values associated with your old passwords. See the online help for LD17, LNAME_OPTION for more information. Please alert others of any changes; for example, all technicians with access to the Meridian 1, the Distributor, and so on.

Continue configuring LAPW and OTM:

```
REQ> chg
TYPE> pwd
PWD2 (your level 2 password)
LNAME_OPTION> yes
NPW1
LOGIN_NAME
NPW2
LOGIN_NAME
LAPW> 88 (example)
PWTP
PW88
```

You will be prompted to enter your new password.

```
LOGIN_NAME> johns (example)
OVLA> all
OVLA
CUST> all
CUST
HOST
OTM> yes
OTM_READ_ONLY> no
OPT
LAPW
FLTH

LOCK
AUDT
INIT
```

```
MEM AVAIL: (U/P): 3352149   USED: 203178   TOT:
3555327
DISK RECS AVAIL: 2764
DCH  AVAIL:    15    USED:     1    TOT:    16
AML  AVAIL:    10    USED:     0    TOT:    10
REQ> end
```

Note: If you are using serial connections, skip this step.

If you are using Ethernet or PPP connections, configure a PTY for each OTM application that will run simultaneously with other applications over Ethernet or PPP.

For example, Maintenance Windows and System Terminal each require a PTY if they run at the same time. If you have enough free ports, Nortel Networks recommends that you configure at least two PTYs. You can allocate a maximum of 8 PTYs (maximum of 4 PTYs on an Option 11C).

Find an empty TTY slot:

```
>ld 22
PT2000

REQ> prt
TYPE> adan tty
```

```
ADAN     TTY 0
  CTYP PTY
  DNUM 0
  PORT 0
  DES  pty0
  FLOW NO
  USER SCH
  XSM  NO
  TTYLOG       0
PORT 7
  DES  jonspty
  FLOW NO
  USER MTC SCH BUG
  XSM  NO
  TTYLOG       0
  BANR YES

ADAN     TTY 8
  CTYP SDI2
  DNUM 8
  DES  TECHSUN
  FLOW NO
  USER MTC SCH CTY BUG
  XSM  NO
  TTYLOG       0
  BANR YES
...

REQ> ****
OVL000
>ld 17
CFN000
MEM AVAIL: (U/P): 3352149   USED: 203178   TOT:
3555327
DISK RECS AVAIL: 2764
DCH  AVAIL:    15    USED:     1    TOT:    16
AML  AVAIL:    10    USED:     0    TOT:    10
```

Choose an empty port number between 0-15. Choose a PTY number 0-7. In this example, we find TTY 13 to be free, and assign PTY 0.

```
REQ> chg
TYPE> adan
ADAN> new tty 13
TTY-TYPE> pty
PORT> 0
DES> 13
DES> new pty
FLOW
USER> mtc bug sch
TTYLOG
BANR

MEM AVAIL: (U/P): 3345946   USED: 209381   TOT:
3555327
DISK RECS AVAIL: 2764
DCH  AVAIL:    15    USED:     1    TOT:    16
AML  AVAIL:    10    USED:     0    TOT:    10

ADAN DATA SAVED
ADAN> end
```

6 Configure ethernet and PPP at the Meridian 1:

The host names and IP addresses used in the following instructions are only examples. *Actual host names and IP addresses should conform to your network plan.*

- In LD 117, configure an IP address at the Meridian 1.

  >LD 117
  >NEW HOST M1ACTIVEIP 47.1.1.10
  >CHG ELNK ACTIVE M1ACTIVEIP

- If you are using a backup (inactive) IOP, use LD 117 to configure it as well. This step does not apply to Option 11C Compact.

- The backup (inactive) IP is only used when switch is in split mode.

  >NEW HOST M1INACTIVEIP 47.1.1.11
  >CHG ELNK INACTIVE M1INACTIVEIP

- Configure the subnet mask.

  >CHG MASK 255.255.255.0

- If you have a default gateway in the network, define the routing table in LD 117.

  >LD 117
  >NEW ROUTE 0.0.0.0 47.1.1.250
  >PRT ROUTE (list the configured routing table)
  >ENL ROUTE # (where # is the route number)

  The first four digits define the network address. The remaining digits specify the gateway address.

  If desired, you can print all information about route, host, gateway and related settings.

  The routing table provides the Meridian 1 with the IP address of the gateway server so the Meridian 1 can send return messages to the gateway for forwarding to the requesting client.

  You can use PRT ROUTE for a list of routes with route numbers.

  You can use STAT ROUTE to see if route was successfully enabled.

- If you are using PPP, use the default addresses unless there is an address conflict. If a conflict exists, obtain a new IP address from your network administrator and configure this address.

>LD 117
>NEW HOST PPPLOCAL 47.0.0.2
>CHG PPP LOCAL PPPLOCAL 1

>LD 117
>NEW HOST PPPREMOTE 47.0.0.3
>CHG PPP REMOTE PPPREMOTE 1

- After you do a series of NEW, OUT, CHG commands, type

  >UPDATE DBS

  to clean up the database before you get out of LD 117.

  >LD 137 (*Note:* overlay 137 prompt is ".")
  .DIS ELNK (disables network)
  .ENL ELNK (enable Ethernet interface)
  .STAT ELNK (verify IP address)

  If the **STAT ELNK** command displays the correct IP address, your IP address configuration is done. Otherwise, you will need to INIT the Meridian 1.

Determine the OTM PC IP address

To find your PC's IP address:

1 From the Start button, select Settings - Control Panel. The Control Panel window opens.

2 Open the Network icon to display the tabbed dialog box. Click on the Configuration tab. A list of installed network components is presented.

3 Select the TCP/IP network component used by your PC. Depending on the number of installed components, you may have to scroll to see the correct component.

4 With the component selected, click on Properties. The TCP/IP tabbed window opens.

5 Click on the IP Address tab. Note the IP address shown. This is the IP address unique to this PC. You will enter this information in Overlay 117 to specify where the alarm event will be received.

6 Close all the control panel related windows and return to your desktop.

Enable alarms with Overlay 117

To enable alarms with Overlay 117:

1 Click on the System Terminal icon from the toolbar in the OTM system window. The System Terminal Selection window opens.

2 Click on the Ethernet/PPP (Overlay Passthru) radio button then click OK. The System Terminal window opens.

3 Log in with your administrator's user name and password.

Note: You must have appropriate access privileges to use Overlay 117.

4 Load Overlay 117 by entering `ld 117` in the command line. The => prompt appears in the Command Results pane indicating the system terminal application is ready to accept your input.

5 Type `prt open_alarm` to see if other users are currently accessing the system. A list of slots currently in use is displayed. Slots are numbered from 0 through 7, for a total of eight available slots. Note the next available slot.

6 Type `set open_alarm` *`n IP_address`* where *`n`* is the next available slot number and *`IP_address`* is the IP address of your OTM PC. See "Determine the OTM PC IP address" on page 108.

Note: Assigning your IP address to a slot currently in use will disconnect that user from the system preventing them from receiving alarms information.

7 Verify the overlay has accepted your entry by typing `prt open_alarm`. The list of slots and IP addresses receiving alarms is displayed. Verify that your particular slot and IP address is included.

Note: Overlay 117 accepts abbreviations of the various commands. For example, you can type the abbreviation `prt op` instead of `prt open_alarm`.

8 Log out and close the system terminal window.

Set Up the Virtual Terminal Service

Virtual Ports

In the Terminal Server application, the Virtual Ports Properties dialog allows the OTM administrator to enable or disable a connection to a particular device. It displays the virtual port number for each configured device, and the corresponding serial or network settings. Launch the Terminal Server application by selecting **Optivity Telephony Manager** then **Terminal Server** in the Windows Programs list in the **Start** menu.

To configure a virtual port:

Click the **Systems** button, or double-click the "Configured Systems" list.

If a device was selected in the Configured Systems list, then the corresponding device is also selected in the Virtual Port Properties dialog. This allows the user to quickly change the settings for a particular device.

In the Virtual Port Properties dialog, a tree displays the devices that can be connected via a virtual port. The tree lists the devices from the OTM database (configured using the OTM Navigator).

For a Meridian 1 system, the VT220 profile is used (Ethernet/network or serial). If Ethernet/network is selected, the software uses the Meridian 1's rlogin connection.

For a Generic system, the profile selected under the Application tab in System Properties is used (Ethernet/network or serial). If Ethernet/network is selected, the software uses a Telnet connection.

To enable virtual port connection for a device:

1 Double-click the disabled item in the tree, or

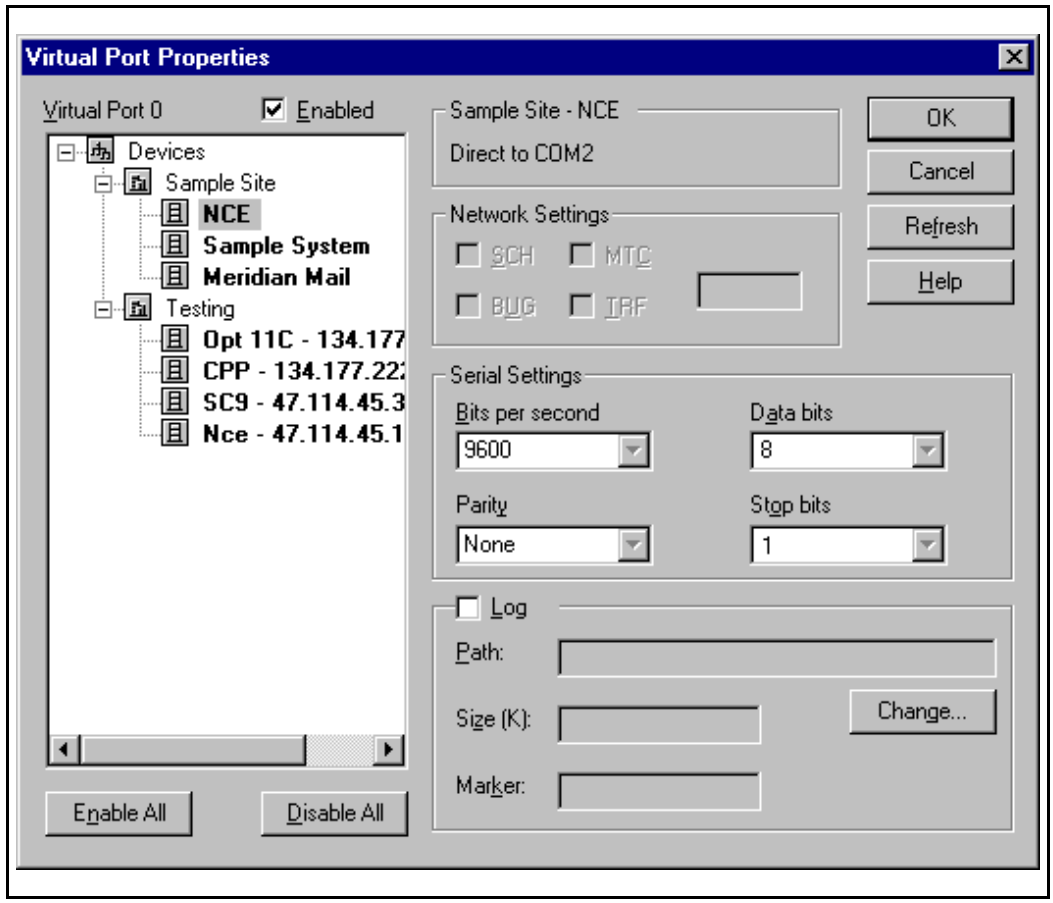
Select the item and check the "Enabled" checkbox, or

Click the "Enable All" button to enable all the items listed in the tree with the default configuration. The item becomes bold to show that it is enabled.

2 The field to the right of the "Enabled" checkbox automatically fills in the Site and System name for the device. This is the name that is displayed in the Terminal Server's main window.

3 For a serial connection, “Direct to Com x” is displayed, where x is the Com port number. (Figure 61):

Figure 61
Configuring Virtual Ports (serial, logging disabled)



The fields for serial port settings are enabled. The default is the serial settings from the OTM database.

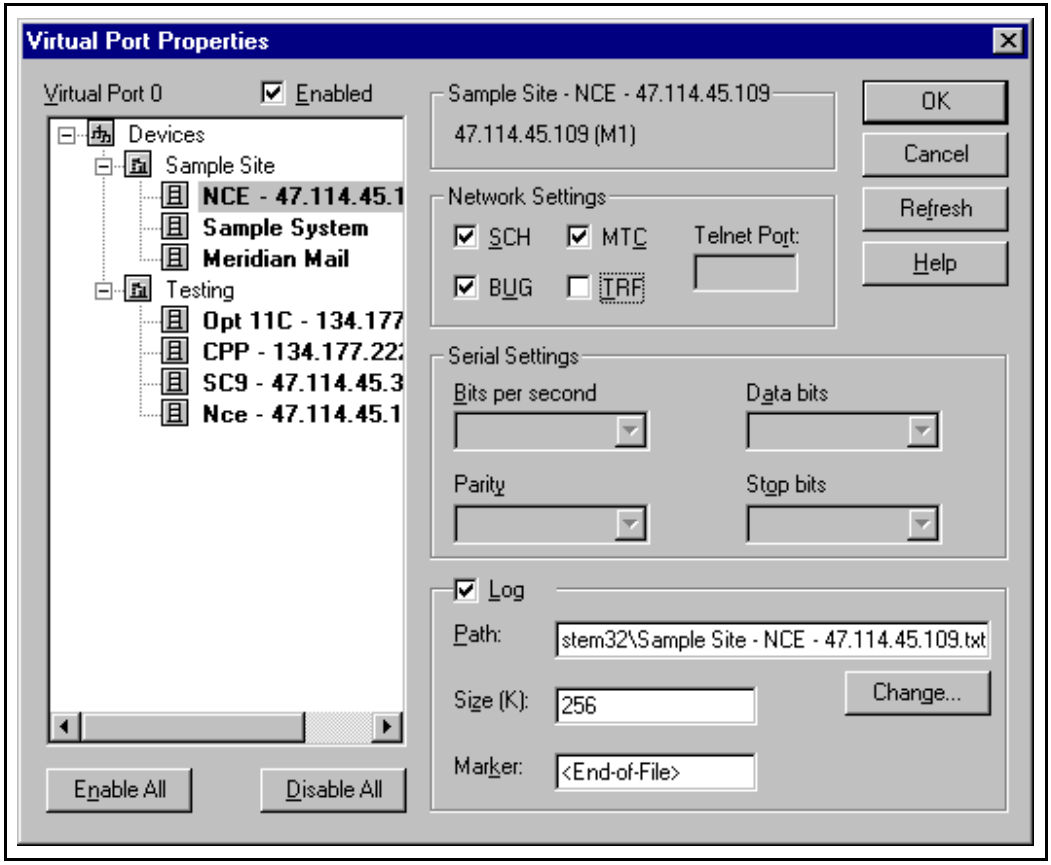
You can change the settings in the dialog box.

4 For a network connection, the IP address is displayed. It also displays whether the system is a Meridian 1 or Telnet.

Make sure the IP address is correct. If the IP address is different from the OTM database setting, click the “Refresh” button to update the all network ports with the latest IP address from the OTM database.

If you select a Meridian 1 system (Figure 62):

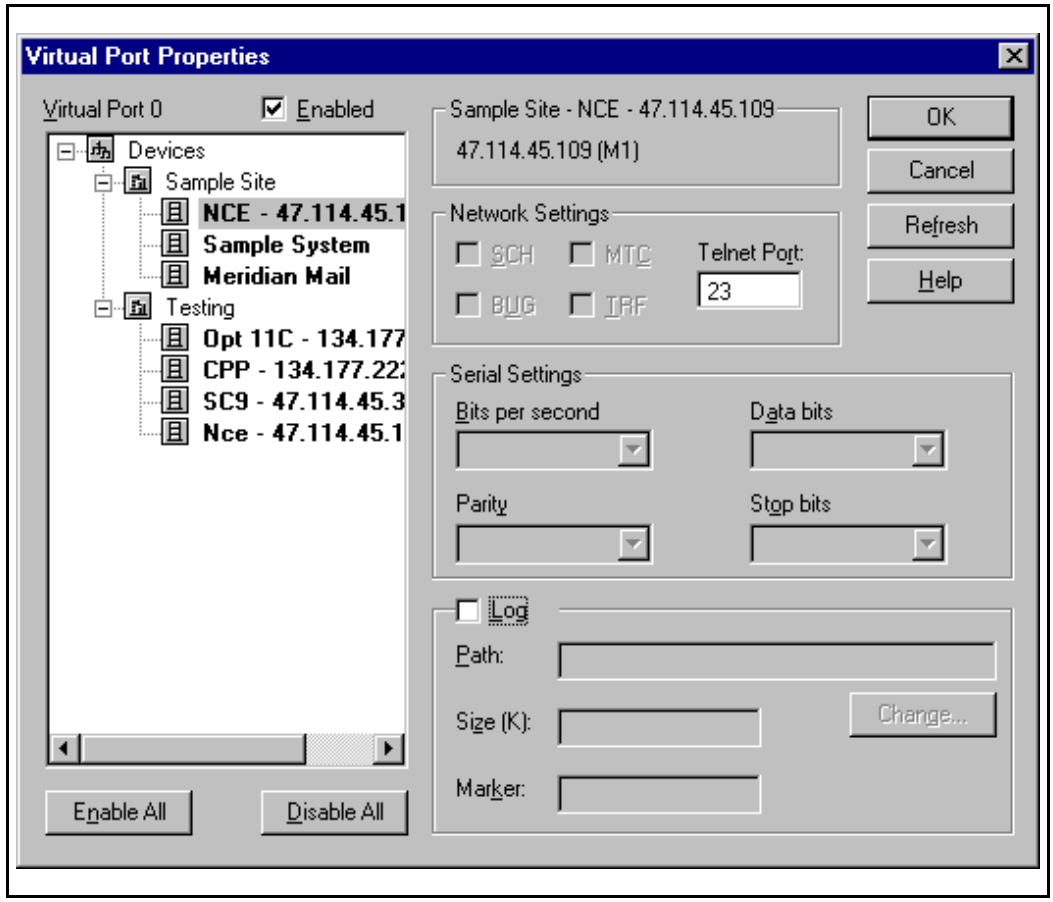
Figure 62
Configuring Virtual Ports (Meridian 1 system, logging enabled)



- The fields for Meridian 1 port user types are enabled (default = SCH).

If you select a non-Meridian 1 system (Figure 63):

Figure 63
Configuring Virtual Ports (Telnet system, logging enabled)



- The fields for both serial and PTY user types are disabled. The border displays Telnet System and the selected device's IP address configured in OTM Navigator. In the "Port" field, you can specify a Telnet port number other than the port number specified in the Applications page in System Properties.

5 Check the “Log” checkbox to turn on data capture. The log file name defaults to the Site and System name plus a .txt extension. The path and the file name can be changed by typing in the edit box or clicking the “Change” button.

The maximum size of the log file is customizable (in the Size field) on a per-system basis, and defaults to 256K. Once the file size reaches the limit, the Terminal Server starts from the beginning of the file, overwriting the oldest logs.

Because of the circular nature of the log, the Terminal Server writes an end-of-file marker (customizable in the Marker field) at the end of the log entries.

The log records the time and date of when a client connects and disconnects to the virtual port, and writes all text received from and sent to the host. This allows a network administrator to keep an activity log of the virtual port connection.

If this ASCII log is to be viewed from a web browser, the file should be stored in a web-accessible path.

6 Click **OK** to store the changes, or Cancel to discard them.

7 To disable a virtual port connection for a device:

- Double-click an enabled item in the tree, or
- Select the item and uncheck the “Enabled” checkbox.
- Click the “Disable All” button to disable all devices listed in the tree.

The item is no longer bold, and does not appear in the Terminal Server main window when you click “OK.”

The Terminal Server application has a limit of 256 total configured ports/devices. It supports up to 8 simultaneous serial connections.

However, the real limit on the number of simultaneous connections depends on the OTM server hardware, the network capacity, the server’s CPU capacity, etc.

Communication Settings

The Terminal Server uses TCP socket ports to communicate with the switch and Virtual Terminal Server. Terminal Server is therefore is **not** directly accessible through a network firewall, unless you enable the ports required. A network administrator determines the access method (e.g., through dial-in accounts, enabling access to the ports used by Terminal Service, etc.).

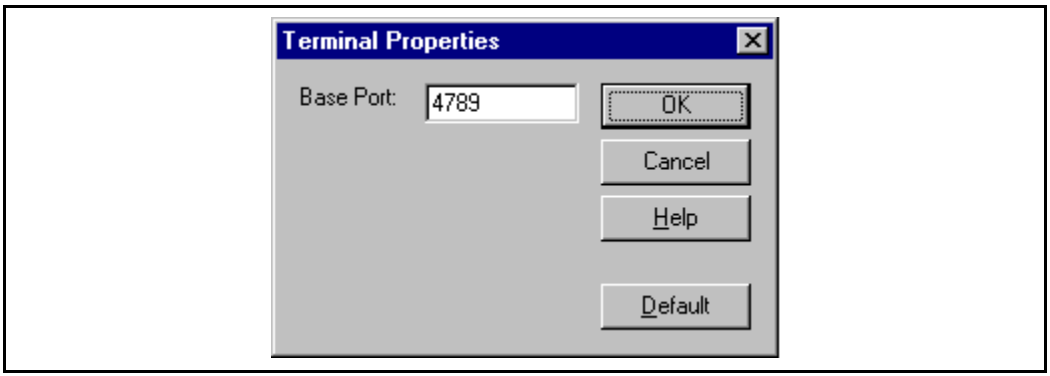
The base port number determines the range of socket ports used to communicate with the Terminal Client. However, do not change this number, unless the default port conflicts with another network application.

By default, the Terminal Server and Terminal Client communicates through network ports 4789 up to 5045 (4789 to send connection requests, 4790-5045 for up to 256 terminal sessions). Of course, the number of ports actually used depends on the number of virtual ports configured.

An administrator can change the range of port numbers by doing the following:

1 In the Terminal Server application, click the **Terminals** button. In the "Terminal Properties" dialog box (Figure 64), enter the new port number. Click the "Default" button to reset to the default value (port 4789).

Figure 64
Terminal Properties dialog box



For more information on the Terminal Server Web Navigator Interface, see the *Web Services* chapter in the *Common Services User Guide*.

Set Up the Data Buffering and Access Application

To configure a DBA Serial Port session:

1. From the DBA Main application window select “New Session” from the File menu.
2. In the “Select an M1 System for Live session” dialog box, a tree displays the Site and Systems that can be used to collect serial data. Select a system from the tree to use for the new session.
3. In the “New Session” dialog box, select a Com port from the “Connect Using” combo box. The “Connect Using” combo box retrieves the available serial ports from the Registry. If you are using an Ethernet connection then set “Connect Using” to “Network.”

   Depending on whether you have selected a serial or network connection, the fields that can be configured will be enabled.
4. Select **Connect Now** once you have configured the settings for the connection. If the connection is successful, the session window will show “Connected” in the window title. For serial connections the session will be connected if the port is available, this does not indicate that the device is connected to the serial port.

There is more information on the Data Buffering and Access Application in *Using Data Buffering and Access* in the *Common Services User Guide*.

Set Up the LDAP Server

The LDAP Server utility allows you to link and synchronize the OTM and Corporate LDAP databases.

You can use the LDAP Server to link an employee entry in the OTM directory to an entry in the LDAP directory. If employee data exists in the LDAP directory, you can select and add the employee entry into the OTM directory. Or if the employee entry resides in both directories, you can select and link the entry.

When you link an entry between the OTM directory and the LDAP directory, OTM updates the entry's attribute data when you synchronize the directories. The following are examples of LDAP attributes:

- First name
- Last name
- Department
- Telephone extension

Note: Scheduled synchronization will only synchronize OTM Directory entries that have their **Publish** check box checked. Synchronization only compares and updates entries that have the same Unique Identifier (UID) in both the OTM Directory and the LDAP compliant server. You can use the LDAP Synchronization Utility or the Import and Export Utility to manually set up the UID.

For detailed instructions on setting up the LDAP server, as well as an example of importing attributes to the OTM directory, see the "LDAP Synchronization" chapter in the *Optivity Telephony Manager Common Services User Guide.*

For information on importing non-LDAP compliant directory information into the OTM directory see the "Import and Export Utilities" chapter in the *Optivity Telephony Manager Common Services User Guide.*

Set Up Alarm Management

Configure each device to send traps to OTM, define the devices and scripts in Alarm Notification, and configure the DBA Serial and Rules Manager to receive serial text alarms and send SNMP traps. For more information, consult the *Alarm Management User Guide*.

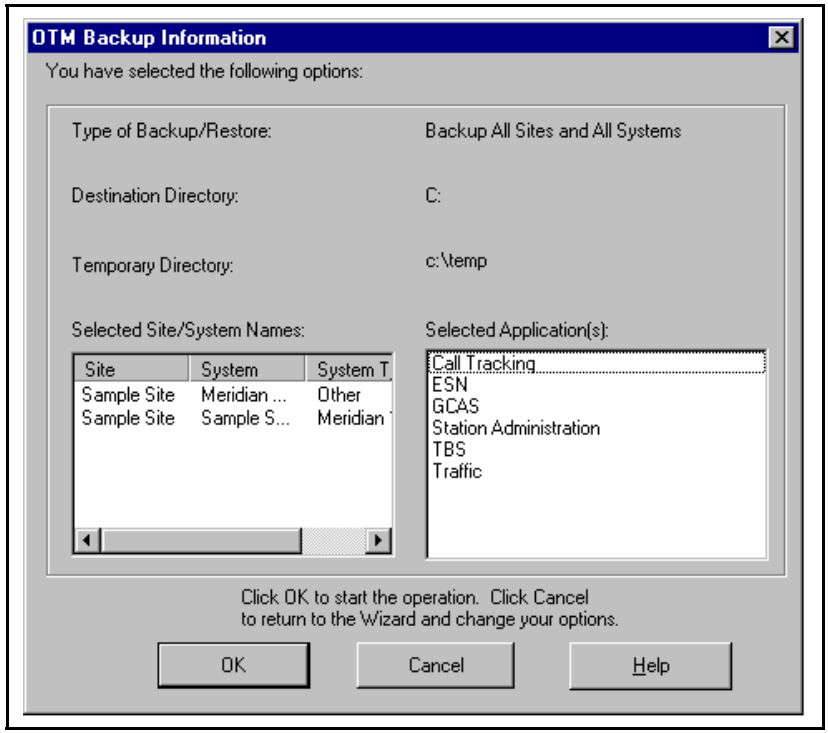
Perform an OTM backup

Select **Backup** from the **Utilities** menu of the OTM Windows Navigator. The next screen to appear is a dialog box (Figure 65) that summarizes your choices. Click **OK** to start the backup operation

- Type of backup (single site, single system, all sites and systems, or disaster recovery)
- Applications (Telecom Billing System, Call Tracking, ESN, Station, and/or Traffic)
- Destination directory for backup files
- Temporary directory for working files created during the operation

Note: The destination and temporary directory screens display a computed space requirement for the files. You can back up and restore data for these OTM applications across multiple sites and systems at the same time.

Figure 65
OTM Backup Information dialog box



OTM Web Browser Client installation

Make sure that the PC Client (or UNIX workstation) requirements have been met, as described in “PC Client requirements” on page 24.

Accessing the OTM Server Web Navigator via the PC Client

To access the OTM Server Web Navigator, use the HTML compliant Web browser on the PC Client, enter the OTM Server IP address or computer name in the location bar, and press “Enter.”

Software “plug-in”

The first time the OTM Server Web Navigator loads, you are prompted to download a software plug-in (Figure 66). The software you download is a standard Java Runtime Environment (JRE) “plug-in” of about 7-8 MB size.

Figure 66
JRE Plug-in download prompt

Appendix A: Windows NT installation example

This section describes an example of Windows NT installation. Due to hardware and software differences, this example may not match your installation.

If a certain component is already correctly installed, then skip the installation of that component.

- "Running the Windows NT Setup Program" on page 122.
- "Installing Windows NT components" on page 124
- "Network Adapter Software Installation" on page 124
- "TCP/IP Configuration" on page 126
- "Initial Workgroup Configuration" on page 128
- "Configuring system settings" on page 128
- "Creating an Emergency Repair Disk" on page 128
- "Completing the Windows NT Installation" on page 129

Additionally, this section describes examples of Remote Access Service, Service Pack 5, and Windows NT Option Pack installation.

Hardware Compatibility Check

Check all hardware against the "Windows NT Hardware Compatibility List" and make sure you have all necessary and latest drivers from the manufacturers. For more detail, please refer to *Microsoft Windows NT Server Basic and Installation, Chapter 5* through *8*. For NT Workstation, please refer to *Microsoft Windows NT Workstation Installation Guide, Chapter 1*.

Running the Windows NT Setup Program

Note: Make sure the first bootup option on CD-ROM in the BIOS is enabled. The installation below requires a server with HDD using a SCSI controller card or a system with RAID. You must get the latest HDD controller from the Manufacturer. For details, check with your server manufacturer.

1 Insert the Windows NT server setup CD-ROM into the CD-ROM drive.

2 Boot the system.

3 On Windows NT Server machines, press "F6" immediately, when "Window NT Setup" comes up.

4 You see "Setup could not determine the type of one or more mass storage devices…". Press "S".

5 You see the "Windows NT Setup" screen and press **Enter** to continue.

6 Insert the manufacturer-supplied hardware support disk (Hard Disk controller or RAID controller driver) into a: or CD-ROM. Press **Enter** when ready.

7 Select appropriate driver from the list and press **Enter**.

8 Press **Enter** if no additional mass storage devices exist.

9 In the Windows NT server setup menu "Welcome to Setup", press **Enter** to setup Windows NT.

10 In the "Windows NT Server Setup" screen, you see "Windows NT has recognized the following mass storage…" Press **Enter**.

11 In the "Windows NT Licensing Agreement", press "Page Down" and choose "F8".

12 You see “Setup has determined that your computer contains the following hardware and software components.”
Press **Enter** to select “The above list matches my computer”.

13 Press “C” to create partition and type the size of partition you want. The largest size boot partition that you can create is 4095MB. If the system was previously configured as an NT Workstation, select “N” for new.

14 Select the “Unpartitioned Space” on the first disk in the list. (Use the up/down arrow key).

15 Press **Enter** to select “Install Windows NT on the unpartitioned space”.

16 Use the down arrow key to select “Format partition using the NTFS file system” for Windows NT partition. NTFS allows management of file security using directory and file permissions. For more details, refer to *Microsoft Windows NT Server Concepts and Planning, Chapter 4*.

Note: The disk format will take approximately 3 minutes for a 4G drive and only a few seconds on a drive controlled by a RAID controller

17 The default “Winnt” is prompted or change the name or location as you want.

18 Press **Enter** to allow Setup to perform an exhaustive secondary examination of the hard disk.

19 Insert the Manufacturer SCSI or RAID driver disk, if applicable, when using a server machine or RAID controller. Press **Enter** to allow the system to copy the files on the disk.

20 Eject the CD-ROM and remove any floppy disk from the floppy drive. Press **Enter** to reboot the system. At this point, you have finished the first part of Windows NT installation. The machine will be rebooted twice. The second reboot is to convert from FAT to NTFS on the partition in which Windows NT was installed.

When the system reboots, press “F2” to instruct the system to boot from the hard drive instead of the CD-ROM.

Installing Windows NT components

1. When the Windows NT Setup screen appears, click **Next** on "Gathering information about your computer".
2. Enter your "Name" and "Organization Name" and click **Next**.
3. Enter the information on "Licensing Modes". Click **Next**.
4. Enter the unique "Computer Name".
5. Select the server type on the "Server Type" screen ("StandAlone Server" is highly recommended).
6. Enter the password for the Local Administrator.
7. Create an Emergency Repair Disk.
8. Select "Components" and Click **Next**.

Note: Do not use open GL screen savers, which use too much processing time.

Network Adapter Software Installation

Before configuring the network adapters, make sure that the adapters are inserted properly into the slots and RJ45 cables are plugged into the adapters. The C-LAN card is recommended to install on the TOP PCI slot and E-LAN on the second from the TOP PCI slot.

1. In the "Windows NT Setup", verify that the "Wired to the network" box is checked and click **Next**.
2. On the "Install Microsoft Internet Information Server" screen, uncheck the box and click **Next**.
3. Click "Select from the List" on the "Network Adapter" screen.
4. Click "Have Disk" and insert the floppy or CD from the Manufacturer (shipped with the network card). Click **OK** and select the appropriate driver from the list. Click **OK** to continue.
5. The next screen displays your LAN card. Since the server has 2 LAN cards, click on "Select from the list" to install the E-LAN card driver and follow the previous step to install the E-LAN card.

6 In the “Network Protocol” screen, only select “TCP/IP protocol” and click **Next** to continue.

7 In the “Network Services” screen, you see the following services. Click **Next**:

- RPC configuration
- NetBIOS Interface
- Workstation
- Server

8 Click **Next** to install selected components.

9 Click **OK** for Adapter Properties.

10 If the E-LAN card is the same type as the previously installed C-LAN card, the following message may be displayed: “ A network card of this type is already installed in the system. Do you want to continue?” Select **OK**.

11 The “Adapter Properties” screen appears for the second LAN card. Click **OK** to continue.

TCP/IP Configuration

Configure TCP/IP as follows:

1 The "TCP/IP Setup" screen appears, as shown in Figure 67 on page 127. If you have a DHCP server and want to configure the IP address from the DHCP server, then select **Yes**. Otherwise Select **No** and do the following.

2 In the "TCP/IP Configuration" screen,

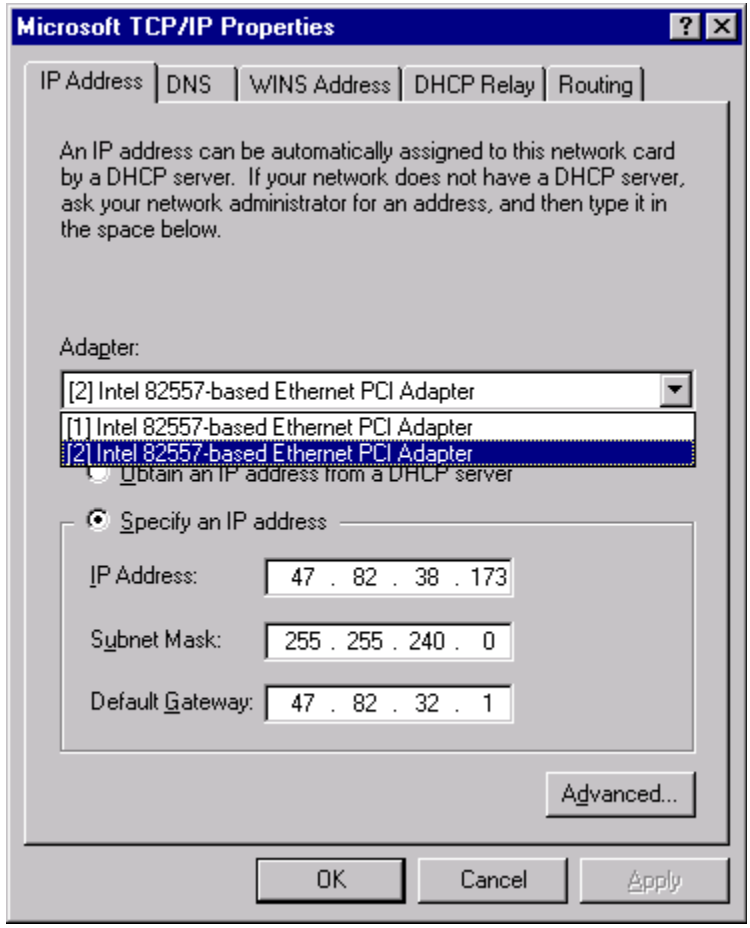
- select adapter "[1]…" and enter the IP Address, Subnet Mask and Default Gateway for the Customer LAN (C-LAN) connection,
- select adapter "[2]…" and enter the IP Address, Subnet Mask and Default Gateway for the Customer LAN (C-LAN) connection. Click **OK** to continue.

3 In the "Show Binding For" screen, click **Next** to continue.

Note: For IP routing, the "Enable IP Forwarding" box is unchecked by default. Nortel Networks recommends leaving this box unchecked to avoid security and performance problems.

For more information, refer to *Microsoft Windows NT Server Basics and Installation, Chapter 7*.

Figure 67
Microsoft TCP/IP Properties window



Initial Workgroup Configuration

1. In "Domain / Workgroup Setting", use the default Workgroup settings and click **OK** to continue.
2. Click **Finish** in the "Finishing Setup" screen.
3. In the "Internet Information Server Installation" screen, remove the gopher selection.
4. Install the SQL server driver.
5. In the "Microsoft Internet Information Server" screen, Click **Cancel**. The Microsoft Internet Information Server will be installed in Option Pack 4.

Configuring system settings

Configure system settings as follows:

1. In the "Date/Time Properties" screen, select your Time Zone.
2. Select the check box (default is checked) for automatically adjusting for Daylight Savings Time,
3. In "Display Setting":

- select **OK** to verify that the video adapter was detected.

Note: if you do not have the correct video driver, you must install the correct driver, after reboot, from the manufacturer's diskette.

- Color Palette: # of colors (Use default setting)
- Desktop Area: 1240 by 768 pixels
- Font Size: Small Fonts
- Refresh Frequency: (Use default setting)

4. Click **Test**, then **OK** to test display. Save the display settings when prompted (select OK to save). Click **OK** to exit the Display Settings.

Creating an Emergency Repair Disk

- In the "Emergency Repair disk" screen, select **Yes** to create an Emergency repair disk.

Completing the Windows NT Installation

- Click “Restart Computer” to reboot the system.

The Windows NT installation is complete.

Remote Access Service Installation

Remote Access Service provides the ability to administer OTM remotely. For more information, refer to *Windows NT Server Network Supplement, Chapter 6.*

1 Open the “Control Panel” and “Network,” select the “Services” tab and click “Add” to add “Remote Access Service” software.

2 Insert the Windows NT server CD and click “Continue”.

3 Select “Yes” to “invoke the modem installer to enable you to add a modem”.

Note: A modem does *not* have to be attached to install this software.

4 In the “Install New Modem” screen, click **Next** to continue.

5 If the system cannot detect the modem for you, you must insert the manufacturer’s disk that comes with the modem, and choose “Have Disk” to install.

6 If the system does not have a modem attached, select “Standard 28800 bps Modem” from the list.

7 In the “Selected Port”, select “COM1” and click **Next**.

8 In the “Location Information” screen, enter your “Area Code” and click **Next**, then **Finish**.

9 A screen appears that lists the modem Port, Type and Device.

Select “Configure…” to choose “Dial out and Receive Calls” as Port Usage. Click **OK**.

10 Select “Network…” to configure “TCP/IP”. Click **OK**.

11 In the “RAS Server TCP/IP Configuration” screen, select “This Computer only”. Select “Use Static Pool and give the initial ranges as 1.0.0.1 to 1.0.0.255. Click OK to return to “Remote Access Setup” screen and click “Continue”.

12 In the “Remote Access Service has been successfully installed” screen, click **OK**.

13 In the “Network” screen , click **OK**. Click **Close**.

14 The system will bind all the network protocol software. Remove the Window NT Server CD and Press Enter to restart your server again.

RAS with TCP/IP

With TCP/IP you can allow an incoming call to access only the RAS server, or you can allow the computer making the incoming call to access the rest of the network as well.

> **CAUTION**
> For security reasons, we recommend allowing the incoming call to access “The computer only,” which is the RAS server itself.

As shown in Figure 68, there are three configurations for getting the IP address from RAS:

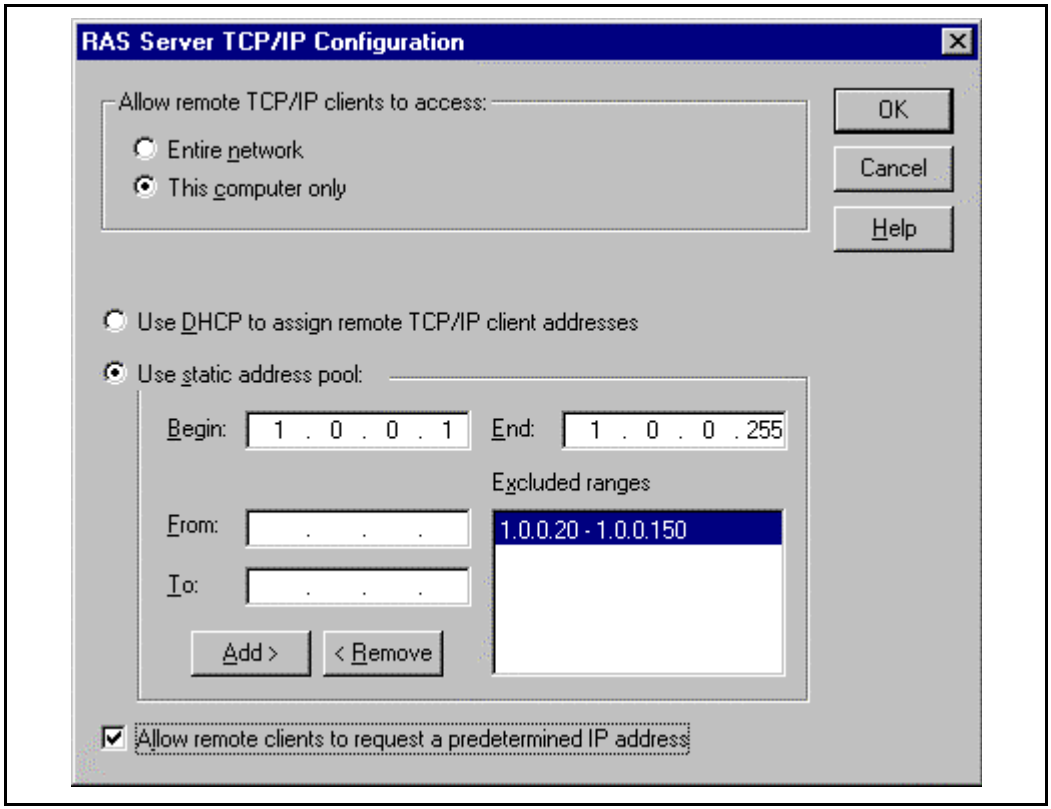
- you can configure to get the IP address via Dynamic Host Configuration Protocol (DHCP),
- you can configure the IP address to come from a pool of IP addresses maintained on the RAS server, or
- you can allow the incoming connection to request its own IP address.

Note: This configuration is only available on Windows NT Server. If you run OTM on a Windows NT Workstation, you do not have this capability.

Grant Permission

After installing Remote Access software on a server, you must grant Remote Access permission to users.

Figure 68
RAS Server TCP/IP Configuration window



Call back

As an additional measure of security, the callback feature ensures that only users from specific locations can access the RAS server. You configure each user's callback privilege when granting Remote Access permission.

Encrypted Passwords and Data Encryption

As shown in Figure 69 on page 133, the default setting for RAS password authentication is to require Microsoft Encrypted Authentication. When you select this option, we assume you only use Microsoft clients (Windows 95/98, Windows NT workstation or Windows NT Server computers) can connect to the RAS Server.

For additional security, if you use the MS-CHAP protocol, then you can also set the RAS device to require data encryption. This will enable data encryption between the RAS Server and client as well as the password exchanged to establish the connection.

Multilink

You can enable Multilink to speed up your remote access. Multilink combines multiple serial data streams into one aggregate bundle. For instance, if you have two 56Kbps modems with Multilink enabled, your bandwidth could be aggregated to 134.4Kbps.

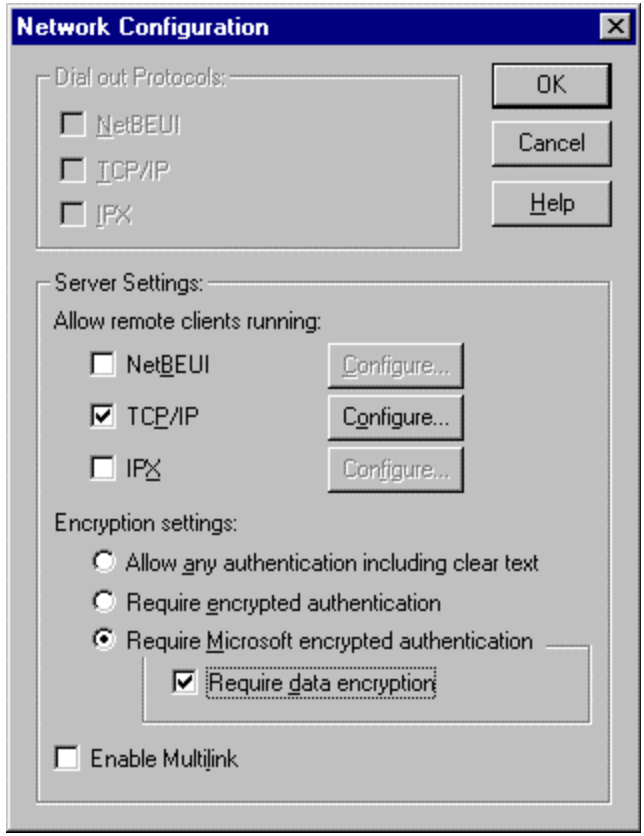
To use Multilink, both the server and client must have Multilink enabled.

For more information, please refer to *Windows NT Server Networking Supplement, Chapter 6*

RAS Client

The security you select must match the security selected on the remote server. However, if either side selects Allow any authentication including clear text, then it does not matter which protocol the other side uses.

Figure 69
Network Configuration window



Note: The data encryption and multilink features are only available on Windows NT Server version.

Testing Network Cards

Test the network cards after you complete the Windows NT installation.

Testing C-LAN (Customer LAN)

1. Configure the Captive Client IP address on the same subnet as the C-LAN. The equivalent subnet would be the BINARY AND of the full Captive Client IP address with the C-LAN subnet mask (e.g. 255.255.240.0). The subnet mask of the Captive Client would be same as that for the C-LAN.
2. Ping the C-LAN IP Address from Captive Client (e.g. 47.82.38.100).

Testing E-LAN (Management LAN)

1. Configure the Captive Client IP address on the same subnet as the E-LAN. The equivalent subnet would be the BINARY AND of the full Captive Client IP address with the E-LAN subnet mask (e.g. 255.255.240.0). The subnet mask of the Captive Client is the same as that for the E-LAN.
2. Ping the E-LAN Address from Captive Client (e.g. 47.114.45.3)

Internet Explorer Installation

Install Microsoft Internet Explorer version 4.01 or higher:

1. Insert Internet Explorer CD (or Windows NT Option Pack 4) into the CD-ROM drive. Select “Install” and “NT Service Pack 3x86”, then “IEx86”, and then “Internet Explorer 4.01 (x86)” or higher version.
2. In the “License Agreement” screen, select “I accept the agreement” and click **Next**.
3. In the “Installation Option” screen, choose the default “Standard Installation” and click **Next**. If you receive a security warning, click **Yes**.
4. In the “Windows Desktop Update” screen, click **Next**.
5. In the “Active Channel Selection” screen, choose your country and click **Next** to continue. If you see an upgrade screen, select “Upgrade Plus.” When asked to select components, select the defaults.
6. In the “Destination Folder” screen, select **Next** to use default location or specify your location for the folder.

7 In the “The Internet Explorer has been successfully installed” screen, click **OK** to restart your computer.

8 After you reboot and log onto the system as Administrator, wait a few minutes for Microsoft Internet Explorer to set up your system.

Windows NT Service Pack 5 installation

Install the Windows NT Service Pack 5:

Note: Carefully read the Read Me file before you install the Windows NT Service Pack 5. You must reinstall the Windows Service Pack 5 after installing the Windows NT 4.0 Option Pack.

1 Insert the Windows NT Service Pack 5 CD into the CD-ROM drive. If you are in US and Canada, use the version 128 bit of Service Pack 5.

2 Double click “update.exe” in the I386/Update folder. Click **Install**.

3 Select “Restart your computer” in the “Service Pack 5 has been successfully installed” screen.

Windows NT 4.0 Option Pack installation

Install the Windows NT 4.0 Option Pack:

Note: Carefully read the Read Me file before you install the Windows NT 4.0 Option Pack.

1 Insert Windows NT Option Pack 4 into the CD-ROM drive.

2 Select “Install Windows NT 4.0 on Pack”.

3 Select “Run this program from this current location” and click **OK** to proceed.

4 In the “Setup has detected that Windows NT 4.0 SP4 or greater is installed …” screen, select **Yes** to proceed.

5 In the “License Agreement” screen, select “Accept”.

6 In the “Microsoft Windows NT 4.0 Option Pack Setup” screen, select “Custom”.

7 In the “Select Components” screen, uncheck the following components:

- FrontPage 98 Server Extension
- Microsoft Index Server

The required components are:

- Internet Information Server 4.0 or above
- Microsoft Transaction Server
- Microsoft Data Access Components (MDAC)
- Microsoft Management Console (MMC)
- NT Option Pack Common Files

8 In the “Setup will install the folder …” screen, use the default folder as your home directory or specify your location or name of directory and click **Next**.

9 In the “Microsoft Transaction Server 2.0” screen, use the default folder and location or specify your own.

10 In the “Configure Administrator Account”, use the default “Local” and click **Next**.

11 In the “Microsoft SMTP and NNTP Services Setup”, use the default value or specify your own. Click **Next** to complete the installation.

12 When the “Finish” screen appears, press **Enter** and click **Yes** to restart your computer.

Reinstall Service Pack 5

Reinstall Service Pack 5 after installing Windows NT 4.0 Option Pack on your system. During the installation, make sure that you select not to overwrite the newer files that Option Pack Setup installed.

Setting up a separate Windows NT account

For security purposes, we recommend that you create an additional Windows NT Administrator account to log in and access OTM instead of the default Administrator setup.

Before installing OTM, you must log into Windows NT as an Administrator.

Please refer to your Windows NT documentation for information on how to create Windows NT accounts.

Appendix B: Configuring a Windows NT Server or Workstation as an IP router

This section shows how to setup a Microsoft NT Workstation or Server to be an alternative IP router for two private subnets on the LAN. In addition, this section shows how to configure a Windows 95/98 TCP/IP protocol and routing table on the Meridian 1 switch, so that one Windows 95/98 PC in a subnet is able to communicate to a Meridian 1 switch in different subnet through the gateway (Microsoft Windows NT workstation/Server IP router).

There are benefits to having a Microsoft Windows NT act as an IP router on the LAN:

- A reduction in broadcast messages exposed to the Meridian 1 switch, and
- The available hardware and software (a Microsoft Windows NT Workstation/Server 4.0 OS version and two Network Interface Cards) make this is a very cost/effect alternative IP router.

Requirements

PC

- Windows NT 4.0 Workstation or Server
- Two network interface cards(NIC)
- TCP/IP protocol stack (this should come with Windows NT Workstation/Server 4.0 CD)
- Appropriate updated Windows NT service pack.

Meridian 1 Core Switch

- Systems running X11 R22 or later
- Ethernet interface

Setup

The following figure is an example of a multi-home (a computer having more than one network interface card) workstation/server Windows NT machine. One network interface card is connected to the private LAN (network ID : 200.45.0.0, class-B subnet). The other resides on a different network ID (192.168.40.0, class-C subnet). All the IP address numbers in the figure are only examples.

You must have different IP address numbers according to your network address scheme. Contact your network administrator for any IP address number assignment.

Note: Windows NT 4.0 Workstation/Server can only route data on two different subnets.

Install two NICs into the Windows NT computer. Refer to the NICs' manuals on how to install the cards and drivers.

In general, configuring TCP/IP protocol for two NICs is the same in both Microsoft Windows NT Workstation and Server. The only difference is that NT workstation only supports static routing, which means the user has to configure the routing table manually, using the 'route' command utility.

Windows NT server supports both static and dynamic routing. Dynamic routing requires installing RIP (Routing Information Protocol) through Network Control Panel. RIP will talk to all neighbor routers and automatically construct and update the routing table.

Windows NT Workstation/Server 4.0 Network Configuration

Open the Control Panel window, and double click on the Network icon. Configure the following data:

Identification tab

Enter identification information.

Computer name: identify the computer name for Microsoft Networking.

Workgroup: set to the workgroup to which the computer belongs.

Protocols tab

Verify that the TCP/IP Protocol is installed.

Refer to the Windows NT documentation for details about installing TCP/IP protocol.

Double click on ‘TCP/IP Protocol’ to open the TCP/IP protocol Properties dialog box.

IP Address tab

The Adapter drop list box now should have two entries for two NIC cards installed earlier. The first NIC is selected as default.

First NIC:

Check 'Specify an IP address'

- IP Address: specify an IP address here; as example, the first NIC is configured as 200.45.20.1
- Subnet Mask: specify subnet mask according to which CLASS is your network; e.g. if class-B, it should be 255.255.0.0
- Default Gateway: leave this field blank.

Select the second entry for the other NIC from the Adapter drop-down list box.

Second NIC:

Check 'Specify an IP address' radio button

- IP Address: enter the IP address for this NIC. For example, as in the diagram, 192.168.40.11
- Subnet Mask: if class-C, set as 255.255.255.0
- Default Gateway: leave this field blank

DNS tab

Enter the DNS server address(es).

WINS Address tab

Enter the WINS server addresses for both subnets.

Routing tab

Check 'Enable IP Forwarding' to enable routing capability on the Windows NT machine.

All the computers belonging to two subnets have to configure their default gateway as the appropriate NIC address. For example, all computers on Network ID (200.45.0.0) will set default gateway as the First NIC (200.45.20.1). Computers on Network ID (192.168.40.0) will configure default gateway as Second NIC (192.168.40.11).

Windows 95 TCP/IP Configuration

Open the Control Panel, double click on the Network icon. This will display the Network dialog.

Configuration tab

Select TCP/IP | Properties.

IP Address: check ‘Specify an IP Address’ and type in the IP address and subnet for this machine.

WINS Config: specify the WINS server addresses here

Gateway: enter the NIC address of the Windows NT router which belongs to this subnet. For example, enter 192.168.40.11, as in the diagram.

DNS Config: enter the DNS server address(es)

Identification tab

Enter the computer name for Microsoft Network

Click the OK button to save all configurations and reboot the machine.

Meridian 1 switch TCP/IP Configuration

As in example figure, the first NIC address will be your M1 switch default gateway. Use Overlay 117 to add the new gateway address into M1 routing table. This will allow the M1 to forward messages back to the PC clients.

The host name and IP addresses below are only *examples*. Consult your network administrator for the actual host names and IP addresses.

1. Use LD 117 to configure an IP address at the M1

```
>LD 117
>NEW HOST M1ACTIVEIP 47.1.1.10
>CHG ELNK ACTIVE M1ACTIVEIP
```

2. Use LD 117 to configure a backup (inactive) IOP

```
>NEW HOST M1INACTIVEIP 47.1.1.11
>CHG ELNK INACTIVE M1ACTIVEIP
```

3. Configure the subnet mask

```
>CHG MASK 255.255.255.0
```

4. Configure a default gateway for M1 in LD117 overlay

```
>NEW ROUTE 0.0.0.0 47.1.1.250
```

5. To view the routing table

```
>PRT ROUTE
```

Troubleshooting

After configuring TCP/IP settings for two NICs, and adding a new route for M1, there are some windows command utilities to test and troubleshoot problems.

Ping command

The 'Ping' utility verifies if the computer is able to communicate to other computers which have TCP/IP protocol installed.

Basic PING command syntax : ping <*IP address*>

You should receive a message similar to the following, where <###.###.###.###> is the computer's IP address you PING:

```
Ping <###.###.###.###> with 32 bytes of data:
Reply from <###.###.###.###>: bytes=32 time=77ms TTL=28
Reply from <###.###.###.###>: bytes=32 time=77ms TTL=28
Reply from <###.###.###.###>: bytes=32 time=77ms TTL=28
Reply from <###.###.###.###>: bytes=32 time=77ms TTL=28
```

If you receive an error message, check that TCP/IP configured correctly, or check the NIC adapter status, reinstall NIC adapters and their drivers. Consult the NIC manuals.

Route command

The 'Route' utility allows you to view, add and delete the entries in the routing table. Enter command at the command prompt and press ENTER.

Example: + 'route print' - to view routing table

Output appears as the following:

```
Active Routes:

Network Address Netmask Gateway Address Interface Metric

0.0.0.0, 0.0.0.0, 47.82.32.1, 200.45.20.11

47.82.32.0, 255.255.240.0, 200.45.20.1, 200.45.20.11

200.45.20.1, 255.255.255.255, 127.0.0.1, 127.0.0.11

47.255.255.255, 255.255.255.255, 200.45.20.1,
200.45.20.11

127.0.0.0, 255.0.0.0, 127.0.0.1, 127.0.0.11

192.168.40.0, 255.255.255.0, 192.168.40.11,
192.168.40.11.1

192.168.40.11, 255.255.255.255, 127.0.0.1, 127.0.0.11

224.0.0.0, 224.0.0.0, 192.168.40.11, 192.168.40.111

224.0.0.0, 224.0.0.0, 200.45.20.1, 200.45.20.11

255.255.255.255, 255.255.255.255, 200.45.20.1,
200.45.20.1 1
```

Traceroute command

The 'TRACERT' command traces the TCP/IP packets to the destination by reporting each router which the packets crossed.

Basic Traceroute command syntax: tracert <*destination IP address*>

You should receive similar messages as below:

```
Tracing route to <destination IP address> over a
maximum of 30 hops:
1 <10 ms <10 ms <10 ms <###.###.###.###>
2 50 ms 50 ms 51 ms <###.###.###.###>
3 70 ms 70 ms 80 ms <###.###.###.###>
4 250 ms 80 ms 50 ms <###.###.###.###>

Trace complete.
```

Where each <###.###.###.###> is the router address the packets crossed. If received a similar messages as following, there must be a problem or configuration error at one of the router on the network. Consult with your network administrator to resolve the problem:

Tracing route to <*destination IP address*> over a maximum of 30 hops:

```
1 <10 ms <10 ms <10 ms <###.###.###.###>
2 * * * Request timed out.
3 * * * Request timed out.
4 * * * Request timed out.
```

or

Tracing route to <destination IP address> over a maximum of 30 hops:

```
1 <10 ms <10 ms <10 ms <###.###.###.###>
2 50 ms 50 ms 51 ms <###.###.###.###>
3 70 ms 70 ms 80 ms <###.###.###.###>
4 <###.###.###.###> reports: Destination net
unreachable.
```

IP Configuration command

The ‘IPCONFIG’ command is available only in Microsoft Windows NT Workstation/Server. This command displays the computer’s TCP/IP settings.

At the command prompt, you can enter the ‘ipconfig /all’ command to list all Windows NT TCP/IP configurations. To get help, enter ‘ipconfig /?’.

Windows IP Configuration command

The ‘WINIPCFG’ command is available in Microsoft Windows 95.
This command list all TCP/IP settings such as IP address, Default Gateway, and WINS servers. At the command prompt, enter ‘winipcfg’ and press Enter.

Appendix C: Windows NT Security Guidelines

This chapter provides a brief overview of the security provided by the Microsoft® Windows NT® operating system environment. It also includes discussions of the general policies recommended by Nortel Networks to maintain a secure environment for your programs and data.

This chapter focuses on areas of special interest to Windows NT system administrators who also perform OTM administration. Refer to the Microsoft Windows NT documentation for additional information about using and administering a Windows NT operating system.

The Windows NT administrator should become familiar with the best practices and caveats discussed in this chapter:

- "Installation" on page 150.
- "General Policies" on page 151
- "Secure the User Accounts on the Windows NT System" on page 151
- "Passwords" on page 153
- "Audit Trail and Security Log" on page 154
- System Services
- Network Sharing
- Networking
- Remote Access

Installation

- Remove hardware components that you consider to be security risks or disable them through the computer BIOS. Assigning a BIOS password is highly recommended.
- Secure the server physically to prevent unauthorized users access inside either the server's case or the room.
- Do not install any other operating system (like DOS, Windows 95, or Linux) on the server.
- Install the computer as a server. Do not install it as a PC controller.
- ALL partitions MUST be formatted with NTFS prior to starting the installation.
- Do not perform a Copy Install, which installs Windows NT by copying the entire system root directory and several other files from one computer to another.
- Apply service packs and security hot fixes when they become available.

General Policies

- Do not share the server's hard drives, CD-ROM, or floppy drive on a network.
- Restrict remote access to the server.
- Prevent unauthenticated remote registry access and Event Log viewing to the server. Do this by defining a registry key, such as "Winreg" or "RestrictGuestAccess."

  To restrict network access to the registry, use the Registry Editor to create the following registry Key

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
  ```
- Do not turn on the registry option "ShutdownWithoutLogon." If customizing your OTM product, do not add a shutdown button on the logon window.
- Do not configure the server for autologon. By default autologon is set to not enabled. Do not modify the registry or use TweakUI to enable autologon.

Secure the User Accounts on the Windows NT System

Windows NT operating systems provide several group accounts that are predefined and ready for use as soon as the Windows NT system software is installed. These group accounts provide increasing levels of access to the data and programs that reside on the Windows NT system.

The access level defined by membership in each predefined group is available to all members of the group, independent of the unit's configuration either as a Windows NT server or a Windows NT workstation.

The NT Administrator account provides the most access to the programs and data that reside on the NT system. A user who has local Administrator rights can add, change, and delete both programs and data from the Windows NT hard drives. Windows NT provides much greater security than that available on Windows 95/98 systems, since the user's access level defines his ability to view and change files on that system. Applications and data files stay hidden from a user who logs on, but whose account does not permit the access level needed to view those files and applications.

Allow Administrative Rights to Administrators Only

Severely limiting the number of users who have administrative access to the Windows NT system is very effective in controlling undesired local access to it.

Membership in the Windows NT Administrator group account is required only when a user will access OTM Navigator directly, either through the web or by using the OTM Windows NT system as a workstation.

Note: Windows clients who connect remotely to an OTM Windows NT server *do not* require Administrator group accounts.

Follow these guidelines to maximize the security of the Windows NT system.

- define the individual user accounts with just enough rights to allow the user to complete their tasks.
- limit membership in the Administrator group to those who must have it.
- select a random combination of letters and numbers as the Administrator account password, and guard it carefully.
- do not leave the system unattended while you are logged on as administrator. Log off the system or lock the workstation using an administrator password. Windows NT is supplied with a password-protected screen saver utility.

  Note: When exiting from OTM, the administrator will be prompted to either log out of OTM or terminate OTM. If OTM is scheduled to complete any other tasks, such as Station Administration Synchronization, ESN or Traffic, you should log out of the system but not terminate, as OTM will continue to run in the background and complete the scheduled tasks.

- OTM Web administrators should be added to the local administrators group. Other technical staff who use the OTM Web can be added to other user-defined NT groups that have lesser privileges.
- OTM Desktop Users (end users who view their telephone information using OTM Web Navigator) do not need to belong to user groups with high privileges.

Here are some specific actions the administrator can take to maintain a secure Windows NT system:

- Assign at least an 7 character password that is composed of random, printable keyboard symbols, intermixing uppercase and lowercase. Do not use common names, dates, or words found in a dictionary.
- Confirm that the Guest account is disabled. That account is disabled by default on Windows NT systems, but *enabled* by default on Windows 95/98 systems.
- The Administrator should lock the workstation when not in use. The "Blank Screen" screen saver that comes with Windows NT can be set to automatically password protect the desktop when inactive. Using any other or third party screen savers is not recommended and it can seriously hamper the performance of your server.
- Rename the local NT Administrator logon account that is included with your NT operating system. Do not share the new account name with non-administrators. This will help limit exposure if the Administrator account password is discovered.
- Do not grant additional access rights to any user who is added to the Backup Operator account. That account provides just enough access to back up and restore files.

  In addition, the administrator can remove rights granted to the predefined groups, when those rights are not required. For the Backup Operator group, remove rights to back up and restore files and directories when the group does not need them.
- Limit the rights granted to users when creating their individual accounts, not just when adding them to groups.

Passwords

- Set up a minimum password length (at least 8 characters).
- Choose unique passwords by combining letters, numbers and punctuation. Do not use words found in a dictionary, or names of people or pets.
- Set up a maximum password age (< 45 days).

Note: Be careful to renew the Administrator password before it expires, or you will be locked out of the system.

- Set password locking in the account policy. This provides automatic lockout after 5 unsuccessful logon attempts in a row.
- Protect the Hashed Password file from hackers by securing the backup copies that are created in Winnt\system32\Config and Winnt\Repair directories.

  Delete the predefined group named Everyone from the accounts that have permission to access those directories.

Audit Trail and Security Log

- Focus on auditing failures, since most hackers use trial and error in their attempts to gain access. Use the OTM Event Viewer to check this on a regular basis.
- Dedicate at least 10 MB of storage for security log settings.
- Use Event Viewer to regularly monitor the audit trail file size. Save the file to long term storage (like magnetic tape), and then clear the contents from the original file that is on the Windows NT system.

System Services

- Disable unnecessary services that run on a regular basis (such as Messenger and alerter).

  Consult the Windows NT system documentation to determine which ones are not needed on this system. Windows NT provides many preinstalled services during the standard system installation.

Network Sharing

- Minimize the number of shared files and folders on the system. Regularly review the Access Control List (ACL) share permission settings for those files, and change or remove the shared settings if security might be an issue.
- Avoid sharing the system root directory. If an application requires this, tighten the ACLs of the root directory.
- Hide any sensitive file sharing by appending $ to the end of sharename. Only those with Administrator rights can see these files.

Networking

- Restrict access from the network. Using the User Manager and the User Rights command, restrict “Access this computer from the network” to the absolute minimum necessary
- Prevent Windows NT from passing cleartext passwords across the network.Windows NT has the ability to communicate with certain non-Windows NT systems that require sending user password unencrypted over the network.

  This feature is disabled by default, and Nortel Networks recommends that the administrator keep that setting.
- Use any available router security features, and if possible, implement a firewall to secure your intranet from the public Internet.

Remote Access

The Remote Access Service (RAS) in Windows NT provides sophisticated security features, such as password encryption, data encryption, and call back security.

- Data encryption:
  Require Microsoft encrypted authentication on the RAS server and select the option Require Data Encryption.
- TCP/IP configuration:
  Allow external users to access the OTM server only, not the entire network.
- Restrict Access:
  Grant remote access capabilities only to users who require it to use the system.
- CallBack:
  Predetermine a client's number before allowing access to the LAN by using the Remote Access Admin.
- Auditing:
  RAS generates audit trails of remote connections. Audit Remote Access activity by using the Windows NT Server Event View utility.
  The administrator can stop the RAS resource if there are no remote users.

NT Option Pack 4—IIS

The NT Option Pack contains Microsoft's Internet Information Server (IIS), which is the Web Server used on OTM.

List of NTFS Permissions Required at an IIS Site

This article lists the proper Windows NT File System (NTFS) access permissions required at an Internet Information Server (IIS) Web or FTP site.

Note: When IIS is installed, it creates the proper NTFS access permissions for the default Web and FTP sites for the anonymous (IUSR_<computer_name>) and, if applicable, application owner (IWAM_<computer_name>) user accounts.

The administrator does not need to change the permissions for normal OTM operation that are set during OTM installation. If the administrator needs to change sharing or access permissions, he should refer to the guidelines described earlier in this chapter.

Grant the IUSR_<computer_name>, and related groups (if any) the following directory permissions:

Table 5
Directory Permissions

Directory	Permissions
Inetpub\Wwwroot	READ (RX) (see 3 below)
Winnt	READ (RX)
Winnt\System32	READ (RX)
Winnt\System32\Inetsrv	READ (RX)
Winnt\System32\Inetsrv\Asp	READ (RX) (and all subdirectories)
Program Files\Common Files	READ (RX) (and all subdirectories)

- Do not alter security permissions on Nortel Networks OMServices and its sub directories
- This directory is set as the root of your Web Server
- Do not give Write, Execute or Browse permissions to Web directories from the Internet Service Manager (Management Console for IIS).
- Do not change the Anonymous User access account to other than the default (IUSR_<computer_name>).
- Changing the installation defaults is not recommended, and administrators should take great care if they decide to do so.

List of Services Needed to Run a Secure IIS Server

The following list outlines which services are required, as well as those that are not required, and those that may be required, to run Internet Information Server (IIS) version 4.0 on a secure server. Your particular network or system configuration can change some of the parameters. For example, some intranets require WINS and DHCP.

The more services that are running on a computer, the more entry points are available to malicious attack. A service is a potential entry point because it processes client requests. To help reduce this risk, disable unnecessary system services.

For more information refer to the security chapter from the *Internet Information Server 4.0 Resource Kit*.

Table 6
Services that can Run on a Secure IIS Server

Required	May Be Required	Probably Not Required
Event Log	Certificate Authority (required to issue certificates)	Alerter
IIS Admin Service	Content Index (required if using Index Server) *	ClipBook Server
License Logging Service	FTP Publishing Service Web services run on different servers)	Computer Browser
MSDTC	FTP Publishing Service *	DHCP Client
Protected Storage	NNTP Service (required if using NNTP Service) *	Messenger
Remote Procedure Call (RPC) Service	Plug and Play (recommended, but not required)	NetBIOS Interface
Server	Remote Access Services (required if you use dial-up access)	Net Logon
Windows NT Server or Windows NT Workstation	RPC Locator (required if doing remote administration)	Network DDE & Network DDE DSDM Front Page extensions

Table 6 (Continued)
Services that can Run on a Secure IIS Server

Required	May Be Required	Probably Not Required
Windows NTLM Security Support Provider	FTP Publishing Service Web services run on different servers) *	Network Monitor Agent
Workstation	FTP Publishing Service *	NWLink NetBIOS
World Wide Web Publishing Service	Certificate Authority (required to issue certificates)	NWLink IPX/SPX Compatible Transport (not required unless you don't have TCP/IP or another transport)
Event Log	Content Index (required if using Index Server) *	Simple TCP/IP Services
IIS Admin Service	Telephony Service (required if access is by dial-up connection)	Spooler
	Workstation (optional; important if you have UNC virtual roots)	TCP/IP NetBIOS Helper
	Uninterruptible Power Supply (optional; but it is recommended that you use a UPS)	WINS Client (TCP/IP)

*: Not required by the OTM Server nor recommended by Nortel Networks.

Nortel Networks strongly recommends that the OTM administrator store no installation application software on the OTM server or workstation, other than Nortel approved software.

Appendix D: Modem Configuration for OTM Applications in Microsoft Windows

To insure that a modem is configured correctly for use with Microsoft Windows 95, Windows 98, or Windows NT Workstation 4.0, use the modem control panel to configure it. The modem control panel will search for and detect a connected modem automatically, and then store the configuration information in the registry for other Windows applications to access.

The same is also true for OTM applications, where the modem configuration information is obtained by searching the Windows registry with the COM port specified in the communication profile. OTM communications software will then set up the Run-Time-Container (RTC) with the modem initialization string and communication profile settings for the application to make its connection to the Meridian 1.

However, there are a number of limitations with this process that the user must take into account when configuring the modems:

- The Windows Modem control panel allows multiple modems to be configured on the same COM port.

  OTM software will always use the first modem found in the registry configured for the specified COM port in the communications profile. To insure proper modem operation, only one modem/communication device should be configured on a given COM port.

- A factory modem initialization (INIT) string is stored in the Windows registry. This INIT string will be used by OTM applications to set up the modem connection.

  The OTM communications software is written to use verbal (V1) result code. If the factory INIT string is set to use numeric (V0) result code, the "Can't set modem parameters" error code will occur and the dial up attempt will be aborted. To modify the factory INIT string, the user must use the registry editor (regedit) to change the factory INIT string to use verbal (V1) result code. Please see the Microsoft Windows documentation for detailed instructions on how to use the Registry Editor or use the instructions below.

- When searching the modem configuration information in the Windows registry, the "AttachedTo" string value is used to identify which COM port is attached to the modem.

  For a PCMCIA modem, this "AttachedTo" string value may not be available in the registry. As a result, no modem will be found during the search and the RTC will only contain the communication profile settings. To correct this problem, the user must use the registry editor (regedit) to add this "AttachedTo" string value of the COM port configured for the PCMCIA modem. Please see the Microsoft Windows documentation for detailed instructions on how to use the Registry Editor or use the instructions below.

High-speed smart modem configuration consideration

As modem technology progresses, the new generation of high speed modems provide additional functionality to achieve the highest possible connection rate. These high speed smart modems use various tones during the handshaking period to negotiate the speed and protocol.

An area needing extra attention is the modem configured on the Meridian 1 SDI port. In most cases, the modem attached to the M1 SDI port is configured to run in dumb mode at the same speed the M1 SDI port is configured for (at 9600 bps or less). This locks the modem into a specific mode of operation to prevent the modem being run in command mode (echo input) or connecting at a different baud rate than the M1 SDI port is configured for.

When a high speed smart modem is used on the OTM PC to dial up the M1 modem, the PC modem will always attempt to connect at its highest possible speed. The switch modem, however, can only connect at the configured speed. So, during the modem online handshaking period, the PC modem will send out different tones to negotiate the speed and protocol, and the switch modem will connect at its configured speed and ignore additional attempts. Once the switch modem is connected, any additional handshaking tones sent by PC modem get translated into data (garbage under this condition) and forwarded to M1 SDI port. These garbage characters may eventually lock up the M1 SDI port. The two modems may still connected, but access to the M1 overlay input is no longer possible.

To avoid this type of problem, the key is to maintain modem compatibility. Here are some recommended steps to avoid potential problems and increase the connection success rate.

- The PC modem should be configured to match the switch modem's settings.
- The speed between the M1 SDI port and switch modem is locked to the M1 SDI port's baud rate if a high speed modem is installed on M1 SDI port.
- To minimize the garbage characters after carrier detect or carrier lost situations, set your modem S9 register to a higher value (for example, 30 = 3 seconds) and S10 register to a lower value (for example, 7 = 7/10 of a second). Note: when increasing the value of S9 register, you may need to do some timing adjustments on some of the modem/buffer equipment scripts.

Troubleshooting modem connections

Modem does not dial

- Verify that your modem is configured to be on the correct COM port on the Control Panel, Modems, Properties, Communications property sheet.

  Test the COM port to which your modem is connected by launching Hyperterminal (under **Start/Programs/Accessories/Hyperterminal**). Hyperterminal prompts you for a connection name and presents you with the phone number property sheet. In the Connect Using drop down list box, select **Direct to COM X**, where X is the COM port to which your modem is connected. Once you are in the terminal, you should be able to type the command **AT** and see the "OK" response back from the modem.

- If your modem does not respond, you may be using the wrong COM port. Go to the File/Properties menu and select **Direct to COM Y,** where Y is a different COM port. Once you have located the correct COM port, go back to OTM Navigator and bring up the properties for the system to which you are trying to connect. Click on the communication tab and select PPP or Serial from the communication profile list. Verify that the COM port you selected for this profile is the COM port that you located your modem on using Hyperterminal. Verify that the baud rate matches the settings for the M1 port into which you will dial.

- If the modem still does not dial, follow the steps above to establish a Hyperterminal connection. After issuing the **AT** command and receiving the "OK" prompt, issue the command **ATDT1234567**, where 1234567 is the phone number for the modem connected to the M1. If you do not hear the modem dialing and connecting at this point, verify that your phone line and modem cables are correctly connected. If the modem dials and connects, verify that you have dial-up-networking installed along with a dial-up-adapter.

Modem dials and connects but the connection details button reveals that scripting failed while waiting for a prompt

- Verify that the baud rate configured for the TTY on the switch matches the baud rate configured for the modem in the Navigator/System Properties/Communication property sheet/PPP or Serial profile for the system to which you wish to connect. Make sure that the data bits, stop bits, and parity match as well.

Modem dials but does not connect

- Verify that the phone number you are dialing is not busy.
- Verify that you have included all necessary digits in the phone number. Check in Navigator/System Properties/Communication property sheet/PPP or Serial profile for the system to which you wish to connect.

Modem dials and connects and the scripting is completed successfully, but the Connection Details button reveals that the session failed

- Verify that the IP address that you assigned to the local PPP interface on the M1 is the same as the IP address you entered in the address field on the Navigator/System Properties/Communication property sheet/PPP profile for the system to which you wish to connect.
- If possible, verify that you can make an Ethernet connection to the same switch.

  After establishing a PPP connection, but before canceling the connection dialog: Open a DOS command prompt (**Start/Programs/MS-DOS Prompt**) and run the ping command by typing **ping 47.1.1.10** where 47.1.1.10 is the M1's local IP address in this examples (see "Configuring Ethernet and PPP at the Meridian 1"). Verify that the data lights on your modem flash as the ping data is sent to the Meridian 1. If you do not receive a response from the M1, verify that the IP address that you assigned to the local PPP interface on the M1 is the same as the IP address you entered in the address field on the Navigator/System Properties/Communication property sheet/PPP profile for the system to which you wish to connect.

Modem dials and connects but you receive the error message "Error writing to COM port" or "Error reading from COM port".

- Verify that the modem you installed in the Control Panel matches your modem type. Remove your installed modem driver and install a generic modem driver in its place.

  From the Control Panel/Modems, click the **Remove** button to remove your modem from the installed list. Click **Add** (to add a new modem driver). Click the check box that says "Don't detect my modem; I will select it from a list" and then click **Next** to move to the next step. Select the standard modem driver matching your modem's baud rate (for example, Standard 14400 bps Modem) and click **Next** to move to the next step. Select the COM port to which your modem is connected, and click Next. Click **Finish** to complete the modem installation. Restart the system, and try to establish a PPP or Serial connection.

Appendix E: Integrating OTM with Optivity NMS

Nortel Networks provides Unified Networks, a solution that integrates voice, video, and data networking through one network management system. The Unified Networks solution lets you manage LAN, WAN, and voice networks as an integrated system. This convergence achieves greater efficiency and reduces operational cost--a transition from today's disparate data and voice networks.

Optivity Telephony Manager (OTM) integrates with Optivity Network Management System (NMS) version 9.0.1 and above. Optivity NMS is a campus and enterprise-level network management solution providing fault, performance, configuration, and security management for Nortel Networks internetworking devices. Now through Optivity NMS, you can monitor your OTM Servers.

This chapter describes what you should know about integrating OTM with Optivity NMS. It includes the following information:

- See “How the OTM with Optivity NMS Integration Works” on page 170.
- See “Integration Requirements” on page 171.
- See “What Happens During the OTM Installation” on page 172.
- See “Checklist for Installing the OTM Integration” on page 172.
- See “About oitInstall” on page 173.
- See “Alarm Integration” on page 174.
- See “Using Optivity NMS InfoCenter” on page 174.
- See “Starting OTM Web Applications” on page 176.
- See “Removing an OTM Server” on page 177.

How the OTM with Optivity NMS Integration Works

OTM Alarm Manager receives Simple Network Management Protocol (SNMP) traps from managed Meridian 1 entities. Through Alarm Notification, OTM sends filtered traps to Optivity NMS.

Using Optivity NMS InfoCenter, you can manually add OTM Servers into the Telephony Managers Resources folder. Properties information that you add about the OTM Servers is added to the Optivity NMS database. For more detailed information about the Optivity NMS documentation, in your Web browser go to *support.baynetworks.com/library/tpubs/*. Go to the Optivity Network Management & IP Services section, then Optivity NMS, and System 9.0.1.

InfoCenter graphically identifies when a device is in an alarm state. Using Optivity InfoCenter, you can set the color for alarm levels. When a device is in an alarm state, you can right-click it to open an Optivity NMS fault management application. For instance, you can start Fault Summary that graphically lists faults for the selected device. You can also set the fault management categories for alarm monitoring.

Integration Requirements

This section lists the conditions upon which OTM integrates with Optivity NMS optimally:

- For optimum performance, install OTM on a separate machine from Optivity NMS. In this configuration, manually copy the OTM Optivity Integration Toolkit (OIT) files onto NMS and run OitInstall. For more information, view the Readme information file in the \Optivity directory on the OTM 1.0 CD-ROM.
- OTM integrates with Optivity NMS through OIT on any NMS platform - see “Checklist for Installing the OTM Integration” on page 172. Co-residence with Optivity NMS, however, is supported only on Windows NT Server.

  Note: There are certain restrictions in OTM application features when installed co-resident with Optivity NMS. For more information about these restrictions, refer to the *Optivity Telephony Manager (OTM) 1.0 General Release Bulletin*.
- All software requirements for OTM should be met. In particular, Windows NT Service Pack 5, Windows Option Pack 4, and MS Internet Information Server (IIS). Install IIS before applying the service pack.
- Always install Optivity NMS prior to installing OTM.
- The OTM installation, upon detection of an Optivity NMS installation, automatically configures itself to co-reside with Optivity NMS.
- Optivity NMS and OTM use different Web servers – Apache and IIS respectively. When installing IIS, make sure to modify the default port for HTTP requests to avoid a conflict with Apache.
- Change the Optivity NMS Apache Web server HTTP port from the default value of 80 prior to running IIS (Windows NT Option Pack 4) installation. Or you may want to change the default port on IIS during installation instead.

What Happens During the OTM Installation

The OTM installation program automatically updates Optivity NMS with the new OIT files when installed on the same machine as Optivity NMS. If you want to install OTM on a different machine than Optivity NMS, manually copy the OTM OIT files onto NMS and run oitInstall. The procedure is documented in a Readme contained on the CD with the OIT files or see the following section.

Checklist for Installing the OTM Integration

This is the checklist for OTM installation on an existing Optivity NMS server.

You can install OIT files for OTM on any platform that runs Optivity NMS as long as it supports the Java Runtime Environment required by OTM Web Applications (JRE 1.2). In this case the user should follow the steps in this section.

In the case of co-residence (only possible on Windows NT) the user only needs to understand the prerequisites and install OTM - OTM installation takes care of the OIT integration steps. Steps 1 through 6 as shown here are then not required.

1 Log into Optivity NMS as Administrator.

2 Check for $LNMSHOME. If this environment variable is present, Optivity NMS is installed and functional.

In Windows NT, view environment variables using the System option in Control Panel on the Environment Variables tab. This variable holds the path of the Optivity installation. Typically c:\Optivity\NMS. All the executables are located in c:\Optivity\NMS\bin.

3 Check for $OITHOME. This environment variable points to the Optivity Integration Toolkit home directory. Typically C:\Optivity\oit. If you cannot find $OITHOME, create it.

4 Copy OTM OIT files to the appropriate sub directories in $OITHOME.

Copy all of the sub directories under \NorMat\Optivity\Oit\ to $OITHOME

5 Run $LNMSHOME\bin\oitinstall -u <full path of OTM OIT file>.

Where -u indicates to upgrade Optivity NMS. If you do not specify the -u parameter, as syntax check only is performed on the OIT file.

This command updates the Optivity NMS database with the new definitions.

6 Proceed with OTM installation, checking for prerequisites (IIS, for instance) as always.

About oitInstall

Optivity NMS includes an program, oitInstall, that extracts the information that Optivity NMS needs for new device application support. This information includes:

- Database schema definitions
- MIB information
- Trap information
- Device management application launch points from within Optivity NMS applications.
- Device discovery information (for OTM, you must manually add the OTM Server.)

The oitInstall program does the following:

- Automatically stops and restarts all Optivity NMS daemons (UNIX) services (Windows).
- Automatically backs up the Optivity NMS databases (by default /usr/oit/oitdb (UNIX) and C:\Optivity\oit\oitdb for Windows. The oitInstall program automatically restores the database if the device support upgrade installation fails.
- Updates Optivity NMS with two new files: new device and device management support, and deletes the database backup if the integration is successful.

OIT definitions for OTM reside in $OITHOME\OTM\omt.oit. It also contains the file rfc1213.mib.

The $OITHOME environment variable is typically C:\Optivity\oit on Windows NT systems and /usr/oit on UNIX.

For platforms other than Windows NT, OIT definitions are updated into Optivity NMS by manually placing the OIT files into the appropriate directories and starting oitInstall from command line.

Alarm Integration

OTM filters and then forwards Meridian traps to Optivity NMS. Since OTM forms the main representative agent for Meridian Voice Switches, all alarms received by Optivity NMS result in the change of status state of OTM depicted in Optivity InfoCenter.

When Optivity NMS and OTM co-reside on the same server, the OTM Trap system disables its Trap Server and instead interfaces with the Optivity Trap Server to receive traps.

Upon receiving a Meridian alarm (or other traps that it has been configured to handle), OTM reformats it and forwards it to Optivity NMS. Optivity NMS recognizes the trap (from OIT definitions) and should now be able to reflect the changed status

Using Optivity NMS InfoCenter

Once OTM is integrated with Optivity NMS with the OIT definition files, you must manually add OTM server objects to the Telephony Managers resource folder in InfoCenter. The OTM integration does not support Autodiscovery of these objects.

Add an OTM server resource for every OTM server that you integrate with Optivity NMS.

Adding new OTM servers to Optivity is done through the Wizards provided in Optivity 9.0.1. These wizards automatically take care of establishing the Device-Agent-Interface relationship in Optivity databases.

A Telephony Managers folder is created in Optivity InfoCenter to contain all the Voice Elements integrated into Optivity (OTM in this case).

Creating an OTM Server Object In Optivity NMS InfoCenter

If Access Control is enabled, you must have a valid local user account (user name and password) and an Optivity NMS user account to log into InfoCenter.

1 From the Windows Start menu, choose Programs > Optivity > InfoCenter.

The Optivity NMS InfoCenter login window opens.

2 Type your user name, password, and the name of the Optivity NMS server and click OK.

Optivity InfoCenter opens.

3 In the Folders pane, click the InfoCenter icon.

4 Double-click the Resources folder to open it.

5 A Telephony Managers folder appears.

A Telephony Managers folder is created in Optivity InfoCenter to contain all the Voice Elements integrated into Optivity.

6 Double-click the Telephony Managers folder to open it.

7 Modify the default view properties of the folder or you will not be able to view the OTM Servers that are added to this folder.

Right-click the Telephony Managers folder and choose Properties. Open the Management Server folder. Select Optivity Telephony Manager, and click Apply.

8 From the InfoCenter menu bar, choose File > New > Object.

The Object Properties dialog box opens with the Device tab displayed.

9 In the Label box, type a label for the new object.

10 In the Type box, select the Management Servers object type.

11 In the Subtype box, select a Optivity Telephony Manager subtype for the object.

12 In the IP address box, type the IP address of the object.

13 Click Private or Global.

Private lets the local user see the device. Global lets all users see the new object.

14 Click OK. A default switch icon appears for the OTM Server.

Viewing OTM Server Object Properties

Follow these steps to view the properties of an OTM Server in InfoCenter.

1 In InfoCenter, open a folder in the Folders pane.

2 Select the OTM Server that you added.

3 From the InfoCenter menu bar, choose File > Properties.

The Object Properties dialog box opens, displaying the properties for the selected network object.

4 Click OK.

Modifying OTM Server Object Properties

Follow these steps to modify the properties of an OTM Server in InfoCenter

1 In InfoCenter, open a folder in the Folders pane.

2 Select the OTM Server that you added.

3 From the InfoCenter menu bar, choose File > Properties.

The Object Properties dialog box opens, displaying the properties for the selected network object.

4 Edit the object properties that you want.

5 Click OK.

Starting OTM Web Applications

You can start OTM Web Applications by choosing a Web Browser from the shortcut menu on the OTM icon in Optivity InfoCenter.

The Web applications are started in a separate command shell to avoid a conflict between the two Java Runtime Environments.

Java Runtime Environment

OTM Web applications require Java Plug-In 1.2.1 on the client browser. This Plug-In is downloaded and installed on the client machine when the user connects to the OTM server for the first time.

Optivity NMS uses JDK 1.1.x that is older than the version used by OTM. OTM Web applications, started from Optivity NMS, run in the new Java Runtime Environment.

Web Server

Optivity NMS uses Apache Web Server for its Web applications, whereas OTM uses Internet Information Server (IIS) from Windows NT Option Pack 4.

Removing an OTM Server

1. In InfoCenter, open a folder in the Folders pane.
2. Select the OTM Server that you want to delete.
3. From the InfoCenter menu bar, choose File > Delete. This action deletes the object from the Optivity

Appendix F: OTM Engineering Guidelines

This appendix helps you to get the most out of Optivity Telephony Manager. It provides a set of guidelines to help you determine the configuration and distribution of OTM servers within a network to efficiently manage Meridian 1 systems.

This appendix includes the following sections:

- "Capacity Factors" on page 179
- "Sample walk-through of computations" on page 181
- "Software Limits" on page 189
- "Operational Limits" on page 190
- "PC Hardware" on page 192
- "OTM Server Minimum Hardware Requirements" on page 193
- "Network Bandwidth" on page 199

Capacity Factors

This appendix examines the following areas where capacity is a factor:

- Features running on the OTM Server and their impact to its resources, such as CPU usage, physical memory (RAM) and disk storage

Note: Analysis was performed on the majority of OTM features. To simplify analysis, only those features are highlighted here that impact these resources

- Web and OTM Clients and their impact on OTM Server Resources
- Meridian 1 and its impact on OTM Server Resources
- Communications between the OTM Server and Meridian 1, OTM/Web Clients, LDAP Server, etc. and their impact on the network to which they are connected.

Based upon this analysis, recommendations are made as to:

- The resources required on the OTM Server
- The number of Clients and Meridian 1's that can be connected to a single OTM Server
- Network bandwidth and routing considerations

The analysis is presented in a set of tables containing the results of benchmark testing. These tables can be used to calculate, for various OTM Server usage scenarios, the resources and connections possible. To aide in this process, this appendix analyzes four typical OTM Server configurations. Using these configurations as examples and the raw table data, you can extrapolate configurations specific to a given customer/distributor setup.

These guidelines provide minimum PC configurations for the OTM Server, OTM Client, Web Client and OTM running in a stand-a-lone mode. **The resource calculations presented herein are centered around the OTM Server, running on a Windows NT Server Platform.**

A table is provided that lists the limitations of running the OTM Server on a Windows NT Workstation, however, the analysis presented here does not cover this platform.

Note: OTM running in a standalone mode will function in a manner that provides access to Meridian Administration tools (MAT)-equivalent features only. As a result, the engineering rules for this setup will mimic those required for MAT. Refer to the MAT Engineering Guidelines for details.

Sample walk-through of computations

This section provides a sample walk-through of computations used to determine how many Meridian 1 and OTM Clients can be connected to an OTM Server. Factors involved include

- Type of OTM feature configuration
- Type of OTM Server and Meridian 1 hardware
- Constraints on CPU usage and off-hours work.

Sample configurations based on application usage and features

The following are the sample configurations based upon application usage and features that impact server resources. These configurations do not reflect how OTM is packaged (for example, Basic, Enhanced, and Premium).

Example 1:

Configuration
Station, ITG, Maintenance Windows, and other applications

Example 2:

Configuration and Alarms Management

Example 3:

Configuration and Alarms Management with Web/OTM Client Access and LDAP Service (Full OTM System)

Example 4:

Alarms Management, Data Buffering & Access (DBA), Call Accounting, traffic
OTM as a Buffer Box replacement (Access Server)

Sample PC and Meridian 1 configurations

The following are the PC and Meridian 1 configurations used for this example:

- OTM Server and OTM Clients connected to a 100 MB network, utilizing no more than 35% of its bandwidth

Note: Refer to Figure F-3 “Connecting OTM to CWAN connected Meridian systems” on page 202.

- 512 Mbytes of physical memory
- ATAPI Hard Disk
- Option 11C averaging 400 lines per switch
  - — Averaging 1 call records/second generated (peak is 6)
- Option 81 with CP4 averaging 2000 lines per switch
  - — Averaging 3 call records/second generated (peak is 32)

Operational constraints

The following are the operational constraints:

- During normal operation do not use more than 80% of the CPU for routine operations to leave time to perform other routine operations. For example, Maintenance windows and ITG configuration.
  Routine operations as defined in Table F-3, “PC Performance by Application,” on page 191 are:
  - — Station Add/Move/Change from server
  - — Station Add/Move/Change from OTM Client
  - — Station web access
  - — Alarms monitoring
  - — CDR and Traffic Collection
- Off-hours operations can use 100% of the CPU, and will be limited as follows (from Table F-3):
  - — Station update will be performed once a week, on the weekend (for these examples, reserve the time from 9 p.m. on Sunday to 6 a.m. Monday, or 9 hours)
  - — Assume, for Option 11C that OTM can run Station update for two Meridian 1 devices simultaneously (based upon processor speed and CPU usage figures)

— CDR Reports will be performed once a day. (For these examples, off-hours from 12 a.m. (midnight) to 6 a.m., or 6 hours).

— LDAP Sync will be performed once a week; on the weekend (for these examples, reserve the time from 9 p.m. Sunday to 6 a.m. Monday, or 9 hours)

Table F-1 and Table F-2 provide OTM capacity estimates, based upon the information provided in the succeeding sections, and using the configuration examples previously defined. In the numbers presented, the most limiting factor from routine operation, off-hours operation and network bandwidth is entered into the tables. The numbers in these tables were calculated as follows:

Table F-1
Maximum configuration for an Option 11C network averaging 400 lines per switch

Configuration Example	Number of M1s	Number of Lines[a]	Number of simultaneous OTM Clients
1	26	10,800	
2	26	10,800	
3	26	10,800	20
4	6	2,600	

a. Assumes two simultaneous switches.

Table F-2
Maximum configuration for an Option 81 network averaging 2000 lines per switch

Configuration Example	Number of M1s	Number of Lines	Number of OTM Clients
1	5	10,800	
2	5	10,800	
3	3	6,480	20
4	2	4,400	

Configuration Calculations

Example 1

Option 11C = 26 M1s or 10,800 lines

- Routine operation:
  - — Add/move/change = ~1% per switch
  - — 80% CPU time/1% per switch = 80 switches
- Off-hours operation:
  - — Station update = 1 record/6 seconds
  - — 9 hours = 32,400 seconds
  - — 32,400 seconds * 1 record/6 seconds = 5,400 records (lines)
  - — 5,400 lines/400 lines per switch X 2 simultaneous switches ~= 26 switches

- Network bandwidth:
  - Station (peak) operations = 40 Kb/second
  - Network = 100 Mb/second
  - % usage per switch = 40 Kb/second/100 Mb/second ~= 0.05%
  - 35% allowed usage/0.05% per switch ~= 700 switches

Option 81 = 5 M1s or 10,800 lines:

- Routine Operation:
  - Add/move/change = ~2.5% per switch
  - 80% CPU time/2.5% per switch = 32 switches
- Off-hours operation:
  - Station update = 1 record/3 seconds
  - 9 hours = 32,400 seconds
  - 32,400 seconds * 1 record/3 seconds = 10, 800 records (lines)
  - 10,800 lines/200 lines per switch ~=5 switches
- Network bandwidth:
  - Station (peak) operations = 80kb/second
  - Network = 100 Mb/second
  - % usage per switch = 80 Kb/second/100 Mb/second~=0.1%
  - 35% allowed usage/0.1% per switch ~=350 switches

Example 2

The average alarms usage impact on routine, off-hour and network bandwidth is negligible. Use the same calculations as Example 1.

Example 3

Option 11C = 26 M1s or 10,800 lines

- Routine operation:
  - — Add/move/change = ~1% per switch
  - — 80% CPU time/1% per switch = 80 switches
  - — OTM Client usage on OTM Server + ~4% per switch (80% CPU time/4% per Client = 20 OTM Clients)
- Off-hours operation:
  - — Station update = 1 record/6 seconds
  - — OTM Client station update = 1 record/5 seconds
  - — LDAP Sync operation = 10 records/5 seconds (for 100,000 records~= 2.8 hours
  - — 9 hours = 32,400 seconds
  - — 32,400 seconds X 1 record/6 seconds = 5,400 records (lines)
  - — 5,400 lines/400 lines per switch * 2 simultaneous switches ~= 26 switches
- Network bandwidth:
  - — Station (peak) operations = 40 Kb/second
  - — LDAP Sync operation = 720kb/second (% usage of network~=0.7%)
  - — Network = 100 Mb/second
  - — Percent usage per switch = 40 Kb/second/100 Mb/second ~= 0.05%
  - — 35% allowed usage/0.05% per switch ~= 700 switches

Option 81 = 3 M1s or 6,480 lines:

- Routine Operation:
  - Add/move/change = ~2.5% per switch
  - 80% CPU time/2.5% per switch = 32 switches
  - OTM Client usage on OTM Server + ~4% per switch
    (80% CPU time/4% per Client = 20 OTM Clients)
- Off-hours operation:
  - Station update = 1 record/3 seconds
  - OTM Client station update = 1 record/5 seconds
  - LDAP Sync operation = 10 records/second
    (for 100,000 ~=2.8 hours)
  - 9 hours = 32,400 seconds
  - 32,400 seconds * 1 record/3 seconds = 6,480 records (lines)
  - 6,480 lines/2000 lines per switch ~=3 switches
- Network bandwidth:
  - Station (peak) operations = 80kb/second
  - LDAP Sync operation = 720kb/second
    (% usage of network ~=0.7%)
  - Network = 100 Mb/second
  - Percent usage per switch = 80 Kb/second/100 Mb/second~=0.1%
  - 35% allowed usage/0.1% per switch ~=350 switches

Example 4 configuration calculations

Option 11C = 6 M1s or 2,600 lines

- Routine operation:
  - Add/move/change = ~1.5% per switch
  - 80% CPU time/1.5% per switch = 53 switches

- Off-hours operation:
  - Parsing plus Cost Report = 20 records/second
  - 18 hours of call collection operation = 64,800 seconds
  - 64,800 seconds * 1 call record/second/switch = 64,800 call records per switch
  - 6 hours of report generation = 21,600 seconds
  - 21,600 seconds * 20 records/second = 432,000 call records in 6 hours
  - 432,000 call records at 64,800 call records/switch ~= 6 switches
- Network bandwidth:
  - CDR plus traffic (peak) operations = 59 Kb/second
  - Network = 100 Mb/second
  - Percent usage per switch = 59 Kb/second/100 Mb/second ~= 0.05%
  - 35% allowed usage/0.05% per switch ~= 700 switches

Option 81 = 2 M1s or 4,400 lines:

- Routine Operation:
  - CDR plus traffic = ~3.5% per switch
  - 80% CPU time/2.5% per switch = 23 switches
- Off-hours operation:
  - Parsing plus Cost Report = 20 records/second
  - 18 hours of call collection operation = 64,800 seconds
  - 64,800 seconds * 3 call records/second/switch = 194,400 call records per switch
  - 6 hours of report generation = 21,600 seconds

— 21,6000 seconds * 20 records/second = 432, 000 call records in 6 hours

— 432, 000 call records/194,400 call records per switch ~= 2 switches

- Network bandwidth:

  — CDR plus traffic (peak) operations = 118kb/second

  — Network = 100 Mb/second

  — Percent usage per switch = 118 Kb/second/100 Mb/second~=0.1%

  — 35% allowed usage/0.1% per switch ~=350 switches

Software Limits

Hard-coded Limits

The following are the known hard-coded limits in the OTM software:

- Data Buffering & Access (DBA)

  — Connect to 256 M1s

  DBA can perform all functions, CDR, Traffic, Backup and restore, etc. using one connection per Meridian 1.

- Corporate Database

  — 20 Organizational Levels

- Call Detail Recording (CDR)

  — 2.5 Million Call records per costing configuration

- Alarms Management

  Circular Queue can contain 1,360 traps

  — A single Meridian 1 produces alarms, on average, at the rate of one every 10 seconds. This means the queue can hold 3.7 hours worth of alarms from a single Meridian 1 without losing alarm information.

— Starting with Release 25 of Meridian 1, there is the capability of filtering traps, on the Meridian 1 side, based upon their categorization, e.g. minor, major, critical, etc. This can greatly reduce the alarm rate by permitting only major and critical alarms to be sent to OTM.

— By using filtering, the number of M1s that can be connected to greatly increases. However, when a single Meridian 1 begins having a problem, it will begin reporting major/critical alarms at the rate of 1 every 2 seconds. This means that the queue can hold only the last 45-minutes worth of alarms from the offending switch, assuming that alarms from the other switches are minimal.

Operational Limits

Table F-3 lists those OTM features that have a significant impact on PC performance. Each feature the table lists their CPU utilization and elapsed time statistics, as appropriate, when connected to a single Meridian 1.

The test setup was:

- A 450 MHz Pentium II with 128 Mbytes of memory and ATAPI hard disk interface
- A Meridian 1 with a CP4 processor (Option 81)
- For an Option 11C machine decrease CPU usage by a factor of 2 and increase elapsed time by the same factor for those features that interact with Meridian 1, for example, Station Update, but not Cost Report.

Table F-3
PC Performance by Application

	Real Time (CPU)		**Elapsed Time**
Application	**Peak**	**Average**	
Station Admin Add/Chg/Del		2.4%	
Station Update with M1	100%		1 record/3 seconds
Web Admin		Negligible	
Alarm Monitor	2%	Negligible	
DBA - CDR Collection	6%	3%	
DBA - Traffic Collection	1%	0.5%	
LDAP Sync[a]	100%		10 records/second
Parsing CDR File	100%		40 records/second
Cost Report	100%		40 records/second
OTM client (Station Update)	4%		1 record/5 seconds

a. LDAP Sync testing was based upon the use of an LDAP server dedicated for this testing. Since Optivity does not control the LDAP Server used in the customer network, the server response time is likely to be less. Factors for the LDAP Server, such as, processor speed, other uses for LDAP Server, for example, Corporate Directory, other LDAP clients, and other services running on the same platform will impact this server's resources.

PC Hardware

This section describes the PC hardware requirements necessary to run OTM optimally. Start with the “OTM Server Minimum Hardware Requirements” on page 193. Also, follow these guidelines using the information provided in sections “Physical Memory” on page 195, “Hard Disk” on page 196, and “Processor Speed” on page 197:

- Add additional serial interface cards as needed.
- Calculate disk storage requirements based on applications usage.
- Implement a backup and restore strategy.
- Follow regular maintenance instructions as documented for OTM features in order to maintain the integrity and capacity of the hard disk.
- Add disk redundancy as required.
- Increase performance by
  - — Adding more system memory
  - — Utilizing a faster hard disk and/or SCSI interface
  - — Using a faster CPU
- Scale your PC for future growth, utilize a PC that:
  - — Has a reserve PCI Card slot for a SCSI Interface Card (See “Hard Disk” on page 196 for details.)
  - — Has a spare storage bay and power for adding an internal hard disk
  - — Can accommodate increasing the memory capacity to 512 Mbytes or greater (Most PC's have 2 to 4 memory card slots that can accommodate 32 Mbytes, 64Mbytes, 128Mbytes, and etc. DIMMS.)

OTM Server Minimum Hardware Requirements

The OTM Server must meet the following minimum hardware requirements.

- 400 MHz Intel Pentium II Processor or equivalent
- 3 GB hard drive (1000 MB free space plus customer data storage requirements) with ATAPI interface (refer to “Hard Disk” on page 196 for details)
- 128 MB of RAM (refer to “Physical Memory” on page 195 for details)
- CD-ROM Drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA Color Monitor and interface card using a minimum monitor setting of 800x600
- Two Ethernet Network Interface cards are required to support connection with the Meridian 1 via Ethernet and Customer LAN
- Hayes-compatible modem is optional for connection to remote systems, required for polling configurations (56K BPS)
- PC COM port with 16550 UART
- Windows compatible mouse or positioning device (PS2 mouse preferred to free up a PC serial port)

OTM running in standalone mode (a computer that directly accesses Meridian 1) requires the following:

- 200 MHz Intel Pentium Processor or equivalent (Pentium II 300 MHz for running Call Accounting)
- 2 GB hard drive with 500 MB of free space with IDE interface
- 64 MB of RAM
- CD-ROM drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA color monitor and interface card using a minimum monitor setting of 800x600
- Ethernet network interface
- Windows-compatible mouse or positioning device
- Windows 95, Windows 98 and Windows NT Workstation 4.0 or Server

An OTM Client (a computer that accesses the OTM Server) requires the following:

- 200 MHz Intel Pentium Processor or equivalent (Pentium II 300 MHz for running Call Accounting)
- 2 GB hard drive with 500 MB of free space with IDE interface
- 64 MB of RAM
- CD-ROM drive and 3 1/2-inch, 1.44 MB floppy disk drive
- SVGA color monitor and interface card using a minimum monitor setting of 800 x 600
- Ethernet network interface
- Windows-compatible mouse or positioning device
- Windows 95, Windows 98 and Windows NT Workstation 4.0 or Server

A Web Client (a computer that uses a web browser to Access OTM Server) requires the following:

- 160 MHz Intel Pentium Processor or equivalent
- 2 GB hard drive with 500 MB of free space with IDE interface
- 32 MB of RAM
- CD-ROM drive and 3 1/2-inch 1.44 MB floppy disk drive
- SVGA color monitor and interface card
- Ethernet network interface
- Windows-compatible mouse or positioning device
- Windows 95, Windows 98 and Windows NT Workstation 4.0 or Server

Physical Memory

The amount of physical memory installed on the server is critical in achieving maximum performance on the PC. Microsoft Windows systems have a feature called Virtual Memory. Virtual Memory allows the PC to continue running programs that require more memory than there is physical memory available. It borrows memory using a memory swapping scheme from available space on the main hard disk. Although this feature permits the PC to perform operations without worrying about running out of physical memory and thus crashing the computer, it sacrifices performance of these operations by requiring access of the hard disk while memory swapping. This degrades performance because:

- Physical memory access is much faster than disk access (by an order of magnitude or greater.
- Accessing the disk while swapping steals disk access cycles away from applications that need to read and write to the hard disk.

The OTM Server software and the Windows NT Server software requires ~150Mbytes without active features.

The amount of memory does not grow significantly as features are running and windows are opened. An OTM Server can operate at full capacity using physical memory only when the PC has 256Mbytes of memory installed.

The one exception to this is OTM Client access. Each OTM Client connection to the OTM Server requires an additional 2MB of memory. For large configurations, such as, 100 M1s and 50 OTM Clients, an additional100MB of memory would be required.

For maximum performance on the largest systems, a minimum of 512Mbytes of memory should be installed.

Hard Disk

Disk Performance

Much of the time spent by OTM Features is in reading and writing data to the hard disk. Features that spend a good percentage of their time accessing the disk are called, disk-intensive applications. For these features, the access time is critical in terms of the time it takes for a feature to complete an operation.

OTM disk-intensive applications analyzed in this document include:

- CDR and traffic collection
- Call Accounting report generation
- Simultaneous Meridian 1 Update of Station Data
- Station Update from a single Meridian 1 is not affected by disk performance, as the speed of transmission from the Meridian 1 is slower than the PC accessing its disk.
- Web/OTM Client Station Access

The “OTM Server Minimum Hardware Requirements” on page 193 recommends a hard disk using the ATAPI interface. It also recommends a single hard disk.

Performance improvements can be achieved by:

- Using an Ultra-Wide SCSI Interface in place of ATAPI.

  — Disk Performance will increase by a factor of 2 or better. This can translate to an increase in feature performance (reduce elapsed time and increase simultaneous operations) by 50% or better.

Note: SCSI Disk drives come in various speeds.

- Add a hard disk to store OTM Data separate from the OS and Programs.

— If the NT Server PC being used is using an ATAPI interface for its main disk, "C:", then installing a SCSI Interface Card and second hard disk to store OTM Data can achieve the majority of the SCSI performance increase.

— If the PC being used has a limit on physical memory that is lower than what is need to run OTM in the desired configuration, then adding a second hard disk will improve performance by separating the virtual memory disk swapping activity on the main disk from the OTM data access on the second disk.

Disk Size

The OTM Server software and the Windows NT Server software requires ~900Mbytes without OTM data or active features.

Need to reserve approximately 300 Mbytes of disk space for Virtual memory and normal OS operations.

CDR = 250 Bytes per record, at peak rates (for a CP4-Option 81 switch) over a one day period, this would create a 700Mbyte file.

Station~ =500Kbytes per 100 sets. From the example Tables 1 and 2:
Disk space = 500 Kbytes/100 sets*10,000 lines = 50 Mbytes of disk space.

Directory~= 80 Kbytes per 100 records. From the example Tables 1 and 2:
Disk space = 80 Kbytes/100 sets * 10,000 lines = 8 Mbytes of disk space.

Processor Speed

The 400 MHZ CPU recommended is sufficient for the maximum configurations presented here.

Increasing CPU power does not, by itself, greatly increase the capacity of the Server.

The PC is so I/O bound, from accessing memory, to accessing the hard disk, that a two-fold increase in CPU power may result in only a 10% increase in OTM capacity.

Replacing the motherboard, not just the CPU chip, can further increase CPU performance, since the newer motherboard would be designed to take advantage of the high processor speeds, e.g., faster CPU bus, faster memory, etc. The PC is still heavily bound to disk access and network speeds.

Windows NT Server and Windows NT Workstation Differences

Table F-4 shows the differences between Windows NT Workstation and Windows NT Server:

Table F-4
Differences Between Windows NT Server and Windows NT Workstation

	Windows NT Server	Windows NT Workstation
Purpose	Network Server	Multitasking Desktop OS
CPU	Up to 4	Up to 2
Incoming concurrent session	Unlimited (limited only by number of licenses possessed)	10
Remote Access Service	Up to 256 simultaneous sessions	1
Directory Replication	Import and Export	Import
Disk Fault Tolerance	Yes	No
Logon Validation	Yes	No
Service for Macintosh	Yes	No
Internet Service	Internet Information Server (IIS)	Peer Web Server (PWS). PWS does not have the feature to restrict access by IP address.

Network Bandwidth

Typical Configurations

Figure F-1 shows how OTM would connect to Meridian Mail and to older Meridian 1 systems that are not packaged with Ethernet. In this scenario, OTM is connected to these systems through their serial ports. Physical limitations on serial connections limit OTM to be placed within 50 feet of these systems to minimize noise, which can cause transmission errors.

Figure F-1
Connecting OTM to legacy Meridian systems (pre-Ethernet)

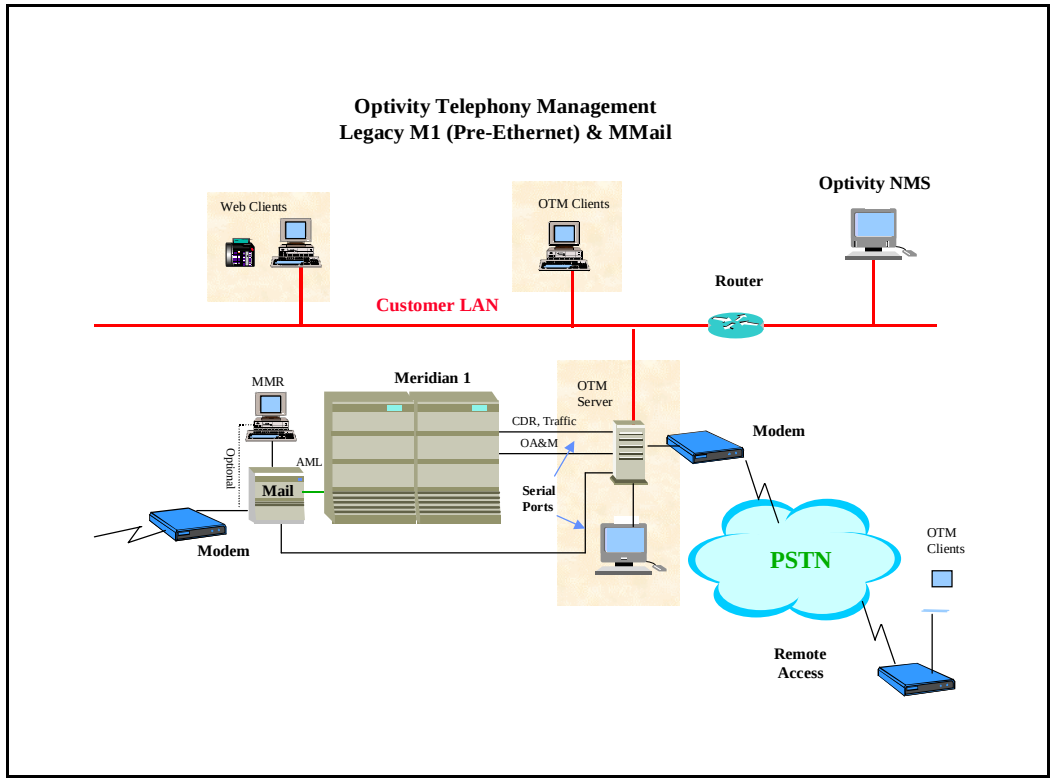


Figure F-2 represents how OTM would connect to Meridian Applications and to Meridian 1 Systems that are packaged with Ethernet. In this picture, OTM is connected to these systems via Ethernet using the Meridian System's ELAN (Embedded LAN). Meridian Systems require that the ELAN be protected from the Customer's LAN. Therefore, if OTM is to be connected to the Customer's LAN (CLAN), such as to provide Client Access to the OTM Server, then OTM must have two Ethernet cards, one for connecting to the ELAN and one for connecting to the CLAN.

This configuration provides optimum performance, in that all communications between OTM and the Meridian Systems are private. In this case, there is no impact to this communication due to Customer LAN traffic. It also meets the requirement of protecting the ELAN from the CLAN as required for Meridian by having OTM acts as a router.

Physical limitations on 10mb ethernet connections limit the ELAN distance to 500 meters using a maximum of four hubs/repeaters. The maximum distance from end device to hub and hub-to-hub is 100 meters. Creating a separate EWAN, which connects ELAN segments, utilizing Switches and/or Routers can be used to increase distance. These Switches/Routers must be used for only this EWAN. The additional cost of an EWAN network configuration, as well as, the additional wiring necessary to connect a geographically disperse environment (one that spans multiple floors and/or buildings), could make the EWAN option less practical.

Figure F-2
Connecting OTM to ELAN connected Meridian Systems

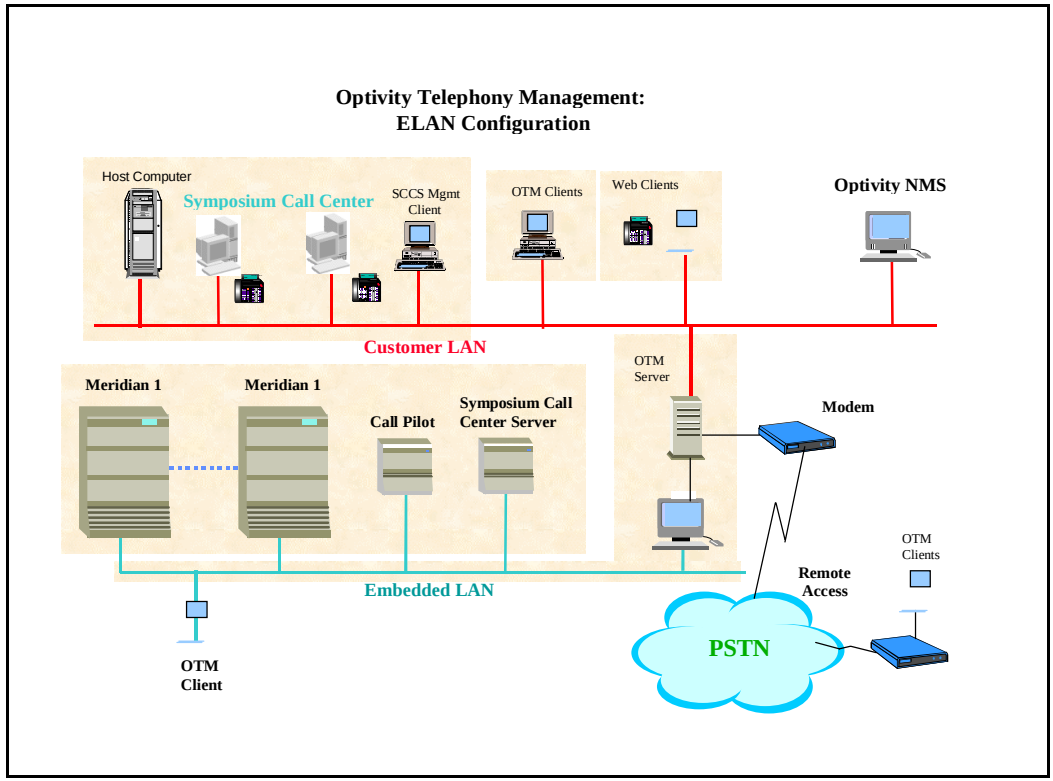


Figure F-3 pictures OTM connected directly to the Customer WAN. Connecting the ELAN to the CWAN via Routers provides protection for the ELAN segments. This configuration solves the problem of connecting a single OTM Server to multiple M1s, when these M1s are geographically disperse, without requiring a separate network. It also permits OTM to be connected to a larger number of M1s from a traffic perspective, for Customer WANs that are utilizing higher bandwidths, e.g. 100mb, 1gb, etc. The disadvantage is that available bandwidth must be shared with Customer traffic.

Figure F-3
Connecting OTM to CWAN connected Meridian systems

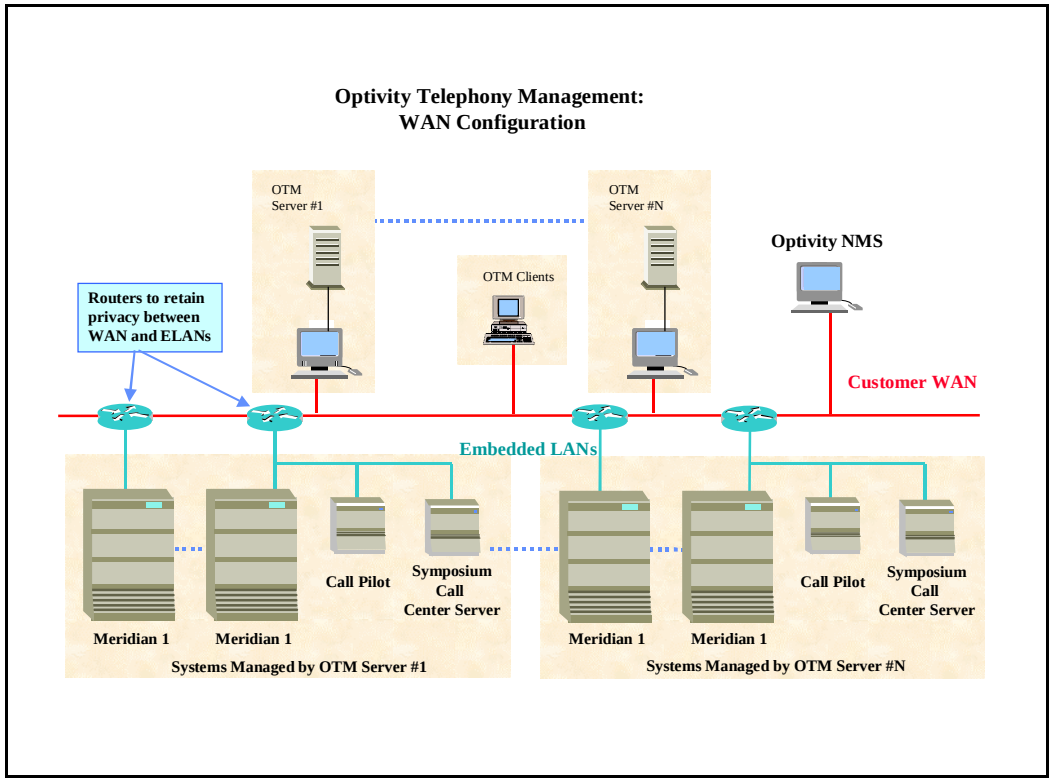


Figure F-4 represents how OTM servers, each of which manages a certain subset of the entire customer Meridian 1 network, can be connected together and accessed from a central OTM Client. In this scenario, the OTM Central Server dials up the OTM Servers via modem. It can then be used to query alarms, access station data, etc. This approach would commonly be used by Distributors to access their Customer's network, without requiring direct access to that Customer's WAN. The majority of traffic exists between the individual OTM Servers and the Meridian Systems that each is managing.

This network connectivity also works for the case presented in Figure F-2, wherein OTM Servers are connected to Meridian ELANs.

Figure F-4
Networking OTM Servers, External to Customer WAN

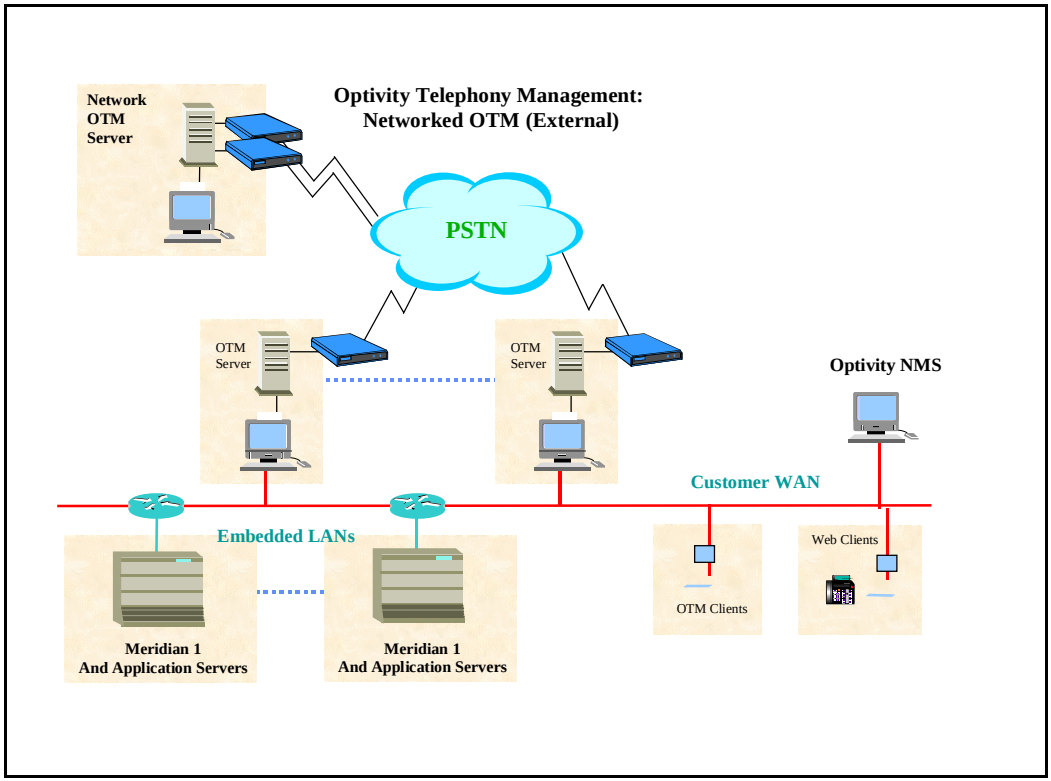
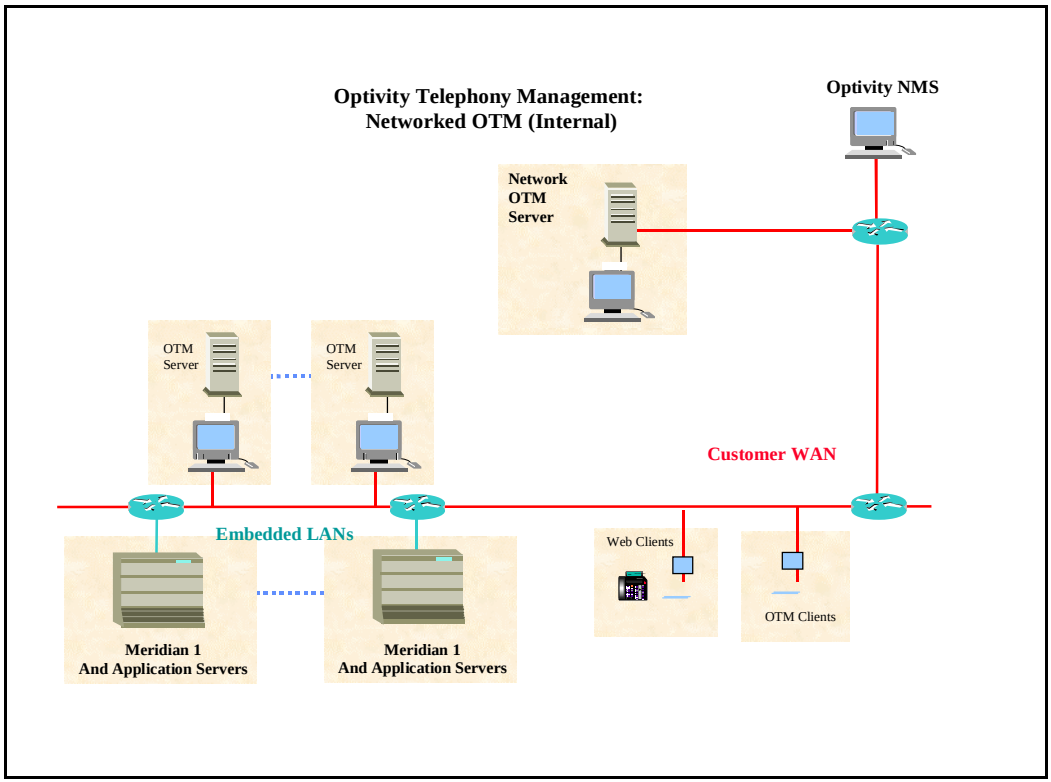


Figure F-5 is identical in function to Figure F-4, except that the OTM Central Server is connected directly to the Customer's WAN. Access via this method is faster since direct WAN connections are much faster than modems.

This network connectivity also works for the case presented in Figure F-2, wherein OTM Servers are connected to Meridian ELANs on one side and to the Customer WAN on the other side.

Figure F-5
Networking OTM Servers, Internal to Customer WAN



Bandwidth Utilization

The trade-off is the cost of OTM versus the cost of increased network bandwidth and/or network subnets. Once OTM Servers are attached to the WAN, the customer network may be impacted, but there is a savings on the number of OTM's needed.

Note: Never expect to fully utilize Ethernet bandwidth. Performance degrades quickly as the utilization exceeds a certain threshold (approximately 35%). Consult the network administrator for details on network bandwidth utilization.

Table F-5 lists the average and peak traffic for the ELAN and CLAN. This is based upon traffic analysis of a Meridian 1 running on a CP4 CPU. For the Option 11C machine, divide the ELAN numbers by 2, except alarms. For the CPP CPU, multiply the ELAN numbers by 4, except for alarms.

Table F-5
Network Bandwidth Usage Per Meridian 1 System

	Transfer Rate (bits/second)	
OTM Activity	**Average**	**Peak**
Station Add/Chg/Del, ELAN	32kb	32kb
Station Sync with M1, ELAN	NA	48kb
CDR, ELAN	35kb	70kb
Traffic, ELAN	24kb	48kb
Alarm, ELAN	01kb	03kb
Sync with LDAP Server, CLAN	NA	720kb
Total, ELAN	~92kb	~201kb
Total, CLAN		~720kb

Optivity Telephony Manager

Installation and Engineering Guide

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.
SL-1 and Meridian 1 are trademarks of Nortel Networks. Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. All other trademarks and registered trademarks are the property of their respective owners.
Publication number: P0910102
Document release: Standard 1.0
Date: July 2000
Printed in the United States of America

NORTEL NETWORKS™