Part No. P0986984
January 2002

Installing and Configuring Optivity Telephony Manager Release 1.2

NORTEL NETWORKS™

Copyright © 2002 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, SL-1, Meridian 1, Succession Communication Server for Enterprise 1000, and Optivity are trademarks of Nortel Networks.

Microsoft, MS-DOS, Windows, Windows NT, and Personal Web Server are registered trademarks of Microsoft Corporation.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

HP and OpenView are trademarks of Hewlett-Packard Corporation.

Intel and Pentium are trademarks of Intel Corporation.

Java is a trademark of Sun Microsystems, Inc.

pcANYWHERE is a trademark of Symantec Corp.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. Optivity* Telephony Manager software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying Optivity Telephony Manager software or installing the hardware unit with pre-enabled Optivity Telephony Manager software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date the Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its

own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Revision History

Date Revised	Version	Reason for revision
June 2001	1.00	Initial Standard release.
Januaary 2002	2.00	Upissued to coincide with the release of OTM Release 1.2.

Contents

Figures

Tables

Preface

Optivity* Telephony Manager (OTM) is designed for managers of telecommunications equipment and authorized Nortel Networks* distributors. OTM provides a single point of access and control for Nortel Networks Meridian 1* and Succession Communication Server for Enterprise (CSE) 1000* system management. OTM uses IP technology to target the following key customer values:

- Single point of connectivity to Meridian 1 systems, Succession CSE 1000 systems, and related devices.
- Data collection for traffic and billing records.
- Collection, processing, distribution, and notification for alarms and events.
- Data entry and propagation (employee names and telephone numbers shared in multiple databases).
- Web-based management applications.

Before you begin

This guide is intended for Meridian 1 system administrators using a Microsoft Windows*-based PC for management activities. This guide assumes that you have the following background:

- Working knowledge of the Windows NT*/Windows 2000 Server operating system.
- Familiarity with Meridian 1 and Succession CSE 1000 system management activities.
- Knowledge of general telecommunications concepts.
- Experience with windowing systems or graphical user interfaces (GUIs).
- Knowledge of Internet Protocol (IP).

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `chg suppress_alarm <n>` where *n* is 0 = all, 1 = minor, 2 = major, 3 = critical, you enter `chg suppress_alarm 3` to suppress all alarms except critical alarms.
bold Courier text	Indicates command names and options and text that you need to enter. Example: Enter **`prt open_alarm`**.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: For additional information, refer to *Using Optivity Telephony Manager*.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Open Alarm destination #0 is 47.82.40.237`
separator (>)	Shows menu paths. Example: Select Utilities > Backup in the Navigator window.

Acronyms

This guide uses the following acronyms:

ASP	active server page
CLI	command line interface
CRS	Consolidated Reporting System

DBA	Data Buffering and Access
DN	directory number
ELAN	embedded local area network
GCAS	General Cost Allocation System
GUI	graphical user interface
IP	Internet Protocol
ITG	Internet Telephony Gateway
LAN	local area network
LDAP	lightweight directory access protocol
MAT	Meridian Administration Tools
NMS	network management system
OTM	Optivity Telephony Manager
PTY	pseudo-TTY (network port)
RAS	remote access server
RU	reporting unit
TBS	Telecom Billing System
TLAN	telephony local area network
TN	terminal number
TTY	teletype (serial port)
uid	unique identifier in LDAP synchronization
VLAN	virtual local area network

Related publications

For more information about using Optivity Telephony Manager for Meridian 1 and associated applications, refer to the following publications:

- *Using Optivity Telephony Manager* (553-3001-330)

  Provides information on using the applications and features available with Optivity Telephony Manager for Meridian 1.

- *Using Optivity Telephony Manager Telemanagement Applications* (553-3001-331)

  Provides information on the following optional telemanagement applications; Telecom Billing System (TBS), TBS Web Reporting, General Cost Allocation System (GCAS), and Consolidated Reporting System (CRS).

- *Meridian Internet Telephony Gateway (ITG) Trunk 1.0/Basic Per-Trunk Signaling* (553-3001-116)

  Describes configuration and maintenance of the 8-port ITG trunk card.

- *Meridian Internet Telephony Gateway (ITG) Trunk 2.0/ISDN Signaling Link (ISL)* (553-3001-202)

  Describes configuration and maintenance of the 24-port ITG trunk card. This card appears to the Meridian 1 switch as a 24-port trunk card with ISDN Signaling Link (ISL) and D-channel signaling.

- *Meridian Internet Telephony Gateway (ITG) Line 1.0/IP Telecommuter* (553-3001-119)

  Describes configuration and maintenance of the ITG line card for IP Telecommuter.

- *Meridian Internet Telephony Gateway (ITG) Line 2.0/i2004 Internet Telephone* (553-3001-204)

  Describes configuration and maintenance of the ITG gateway card for the Meridian Internet Telephone, also referred to as the i2004 telephone.

- *M3900 Series Meridian Digital Telephones; Description, Installation and Administration* (553-3001-216)

  Describes M3900 series telephones and related features. The M3904 and M3905 telephones provide access to an OTM generated Corporate Directory.

- *X11 Software Features Guide* (553-3001-306)

  Describes features associated with the Meridian 1 system. For each feature, information is provided on feature implementation, feature operation, and interaction between features.

- *Software Input/Output Guide, X11 Administration* (553-3001-311)

  Describes the prompts and responses for the Meridian 1 system's command line interface (CLI). This guide includes information on overlay programs that are classified as administration overlays.

- *Software Input/Output Guide, System Messages* (553-3001-411)

  Describes the meaning of the messages generated by the Meridian 1 system.

- *Software Input/Output Guide, X11 Maintenance* (553-3001-511)

  Describes the prompts and responses for the Meridian 1 system's command line interface (CLI). This guide includes information on overlay programs that are classified as maintenance overlays.

- *Option 11C Planning and Installation* (553-3021-210)

  Provides information on the Survivable IP Expansion (SIPE) feature for Option 11C systems.

- *Succession Communication Server for Enterprise 1000 Planning and Installation Guide* (553-3023-210)

  Provides information on the Survivable IP Expansion (SIPE) feature for Succession CSE 1000 systems.

- *Succession Communication Server for Enterprise 1000 Input/Output Guide, Administration* (553-3023-311)

  Describes the prompts and responses for the Succession CSE 1000 system's command line interface (CLI). This guide includes information on overlay programs that are classified as administration overlays.

- *Succession Communication Server for Enterprise 1000 Input/Output Guide, System Messages* (553-3023-411)

  Describes the meaning of the messages generated by the Succession CSE 1000 system.

- *Succession Communication Server for Enterprise 1000 Input/Output Guide, Maintenance* (553-3023-511)

  Describes the prompts and responses for the Succession CSE 1000 system's command line interface (CLI). This guide includes information on overlay programs that are classified as maintenance overlays.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe* at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader*.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at www.nortelnetworks.com. From the main page, select Customer Support followed by Documentation.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Chapter 1
Initial installation tasks

This chapter contains:

- Optivity Telephony Manager (OTM) installation requirements
- A checklist that is designed for you to use as a reference when beginning a new OTM installation
- Procedures to install the OTM server software, validate the installation, and configure OTM features

OTM Server software installation begins on page 33.

A Microsoft* Windows NT* installation example to help the new Windows NT and OTM administrator get started begins on page 189. OTM is designed for use in either Windows NT, Windows 95, Windows 98, or Windows 2000 operating environments. Only the Windows NT and Windows 2000 environments support 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 "Integrating OTM with Optivity NMS" on page 147 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 "Configuring a Windows NT Server or Workstation as an IP router" on page 204.

For installation recommendations that will help to create a secure environment for your OTM data and users, refer to "Security guidelines for Windows NT" on page 211.

To configure modems for use with OTM, refer to "Configuring a modem for OTM applications in Windows" on page 72.

For detailed hardware and software guidelines to consider when planning OTM installations, refer to Appendix A, "OTM engineering guidelines."

OTM requirements

OTM requirements include:

- "Meridian 1 X11 system software release and package requirements"
- "OTM Server hardware requirements" on page 27
- "OTM Server software requirements" on page 28
- "PC Client requirements" on page 29

Meridian 1 X11 system software release and package requirements

In general, OTM 1.1 requires no special X11 system software release to run. Table 1 is a list of X11 releases and packages required based on the OTM applications.

Table 1 Meridian 1 X11 system software release and packages

OTM Application	Minimum X11 Release Required	X11 Pkgs Required
Alarm Management	X11 R22 or later	Pkg 164, 242, 243, and 296
-Additional pkgs for Alarm Notification		Pkg 55, and 315
Maintenance Windows	X11 R22 or later	Pkg 164, 242, 243, and 296
System Terminal - Overlay Passthru	X11 R22 or later	Pkg 164,242, and 296
Ethernet connection (for Station Administration, Traffic Analysis, and ESN ART)	X11 R22 or later	Pkg 164, 242, and 296
SMNP Alarms (Open Alarms)	X11 R22 or later	Pkg 315
Data Buffering and Access- Ethernet	X11 R24 or later	Pkg 351
Data Buffering and Access- Serial	N/A	N/A

Table 1 Meridian 1 X11 system software release and packages (continued)

OTM Application	Minimum X11 Release Required	X11 Pkgs Required
M1 Database Disaster Recovery	X11 R24 or later	Pkg 164, 242, 296, and 351
Virtual Terminal Server	X11 R22 or later for access over IP	Pkg 164, 242, and 296

OTM Server hardware requirements

The OTM Server must meet the following minimum hardware requirements. Refer to Appendix A, "OTM engineering guidelines" 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 recommended)

Note: OTM does not support software based WinModems.

- PC COM port with 16550 UART
- Printer port (LPT) required for dongle
- Dongle (for server or standalone only)

- Windows-compatible mouse or pointing device (PS/2 mouse preferred to free up a PC serial port)

Note: Do not install OTM on a Microsoft Windows NT system that is configured as a primary domain controller (PDC).

OTM Server software requirements

OTM requires a Windows NT 4.0 or Windows 2000 Server or a Windows NT Workstation with the following software:

- TCP/IP Protocol
- Remote Access Service
- NT Server 4.0, Service Pack 5, and Option Pack 4 (for Windows NT)

  The required components from Option Pack 4 are:

  — Internet Information Server (IIS) 4.0 or above

Caution: ITG file transfers may fail if there is another file transfer protocol (FTP) service running on the OTM Server. By default, IIS will install the FTP Publishing Service. This service may be set to start automatically and will cause ITG applications to fail.

  — Microsoft Transaction Server
  — Microsoft Data Access Components (MDAC)
  — Microsoft Management Console (NMC)
  — NT Option Pack Common Files

Note: Chapter 3, “Windows NT reference,” on page 189 provides detailed information on installing and configuring Windows NT for use with OTM.

- Windows 2000 Server, and Service Pack 1 (for Windows 2000)
- Microsoft Internet Explorer 5.01 or Netscape Navigator 4.5 or higher

- Network card drivers

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

Support for Microsoft Windows 2000™

Support for the Windows 2000 operating system was introduced with OTM 1.01. The following configurations are supported:

- Windows 2000 Server as an OTM 1.2 server
- Windows 2000 Server as an OTM 1.2 server with a combination of Windows 95, Windows 98, Windows NT 4.0 Workstation, or Windows 2000 Professional as clients
- Windows 2000 Professional as an OTM 1.2 standalone PC
- Windows 2000 Professional as an OTM 1.2 Web server

The following configuration of OTM 1.2 is not supported on Windows 2000:

- Windows 2000 Professional as an OTM 1.2 Windows file server

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 (128 MB of RAM is recommended for improved performance and for the Billing Enhanced level applications).
- 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, Windows 2000, or Windows NT Workstation 4.0 or Server

Note: When installing OTM on a Client running Windows 95, ensure that your version of Windows 95 is Y2K compliant.

- The correct Java Runtime Environment (currently version 1.3.1) installed on the client machine
- A Microsoft Active Server Page (ASP) and HTML-compliant Web browser

Installation Checklist

Use the following quick reference as a checklist or reminder when starting a new OTM installation.

Meridian 1 Installation Requirements

Software and memory:

[ ] Required X11 packages (296, 315, and 351 depending on applications being installed)

[ ] Minimum of 48 MB of memory on the Meridian 1

For Ethernet connections:

[ ] X11 Release 22 or later

[ ] Release 24B or later is required for Data Buffering and Access

[ ] IOP, IOP/CMDU or IODU/C cards for Options 51C, 61C, 81, 81C

[ ] Ethernet AUI cables to be attached to each IOP (Options 51C, 61C, 81, 81C)

[ ] NTDK27 Ethernet cable for Option 11C

[ ] Transceivers to connect to the LAN

[ ] Router

For PPP connections:

[ ] Hayes compatible modem

[ ] SDI port available on the Meridian 1 (configured for SCH only)

[ ] Serial cable to connect the modem to the SDI port

For serial connections:

[ ] SDI port available on the Meridian 1 (configured for SCH only)

[ ] Hayes compatible modem for remote connection (optional)

[ ] Serial cable to connect the modem to the SDI port

Programming the Meridian 1:

[ ] Enable Name Option in LD 17

[ ] Define Limited Access Password in LD 17

[ ] For Serial communication: Configure a TTY with User = SCH in LD 17

[ ] For Ethernet or PPP communication: Configure a pseudo TTY (PTY) with User = SCH in LD 17

[ ] Configure Ethernet at the Meridian 1 in LD 117

[ ] Define the Gateway (router) IP address on the Meridian 1 in LD 117

[ ] Configure PPP at the Meridian 1 in LD 117

[ ] INIT the Meridian 1

[ ] Enable the new IP address (defined in LD 117) in LD 137

[ ] Enable Database Disaster Recovery (DDR) in LD 117

[ ] Set open alarm destination in LD 117

[ ] Set up Data Buffering and Access in LD 177

[ ] Set up filtering in the Meridian 1 to filter out information and minor messages

PC/Server Installation Requirements

Single (Stand alone) OTM Installation:

[ ] 200 MHz minimum Intel Pentium II Processor or equivalent. Pentium II running at 300 MHz is minimum for Telecom Billing System application.

[ ] 2 GB hard drive with 500 MB of free space

[ ] 64 MB of RAM

[ ] Ethernet Network Interface Card

[ ] Windows 95, Windows 98, Windows 2000 Server, Windows 2000 Professional or Windows NT Workstation 4.0 or Server

[ ] OTM Dongle

[ ] OTM CD and Keycode

[ ] Remote Access Service (RAS) (optional)

[ ] Modem(s) for remote access (optional)

OTM Server Installation:

[ ] 400 MHz minimum Intel Pentium II Processor or equivalent.

[ ] 3 GB hard drive (1 GB of free space plus customer data storage requirements)

[ ] 256 MB of RAM

[ ] Two Ethernet Network Interface Cards

[ ] PC COM port with 16550 UART

[ ] Hayes compatible modem (optional)

[ ] Windows NT Server 4.0 and Service Pack 5 or Windows 2000 Server

[ ] Windows NT Option Pack 4 or Windows 2000 Server

[ ] Remote Access Service

[ ] OTM Dongle

[ ] OTM CD and Keycode

[ ] Configure and test network interfaces

[ ] Enable IP routing (if applicable)

OTM Client Installation:

[ ] **Windows Client** - 200 MHz minimum Intel Pentium Processor or equivalent (300 MHz Pentium II required for Telecom Billing System application). **Web Client** - 160 MHz Intel Pentium Processor or equivalent.

[ ] 2 GB hard drive with 500 MB of free space

[ ] **Windows Client** - 64 MB of RAM (128 MB of RAM is recommended for improved performance and for the Billing Enhanced level applications) **Web Client** - 32MB of RAM

[ ] **Windows Client** - PC COM port with 16550 UART

[ ] Ethernet Network Interface Card

[ ] Windows 95, Windows 98 Windows 2000, or Windows NT Workstation 4.0 or Server

[ ] **Windows Client** - Remote Access Service

[ ] **Windows Client** - OTM CD and Keycode (no Dongle required)

[ ] **Web Client** - Java Runtime Environment (JRE) 1.2.2.006 and Microsoft Internet Explorer 5.01 or Netscape Navigator 4.5

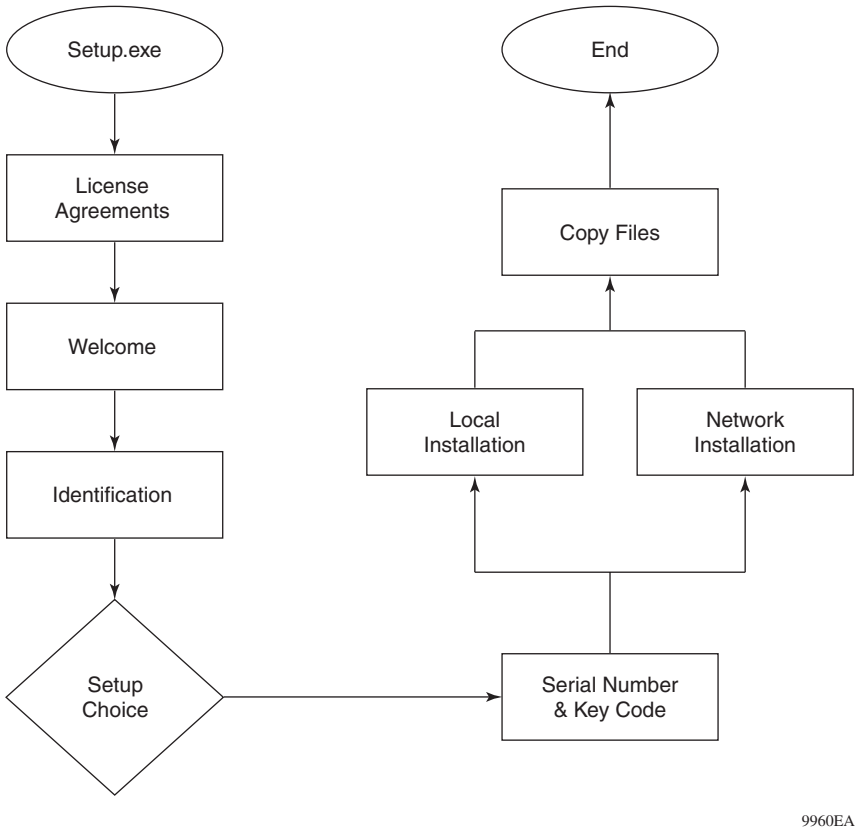
OTM Server software installation

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.

Note: Before installing OTM software, exit all Windows programs and disable any virus detection software.

Figure 1 presents a high level outline of the installation screens.

Figure 1 High level outline of the installation screens

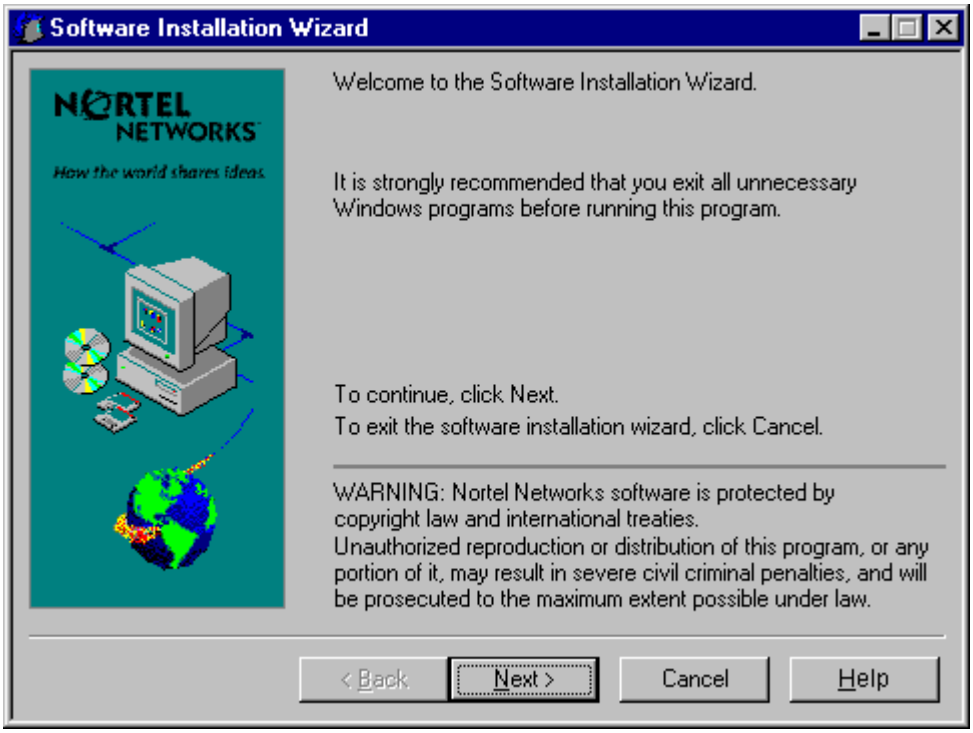


Note: At the beginning of OTM software installation, the setup program checks for various prerequisites, and displays appropriate messages if one or more required components are not present. Additionally, a log records all errors. During installation, the log resides in the following directory path: *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.

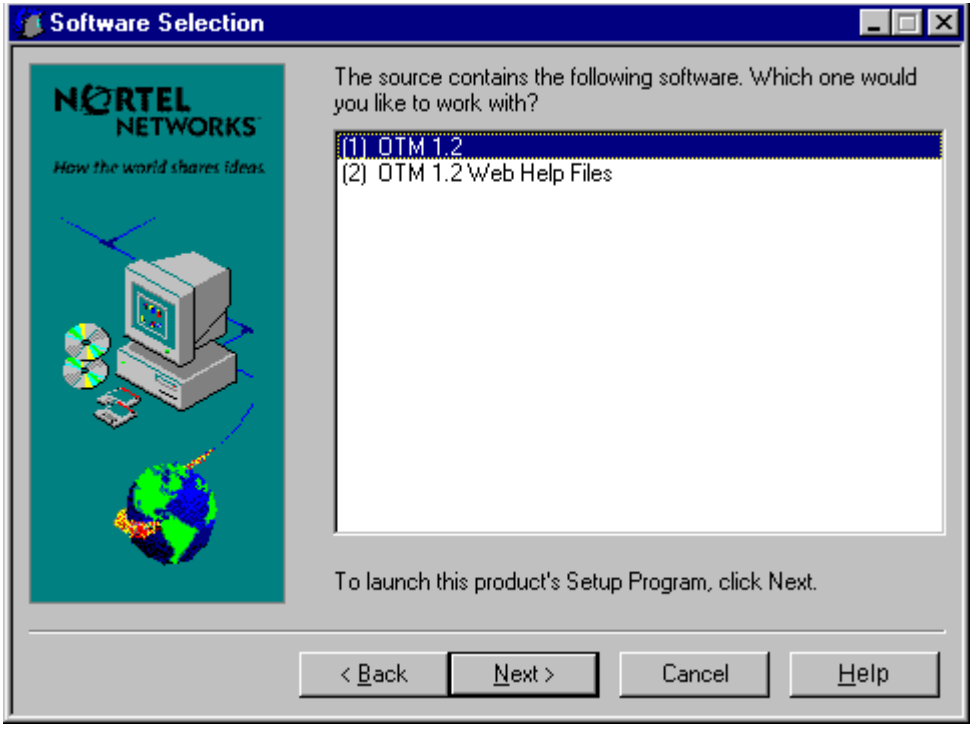
2 Double-click the *Setup.exe* file on the OTM CD-ROM. The welcome screen is displayed (Figure 2). Click Next to continue.

Figure 2 Software Installation Wizard



3 Select OTM. The other option is OTM Web Help files (Figure 3). OTM Web Help can be installed once the OTM Application installation is complete.

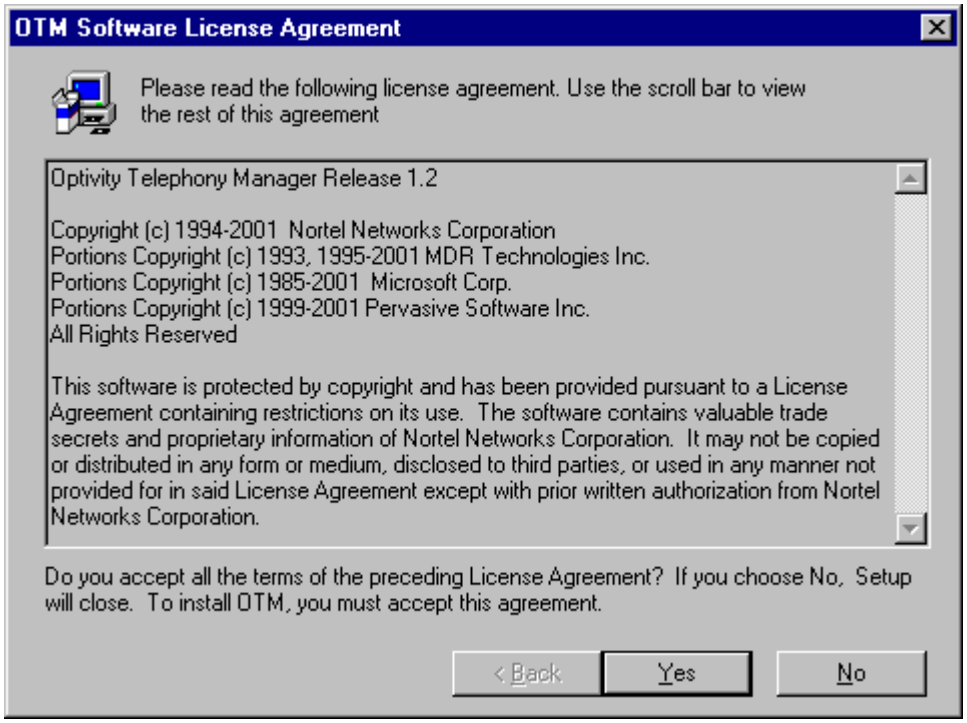
Figure 3 Software Selection



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

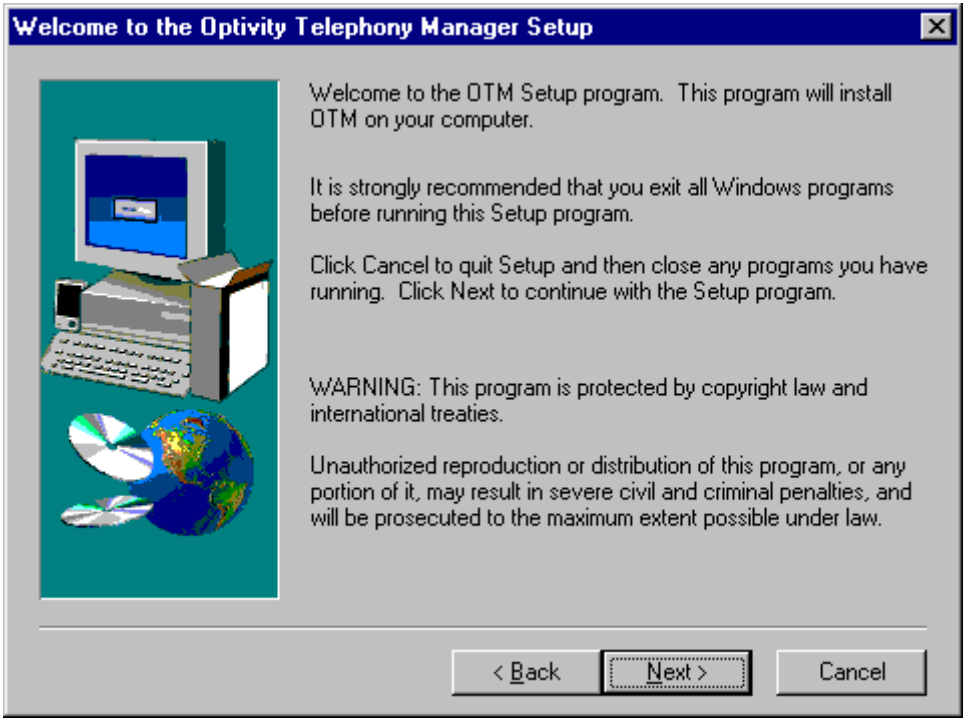


Welcome

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

5 Click Next to continue.

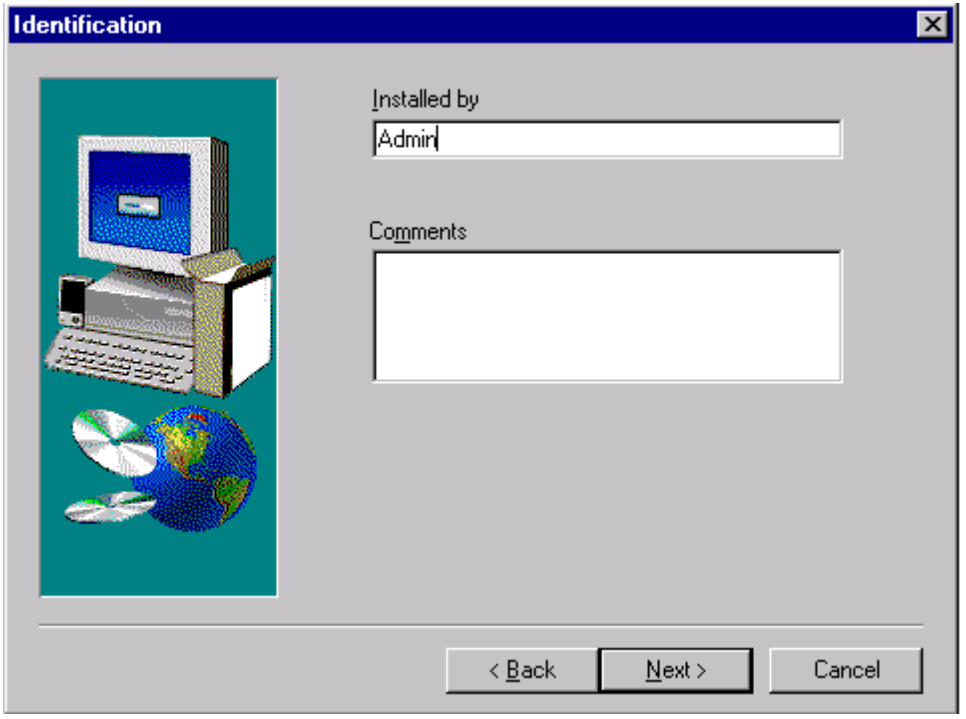
Figure 5 Welcome



Identification

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

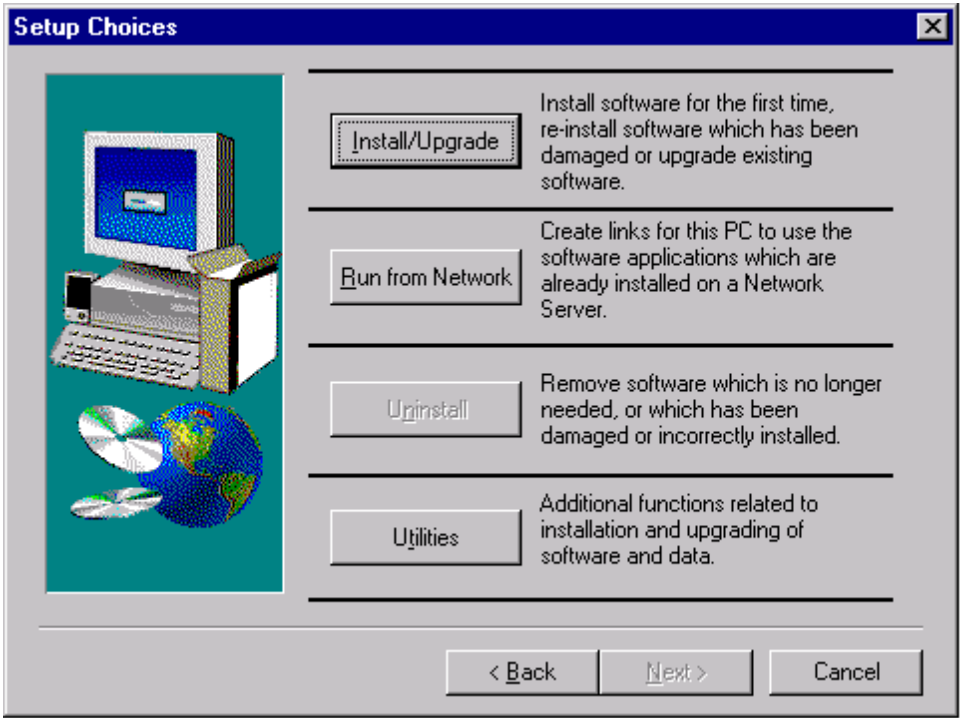
Figure 6 Identification



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 48.

Figure 7 Setup Choice



Note: 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 on page 68.

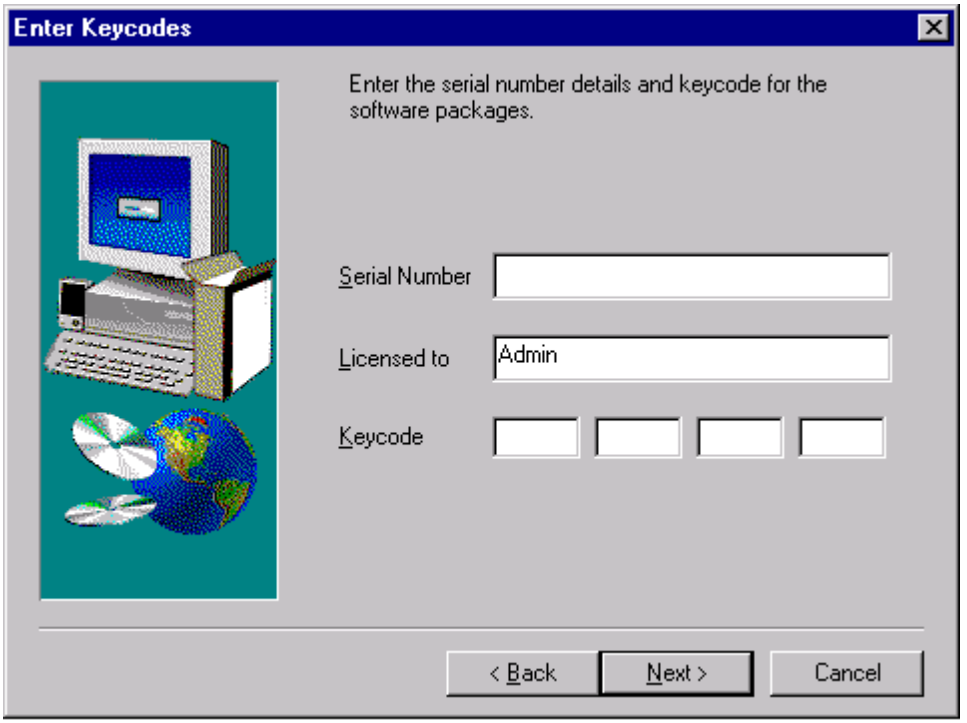
Run from Network is used to install an OTM client. The client has applications/executables, but uses the common data from the OTM server. You must have the OTM Server software installed prior to installing the client software.

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 sets (telephones), and

OTM Clients that can be configured in your OTM system. In determining your maximum number of TNs, only telephone TNs and virtual TNs are counted. Trunk TNs are not included. To purchase licensing for additional TNs or Clients, please contact your OTM vendor. Click Next to continue.

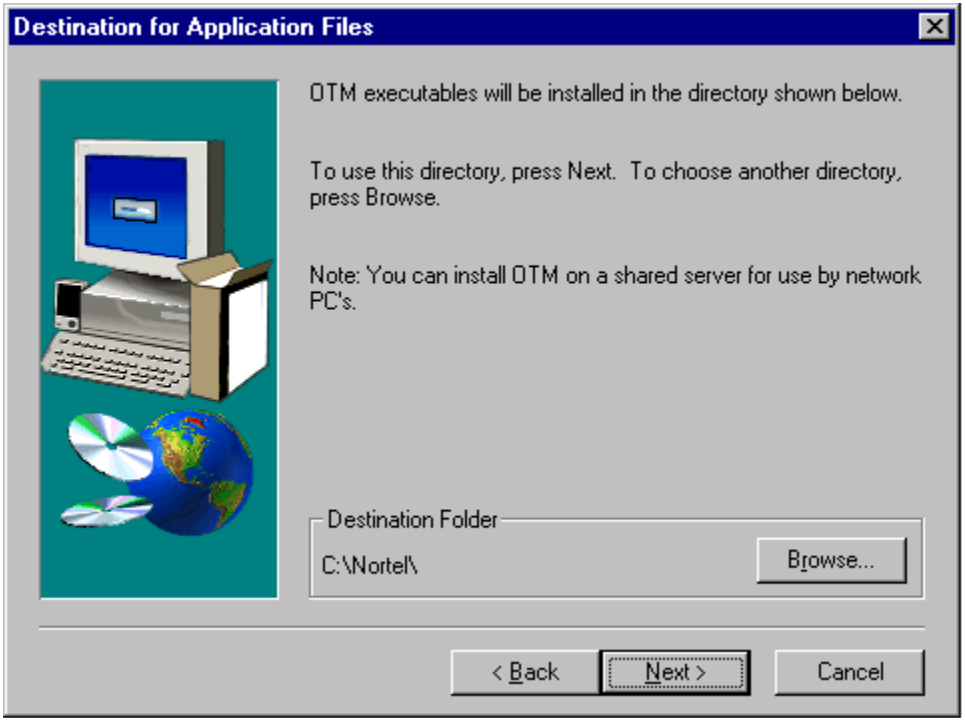
Figure 8 Enter Keycodes



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.

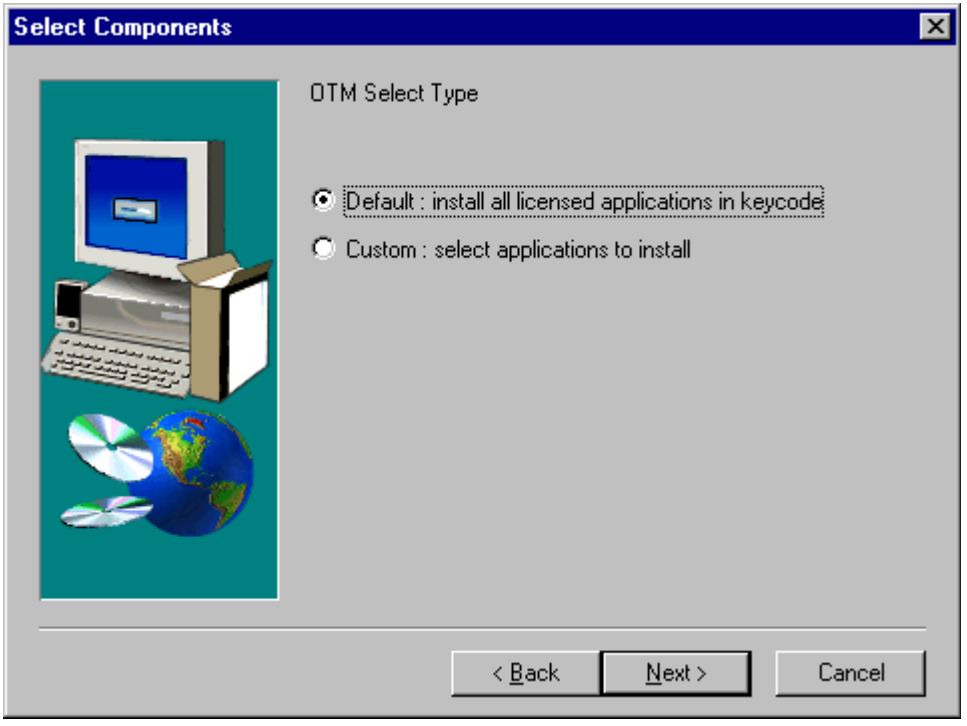
Destination for Local Data

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

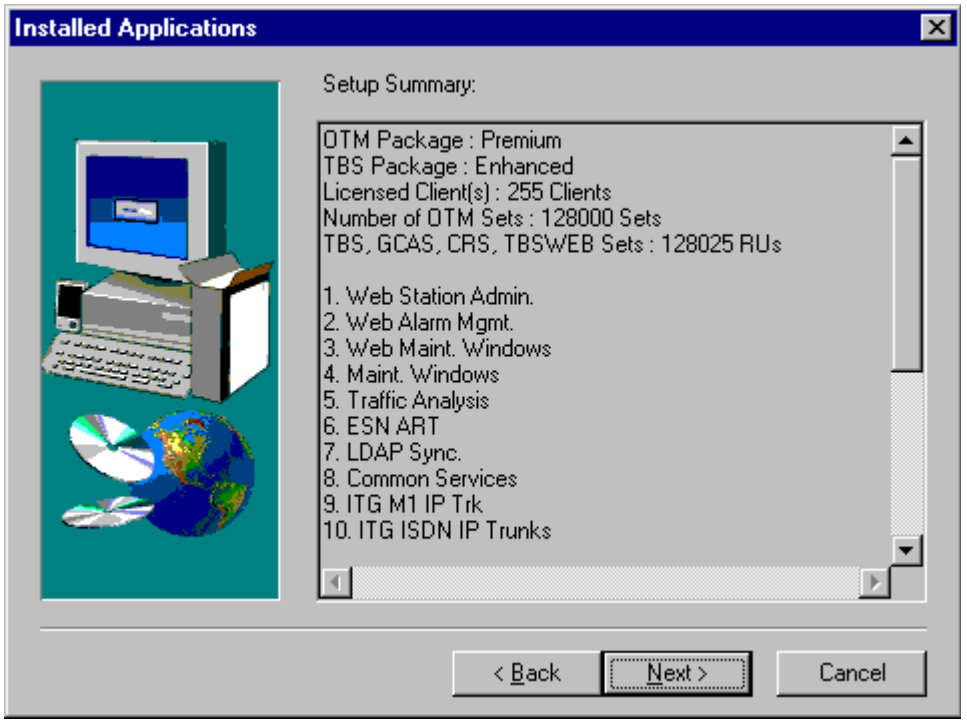
12 Specify Custom or Default installation. Select Default to install all purchased applications, select Custom to select the OTM applications that you want Setup to install (Figure 10).

Figure 10 Select Components



If you select Default, a summary of the default applications for the level of OTM that you have purchased is displayed.

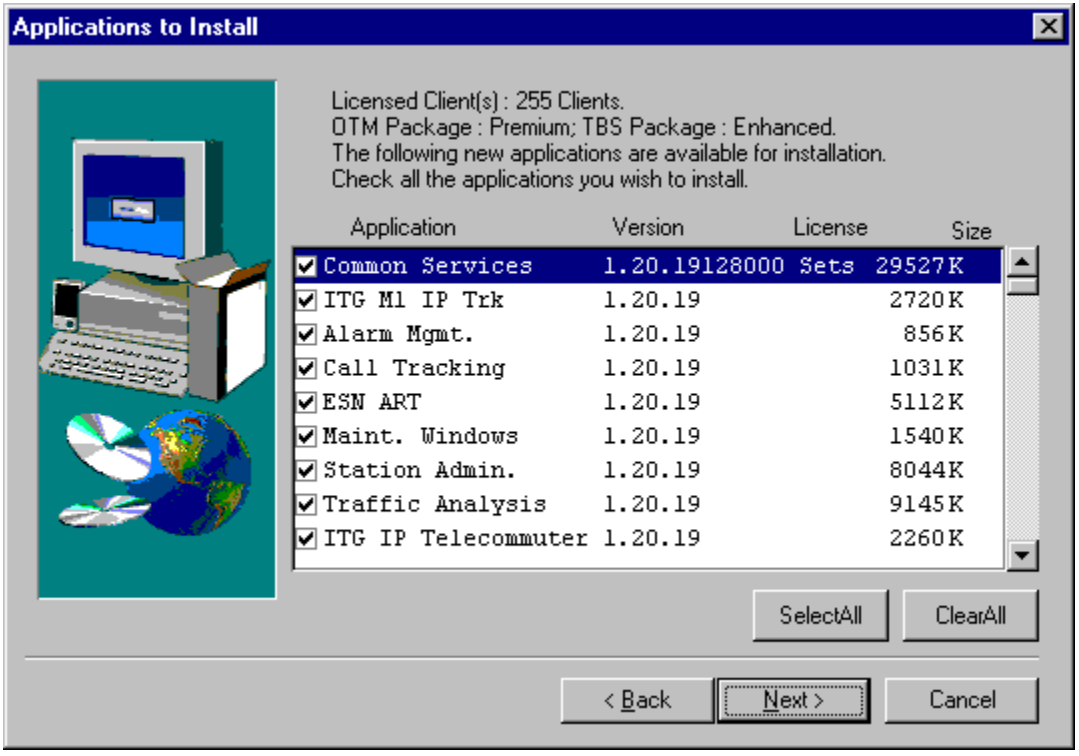
Figure 11 Summary of default applications



Applications to Install

13 If you selected Custom Install, you are given a list of applications to install (Figure 12). Check the appropriate applications.

Figure 12 Applications to Install

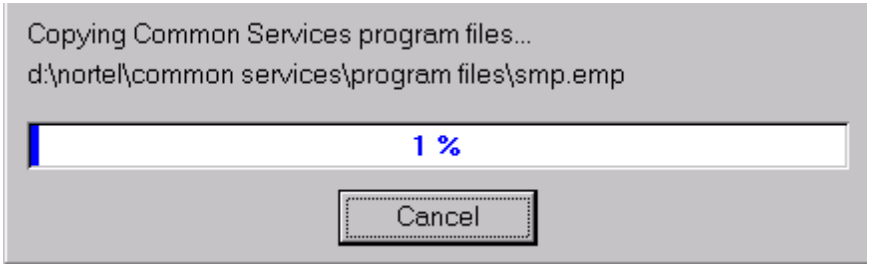


14 Click Next to continue.

Copy files

This dialog box displays the percentage status of OTM installation, which application files are being copied and their locations (Figure 13).

Figure 13 Copy files

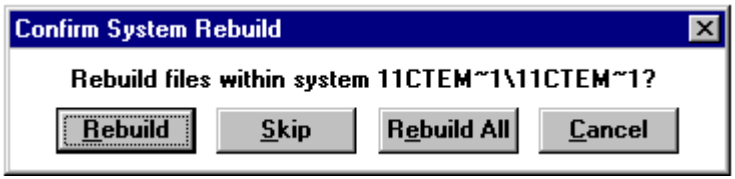


Database Rebuild

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 14:

- **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 14 Station Database Rebuild



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

Note: On a new installation, you should choose Rebuild All so that the installation process will build the Sample Data included with OTM.

You may decide to rebuild specific sites and systems only, using the Skip button. When installing for the first time, click 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 you have installed applications that require Java* Runtime Environment (JRE), you will then be prompted to install JRE at this point (Figure 15).

17 Click Yes to install JRE.

Figure 15 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\jre-1_3_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 the DECT application.

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.

19 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 Local Data directory where you installed the application.

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

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

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" on page 33 to view the installation screens that are common to both procedures.

Note: Before installing OTM software, exit all Windows programs and disable any virus detection software.

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

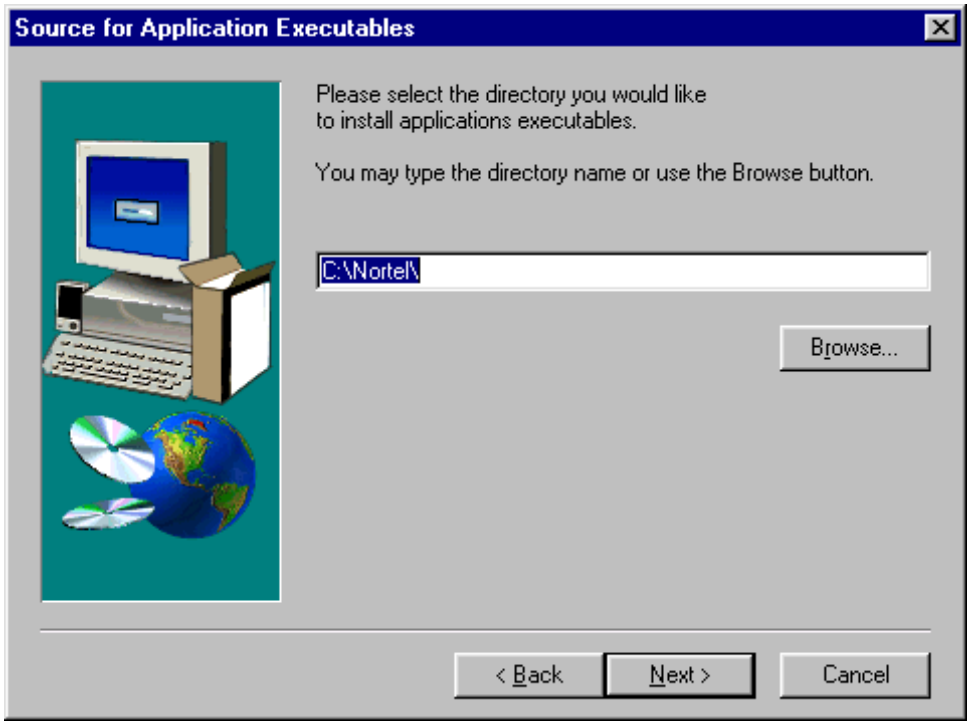
Note: If required, the setup program installs DCOM at this point if it is not present on the PC. Once installed, the PC must be rebooted. After you reboot and log in, the OTM software installation continues.

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

Note: In the OTM Client installation process, it is extremely important that you select the Run from Network option.

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

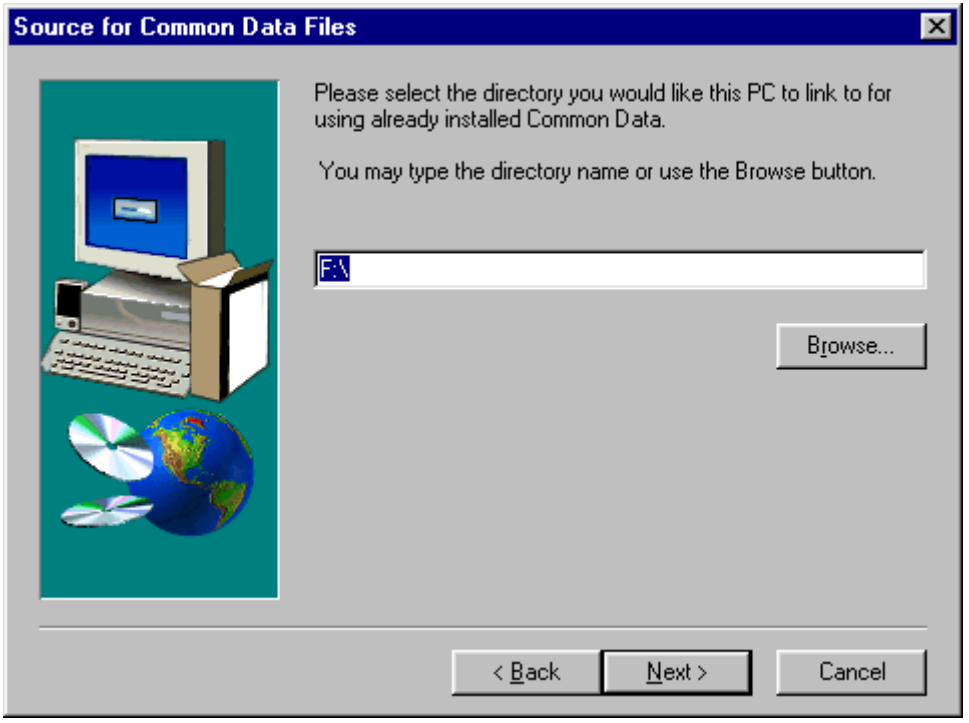
Figure 16 Source for Application Executables dialog box



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

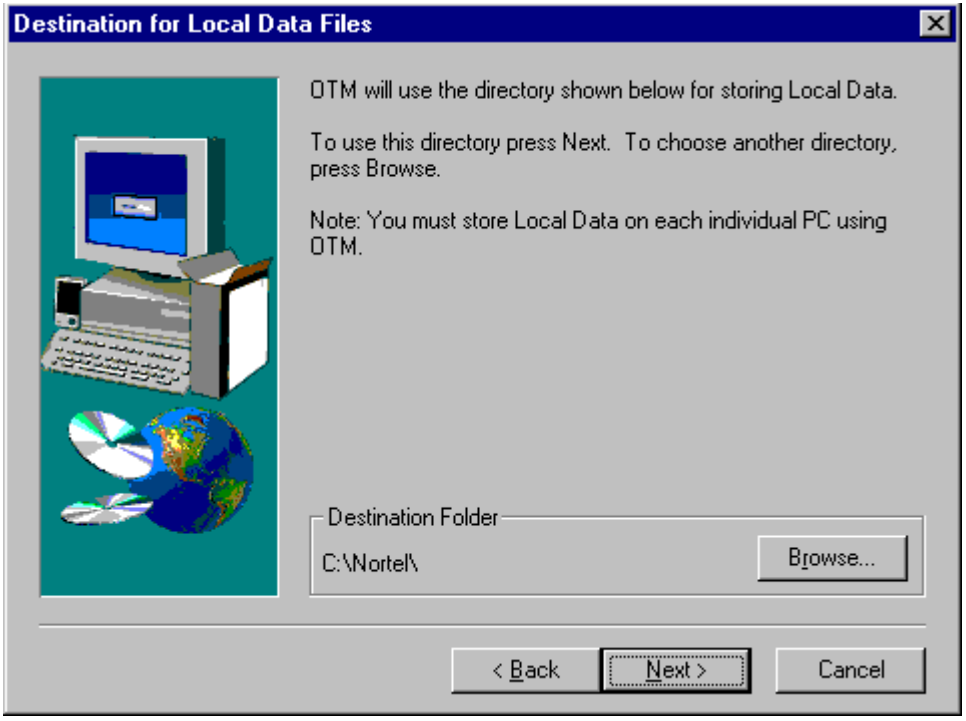
6 Select the directory, on the OTM Server, where the common data files are stored as shown in Figure 17. Click Next to continue.

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.

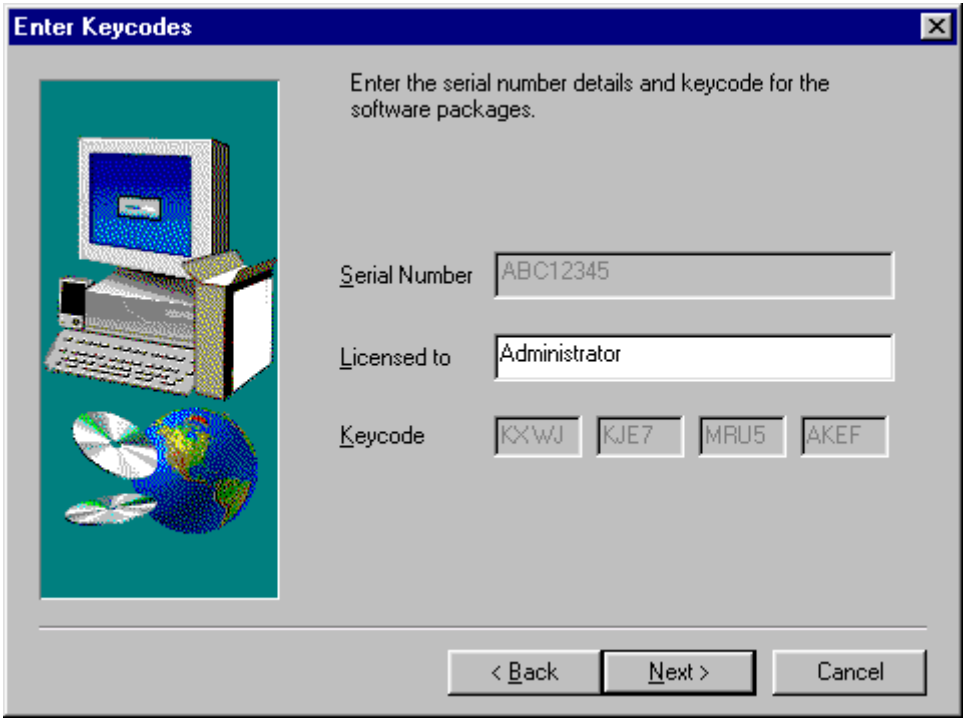
Figure 18 Destination for Local Data Files dialog box



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.

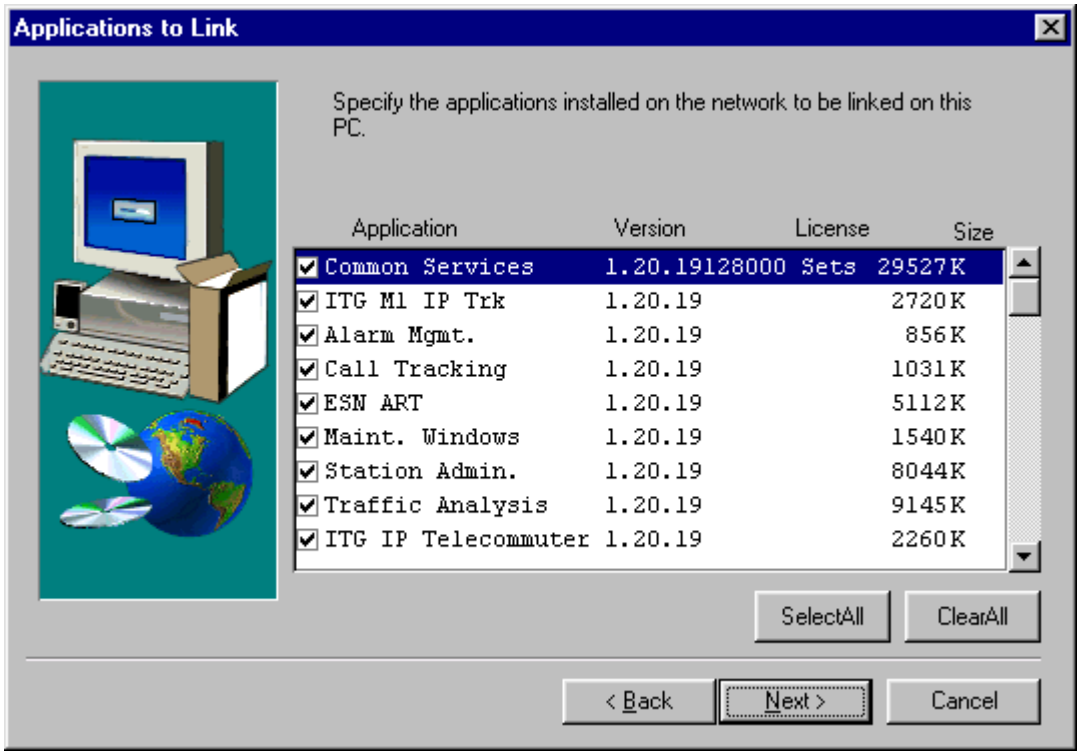
8 The Enter Keycodes dialog box appears. See Figure 19. The fields contain the data stored on the OTM Server. Click Next to continue.

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 Applications to Link dialog box



10 The following screens are displayed (see "OTM Server software installation" on page 33 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 General to Premium)
- to increase the maximum number of OTM clients or the maximum number of sets (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 sets (telephones).

Upgrading your OTM PCs to Windows 2000

Upgrading an existing version of OTM

On an existing Windows NT 4.0 server/workstation or a Windows 95/98 PC that is being upgraded to Windows 2000, use the following procedure:

Note: In this case, a previous version of OTM exists on the PCs hard drive.

1. Back up the Common Data folder to a temporary directory.
2. Uninstall OTM.
3. Upgrade the PC to Windows 2000.
4. Create a directory where the new version of OTM will be installed, for example *C:\Nortel*.
5. Copy the Common Data folder from the temporary directory created in step 1 to the new directory that you created in step 4.
6. Perform a fresh installation of your new version of OTM. See “OTM Server software installation” on page 33. Select the directory created in step 4 as the root directory.
7. The installation program will ask whether or not the existing Common Data folder is from MAT. Select “NO”.

This action skips the MAT data migration process.

Note: The build-to-build conversion process will convert the existing OTM data to the newer version of OTM. All other existing data in the Common Data folder will be preserved.

Note: If an OTM server is upgraded to a new version of OTM, all existing clients will need to upgrade to the new version.

Installation on a new Windows 2000 PC

On a new PC with Windows 2000 or an existing PC that has had its hard drive initialized before the installation of Windows 2000, use the following procedure:

1. Create a directory where the new version of OTM will be installed, for example *C:\Nortel*.
2. Copy the Common Data folder in the Nortel directory of the current copy of OTM to the new directory created in step 1.
3. Perform a fresh installation of the new version of OTM on the new Windows 2000 PC. See "OTM Server software installation" on page 33. Select the directory created in step 1 as the root directory.
4. The installation program will ask whether or not the existing Common Data folder is from MAT. Select "NO".

   This action skips the MAT data migration process.

Note: The build-to-build conversion process will convert the existing OTM data to the newer version of OTM. All other existing data in the Common Data folder will be preserved.

Note: If an OTM server is upgraded to a new version of OTM, all existing clients will need to upgrade to the new version.

Upgrade to a new release of OTM

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

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.

Note: If the client PC is a Windows 95/98 or Windows NT machine that is being upgraded to Windows 2000, delete any existing OTM directory and perform a fresh installation of the new version of OTM using the "Run from Network" option.

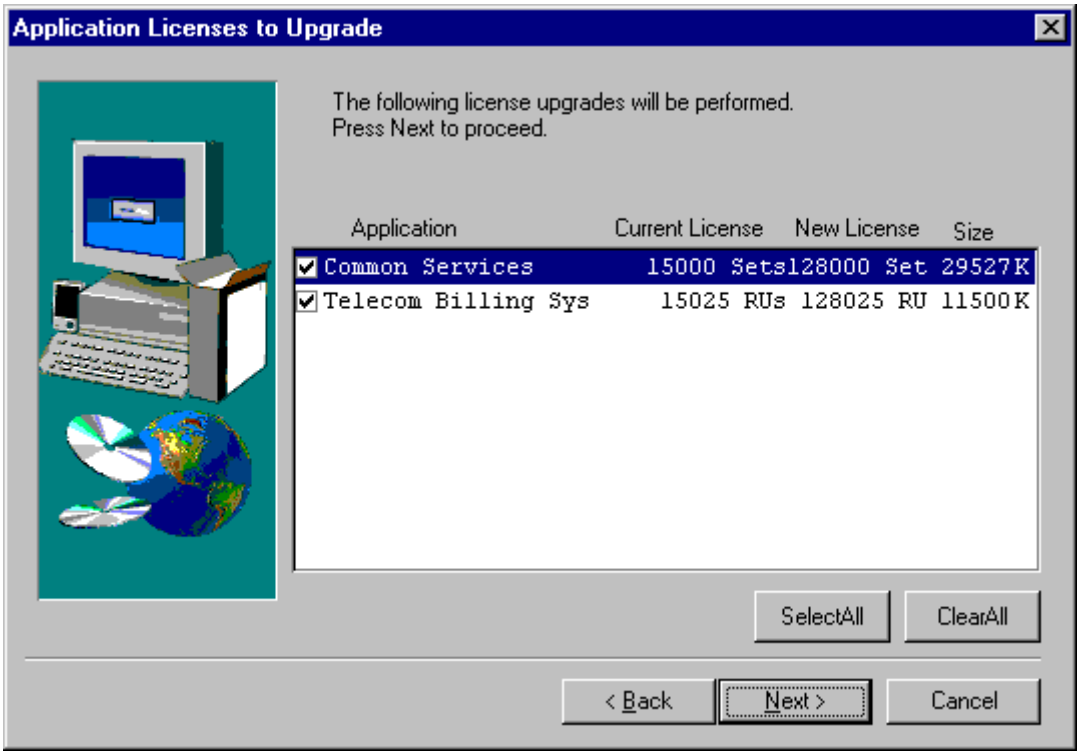
Note: If the client PC is an existing OTM client that is not being upgraded to Windows 2000, run an upgrade installation of OTM from the existing OTM server after the server has been upgraded to the new version of OTM.

To upgrade to a new release of OTM:

1. Back up the Common Data folder to a temporary directory.
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
   - **d** Setup Choices. Select "Install/Upgrade" to upgrade the OTM Server, or select "Run from Network" to upgrade an OTM Client.
   - **e** Serial Number and keycode.
   - **f** Destination for files.

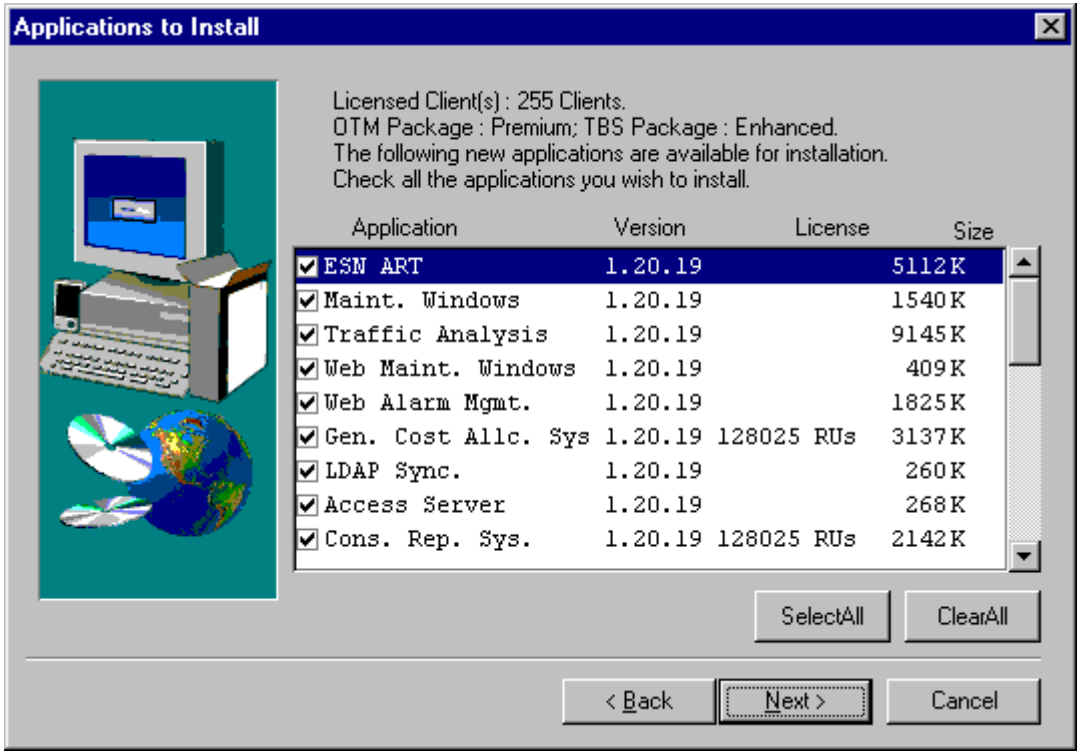
g Application licenses to upgrade. See Figure 21.

Figure 21 Application Licenses to Upgrade



h New applications to install. See Figure 22.

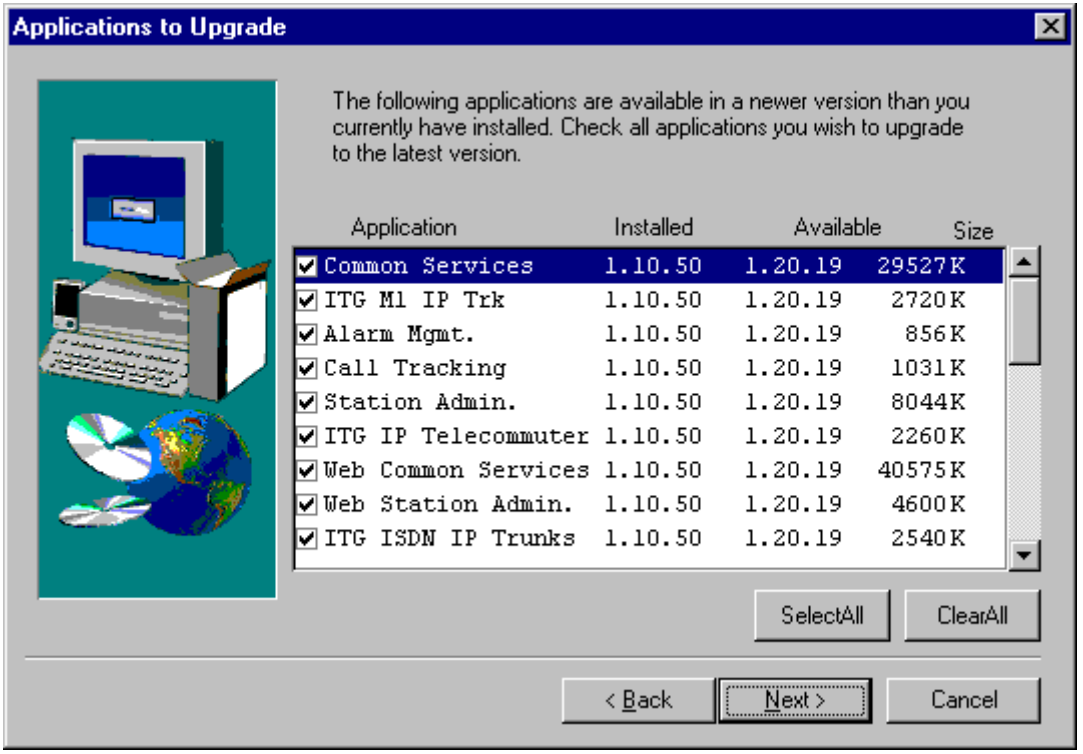
Figure 22 Applications to Install



4 Applications to upgrade. See Figure 23.

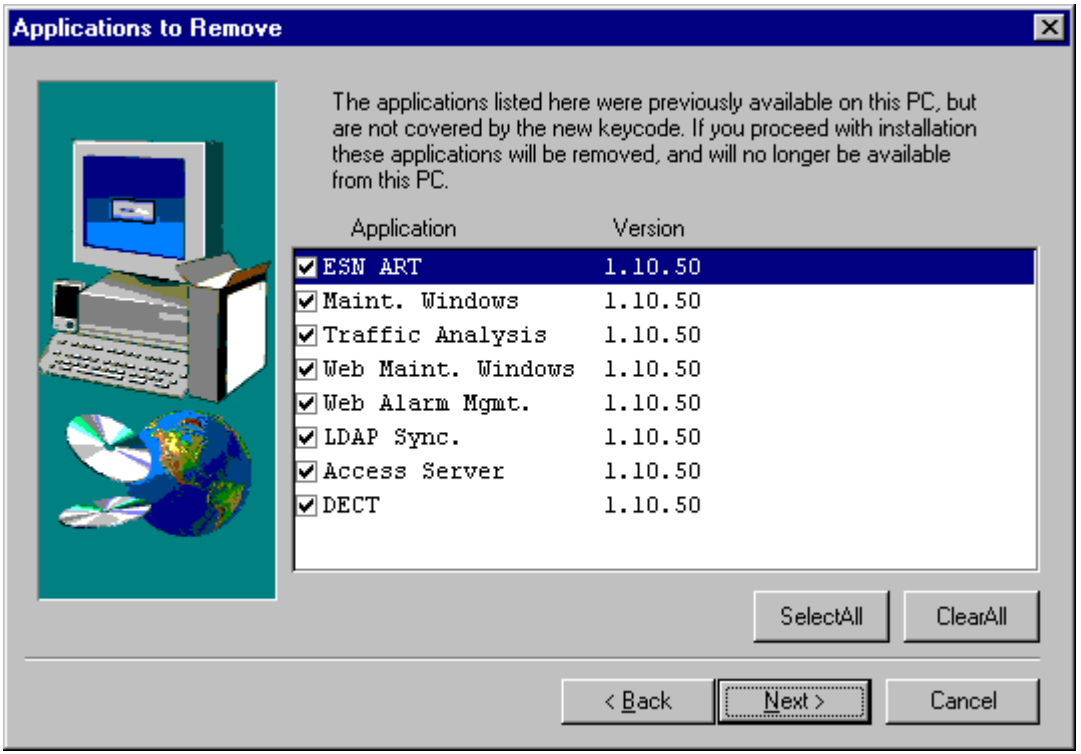
Note: When upgrading from an older release of OTM, you must choose to install the new versions of your existing applications. This is also a requirement when you are upgrading from the General or Enhanced package to the Enhanced or Premium package. If you do not install the new versions, the functionality provided in the new release of OTM will not be available.

Figure 23 Applications to Upgrade



5 Applications to remove. These are applications available in the old keycode, but not available in the new keycode. See Figure 24.

Figure 24 Applications to Remove



6 Copying files.

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

8 Install JRE, if required.

9 Install OTM Web Help, if required.

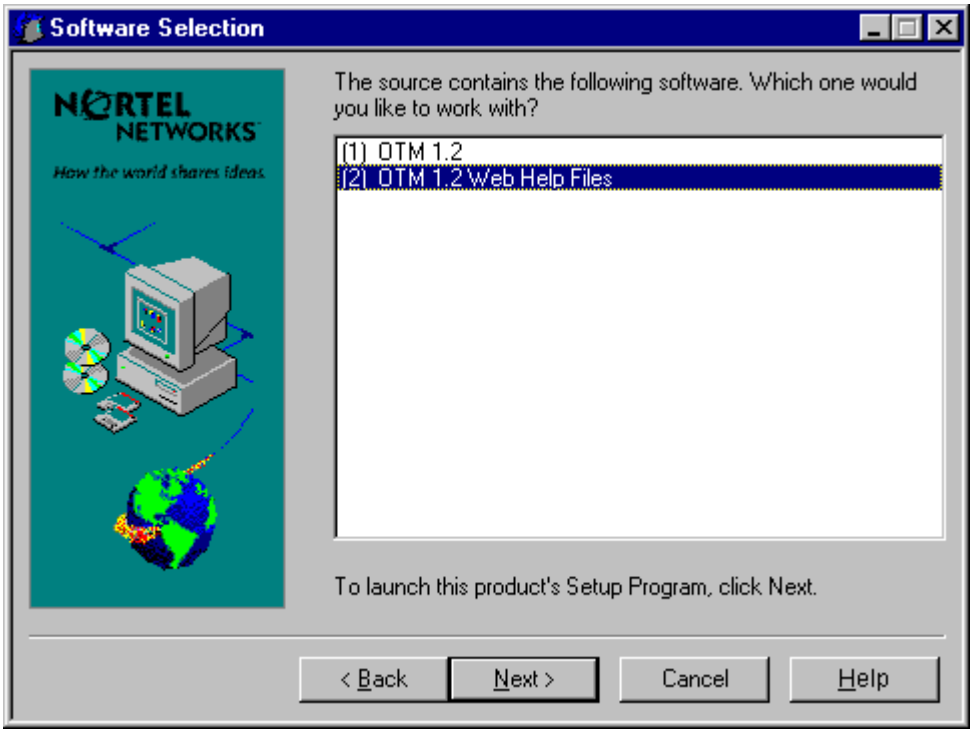
10 Reboot the PC.

Web Help Installation

If you will be using OTM Web Services, install the Web based help files by selecting the option in the Software Selection dialog box (Figure 25).

1. Double click the *Setup.exe* to launch the Software Installation Wizard (see Figure 2 on page 35).
2. Select the OTM Web Help Files option and click the Next button (Figure 25).

Figure 25 Software Selection: Web Help



3. In the Select Components dialog box (Figure 26), click the Next button to install all English Web Help or click the Change button to select the sub-components that you want to install(Figure 27).
4. Click the Continue button in the Select sub-components dialog box (Figure 27) to return to the Select Components dialog box (Figure 26).
5. Click the Next button to start the Web Help installation process.

Figure 26 Select Web Help components dialog box

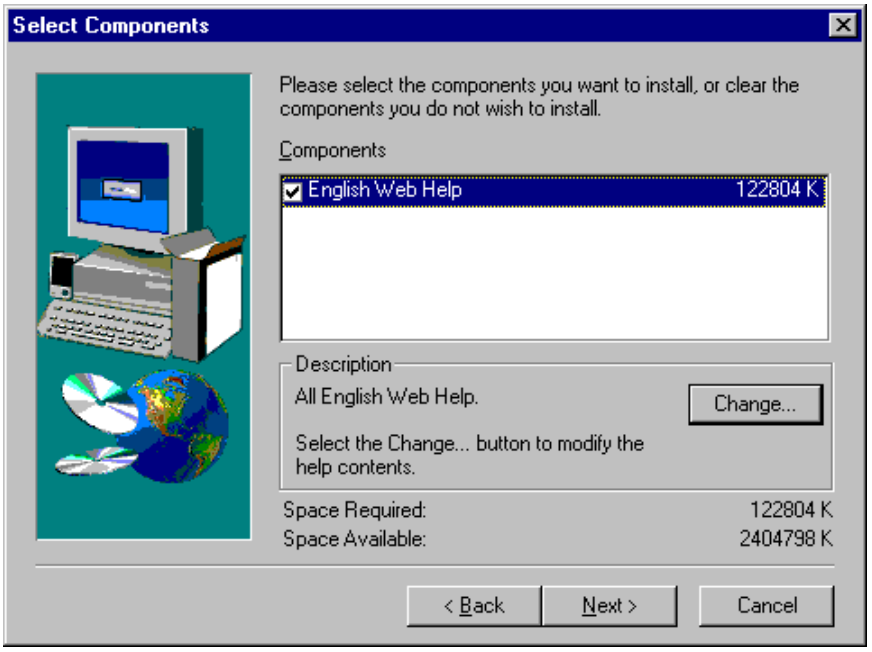
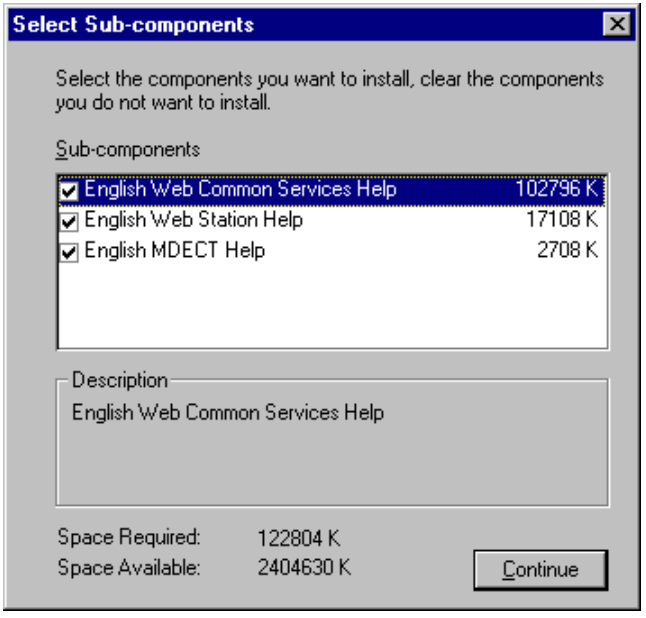


Figure 27 Select Web Help sub-components dialog box



Migration from MAT to OTM

This upgrade is performed when upgrading from MAT 6.6 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.)

Note: The Call Accounting database (MAT) cannot be migrated to the Telecom Billing System (TBS) application (OTM). Print your Call Accounting reports before upgrading from MAT to OTM.

There are four scenarios:

1. Installing OTM on a Windows 95/98/2000/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 65.
4. Installing OTM on a MAT PC which is being upgraded to Windows 2000. See "Migrating data from MAT to OTM on a PC that is being upgraded to Windows 2000" on page 66.

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 28.

Figure 28 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.

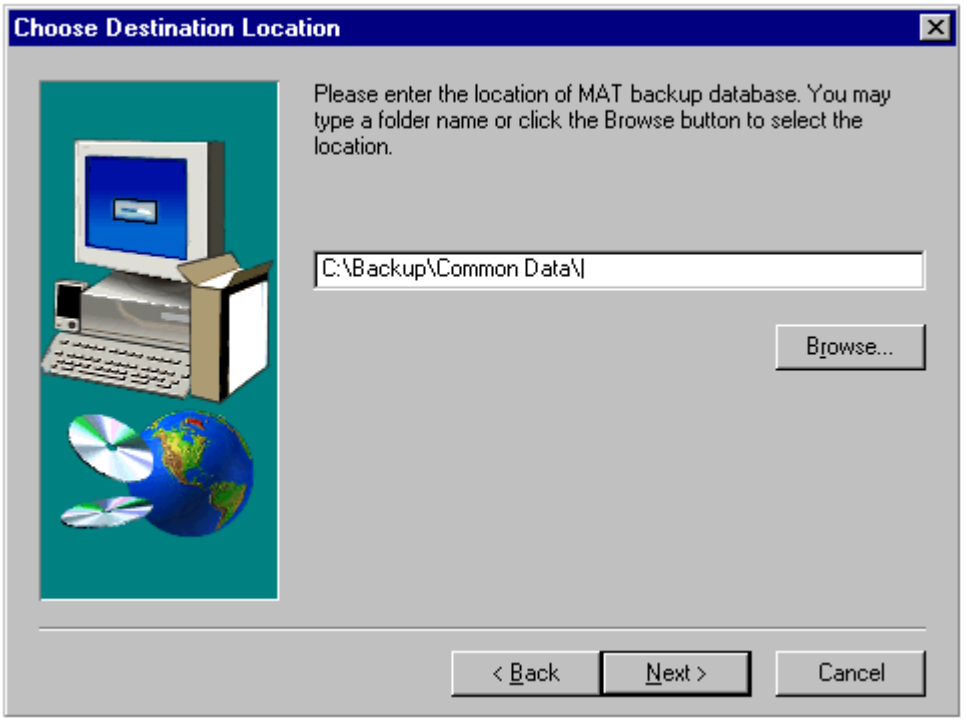
Installing OTM on a Windows NT server being used as a MAT file server.

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 29.

Figure 29 MAT Backup Database: Choose Destination Location



1 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.

Migrating data from MAT to OTM on a PC that is being upgraded to Windows 2000

On an existing Windows NT 4.0 server/workstation or a Windows 95/98 PC that is being upgraded to Windows 2000, use the following procedure:

Note: In this case, a current copy of MAT exists on the PCs hard drive.

1 Back up the Common Data folder to a temporary directory.

2 Uninstall MAT.

3 Upgrade the PC to Windows 2000.

4 Perform a fresh installation of OTM. See "OTM Server software installation" on page 33.

5 From the Start button, select Programs > Optivity Telephony Manager > Database Migration Utility. When asked for the location of the MAT database, type or browse to the location where the Common Data folder was backed up in step 1.

Note: For additional information on migrating the database from MAT to OTM, see "Migrating data from MAT to OTM on the same PC" on page 63.

Migrating data from MAT to OTM on a new Windows 2000 PC

On a new PC with Windows 2000 or an existing PC that has had its hard drive initialized before the installation of Windows 2000, use the following procedure:

1. Copy and rename the Nortel directory in the current copy of MAT.
2. Move the renamed Nortel directory to the Windows 2000 PC.
3. Perform a fresh installation of OTM on the new Windows 2000 PC. See "OTM Server software installation" on page 33.
4. Follow the procedure outline in "Migrating data from MAT to OTM on the same PC" on page 63, beginning with step 4, to migrate the data from MAT to OTM.

MAT/OTM migration summary

Table 2 and Table 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		
6.6	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 in standalone mode

	MAT data migration for OTM in 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		
6.6	95/98/WS/server	95/98/WS/server

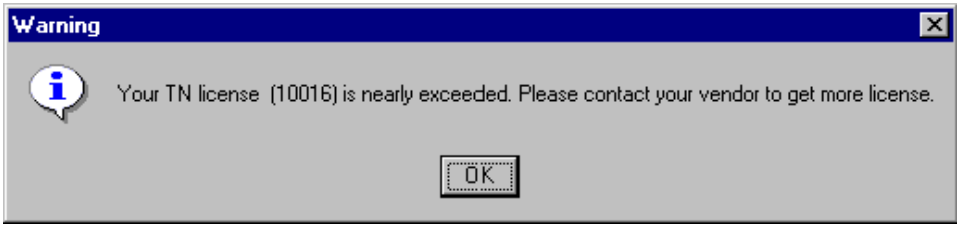
License Management

The serial number and keycode which you received with your OTM software package determine the maximum number of terminal numbers (TNs), or telephones, reporting units (RUs) and OTM Clients that can be configured in your OTM system. To purchase licensing for additional TNs, RUs, 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 set TNs (telephone TNs and virtual TNs) configured in your system is approaching the maximum for your license, the dialog box shown in Figure 30 will appear.

Figure 30 TN license warning dialog box



If your TN license has been exceeded, the error message shown in Figure 31 will appear. This message will appear every 15 minutes. Contact your vendor to obtain a license for additional TNs.

Figure 31 TN license error dialog box

Note: TN checking is performed on bootup and after every 12 hours of operation. If you delete a site, the TN licenses associated with that site will become available for reuse after the next TN check. If you are unable to wait for the next TN check, you can reboot the OTM server.

RU license

Reporting Units (RUs) are the base used for licensing the telemanagement applications in OTM. An RU represents a single entity in the OTM Corporate databases to which costs/usage can be assigned and reported on through the telemanagement applications. An entity can be either an employee in the Employee database, an external party in the External Parties database, or a role or project in the Roles/Projects database.

Each time you launch a telemanagement application in OTM, your RU license is checked. If the number of RUs configured in your system is approaching the maximum for your license, a warning dialog box will appear.

If your RU license has been exceeded, you will receive an error message. The TBS application will continue to collect data; however, you will not be able to cost the data and generate reports. The GCAS application will launch, but you will not be allowed to generate reports. Contact your vendor to obtain a license for additional RUs.

See *Using Optivity Telephony Manager Telemanagement Applications* (553-3001-331) for more information.

Client license

When you install an OTM Client, the host name 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 32 will open.

Figure 32 Client removed dialog box

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

If the host name of an OTM Client machine is changed, the OTM Administrator can use the Client Utility to update the host name in the OTM database. For information on the Client Utility, please refer to *Using Optivity Telephony Manager* (553-3001-330).

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.

Chapter 2
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 or Succession CSE 1000 system and change the default OTM password.

Test the connection using the sample site and system configuration. See "Test the connection" on page 78.

After connecting successfully, refer to "Add sites and systems via the OTM Navigator window" on page 86 to configure your own sites and systems.

The complete list of OTM configuration procedures includes:

- "Integrating OTM with HP OpenView" on page 164

Configuring a modem for OTM applications in Windows

To insure that a modem is configured correctly for use with Microsoft Windows 95, Windows 98, Windows 2000, 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 or Succession CSE 1000 system.

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 or Succession CSE 1000 SDI port. In most cases, the modem attached to the SDI port is configured to run in dumb mode at the same speed the Meridian 1 or Succession CSE 1000 SDI port is configured for (at 9600 bps or less). This locks the modem into a specific mode of operation to prevent the modem from being run in command mode (echo input) or connecting at a different baud rate than the Meridian 1 or Succession CSE 1000 SDI port is configured for.

When a high speed smart modem is used on the OTM PC to dial up the Meridian 1 or Succession CSE 1000 modem, the PC modem will always attempt to connect at its highest possible speed. The Meridian 1 or Succession CSE 1000 system’s 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 Meridian 1 or Succession CSE 1000 SDI port. These garbage characters may eventually lock up the Meridian 1 or Succession CSE 1000 SDI port. The two modems may still be connected, but access to the Meridian 1 or Succession CSE 1000 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 Meridian 1 or Succession CSE 1000 SDI port and Meridian 1 or Succession CSE 1000 system's modem is locked to the Meridian 1 or Succession CSE 1000 SDI port's baud rate if a high speed modem is installed on 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 on the correct COM port. From the Start button, select Settings > Control Panel. Open the Modems file and click the Properties button.

  Test the COM port to which your modem is connected by launching HyperTerminal. From the Start button, select 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 Meridian 1 or Succession CSE 1000 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 **ATDT*1234567***, where ***1234567*** is the phone number for the modem connected to the Meridian 1 or Succession CSE 1000 system. 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 PPP or Serial Communications profiles for the system to which you wish to connect. Make sure that the data bits, stop bits, and parity match as well. To view the Communications profiles for a system, right click on the desired system in the Navigator window. Select Properties from the pop up menu, and click on the Communications tab in the Properties dialog box.

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 the PPP or Serial Communications profiles for the system to which you wish to connect. To view the Communications profiles for a system, right click on the desired system in the Navigator window. Select Properties from the pop up menu, and click on the Communications tab in the Properties dialog box.

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 Meridian 1 or the Succession CSE 1000 is the same as the IP address you entered in the address field in the PPP Communications profile for the system to which you wish to connect. To view the Communications profiles for a system, right click on the desired system in the Navigator window. Select Properties from the pop up menu, and click on the Communications tab in the Properties dialog box.
- If possible, verify that you can make an Ethernet connection to the same system.

  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 Meridian 1 or Succession CSE 1000 system's local IP address. See "Set Up the Meridian 1 or Succession CSE 1000 system" on page 120 for information on configuring Ethernet and PPP on the Meridian 1 or the Succession CSE 1000. Verify that the data lights on your modem flash as the ping data is sent to the Meridian 1 or Succession CSE 1000 system. If you do not receive a response from the Meridian 1 or Succession CSE 1000 system, verify that the IP address that you assigned to the local PPP interface on the Meridian 1 or Succession CSE 1000 system is the same as the IP address you entered in the address field in the System Properties—Communication, PPP connection type dialog box for the system to which you want 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 Start > Settings > Control Panel, double-click 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 28800 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.

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:

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

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

3 Click the OK button.

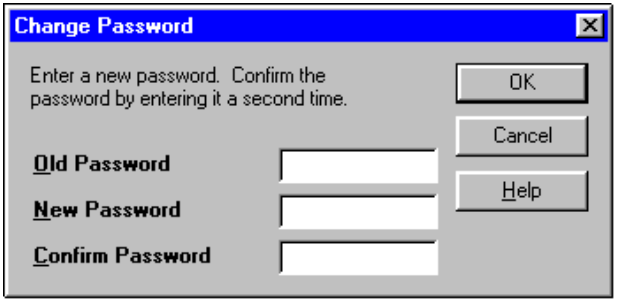
After OTM accepts your ID and password, the OTM Windows Navigator opens.

4 Change the default password to ensure security:

- In the Navigator window, choose Security > Change Password.

  The Change Password dialog box opens (Figure 33).

Figure 33 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 the OK button.

- A message box informs you that the password was successfully changed. Click the OK button to close the message box.

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

When exiting from OTM, you 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. For detailed instructions on adding sites and systems, see "Add sites and systems via the OTM Navigator window" on page 86.

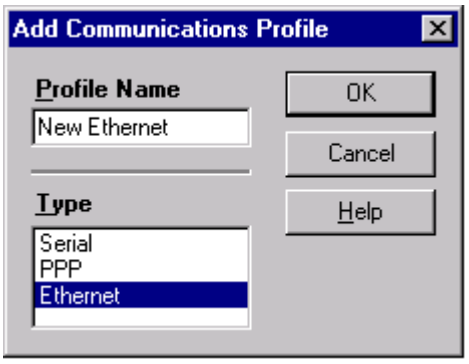
Set up communications information

1. Double-click Sample Site in the OTM Navigator window.
2. Click Sample System and choose File > Properties.

   The System Properties dialog box opens with the General tab displayed.
3. Click the Communications tab.
4. Click the Add button.

   The Add Communications Profile dialog box opens (Figure 34).

Figure 34 Add Communications Profile dialog box



5 In the Type box, select a connection type that will be used by OTM.

6 Enter a Profile Name.

7 Click the OK button.

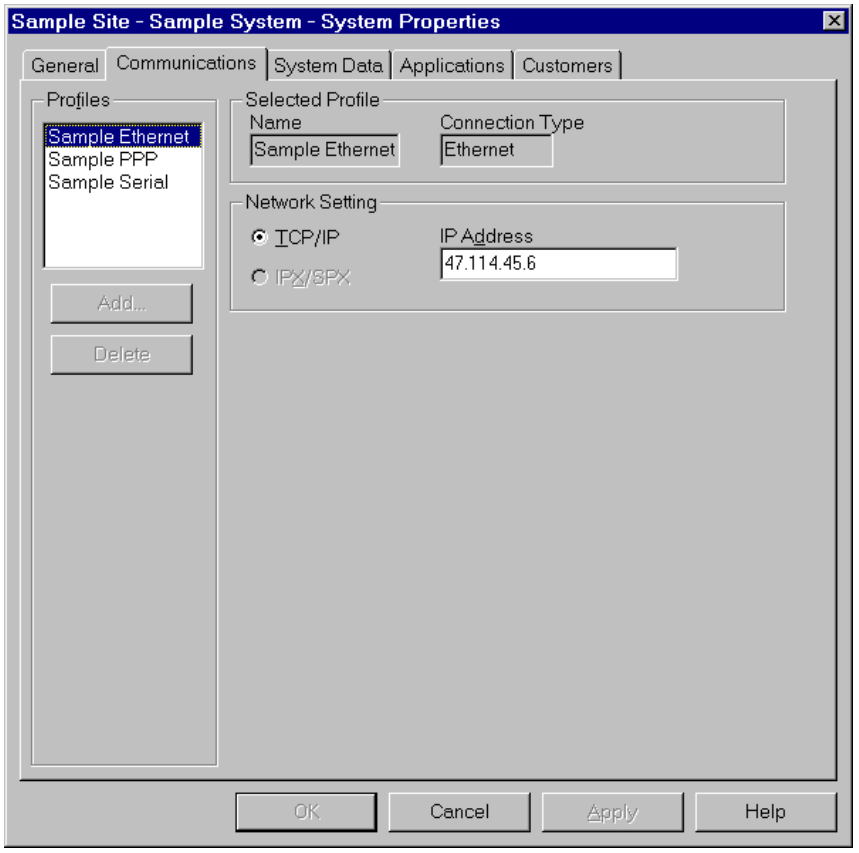
8 Enter the information in the System Properties—Communications dialog box for the connection type selected in step 5.

For an Ethernet connection type (Figure 35):

a Enter the IP address that you configured on the Meridian 1 or Succession CSE 1000 system.

b Click the Apply button.

Figure 35 System Properties—Communications, Ethernet connection type



For a PPP connection type (Figure 36):

a Enter all modem parameters and dialup information.

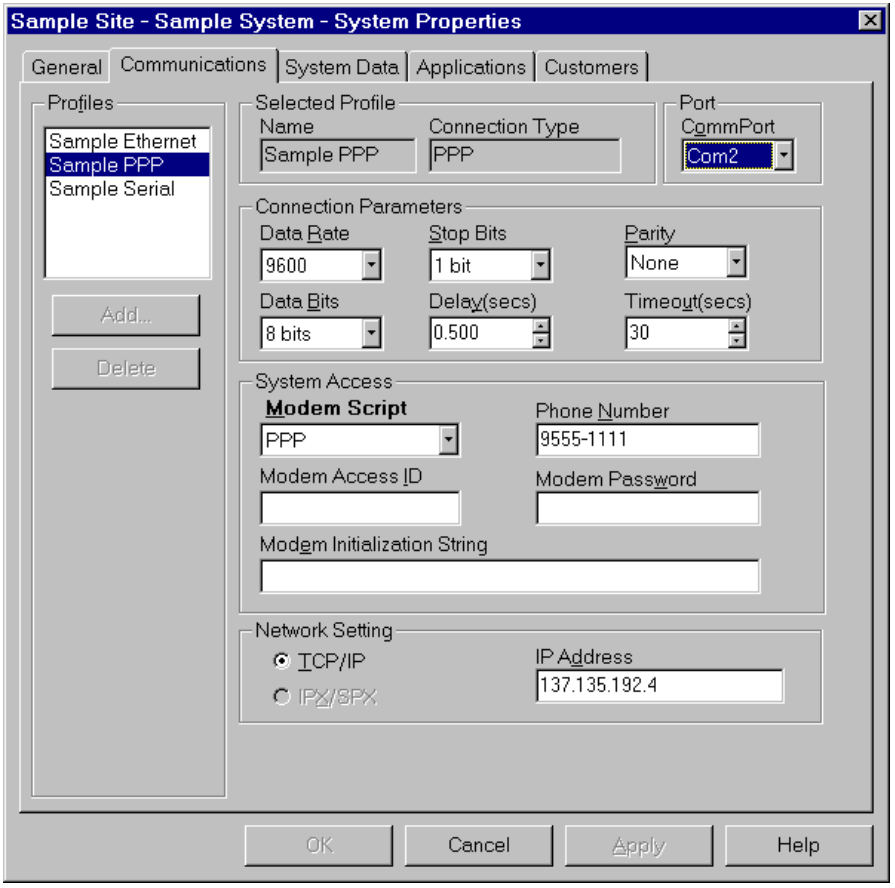
b Select PPP in the Modem Script text box and enter the phone number.

Note: There may be conditions, depending on your particular installation, where you may be required to enter a Modem Access ID, a Modem Password, and a Modem Initalization String.

c Set the IP address to the local IP address, as configured on the Meridian 1 or Succession CSE 1000 system.

d Click the Apply button.

Figure 36 System Properties—Communications, PPP connection type



For a Serial connection type (Figure 37):

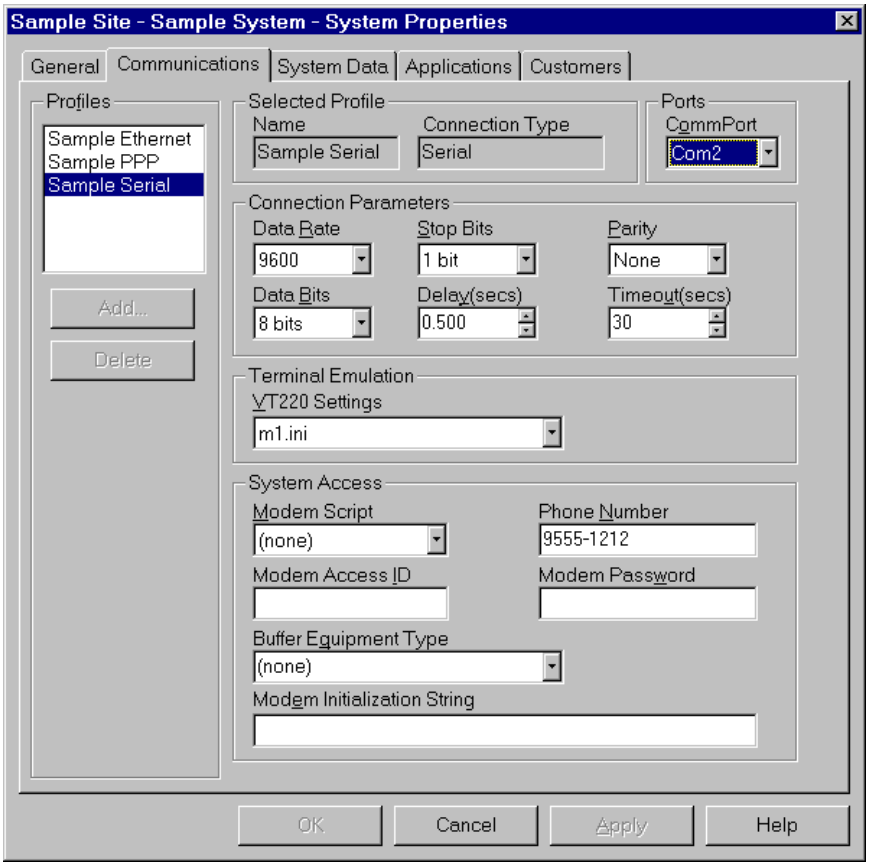
a Enter all modem parameters and dialup information.

b Select the appropriate value in the Modem Script text box.

Note: This will commonly be “None” unless a specific value is defined for your system.

c Click the Apply button.

Figure 37 System Properties—Communications, Serial connection type



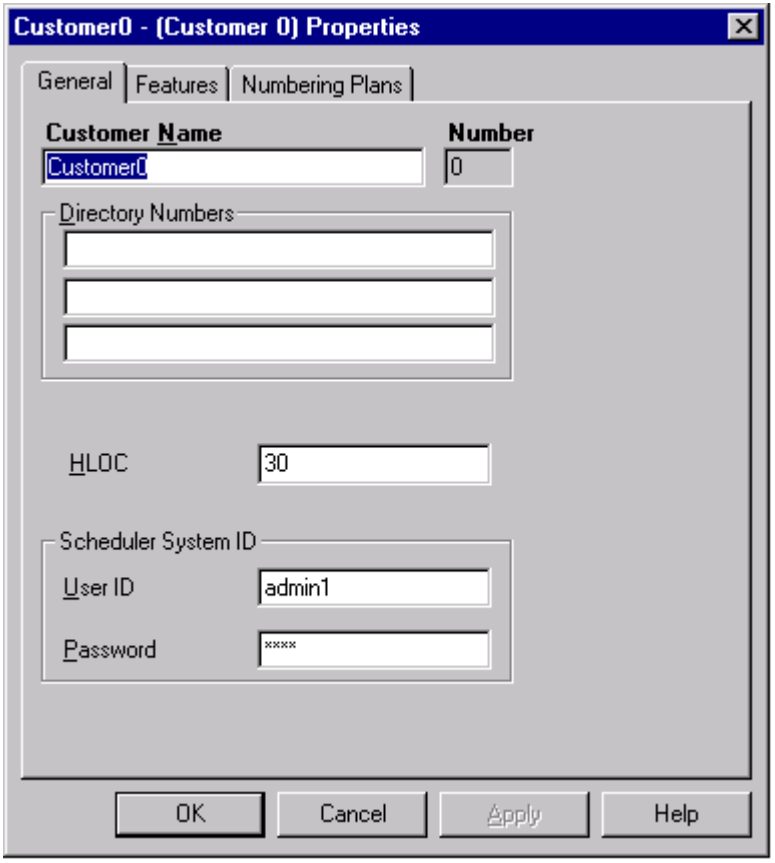
Set up customer information

1 Click the Customers tab.

2 Click the Properties button.

The Customer Properties dialog box opens with the General tab displayed (Figure 38).

Figure 38 Customer Properties—General dialog box



3 In the Scheduler System ID box, change the User ID and Password to one that is valid for logging onto the Meridian 1 or Succession CSE 1000 system, then click the OK button.

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

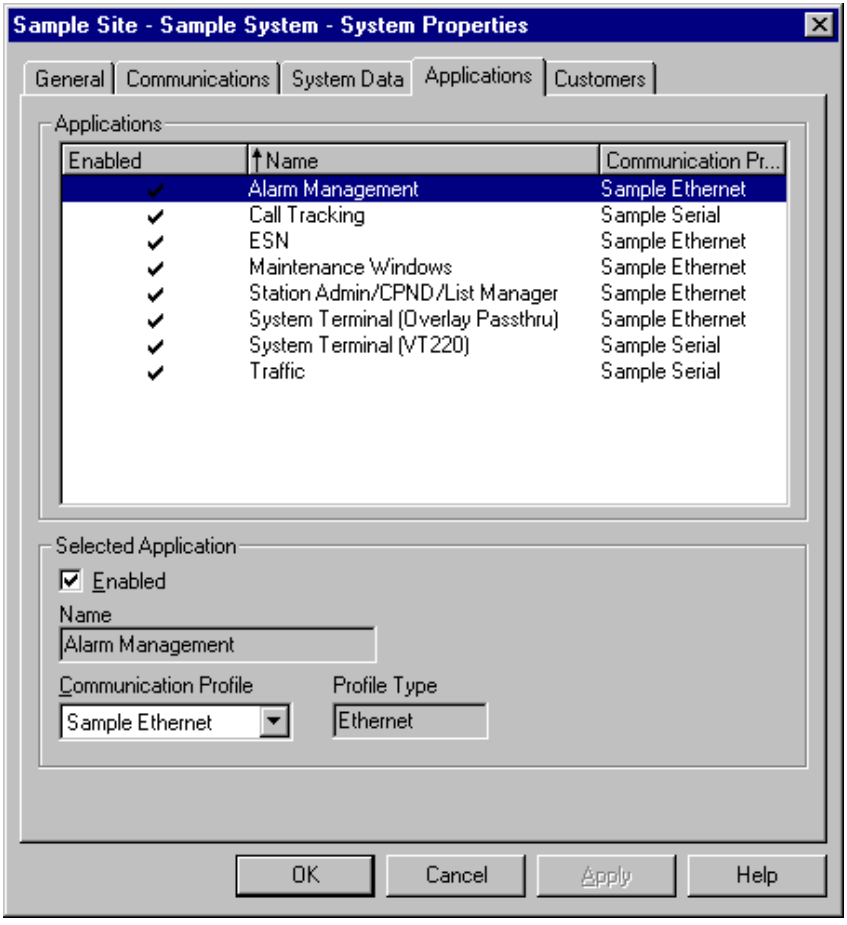
Set up OTM applications

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

1 Click the Applications tab.

The System Properties—Applications dialog box is displayed (Figure 39).

Figure 39 System Properties—Applications dialog box



2 Enable each OTM Windows application:

— Select the application.

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

A check mark appears in the Enabled check box and next to the application name.

3 Click the OK button.

Set up system data

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

2 Choose File > Update System Data.

3 Select the options “Update Data Stored in the PC” and “Do it Now”.

4 Click the OK button.

The system data (such as the machine type and software packages) is copied into OTM directly from the Meridian 1 or Succession CSE 1000 system.

Add sites and systems via the OTM Navigator window

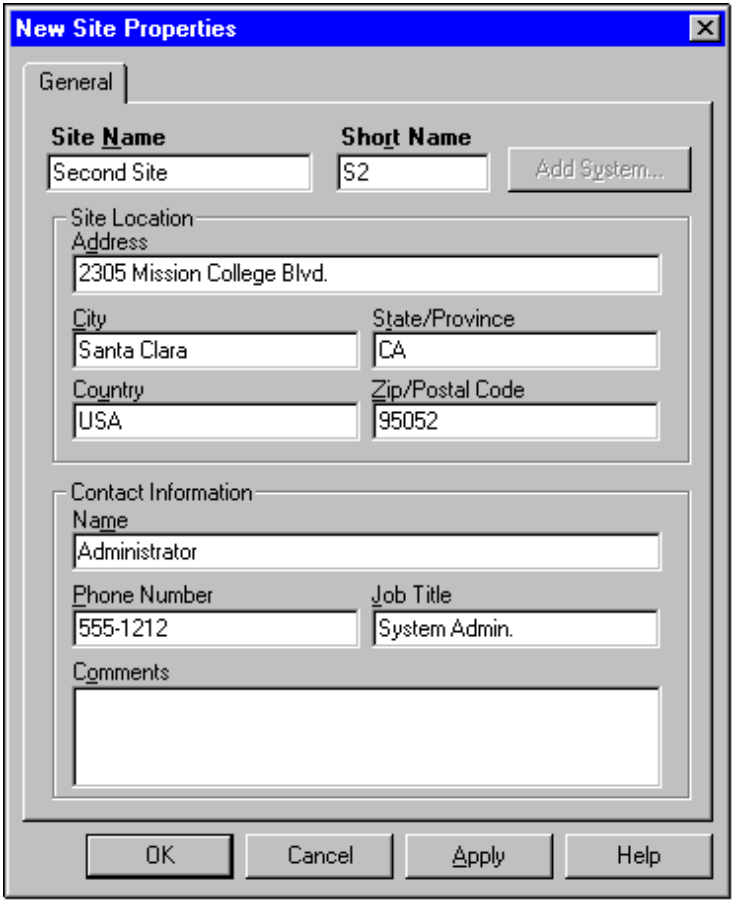
Adding a site

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

1 Choose Configuration > Add Site in the OTM Navigator window.

The New Site Properties dialog box opens (Figure 40).

Figure 40 New Site Properties dialog box



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.

5 Click the Apply button.

6 To add a new system to this site:

a Click the Add System button.

b Follow the instructions for "Adding a Meridian 1 or Succession CSE 1000 system" on page 88 or "Adding a Generic system or device" on page 103.

7 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. Repeat step 6 to add another system.
- Cancel closes the dialog box without adding the site.

Adding a Meridian 1 or Succession CSE 1000 system

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

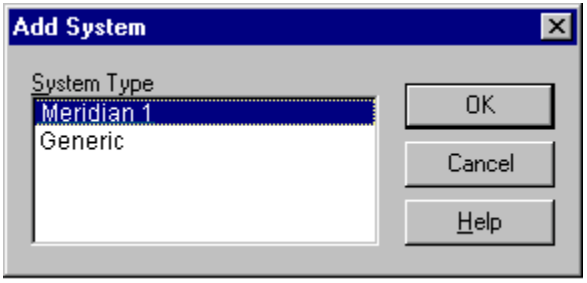
1 In the Navigator window, select the desired site.

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

2 Choose Configuration > Add System or right click and select Add System.

The Add System dialog box opens (Figure 41).

Figure 41 Add System dialog box



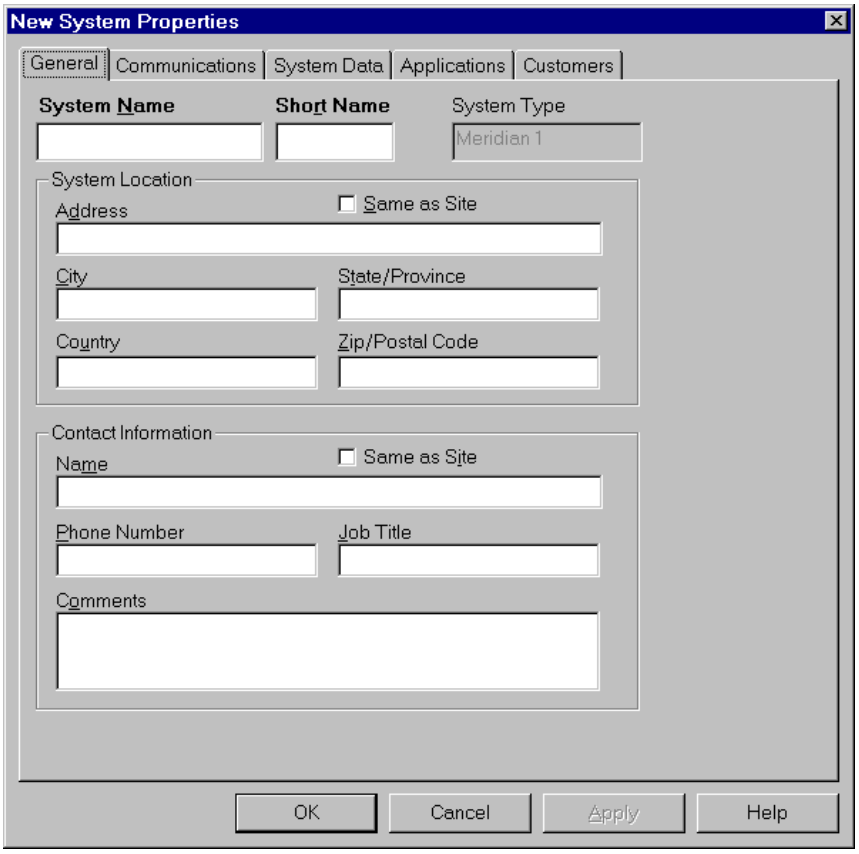
Note: For Succession CSE 1000 systems, select Meridian 1 as the system type.

Note: You may need to install additional software to enable other system types not listed in Figure 41. Follow the installation instructions included with your order.

3 Select the type of system you want to add. Click the OK button.

The System Properties dialog box opens with the General tab selected (Figure 42).

Figure 42 System Properties—General tab



4 Enter the System Name and Short Name (required fields) and other information as needed. Click the Apply button.

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

Note: For Option 11C systems with Survivable Expansion Cabinets, you should choose site and system names that will enable you to easily identify the main cabinet and its associated Expansion Cabinets.

Note: For Succession CSE 1000 systems, you should choose site and system names that will enable you to easily identify the Call Server and its associated Media Gateways.

Note: Bold 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.

Use the System Properties—Communications dialog box to define communications profiles that may be applied to system applications. One profile may be used for multiple applications.

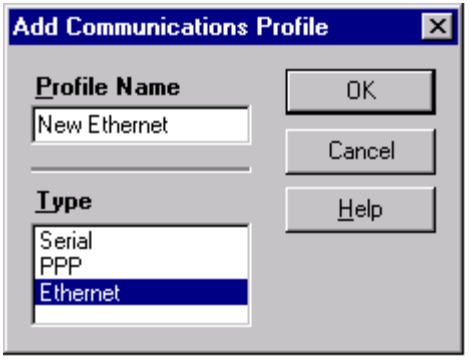
To add a new communication profile:

5 Click the Communications tab.

6 Click the Add button.

The Add Communications Profile dialog box opens (Figure 43).

Figure 43 Add Communications Profile dialog box



7 In the Type box, select a connection type that will be used by OTM.

8 Enter a Profile Name.

9 Click the OK button.

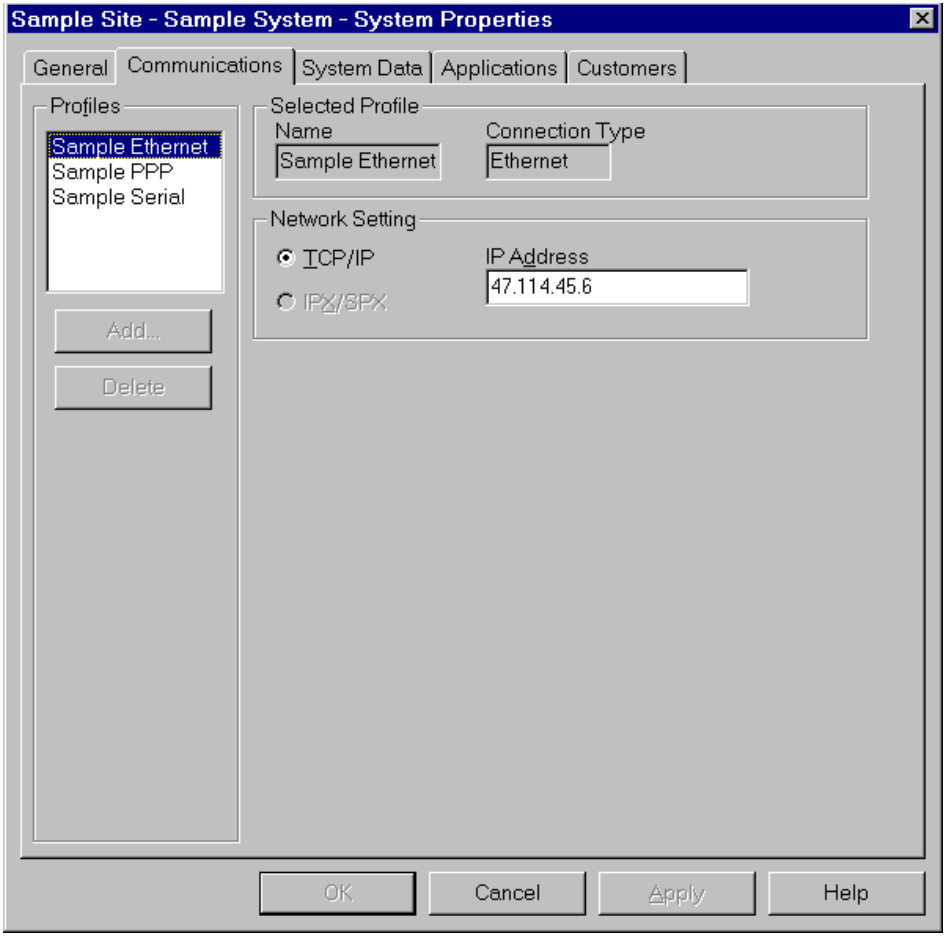
10 Enter the information in the System Properties—Communications dialog box for the connection type selected in step 7.

For an Ethernet connection type (Figure 44):

a Enter the IP address that you configured on the Meridian 1 or Succession CSE 1000 system.

b Click the Apply button.

Figure 44 System Properties—Communications, Ethernet connection type



For a PPP connection type (Figure 45):

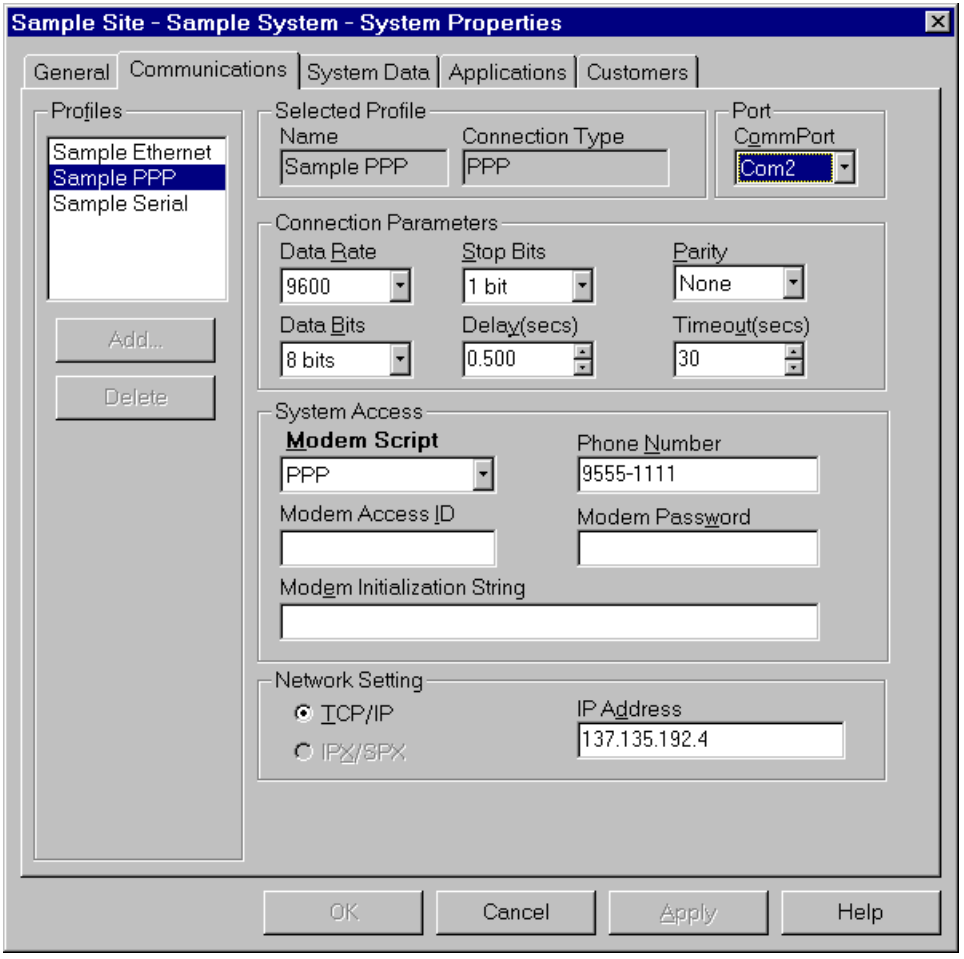
a Enter all modem parameters and dialup information.

b Select PPP in the Modem Script text box.

c Set the IP address to the local IP address, as configured on the Meridian 1 or Succession CSE 1000 system.

d Click the Apply button.

Figure 45 System Properties—Communications, PPP connection type



For a Serial connection type (Figure 46):

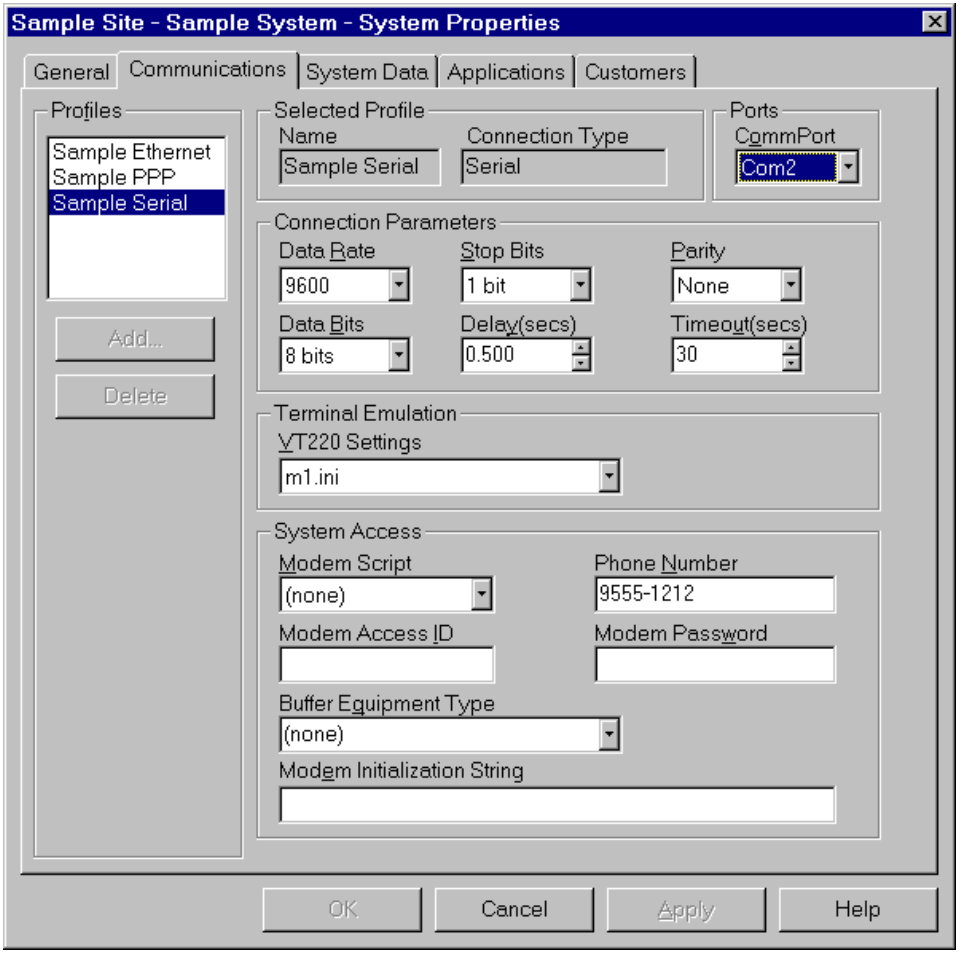
a Enter all modem parameters and dialup information.

b Select the appropriate value in the Modem Script text box.

Note: This will commonly be “None” unless a specific value is defined for your system.

c Click the Apply button.

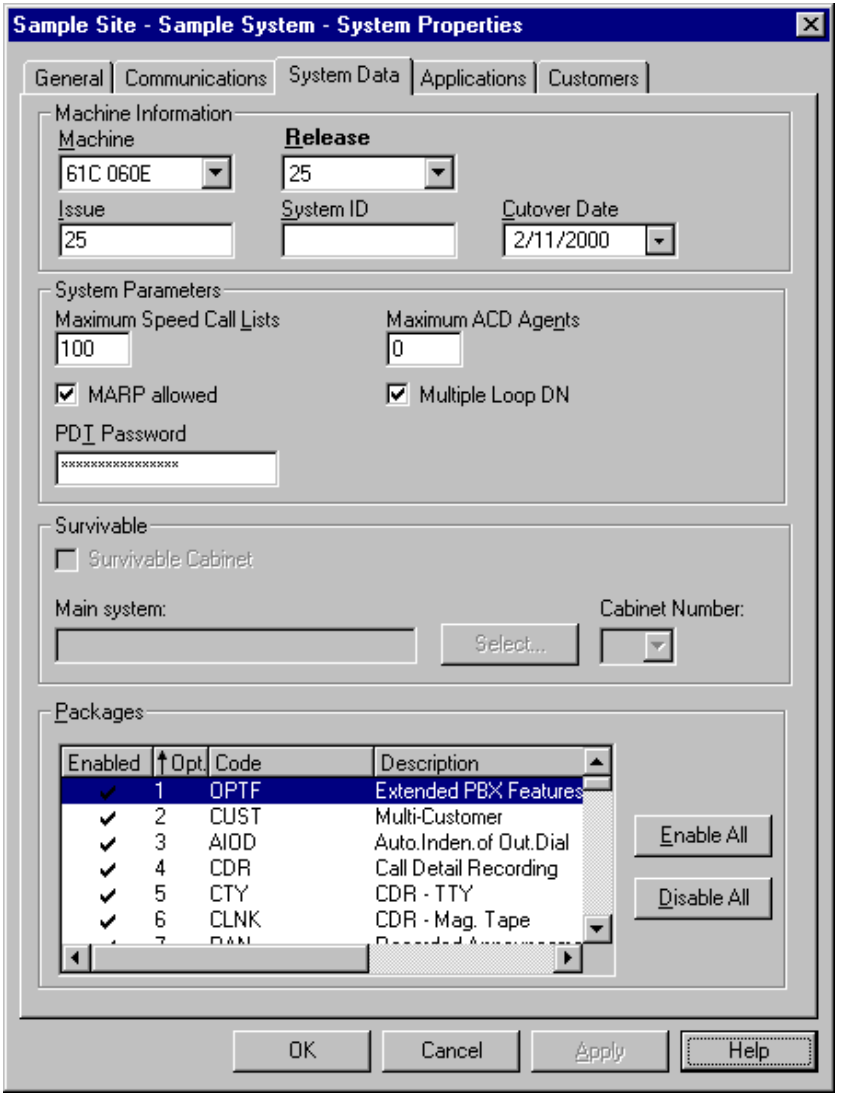
Figure 46 System Properties—Communications, Serial connection type



11 Click the System Data tab.

The System Properties—System Data dialog box opens (Figure 47).

Figure 47 System Properties—System Data dialog box



a In the Machine Information box, enter the machine/system type and release version for the system. For example, if your Meridian 1 is an Option 61C running X11 Release 25.25 software, select 61C in the Machine field, select 25 in the Release field, and enter 25 in the Issue box.

Note: For Succession CSE 1000 systems, select 11C in the Machine field, and select a minimum of 25 in the Release field. Enter the issue number of the software in the Issue field. Succession CSE 1000 systems require a minimum software release of 25.30 (Release 25, Issue 30).

b If the system is an Option 11C survivable cabinet or a Succession CSE 1000 survivable Media Gateway, use the Survivable box to configure the cabinet:

— Click the Survivable Cabinet check box.

— Click the Select button to choose a main system.

— Select an available cabinet number from the Cabinet Number drop down list.

Note: If the current system is an Option 11C main system or Succession CSE 1000 Call Server, and you change the Machine field to a machine type different from 11C or the Release and Issue fields to an X11 release lower than 25.30, all of the survivable systems related to this main system will be removed.

For information on configuring ITG Line 2.0 data on OTM, see "Configure Option 11C and Succession CSE 1000 systems for survivability" on page 131.

For additional information on Option 11C Survivable Expansion Cabinets, see *Option 11C Planning and Installation Guide* (553-3021-210).

For additional information on Succession CSE 1000 Survivable Media Gateways, see *Succession Communication Server for Enterprise 1000 Planning and Installation Guide* (553-3023-210).

c In the System Parameters box, make selections for MARP and Multiple Loop DN. If required, make adjustments to the maximum number of

Speed Call lists, the maximum number of ACD Agents and PDT Password.

Note: In the System Parameters box, the PDT Password edit box allows you to set the Level 2 password for the Problem Determination Tool (PDT). If you change this password, you must manually change the PDT password on the system so that they match.

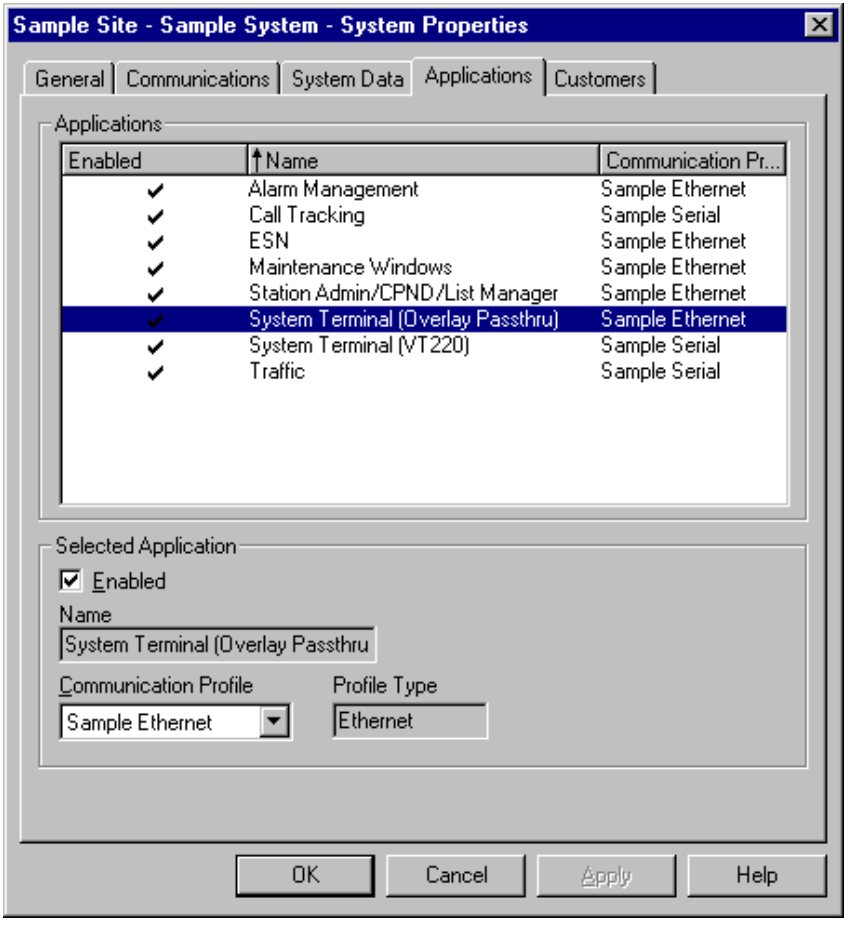
d Use the Packages box to enable or disable Meridian 1 or Succession CSE 1000 software packages.

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.

12 Click the Applications tab

The System Properties—Applications dialog box opens (Figure 48).

Figure 48 System Properties—Applications dialog box



Note: If the system is an Option 11C survivable cabinet or a Succession CSE 1000 survivable Media Gateway, the ESN and Station Admin/ CPND/List Manager applications are not available.

This tab defines the OTM applications that will appear in the System window and the communications profile to be used with each application.

Note: You must enable an application for it to be available in the System window.

To enable an application:

a Select the application in the Applications box.

b Select a Communication Profile from the drop-down list in the Selected Application box.

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

To disable an application:

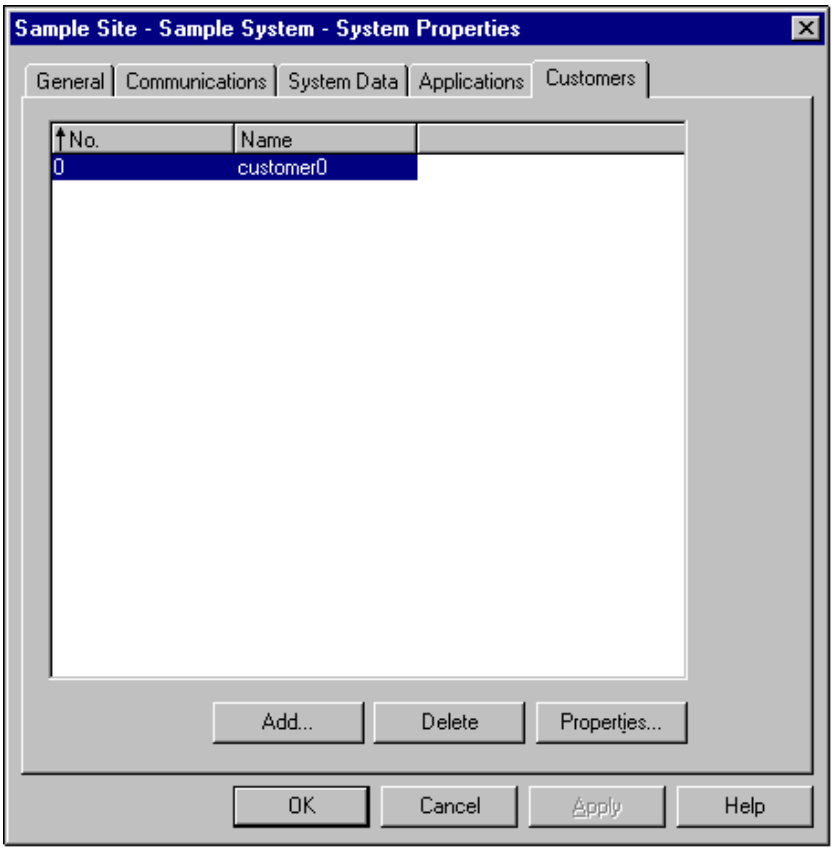
a Select the application in the Applications box.

b In the Selected Application box, click the Enabled check box to remove the check mark.

13 Click the Customers tab

The System Properties—Customers dialog box opens (Figure 49).

Figure 49 System Properties—Customers dialog box



This dialog box lists the customers currently defined for this Meridian 1 or Succession CSE 1000 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 or Succession CSE 1000 system features and numbering plans that are available to the customer. This information it is not automatically updated on the Meridian 1 or Succession CSE 1000 system and must be updated by using LD 15 (customer data block).

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

To add a customer:

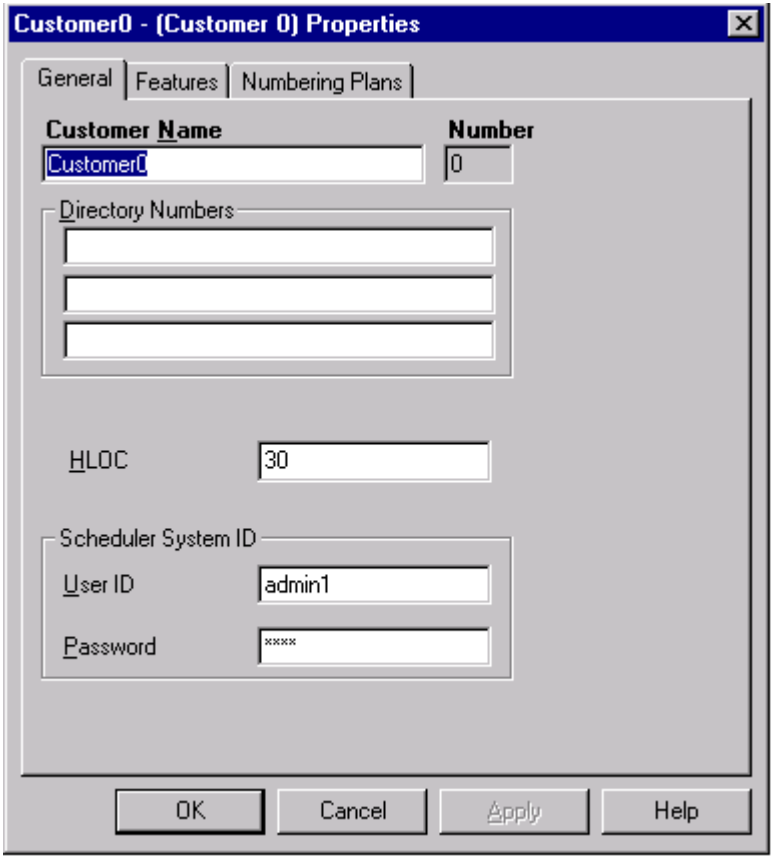
a Click Add.

b Select a Customer number.

c Click OK.

The Customer Properties dialog box opens with the General tab displayed (Figure 50).

Figure 50 Customer Properties—General dialog box



d Fill in the customer information.

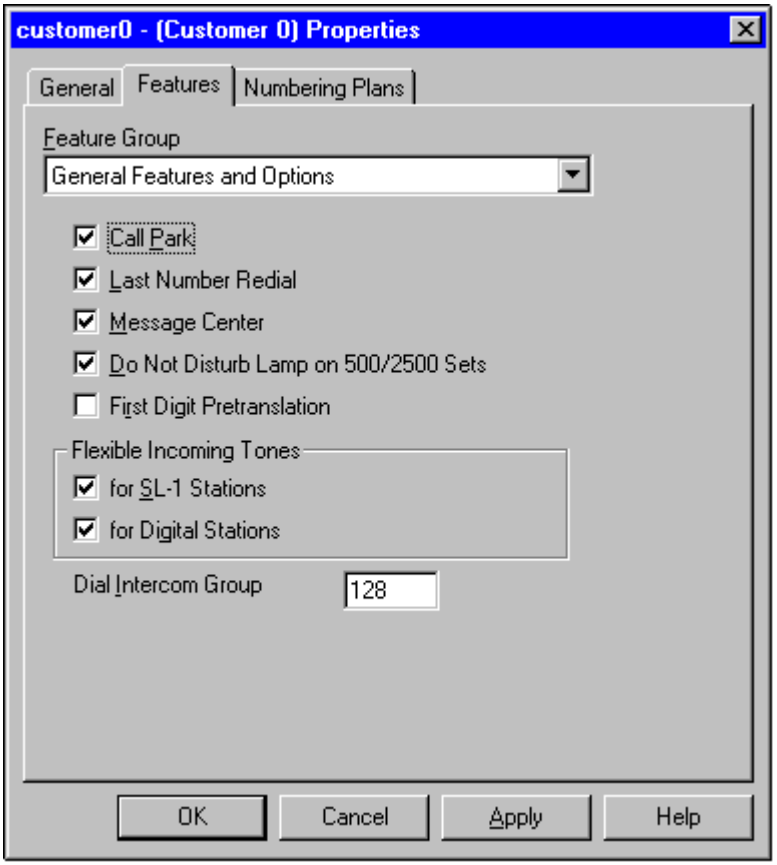
Note: HLOC displays the home location code defined in LD 90.

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.

e Click the Features tab.

The Customer Properties—Features dialog box opens (Figure 51).

Figure 51 Customer Properties—Features dialog box

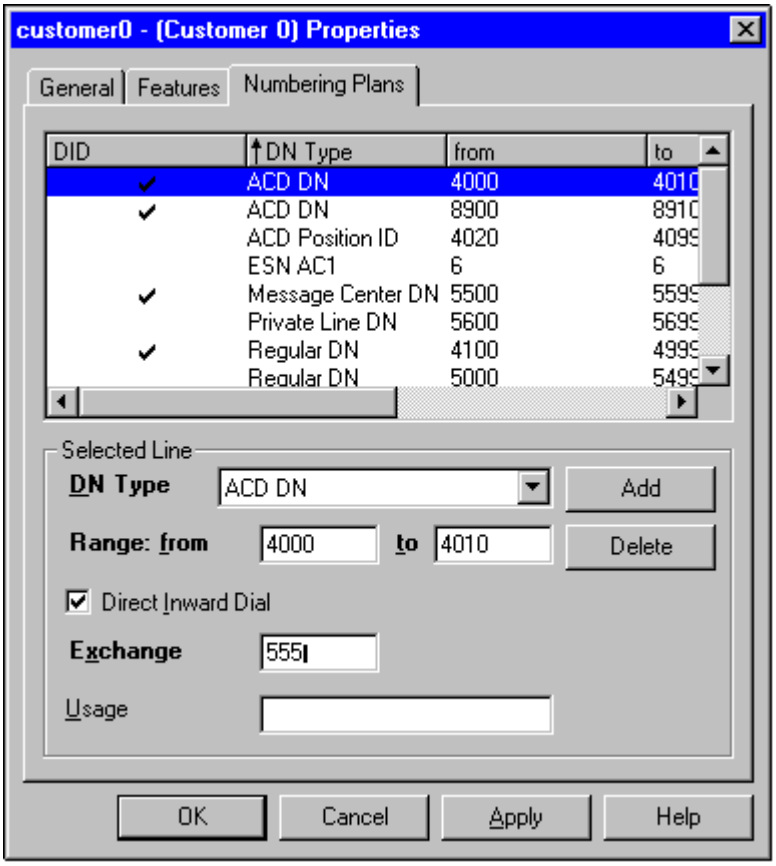


f Fill in the customer information.

g Click the Numbering Plans tab.

The Customer Properties—Numbering Plans dialog box opens (Figure 52).

Figure 52 Customer Properties—Numbering Plans dialog box



h Fill in the customer information.

i 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.

14 To delete a customer, click Delete in the System Properties—Customers dialog box (Figure 49). A delete confirmation box opens. Click OK.

15 To modify customer information, click Properties in the System Properties—Customers dialog box (Figure 49). The Customer property sheet opens. Modify information in the appropriate tabs and click OK.

16 In the System properties dialog box, 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

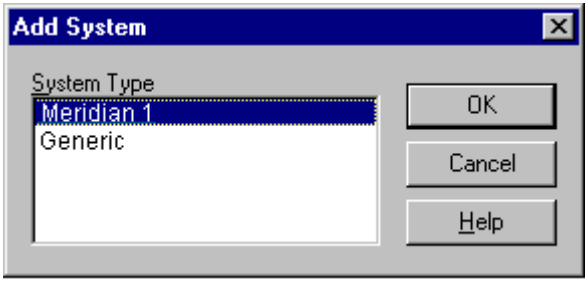
You can add as many systems (including non-Meridian 1 systems) to a site as you want. You must have administrator privileges to add a system.

1 In the Navigator window, select the desired site.

2 Choose Configuration > Add System or right click and select Add System.

The Add System dialog box opens (Figure 53).

Figure 53 Add System dialog box



Note: You may need to install additional software to enable other system types not listed in Figure 41. Follow the installation instructions included with your order.

3 Select Generic in the System Type box.

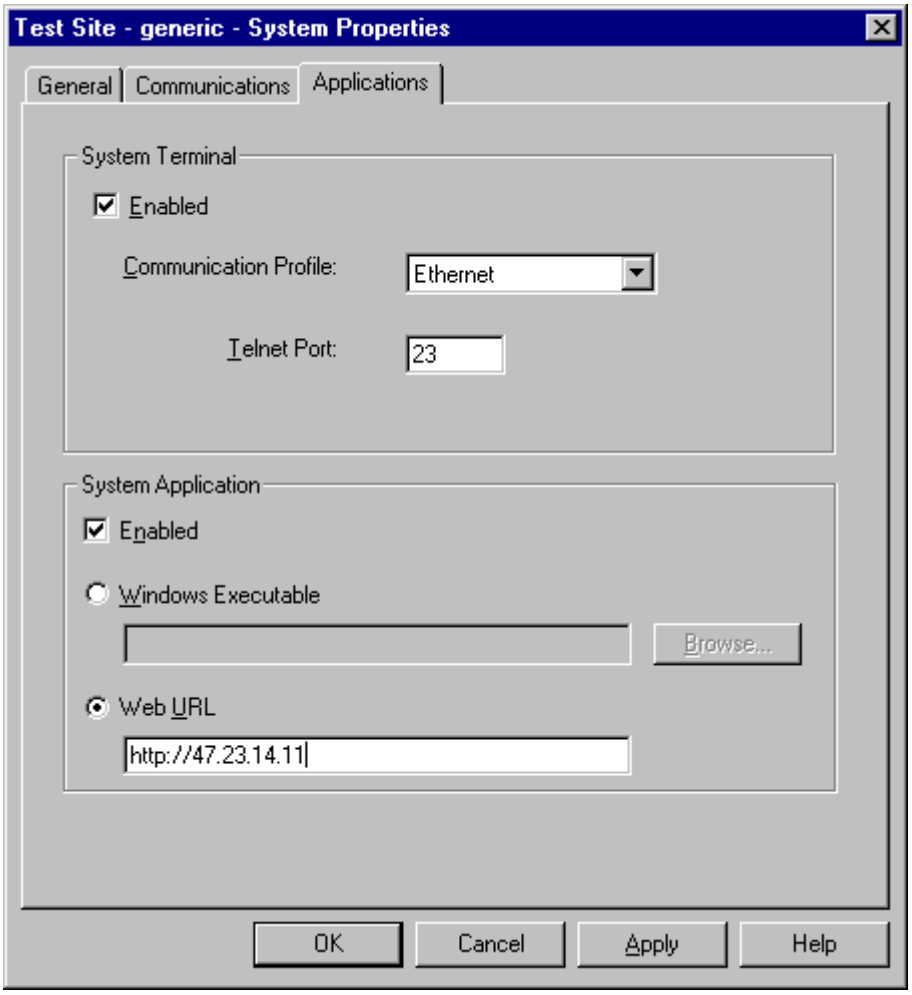
4 Click the OK button.

5 Complete the System Properties—General and System Properties—Communications dialog boxes as you would for a Meridian 1 or Succession CSE 1000 system. See "Adding a Meridian 1 or Succession CSE 1000 system" on page 88.

6 Click the Application tab.

The System Properties—Applications dialog box for non-Meridian 1 devices opens (Figure 54).

Figure 54 System Properties—Applications for non-Meridian 1 devices



7 In the System Properties—Applications dialog box 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 is selected, the web site can be accessed from either the Windows or Web Navigators.

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

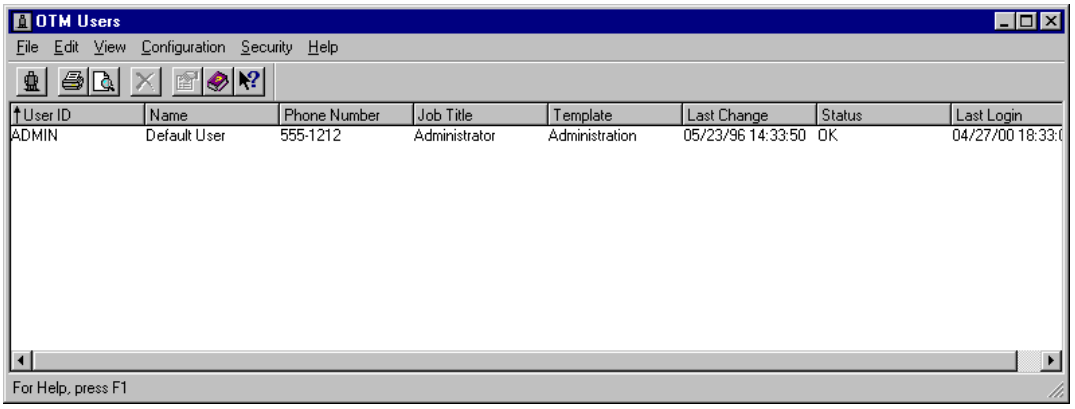
Add OTM Windows users via the OTM Windows Navigator

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

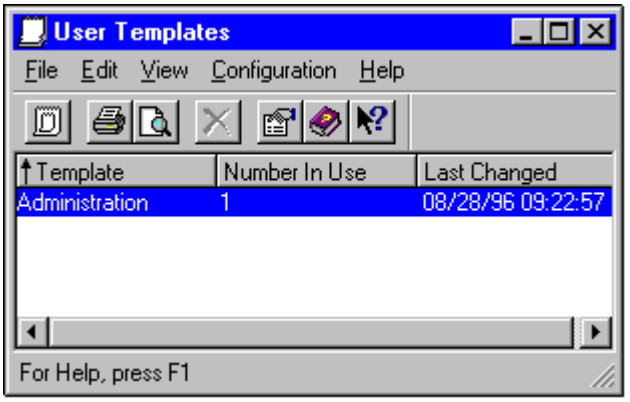
1 In the Navigator window, choose Security > OTM Users to display the OTM Users window (Figure 55).

Figure 55 OTM Users window



2 Choose Configuration > User Templates. The User Templates window opens (Figure 56).

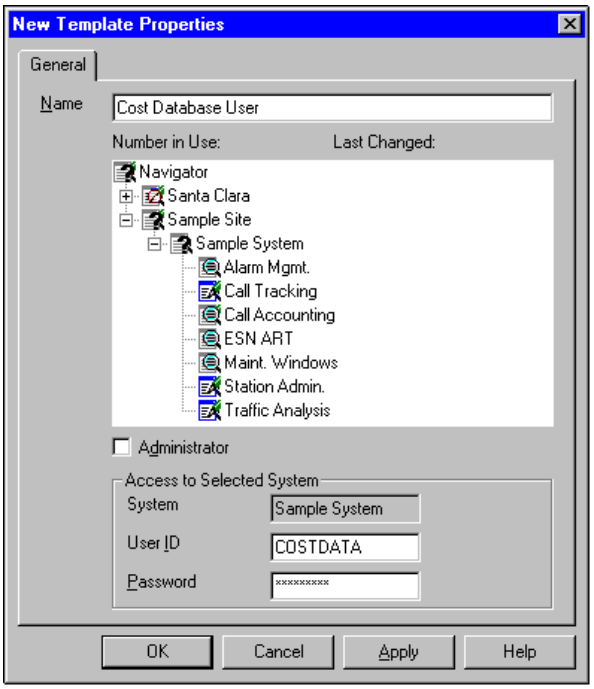
Figure 56 User Templates Window



3 Choose Configuration > Add Template.

The New Template property sheet opens (Figure 57).

Figure 57 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 and write, read only, or no access, see Table 4. Select the Administrator box, if appropriate. The icons beside the site and system names 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.

Table 4 Access privilege icons

Icon	Explanation
	Read and write access
	Read only access
	No access

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 they want to connect.

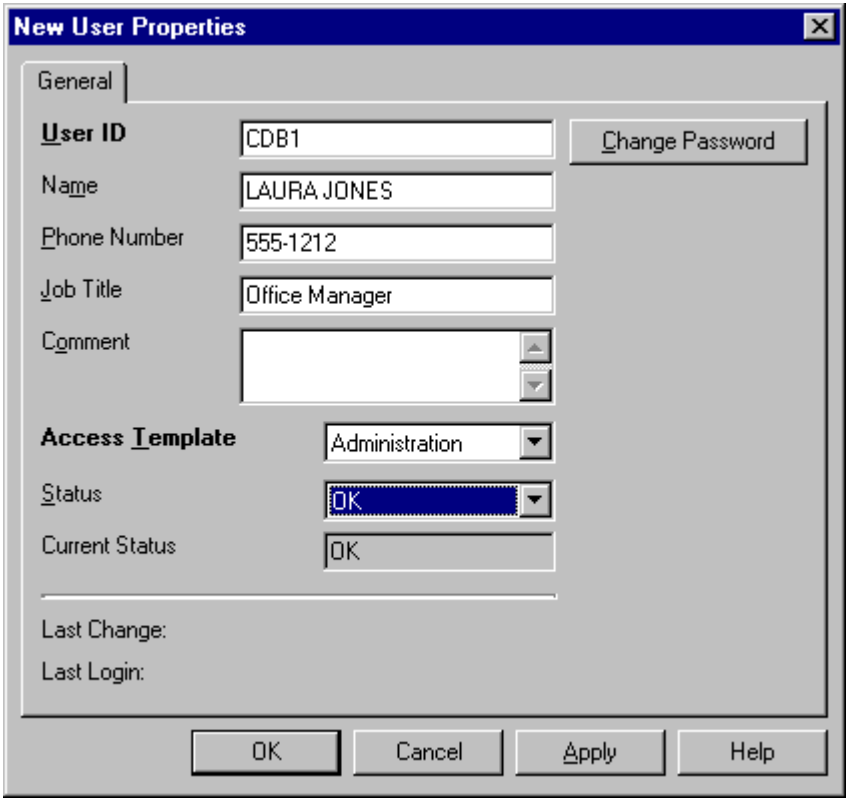
6 Click OK.

Adding a user

1 In the OTM Users window, choose Configuration > Add User.

The New User Properties dialog box opens (Figure 58).

Figure 58 New User Properties dialog box



2 Enter a User ID.

3 From the Access Template drop-down list, select the template that you will use as the basis for this user definition.

4 Fill in other data as required.

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

6 Click OK.

You are prompted to enter a password and confirm it after clicking the OK or Apply buttons.

The new user appears in the OTM User window. Close the OTM User window.

Refer to *Using Optivity Telephony Manager* (553-3001-330) for detailed information on adding OTM users.

Adding OTM Web Navigator users

Access to the OTM Web Navigator is set up using the users and groups functionality in Windows NT and Windows 2000.

The OTM Web Navigator provides the following:

- A list of systems and devices; users click on a system or device to:
  - — open a Web System Terminal or URL to manage a system or device
  - — open Maintenance Pages for performing maintenance operations on M1 hardware
- Web-based alarm browser to view alarms and events from multiple systems and devices
- The ability to locate telephones, view and change configuration data
- Web-based Maintenance Pages to perform maintenance operations (enable, disable, etc.) on Meridian 1 or Succession CSE 1000 system hardware.
- OTM Web configuration pages (login access, LDAP sync reports, and so forth).

The OTM administrator has the responsibility of installing, configuring, and maintaining OTM Web Services.

User Login and Security

The user logs into the OTM Web Navigator using their Microsoft Windows NT or Windows 2000 userID and password. Login security for OTM Web Services ensures protection against unauthorized entry and enforces access permissions for logged on users.

There are three categories of users:

- Administrators — OTM administrators
- HelpDesk — OTM help desk users

- EndUser — OTM end users

In addition, there is a Default user category. Default users are able to successfully log in to the Web Navigator, but they do not have an access profile defined in their Directory record.

OTM administrators and help desk users have user accounts in a Windows domain. End users may have accounts either in a Windows domain or through an LDAP server. Administrators must be set up in a Windows Administrator group on the server itself not on a remote machine.

OTM administrators and help desk users can access and change their own telephones through either the Web Navigator or the Desktop Services end user pages. Access to the end user pages requires the appropriate OTM directory setup (user login and user group) for these administrators and help desk users.

OTM Web application access permissions are controlled by the Administrator on a per-Windows user group basis. For example, the administrator may limit the OTM users access to only some of the OTM Web-based functionality. The OTM Web Navigator controls access to applications by shielding Web links that the user does not have access to. The directories and files comprising those applications are similarly protected.

You configure Windows NT or Windows 2000 user groups and individual users using the Windows user interface on the OTM server. You then determine the access permissions for each user group by using the OTM Web Navigator page. For information about setting user access, refer to "OTM Web Access security" on page 116.

Note: As a security precaution, with any upgrade or reinstallation of OTM software, access profiles for all user groups except Administrator are reset. Using the Web Access Security feature, any member of the Administrator user group can log in and set up access profiles for members of the Help Desk, End User and Default user groups.

When an administrator or help desk user first points a browser to the OTM Navigator Web site, a check is performed to see if the user has the required OTM Java plug-in. If the plug-in is not installed, the administrator or help desk user is given the option of downloading and installing the plug-in. This operation is similar to the standard download operations in that the user must download the plug-in to their hard disk then it self installs onto the machine.

While the plug-in check is being performed, the OTM splash screen is displayed. If the plug-in is installed, or after installation of the plug-in, the user is taken to the login page.

The default OTM URL is the end user login page. To navigate to the administrator login page, place **`/admin`** after the OTM IP address or host name.

Access permissions

When OTM starts for the first time, the Administrator profile is the only active profile. You must assign access permissions for the other Windows NT or Windows 2000 Groups that you have setup on the OTM Server.

Administrator Group access permissions

Persons belonging to the Administrators user group on the OTM Server can log on to the OTM Web site and get unrestricted access. The Administrators group has unrestricted access by default. You are not able to alter access permissions for the Administrators user group.

Users of the OTM Administration Site belong to a distinct user group and are assigned the security profile for that user group. For example, the Administrators user group has access to all Web applications.

Note: Important advisement for localized operating systems — There must always be an "Administrators" Windows NT group with the spelling exactly as shown. This group should include the names of any users that will require Administrator level access. For systems that are running on operating systems that have been localized into languages other than English, members of this group should include the members of any group that is a translated version of "Administrators". If this group does not appear on the server - such as in the German OS where it is called "Administoren", create it. Make the administrator and other users who require OTM Web Administrator permissions members of this group.

User group access permissions

You, the network administrator, log on to the OTM Administration Web site and assign access permissions to the other Windows NT or Windows 2000 groups. By default, a member of any group other than Administrators does not have any access to OTM Web Applications unless you specifically grant that group appropriate permissions.

From the Web Navigator Access page you grant or deny access to web applications to a group - not to individual users. To change the security access for individual users their group membership should be changed from Windows. For new groups added to the Windows system, the Administrator must assign access permissions for web applications before any users from that group can log on. For more information about setting user access, refer to "OTM Web Access security" on page 116.

All OTM Web Navigator users for the Administration site should have a Windows NT or Windows 2000 account on the local OTM Server.

When you select an access group other than Administrators for the first time, you may get a data retrieval error message. OTM will automatically generate a new profile. Select Administrators again and then select the group that initially gave the error. You will now be able to assign access permissions for the new group.

With the exception of Administrators, do not place a person in multiple groups. The first group detected by OTM is used to determine access permissions. There is no restriction on the Administrators group. A user may belong to other groups but if they belong to the Administrators group the Administrators profile will override all other profiles.

While assigning access permissions be certain that you select the top level application for every sub application that you assign. For example if you are selecting “System Alarms” you must also select “Equipment”. Failure to do so may result in members of the user group being denied access to the Web site.

Desktop User Access

The end user Access page allows you to select the method of user login authentication. The options are:

- LDAP Server

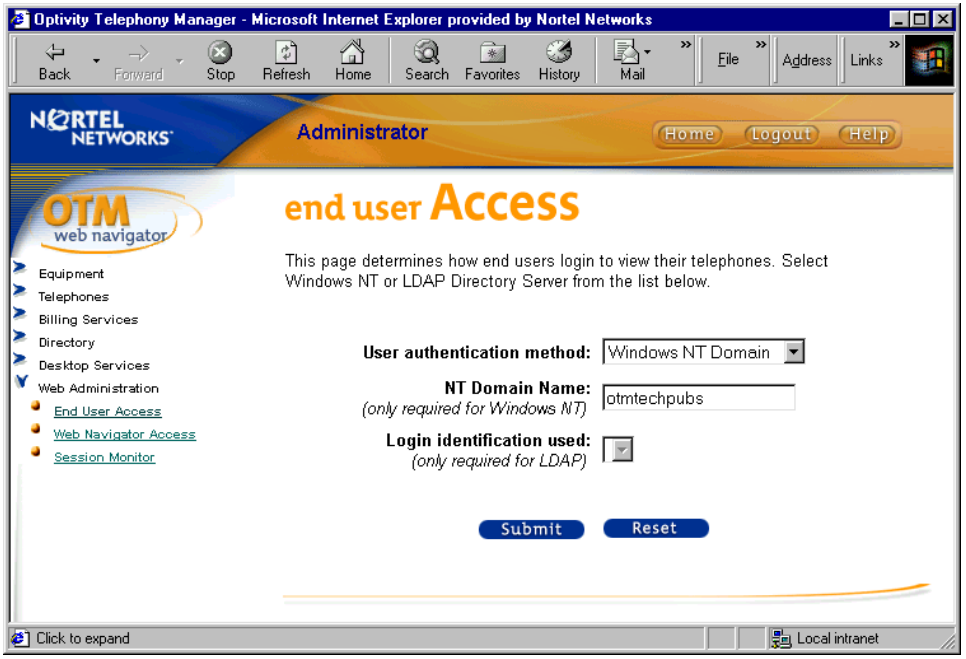
Note: User login identification is required for LDAP. The drop down menu only contains employee ID (UID) and e-mail.

- Windows NT Domain.

Note: The edit box for the Windows NT domain name is required for Windows NT authentication.

For information on configuring users for desktop access, see "Enable Web desktop access in the OTM Directory" on page 118.

Figure 59 OTM Administrator End User Access screen

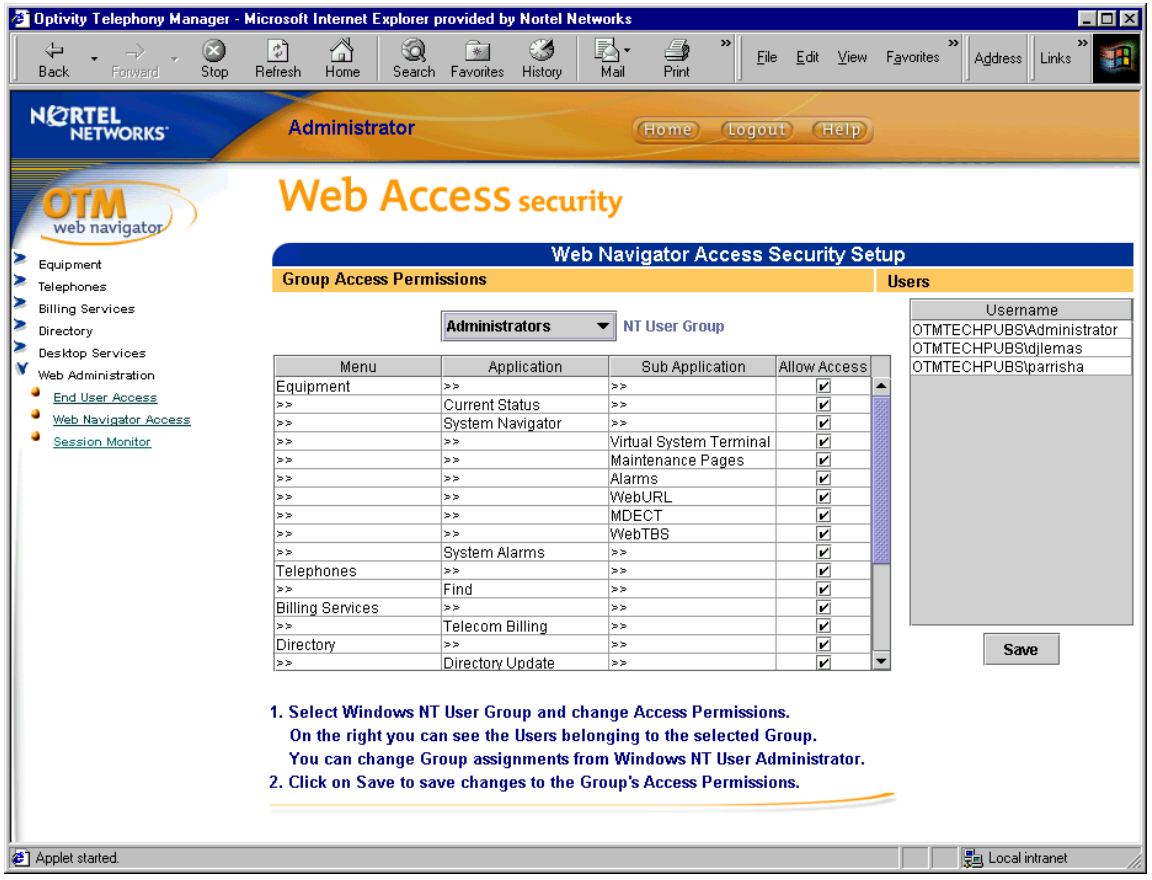


OTM Web Access security

The OTM Web Access security page determines which OTM Web Navigator pages are available to users. Before you can set access permissions for a group, you must create the group using the Windows NT or Windows 2000 Server user interface. Select the user group from the drop down box and then check the pages that you want to be visible to users in that group. The list of pages mirrors the hierarchical structure in the OTM Web Navigator tree.

Note: The Save button only submits the changes on the selected User Group.

Figure 60 OTM Administrator Web Access Security page



Installation and Configuration of Desktop Services

The following procedure outlines the steps that you must take to install and configure Desktop Services:

1. Install OTM. See "Initial installation tasks" on page 25.
2. Create Windows NT accounts for Help Desk users and End Users as required.
3. Log on to the Web Navigator as Administrator and go to the Access Profiles page.

Note: To navigate to the Administrator Login page, place **`/admin`** after the OTM IP address or host name in your Web browser.

4. Configure the Help Desk, Default, and End User Access Profiles as desired.

Note: By default, Help Desk users are given read/write access to all features. Default and End Users have read-only access to 21 features.

5. Go to the Web Access Security page and set the Web Navigator access permissions for the Help Desk and Default user groups. See "OTM Web Access security" on page 116.

Note: To allow Help Desk users to make changes to other user's telephone configuration data, make sure that they have access to the Find Telephones page.

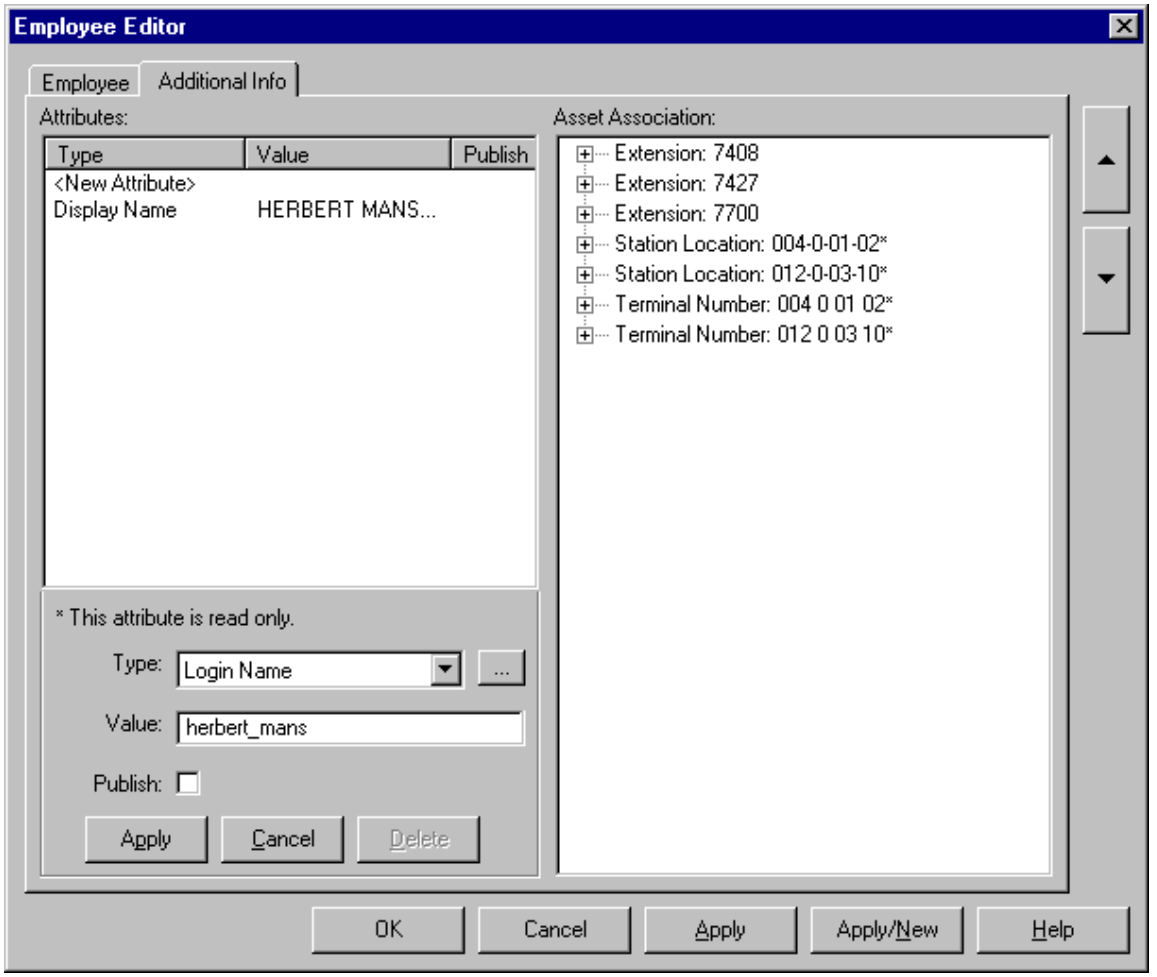
6. Enter the Help Desk users' Login Name and Access Profile in the users' OTM Directory entry. See "Enable Web desktop access in the OTM Directory" on page 118.
7. Enter the End Users' Login Name and Access Profile in the users' OTM Directory entry. See "Enable Web desktop access in the OTM Directory" on page 118.
8. Select the desired Web Reporting Role in the user's OTM Directory entry.

Enable Web desktop access in the OTM Directory

Before users can access Web Desktop Services, you must enter their Login Name and Desktop User Group using the Windows-based Employee Editor.

1. From Station Administration, select View > Employee Selector.
2. Double click an employee's name in the Employee Selector.
3. Click the Additional Info tab in the Employee Editor window. See Figure 61.

Figure 61 Entering Login Name attribute



4 Select <New Attribute> in the Attributes pane.

5 Select Login Name from the Type drop down box.

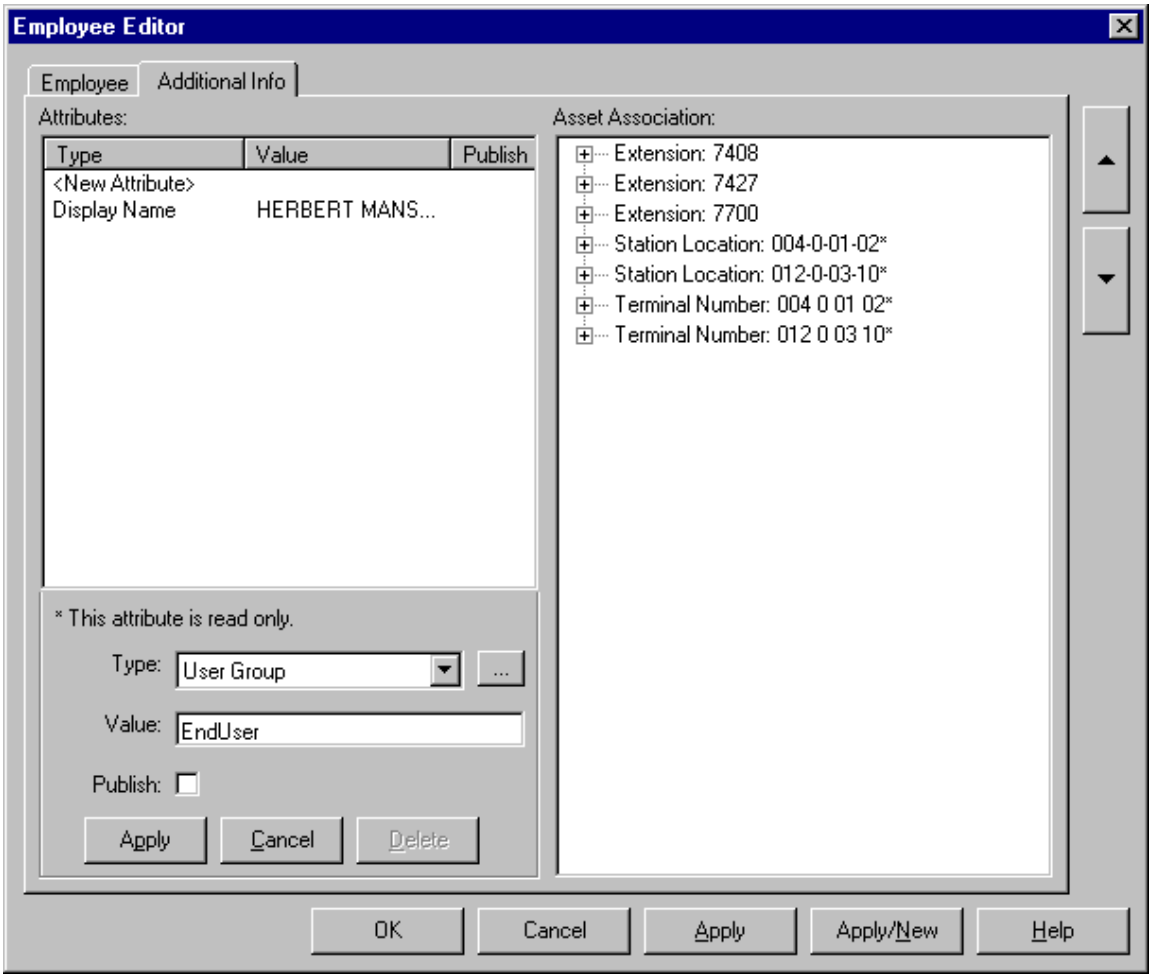
6 Enter the user's Windows NT Login Name for the attribute Value (If Windows NT is the authentication method chosen for desktop users).

7 Click the Publish check box to enable synchronization with an optional LDAP compliant server.

8 Select <New Attribute> in the Attributes pane.

9 Select User Group from the Type drop down box. See Figure 62

Figure 62 Entering User Group attribute



10 Enter “EndUser” for the attribute Value to enable End User Web desktop access - both for LDAP and Windows NT access.

Enter “HelpDesk” for the attribute Value to enable Help Desk Web desktop access - both for LDAP and Windows NT access.

Note: For Desktop User Groups, you can use the Directory Update page in the OTM Web Navigator to simplify this process. See “Web Services” in *Using Optivity Telephony Manager* (553-3001-330).

If you have access to the Login Names in another database, consider using the Import/Export utility in the OTM System Window to simplify this process. See “Import and Export Utilities” in *Using Optivity Telephony Manager* (553-3001-330).

Note: “Appendix A” in *Using Optivity Telephony Manager* (553-3001-330) contains End User reference information. You can extract this appendix and distribute it as a User Guide.

Set Up the Meridian 1 or Succession CSE 1000 system

1 Verify that the Meridian 1 or Succession CSE 1000 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:
  - — X11 Release 22 or later
  - — 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 or Succession CSE 1000 system to a corporate network, an Ethernet gateway or router is required to separate the system from the corporate network. Connecting the Meridian 1 or Succession CSE 1000 system without a gateway or router will adversely affect the system's call handling ability.

3 For PPP communication, you will need the following:

- Hayes command compatible modem
- modem cables
- Meridian 1 or Succession CSE 1000 SDI ports will require user type MTC and SCH be set in LD17.

4 For serial communication, 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

- Meridian 1 and Succession CSE 1000 SDI ports will require that the appropriate user type be set in LD 17 for each OTM application (Table 5).

Table 5 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 or Succession CSE 1000 system

5 Configure OTM users on the Meridian 1 or Succession CSE 1000 system:

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

- Install the appropriate release (minimum is Release 22 for Meridian 1 and Release 25.30 for Succession CSE 1000) 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 and Succession CSE 1000 systems through LAPW IDs and passwords configured on the Meridian 1 and Succession CSE 1000 systems.

  >**logi <*ID*>** where ***ID*** is the login ID.

Note: When a Limited Access Password (LAPW) is defined to collect traffic data from LD 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 *X11 Software Features Guide* (553-3001-306).

PASS?> <***XXXXXX***> where ***XXXXXX*** is 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 LD 17, LNAME_OPTION for more information. Please alert others of any changes; for example, all technicians with access to the Meridian 1 or Succession CSE 1000 system, 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> <n>  where n  is the Limited Access Password
PWTP
PWn  where n is the Limited Access Password
```

You will be prompted to enter your new password.

```
LOGIN_NAME> <xxxxxx>  where xxxxxx is your login name.
OVLA> all
OVLA
CUST> all
CUST
HOST
MAT> yes
MAT_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 or a Succession CSE 1000 system).

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 <n> where n is an available TTY port (0-15).
TTY-TYPE> pty
PORT> <z> where z is an available PTY port (0-7).
DES> <n>
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 or Succession CSE 1000 system:

Note: The host names (***M1ACTIVEIP***, ***M1INACTIVEIP***) 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 or Succession CSE 1000 system:

  ```
  >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 systems.
- 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 *47.1.0.0 47.1.1.250***

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

  >**PRT ROUTE** (list the configured routing table)
  >**ENL ROUTE #** where **#** is the route number

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

  The routing table provides the Meridian 1 or Succession CSE 1000 system with the IP address of the gateway server so the Meridian 1 or Succession CSE 1000 system 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 *M1ACTIVEIP*

  >LD 117
  >NEW HOST PPPREMOTE *47.0.0.3*
  >CHG PPP REMOTE PPPREMOTE *M1ACTIVEIP*

- After you perform a series of **NEW**, **OUT**, **CHG** commands, type:

  >UPDATE DBS

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

- Use Overlay 137 to verify the IP address:

  >**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 or Succession CSE 1000 system.

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.

Enabling Meridian 1 and Succession CSE 1000 system alarms with LD 117

To enable alarms with LD 117:

1. In the OTM system window, on the toolbar, click the System Terminal icon.

   The System Terminal Selection dialog box opens.
2. Click on the Ethernet/PPP (Overlay Passthru) button, and then click OK.

The System Terminal window opens.

3 Log in with the administrator user name and password.

You must have appropriate access privileges to use LD 117.

4 Enter:
`LD 117`

The => prompt appears in the Command Results pane indicating that the system terminal application is ready to accept your input.

5 Enter:
`prt open_alarm`

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 number of the next available slot.

6 Enter:
`set open_alarm <`*`n`***`> <`***`IP_address`***`>`**

where *`n`* is the next available slot number and *`IP_address`* is the IP address of your OTM Server. See "Determine the OTM PC IP address" on page 129 for more information.

Caution: Assigning your IP address to a slot currently in use disconnects that user from the system preventing them from receiving alarm information.

7 Enter:
`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.

Configure Option 11C and Succession CSE 1000 systems for survivability

Configure ITG Line 2.0 data for an Option 11C system

When distributing ITG line cards across different Survivable Expansion Cabinets, the Survivable Expansion Cabinets can be configured to each have their own node or to belong to the same node. If the Survivable Expansion Cabinets are not in the same location as the Main Cabinet, each Survivable Expansion Cabinet must have its own node.

This is related to which Survival IP address is configured on the ITG line cards. For a remote location, the Survival IP address of the ITG line cards on that node is the IP address of the SSC on that node. For situations where the Survivable Expansion Cabinets are in the same location as the Main Cabinet, the Survival IP address on all ITG line cards are configured to a single Survivable Expansion Cabinet SSC IP address.

The information below provides more information on these two options:

Survivable Expansion Cabinets in separate nodes for ITG line cards - Mandatory if Survivable Expansion Cabinets are in a different location than the Main Cabinet

- Trunks and Gateway channels are available in all Survivable Expansion Cabinets.
- More administration is required since there is more than one node to manage.
- If the ITG line card fails, i2004 telephones can register to another ITG line card only if it is contained within the same cabinet.
- Users cannot make i2004 calls from one Survivable Expansion Cabinet to another.

Survivable Expansion Cabinets in the same node for ITG line cards

- Trunks and Gateway channels are only available for i2004 telephones on one Survivable Expansion Cabinet but can be used by all ITG line cards.
- Less administration since there is only one node to manage.

- If the ITG line cards fails, i2004 telephones can register to other ITG line cards in different Survivable Expansion Cabinets.
- Users can make i2004 calls from one Survivable Expansion Cabinet to another.

Summary of steps to configure ITG Line 2.0 data on OTM

Refer to *ITG Line 2.0/i2004 Internet Telephone* (553-3001-204) for a detailed description of these steps.

1. Manually add an ITG card node. It is required that each Survivable Expansion Cabinet have its own node if the cabinets are not in the same location as the Main Cabinet.
2. Configure the ITG line card properties.
3. Configure the DSP profile data.
4. Configure the Main Cabinet ELAN IP address, Survivable Expansion Cabinet E-LAN IP address and TLAN voice port.

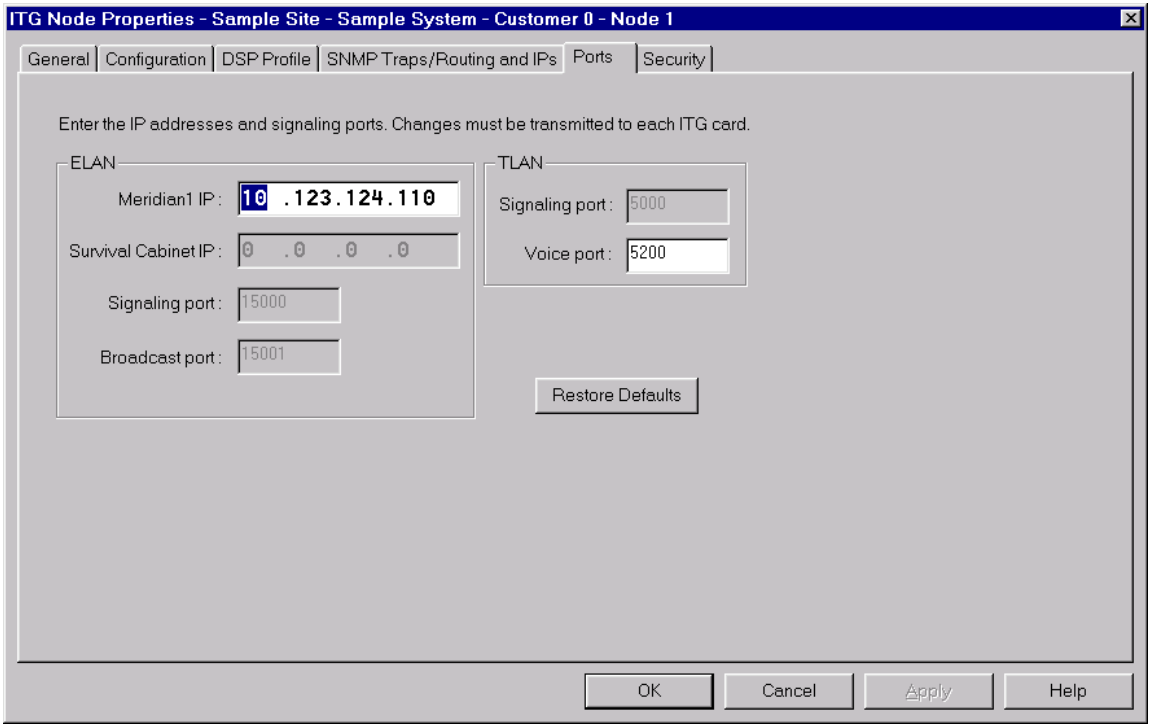
   Enter the Meridian 1 ELAN IP address of the Main Cabinet

   Define the Survivable Expansion Cabinet IP address in OTM. There is an extra field in OTM to configure the Survivable Expansion Cabinet IP address and TLAN port. Use the same secondary IP address as the Survivable Expansion Cabinet's ELAN address. If the Expansion Cabinet is non-survivable, leave the default value of "0.0.0.0" (Figure 63).

Note: The ELAN IP address of the Survivable Expansion Cabinet must be on the same subnet as the Main Cabinet. If the Expansion Cabinet is on a different subnet, use the VLAN concept to keep both ELAN addresses on the same subnet.

5. Configure SNMP traps and ELAN GW Routing table
6. Configure security for SVMP access.
7. Configure the Alarm Notification feature in OTM.

Figure 63 ITG IP Phones - ITG Node Properties - Ports dialog box



Configure ITG Line 2.0 data for a Succession CSE 1000 system

When distributing ITG line cards across different Media Gateways, the Media Gateways can be configured to each have their own node or to belong to the same node. If the Media Gateways are not in the same location as the Call Server, each Media Gateway must have its own node.

This is related to which Survival IP address is configured on the ITG line cards. For a remote location, the Survival IP address of the ITG line cards on that node is the IP address of the SSC on that node. For situations where the Media Gateways are in the same location as the Call Server, the Survival IP address on all ITG line cards are configured to a single Media Gateway SSC IP address.

The information below provides more information on these two options:

Media Gateways in separate nodes for ITG line cards - Mandatory if Media Gateways are in a different location than the Call Server

- Trunks and Gateway channels are available in all Media Gateways.
- More administration is required since there is more than one node to manage.
- If the ITG line card fails, i2004 telephones can register to another ITG line card only if it is contained within the same cabinet.
- Users cannot make i2004 calls from one Media Gateway to another.

Media Gateways in the same node for ITG line cards

- Trunks and Gateway channels are only available for i2004 telephones on one Media Gateway but can be used by all ITG line cards.
- Less administration since there is only one node to manage.
- If the ITG line cards fails, i2004 telephones can register to other ITG line cards in different Media Gateways.
- Users can make i2004 calls from one Media Gateway to another.

Summary of steps to configure ITG Line 2.0 data on OTM

Refer to *ITG Line 2.0/i2004 Internet Telephone* (553-3001-204) for a detailed description of these steps.

1. Manually add an ITG card node. It is required that each Media Gateway have its own node if the cabinets are not in the same location as the Call Server.
2. Configure the ITG line card properties.
3. Configure the DSP profile data.
4. Configure the Call Server ELAN IP address, Survivable Media Gateway ELAN IP address and TLAN voice port.

   For the Meridian 1 ELAN IP address, enter the Succession CSE 1000 ELAN IP address of the Call Server

Define the Survivable Media Gateway IP address in OTM. There is an extra field in OTM to configure the Survivable Media Gateway IP address and TLAN port. In the text box labeled “Survivable Cabinet IP”, enter the same secondary IP address as the Media Gateway’s ELAN IP address. If the Media Gateway is non-survivable, leave the default value of “0.0.0.0”. See Figure 63 on page 133.

Note: The ELAN address of the Survivable Media Gateway must be on the same subnet as the Call Server. If the Media Gateway is on a different subnet, use the VLAN concept to keep both ELAN addresses on the same subnet.

5 Configure SNMP traps and ELAN GW Routing table

6 Configure security for SVMP access.

7 Configure the Alarm Notification feature in OTM.

Transmit ITG Line 2.0 node configuration data from OTM to the ITG Line 2.0 cards

Once the ITG Line 2.0 node and card properties are configured using the ITG IP Phones application within OTM, the data must be transmitted to the ITG line cards. OTM converts the configuration data to text files and transmits the files to the line cards.

Refer to *ITG Line 2.0/i2004 Internet Telephone* (553-3001-204) for a detailed description of these steps.

1 Set the Leader 0 IP address using a TTY connected to the local RS232 maintenance port.

2 Reboot Leader 0.

3 Transmit the node and card properties from the OTM ITG IP Phones application to Leader 0.

4 Reboot Leader 0.

5 Transmit the card properties to all of the cards in the node.

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:

1 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 or Succession CSE 1000 system, the VT220 profile is used (Ethernet/network or serial). If Ethernet/network is selected, the software uses the Meridian 1 or Succession CSE 1000 system'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 Do one of the following:

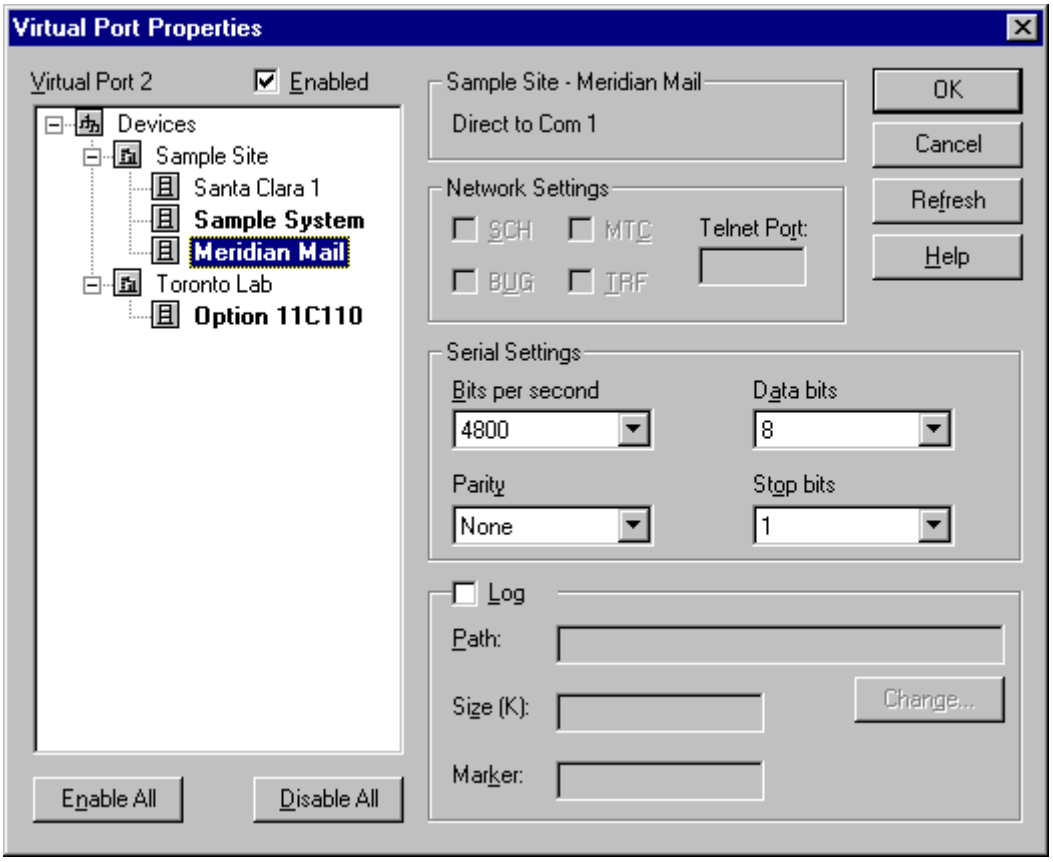
- Double-click the disabled item in the tree.
- Select the item, and check the "Enabled" check box.
- Click the "Enable All" button to enable all the items listed in the tree with the default configuration.

The item becomes bold to show that it is enabled.

The field to the right of the “Enabled” check box 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.

For a serial connection, “Direct to Com *x*” is displayed, where *x* is the Com port number (Figure 64).

Figure 64 Configuring Virtual Ports (serial, logging disabled)



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

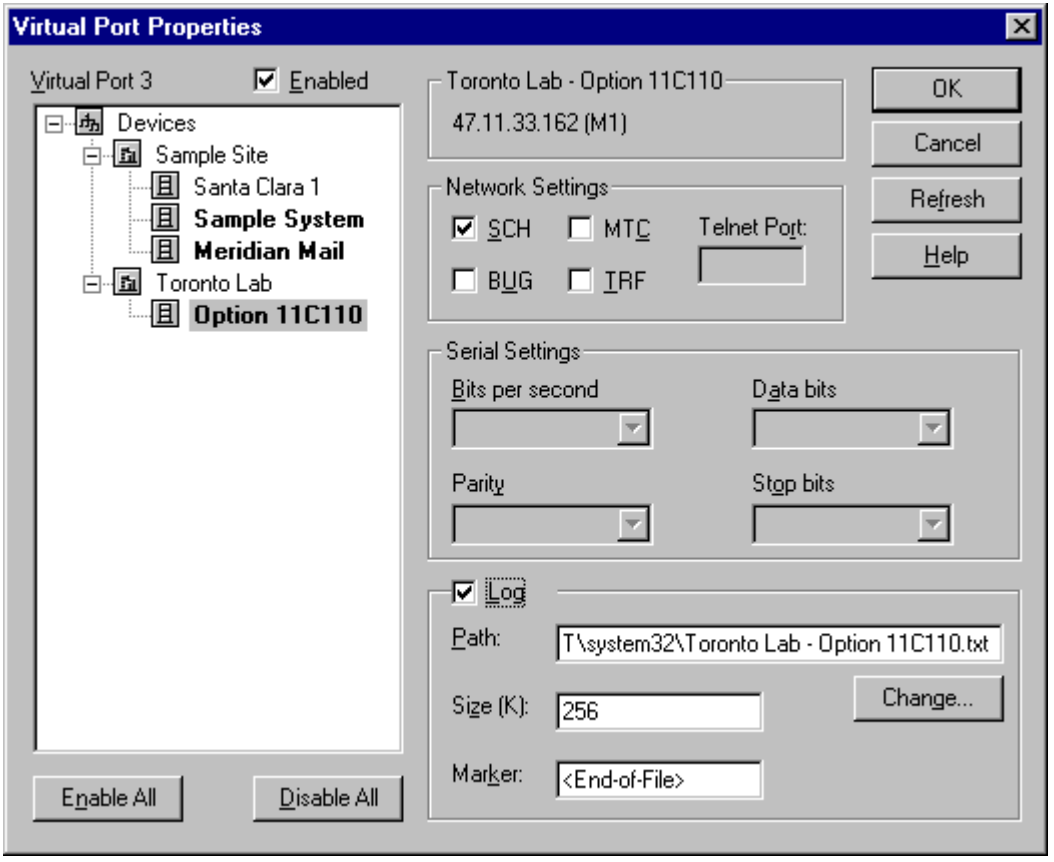
You can change the settings in the dialog box.

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

2 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 or Succession CSE 1000 system a Virtual Port Properties dialog box similar to Figure 65 opens.

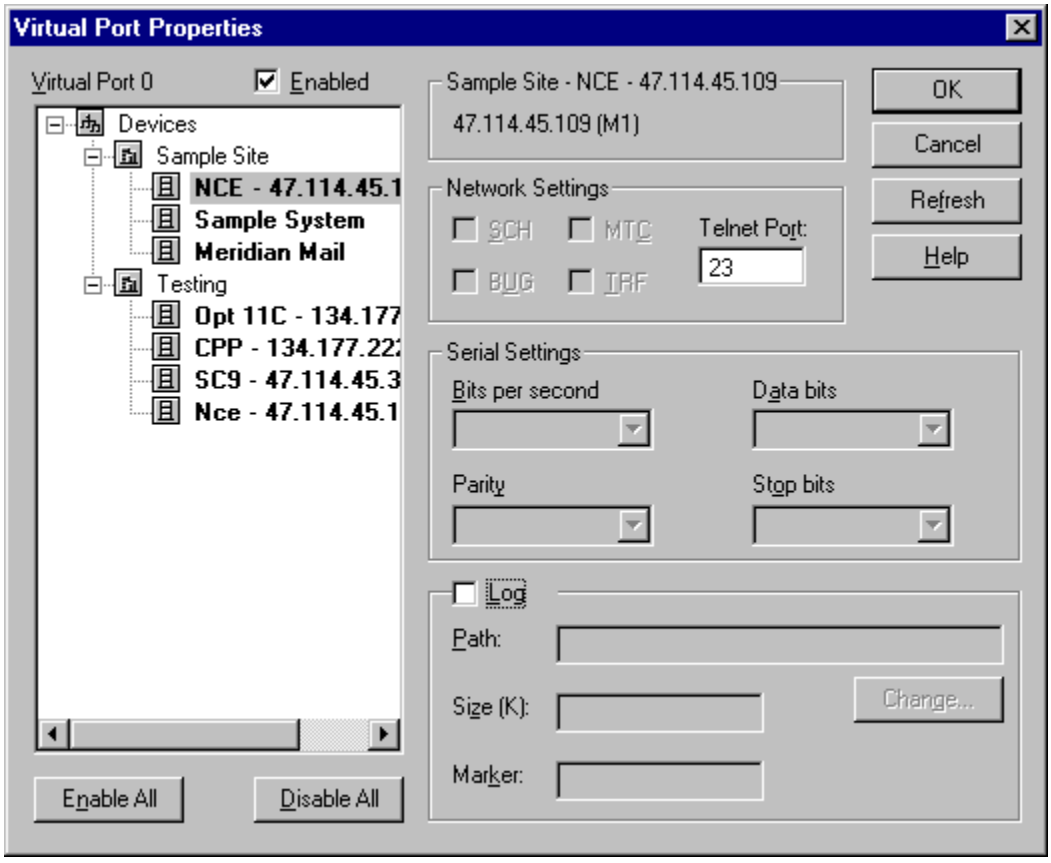
Figure 65 Configuring Virtual Ports (Meridian 1 system, logging enabled)



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

If you select a non-Meridian 1 system a Virtual Port Properties dialog box similar to Figure 66 opens.

Figure 66 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.

3 Check the Log check box 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, which is 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.

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

5 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" check box, or
- 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.

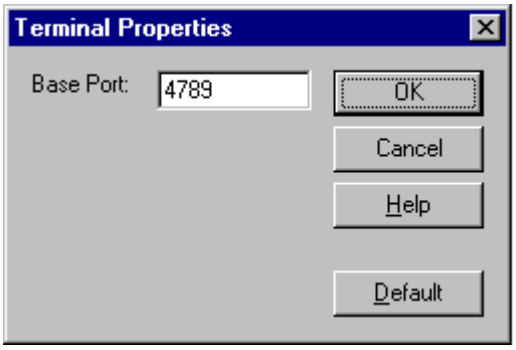
By default, the Terminal Server and Terminal Client communicates through network ports 4789 up to 5045 (4789 to send connection requests, 4790-5045 for up to 256 terminal sessions). Of course, the number of ports actually used depends on the number of virtual ports configured.

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

1 In the Terminal Server application, click the Terminals button.

The Terminal Properties dialog box opens (Figure 67).

Figure 67 Terminal Properties dialog box



2 Enter the new port number. Click the Default button to reset to the default value (port 4789).

For information on the Terminal Server Web Navigator Interface, see *Using Optivity Telephony Manager* (553-3001-330).

Set Up the Data Buffering and Access Application

To configure a DBA Serial Port session:

1 From the Navigator window, choose Utilities > Data Buffering & Access.

The DBA main application window opens.

2 From the DBA Main application window select File > New Session.

3 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.

4 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.

5 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.

For more information on the Data Buffering and Access Application, see *Using Optivity Telephony Manager* (553-3001-330).

Set Up the LDAP Server

The LDAP Server utility allows you to link and synchronize the OTM and Corporate LDAP databases. OTM acts as an LDAP Client to the Corporate LDAP Server database.

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 *LDAP Synchronization* in *Using Optivity Telephony Manager* (553-3001-330).

For information on importing non-LDAP compliant directory information into the OTM directory see *Import and Export Utilities* in *Using Optivity Telephony Manager* (553-3001-330).

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 *Alarm Management* in *Using Optivity Telephony Manager* (553-3001-330).

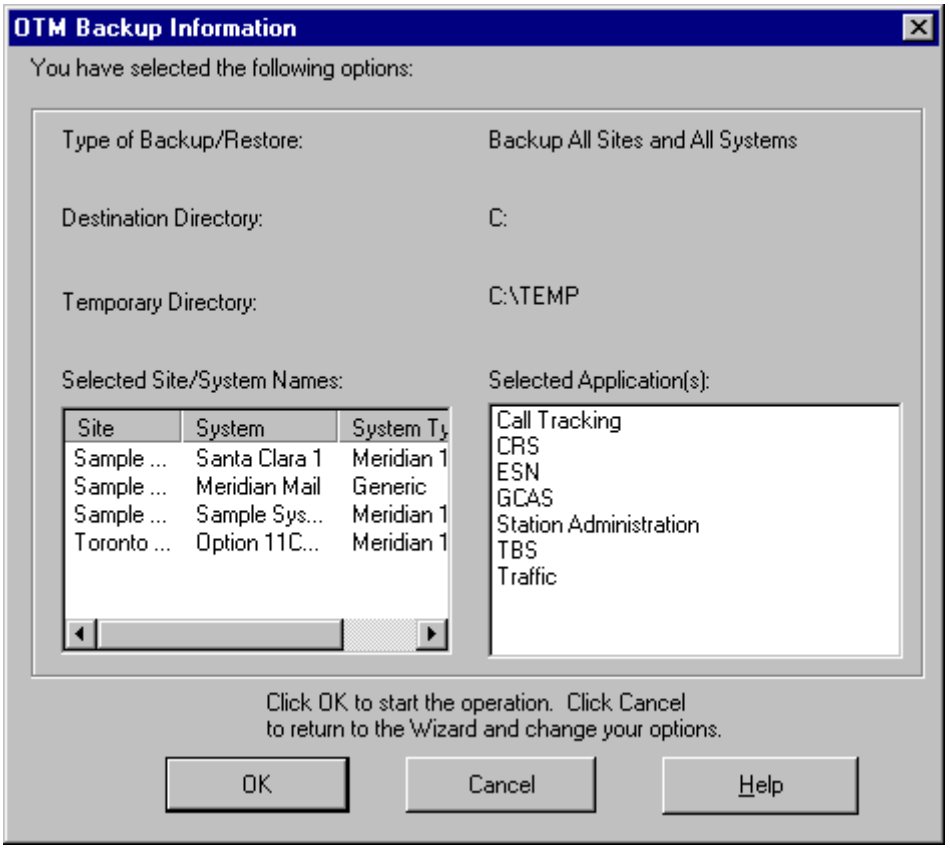
Perform an OTM backup

To perform a backup of your OTM data and applications:

1 In the OTM Windows Navigator, select Utilities > Backup.

The OTM Backup Information dialog box opens (Figure 68).

Figure 68 OTM Backup Information dialog box



This dialog box summarizes the options selected for the backup:

- Type of backup (single site, single system, all sites and systems, or disaster recovery)
- Applications (Telecom Billing System, Call Tracking, ESN, Station, Traffic, GCAS, and or CRS)
- 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.

2 Click the OK button to start the backup operation, or click the Cancel button to go to the backup wizard and change your options.

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 29.

Accessing the OTM Server Web Navigator via the PC Client

To access the OTM Server Web Navigator:

1 Enter the OTM Server IP address or computer name in the location bar of the Web browser on the PC Client.

2 Press the Enter button.

Software "plug-in"

The first time the OTM Server Web Navigator loads, you are prompted to download a software plug-in (Figure 69). The software you download is a standard Java Runtime Environment (JRE) "plug-in" of about 7-8 MB size.

Figure 69 JRE Plug-in download prompt

Integrating OTM with Optivity NMS

Optivity Telephony Manager (OTM) integrates with Optivity Network Management System (NMS) version 9.0.1 and above. Optivity NMS is an 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 section describes what you should know about integrating OTM with Optivity NMS. It includes the following information:

How the OTM with Optivity NMS Integration Works

OTM Alarm Manager receives Simple Network Management Protocol (SNMP) traps from managed Meridian 1 and Succession CSE 1000 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 www.nortelnetworks.com/documentation. Go to the Optivity Network Management & IP Services section, then Optivity NMS, and select the appropriate release of Optivity NMS.

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 CD-ROM.
- OTM integrates with Optivity NMS through OIT on any NMS platform - see "Checklist for Installing the Optivity Integration Toolkit (OIT)" on page 150. 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) 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.

  In the OTM installation, 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 "Checklist for Installing the Optivity Integration Toolkit (OIT)" on page 150.

OTM OIT files

OTM contains the following OIT files:

- otm_1.oit

  OTM Server device support entries

  OTM Open Alarm II definitions
- otmApp_1.oit

  OTM Web Application integration entries

OTM also contains the following mib file:

- rfc1223.mib

  Standard RFC 12313 MIB definitions

Run oitInstall for each .oit file, one at a time. The .mib file must be present in the same directory when oitInstall is executed. See step 5 under "Checklist for Installing the Optivity Integration Toolkit (OIT)."

Checklist for Installing the Optivity Integration Toolkit (OIT)

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

Note: This section provides general information on OIT. Refer to the NTPs, release notes, and read me files that are provided with your Optivity NMS software package for specific information on OIT.

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 1.2.2). 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 the environment variable LNMSHOME.

   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 the environment variable 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.

   All of the sub directories under \Optivity\Oit\ on the OTM CD-ROM are copied to OITHOME
5. Run LNMSHOME\bin\oitinstall -u <*full path of OTM OIT file*> for every .oit file in the OTM directory.

Where -u indicates to upgrade Optivity NMS. If you do not specify the -u parameter, only a syntax check 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 a 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

Note: For OTM, you must manually add the OTM Server.

OIT definitions for OTM reside in $OITHOME\OTM\otm.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 the command line.

The oitInstall program does the following:

- Automatically stops and restarts all Optivity NMS daemons (UNIX) or 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.

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 resources folders in InfoCenter. The OTM integration does not currently support Autodiscovery of these objects.

To configure Optivity NMS InfoCenter for OTM:

Note: You must be logged on as administrator / root in order to perform this activity.

1. Create a Voice Management folder in InfoCenter to contain all of the Voice Elements integrated into Optivity NMS (OTM in this case).
2. Modify the default Properties of the Voice Management folder to display the Optivity Telephony Manager objects added to this folder:
   a. Right-click the Voice Management folder and choose Properties (Figure 70).
   b. Open the ManagementServer folder.
   c. Select Optivity Telephony Manager (Figure 71).
   d. Click Apply.

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

Figure 70 InfoCenter Resources

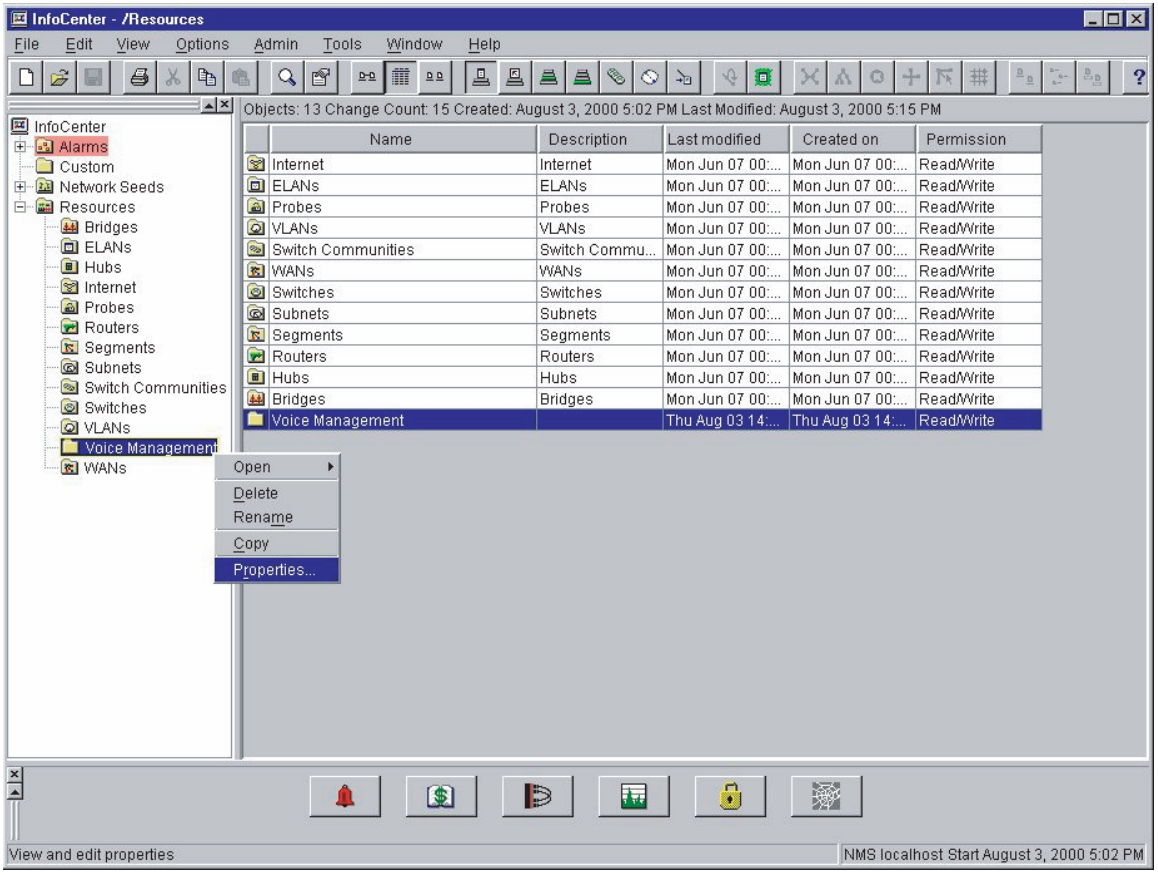
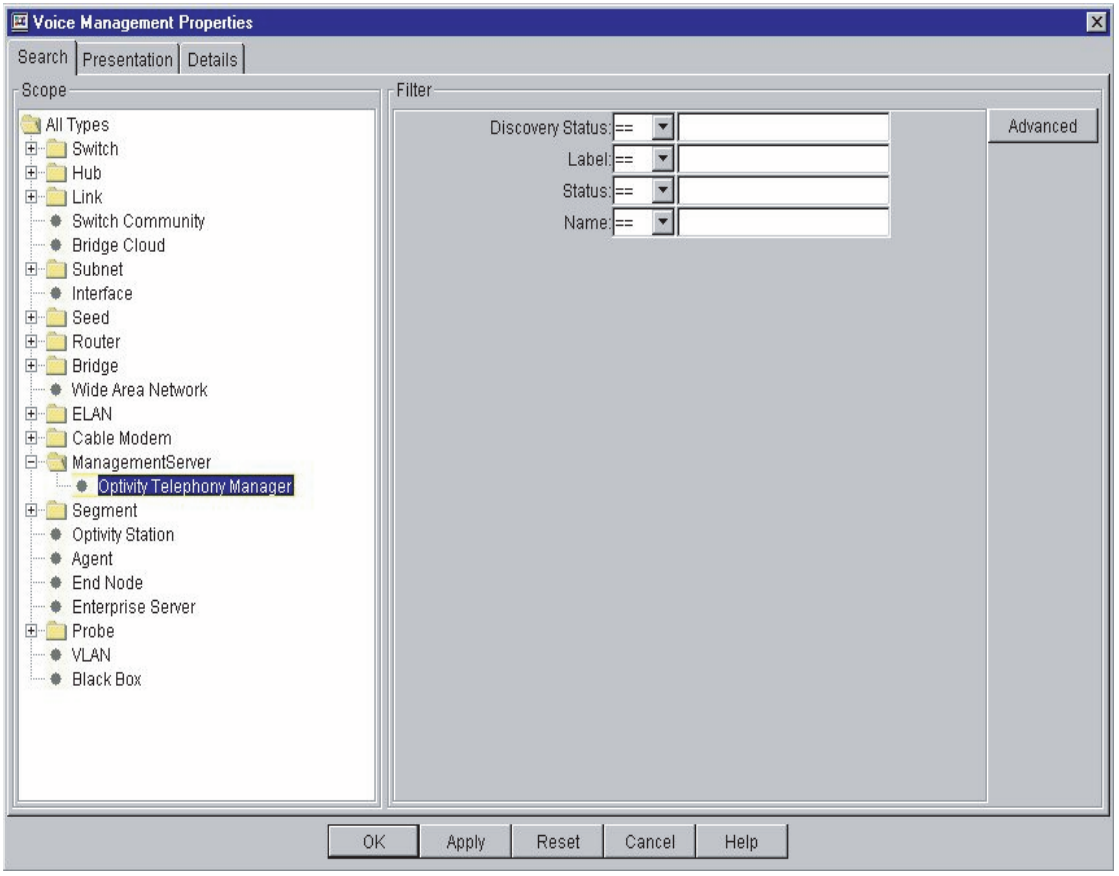


Figure 71 InfoCenter Voice Management Properties dialog box



Adding OTM Server Object to Optivity NMS InfoCenter

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

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 NMS 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 NMS InfoCenter to contain all the Voice Elements integrated into Optivity NMS.

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 selected (Figure 72).

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

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

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

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

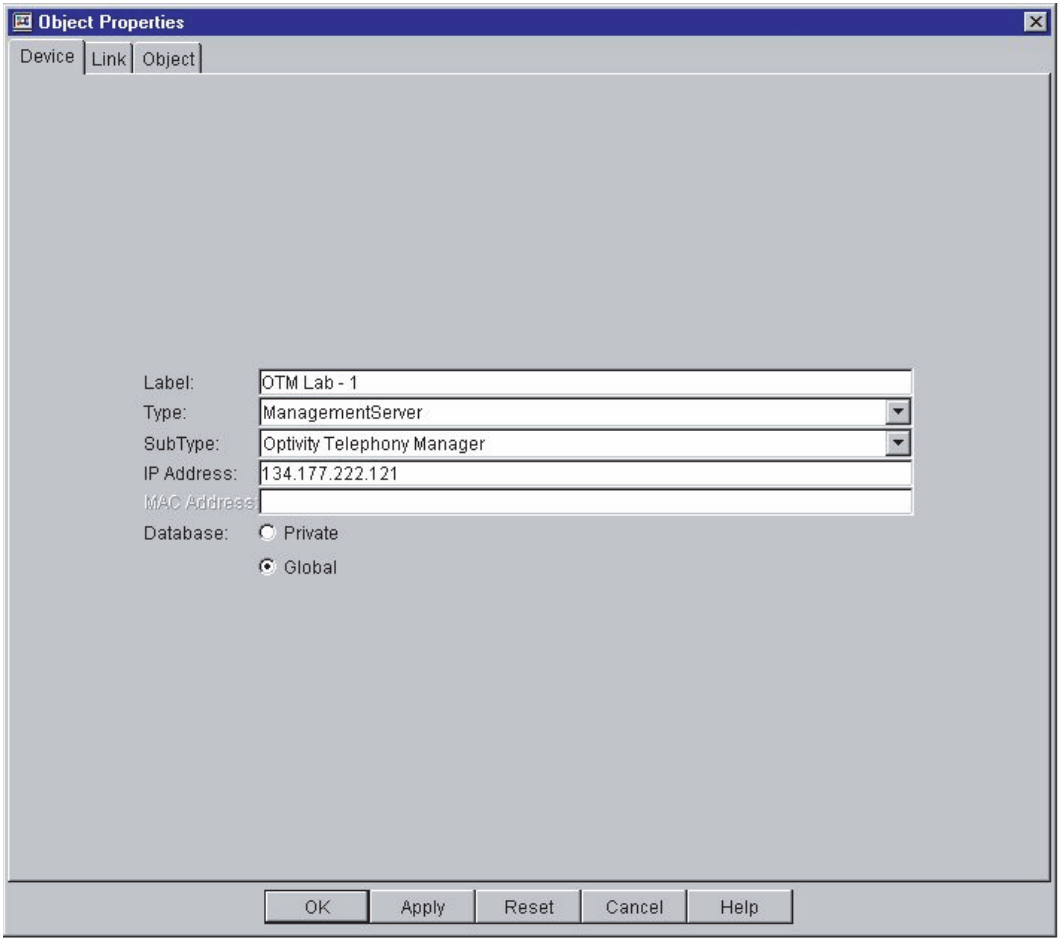
e Click Private or Global.

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

f Click OK.

A default switch icon appears for the OTM Server.

Figure 72 InfoCenter Object Properties dialog box



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

OTM Web Application links are integrated with Optivity NMS when an OTM Server is added.

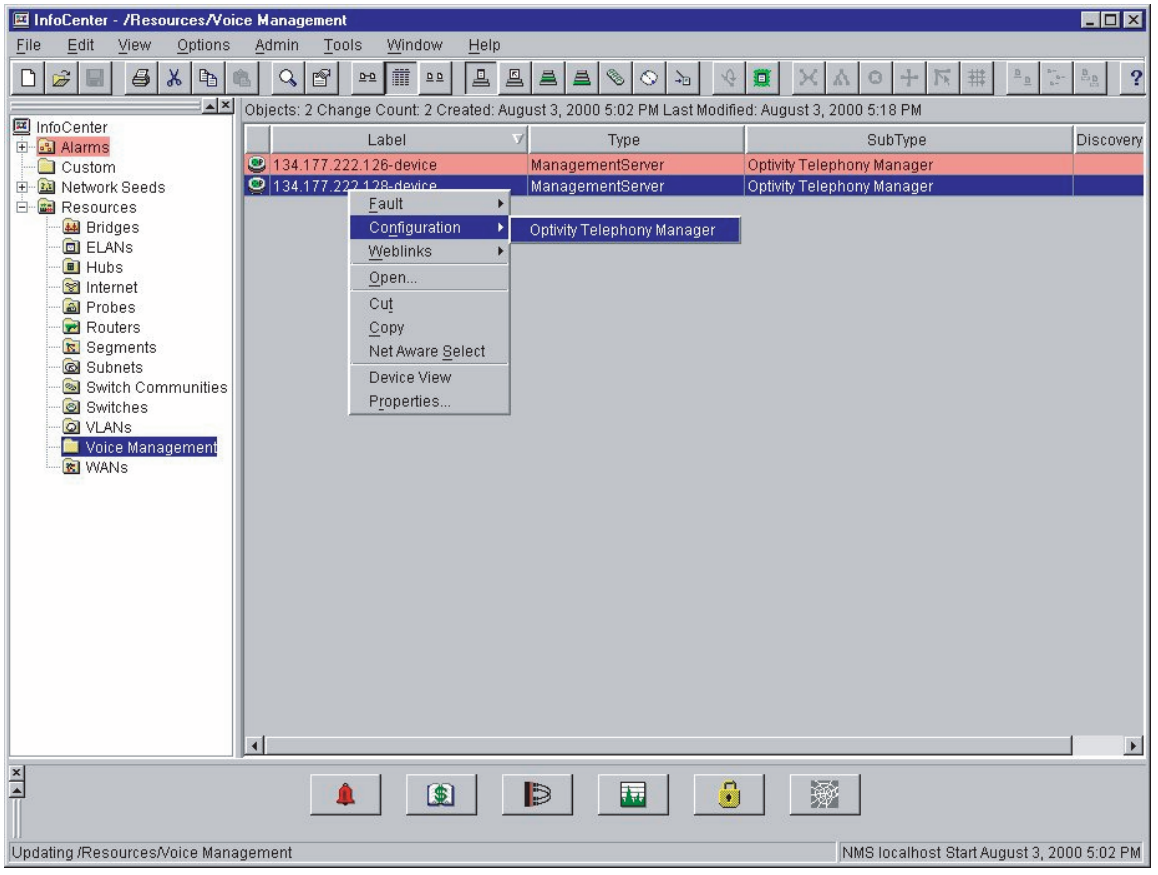
The OTM system being accessed can be running on the same server as Optivity NMS (for Windows NT), or it may be connected remotely through the network.

You can start OTM Web Applications by choosing Configuration and selecting Optivity Telephony Manager from the shortcut menu on the OTM icon in Optivity NMS InfoCenter (Figure 73).

This action will launch the default Web browser for your system and connect to the OTM Web Server.

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

Figure 73 Starting OTM Web Applications



Java Runtime Environment

OTM Web applications require Java Plug-In 1.2.2 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.

Using Fault Summary

OTM filters and then forwards Meridian 1 and Succession CSE 1000 traps to Optivity NMS. Since OTM forms the main representative agent for Meridian 1 and Succession CSE 1000 systems, 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.

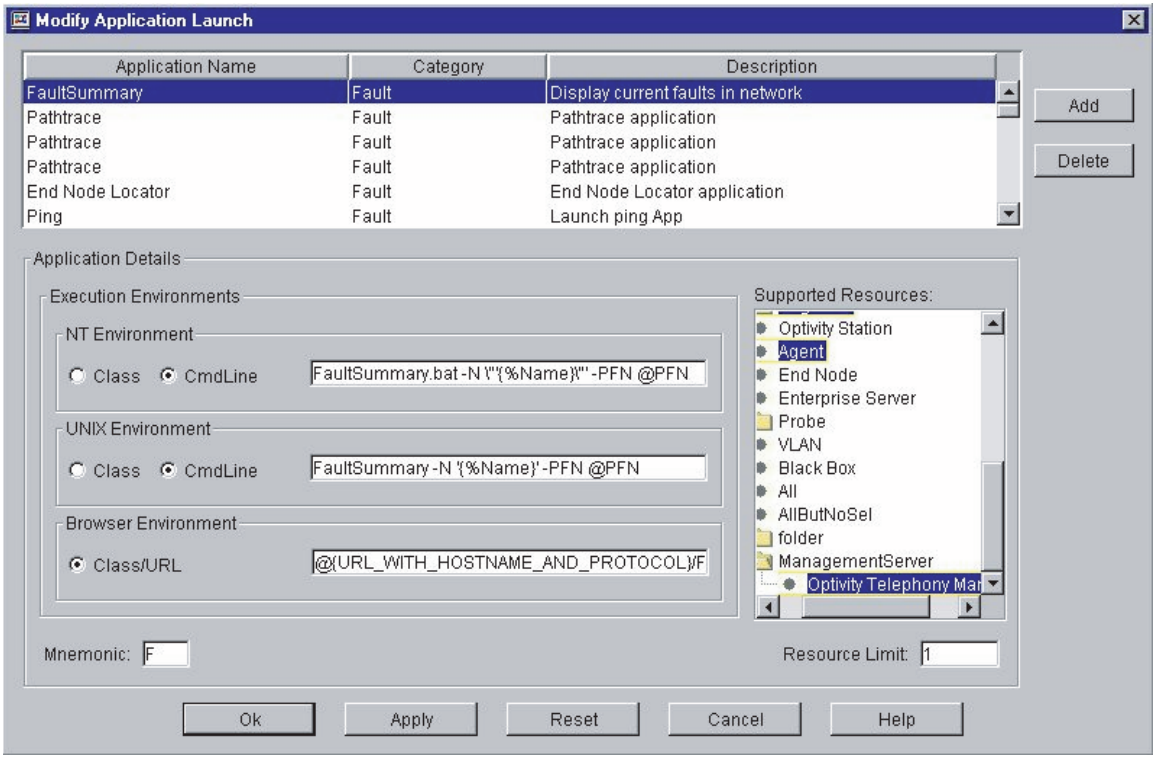
Upon receiving a Meridian 1 or Succession CSE 1000 alarm (or other traps that it has been configured to handle), OTM reformats it and forwards it to Optivity NMS. Optivity NMS recognizes the trap (from OIT definitions) and should now be able to reflect the changed status

Setting up Fault Summary

To set up Fault Summary:

1. Select Application Launch from InfoCenter's top menu.
2. Select the Fault Summary application (Figure 74).
3. While holding down the Ctrl and Shift keys, select the ManagementServer > Optivity Telephony Manager resource to enable Fault Summary for OTM.
4. Click Apply.

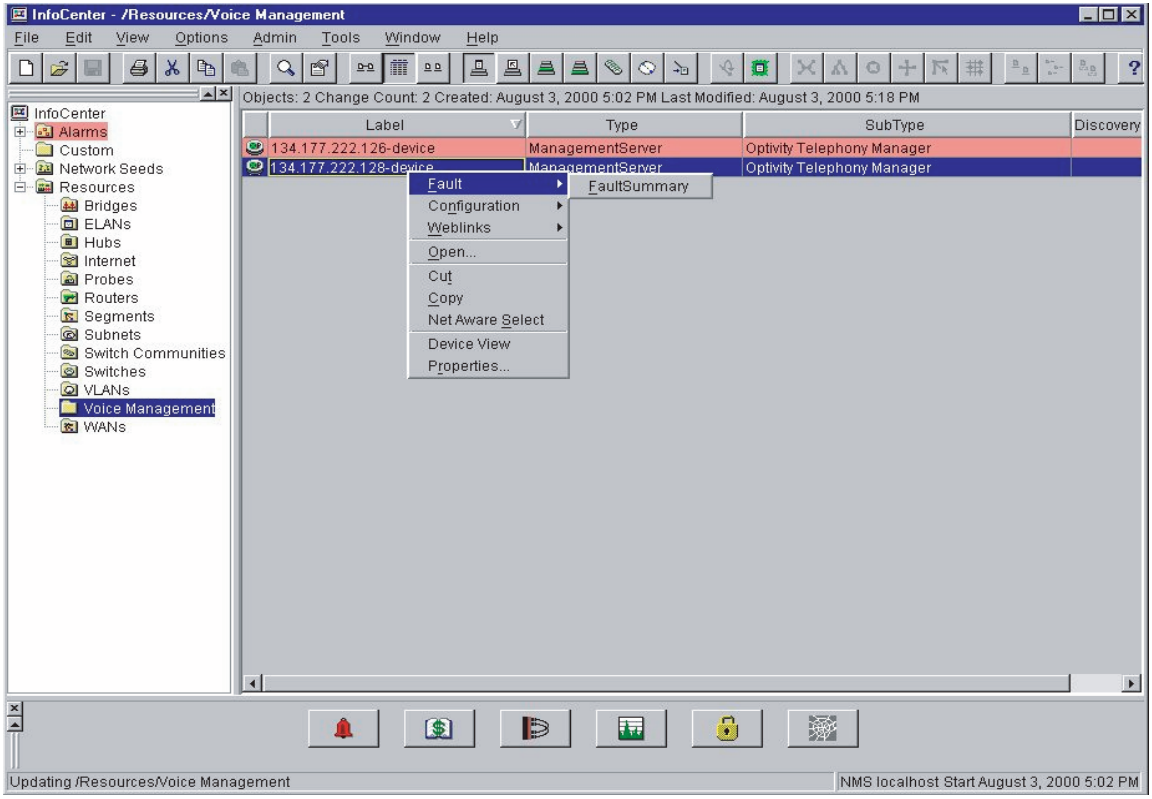
Figure 74 Modify Application Launch dialog box



To Launch Fault Summary:

➔ Select the OTM icon and use the right click menu to launch Fault Summary (Figure 75).

Figure 75 Launch Fault Summary



Configuring OTM

The Optivity Telephony Manager Server needs to be set up to forward traps to Optivity NMS. Forwarded traps must be in the OTM Open Alarm II format in order to be recognized.

The OTM Alarm notification application is used to forward traps of interest to Optivity NMS.

Sample scripts are provided with the Alarm Notification application that you can modify in the following ways to forward traps:

- Change the target IP to the address of the Optivity NMS Server.

- Select the severity of the traps that you want to forward — Critical, Major, Minor, etc.
- Modify the sample scripts to forward traps from devices other than Meridian 1, Succession CSE 1000, and other OTM devices to Optivity NMS.

Note: Take care to translate the incoming trap to OTM Open Alarm II and set the proper device identification and error code fields.

These traps, when received by Optivity NMS will result in a change of status of OTM and can be viewed through the Fault Summary.

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 Optivity NMS.

Troubleshooting

If you do not see the OITHOME environment variable you must manually set it before installing OTM or manually running oitInstall to update the Optivity NMS database.

If you do not see ManagementServer type and Optivity Telephony Manager sub-type on the Device — Add panel:

- Check to see if the OITHOME variable was set.
- Check to see if the OTM OIT files are present and in the correct folder.
- Check the oitInstall log file to verify that the OTM entries were updated.
- You may need to run oitInstall again.

If you cannot see OTM server that you have added:

- Check the View Properties of the folder to verify that it can display OTM servers.

If you cannot launch or connect to OTM Web Applications:

- Verify that the IP Address of the OTM Server entered in InfoCenter is correct.
- Verify that the OTM Web Server is running.
- Verify that you have the proper Java Plug-In installed.

If you are not receiving traps from an OTM Server:

- Verify that the OTM Alarm Notification application is running.
- Verify that the OTM Alarm Notification scripts are configured to send traps to Optivity NMS.
- Check the oitInstall log files to verify that the OTM entries were updated.
- Check the status of Optivity NMS daemons from Control Panel > Services or by typing optstatus -fe at the command prompt.

If you cannot launch Fault Summary for OTM

- Check the Application Launch entries. Fault Summary should be enabled for ManagementServer > Optivity Telephony Manager.

Integrating OTM with HP OpenView

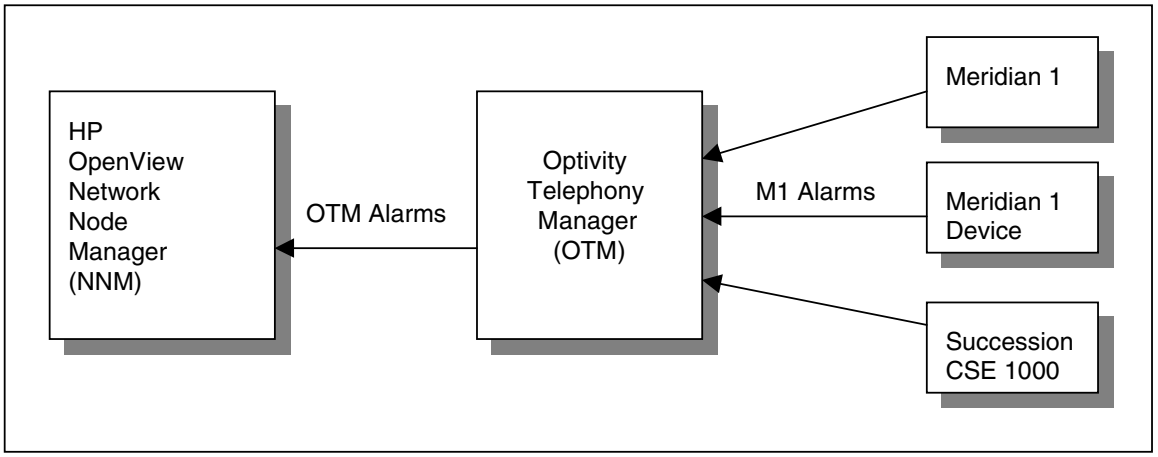
Overview

This section provides information on the integration of the HP* OpenView* (HP OV) Network Node Manager (NNM) management platform with Nortel Networks' Optivity Telephony Manager (OTM). It discusses the type of integration supported. The included procedures provide detailed step-by-step instructions on how to configure HP OV NNM to access OTM related functionalities and information.

Note: Nortel Networks' technical support for this feature is limited to support of the two software files that are distributed with OTM, *OtmOpenAlarms.mib* and *OtmStMon.exe*. These files are compatible with the version of HP OpenView that was current at the time your OTM software was released.

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

Figure 76 OTM alarm integration with HP OpenView Network Node Manager (NNM)



As seen in Figure 76, Meridian 1 systems, Succession CSE 1000 systems, Meridian Mail, and other M1 devices, send their alarms to the OTM server which can then collect the alarms and forward them to the NNM. The NNM displays the OTM alarms in its Alarm Browser and updates the color of the OTM object in the Network Map to reflect the current status of the OTM server, or the status of the devices the OTM server manages. In addition, the NNM can also be configured to allow the network administrator easy access to the OTM server.

Note: Refer to *Using Optivity Telephony Manager* (553-3001-330) for information on configuring the OTM Server to forward alarms to an external management station.

Limitations

- OTM integration with NNM is supported on HP OV NNM Release 6.*x* running on the Windows NT platform only.
- Co-residency is not supported for NNM and OTM on the same PC.
- The OTM Server will not support auto-discovery from NNM.

Hardware and Software Requirements

PC Hardware Requirements (HP OV PC)

Please refer to HP OV NNM documentation for details.

PC Software Requirements (HP OV PC)

- HP OV NNM Release 6.*x*
- OTM Alarm Integration Package:
  - OTM alarm MIB (OtmOpenAlarms.mib)
  - OTM Status Monitor (OtmStMon.exe)

OTM Software Requirements (OTM PC)

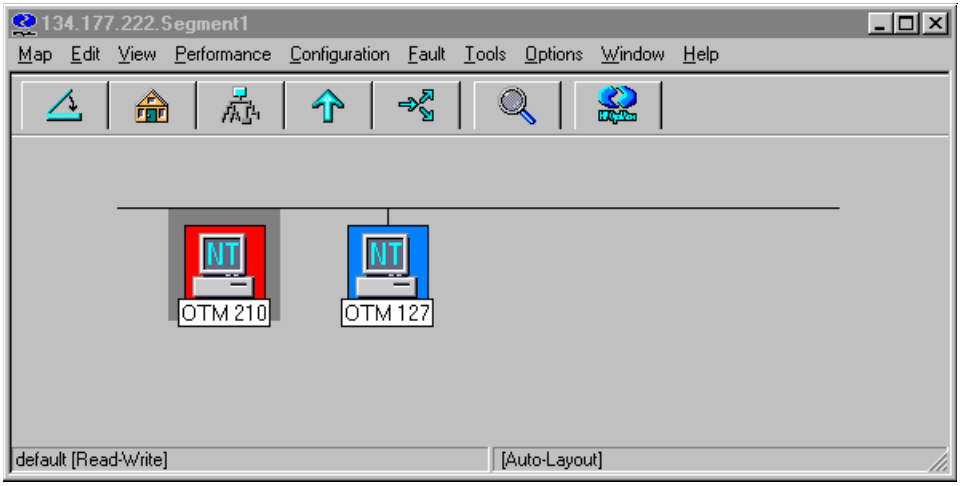
- OTM Release 1.01 or above with:
  - Alarm Notification application
  - Web-based alarm browser

System Integration

HP OV NNM Network Map

On the NNM Network Map (Figure 77), an OTM server can be represented as an object. Incoming events can be configured to trigger a color change to the object icon to indicate the current status of the OTM Server or of the devices monitored by the OTM Server.

Figure 77 HP OpenView Network Node Manager Network Map

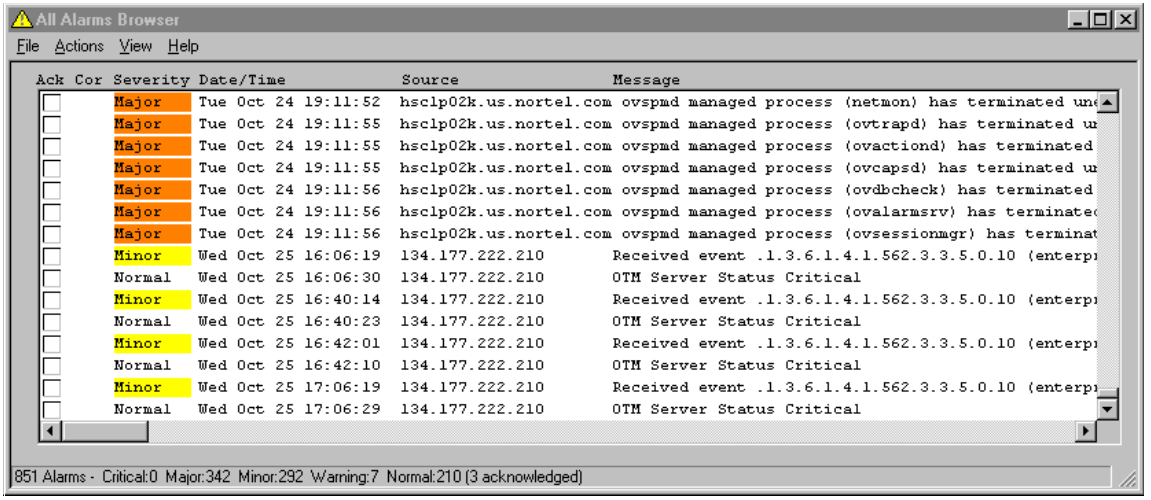


The OTM Status Monitor (OtmStMon) is the program that is used to update the color of the icon for an OTM object. When the color is changed upon the receipt of an incoming event, a message is also logged and displayed in the NNM Alarm Browser to indicate the status update.

HP OV NNM Alarm Browser

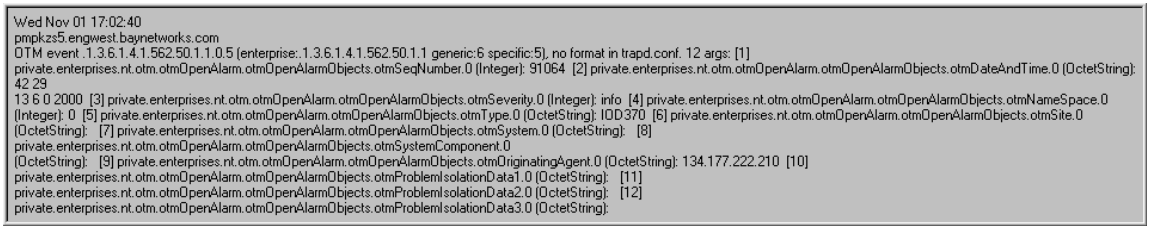
You can display contents of incoming OTM events in the NNM Alarm Browser (Figure 78).

Figure 78 HP OV NNM Alarm Browser



You can also highlight a specific alarm message on the NNM Alarm Browser, and right-click to display the message content in a separate window (Figure 79). You may then analyze the different variables and their values.

Figure 79 Alarm Message Content

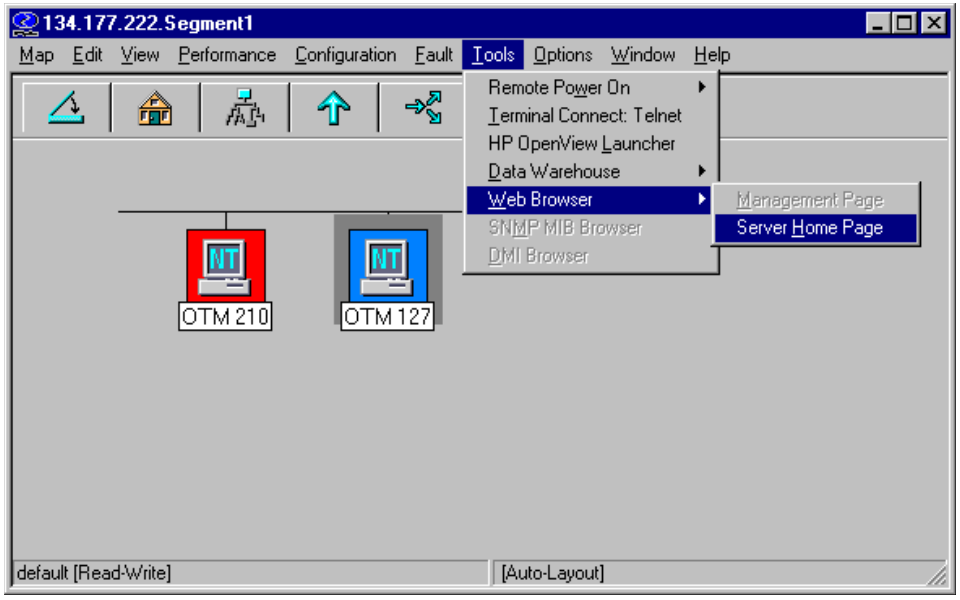


OTM Web Access

To access the OTM server from NNM:

1. Highlight the OTM object on the Network.
2. Select Tools > Web Browser > Server Home Page (Figure 80).

Figure 80 OTM Web Access



Your default web browser will be brought up with the web-based OTM interface. You can log in to the OTM Web Navigator and access the various OTM applications including the OTM Alarm Browser.

Installation and Configuration

OTM Alarm Integration Package (HP OV PC)

1 Copy the OtmStMon.exe to the Openview/bin ($OV_BIN) directory.

2 Copy the OtmOpenAlarms.mib to the directory $OV_SNMP_MIB/Vendor/NortelNetworks. Create this directory if it does not already exist.

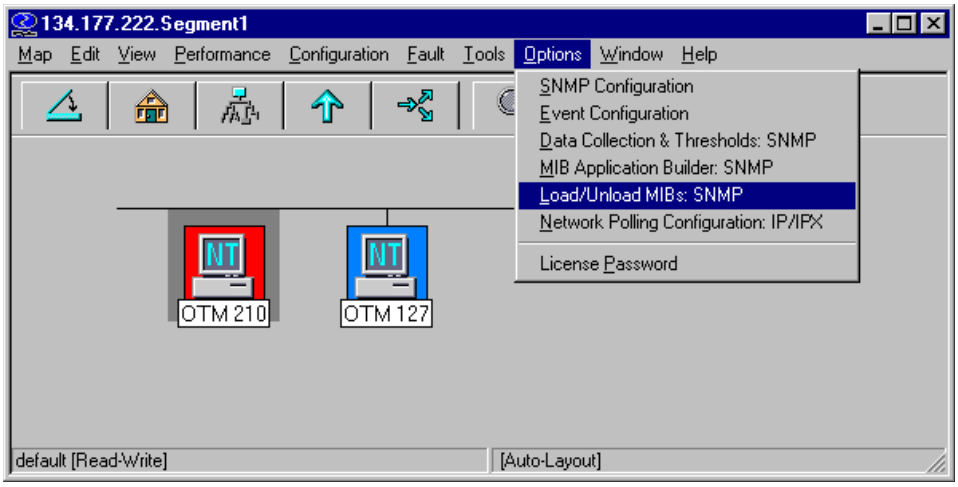
HP OV NNM (HP OV PC)

The following configuration procedures are performed while NNM is running:

OTM Alarm MIB installation

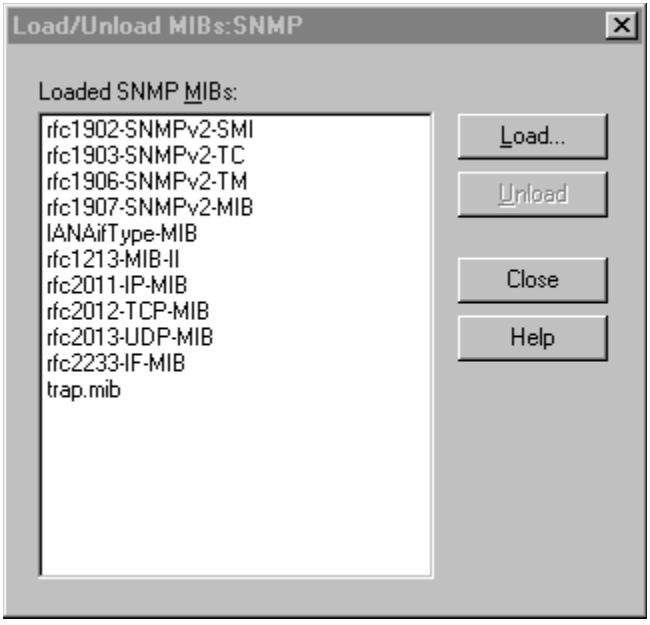
1 Select Options > Load/Unload MIBs:SNMP (Figure 81).

Figure 81 NNM Load/Unload MIBs



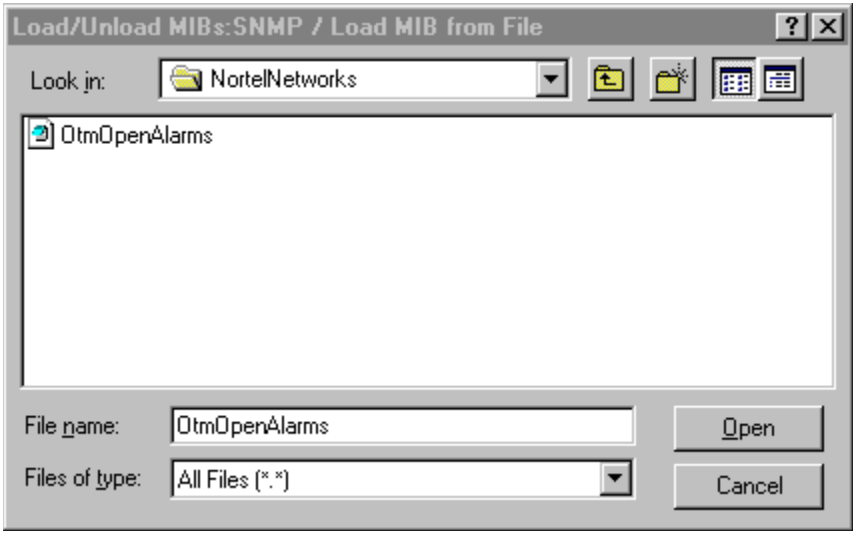
2 Click Load in the Load/Unload MIBs dialog box (Figure 82).

Figure 82 Load/Unload MIBs



3 Open the OtmOpenAlarms.mib file (Figure 83).

Figure 83 Load MIB



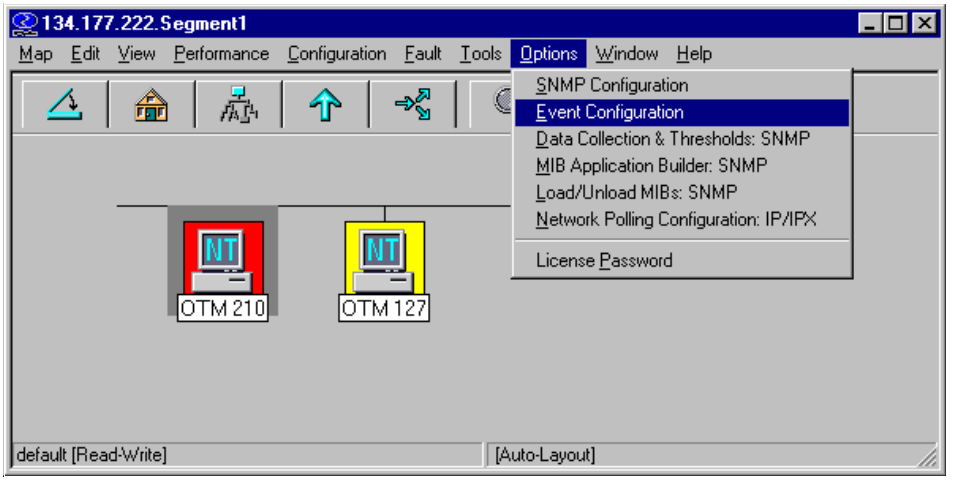
The OTM alarm MIB definitions are now loaded into the NNM's MIB database.

Event Configuration

After the OTM Alarm MIB is loaded, actions need to be defined through the NNM Event Configuration for each OTM event.

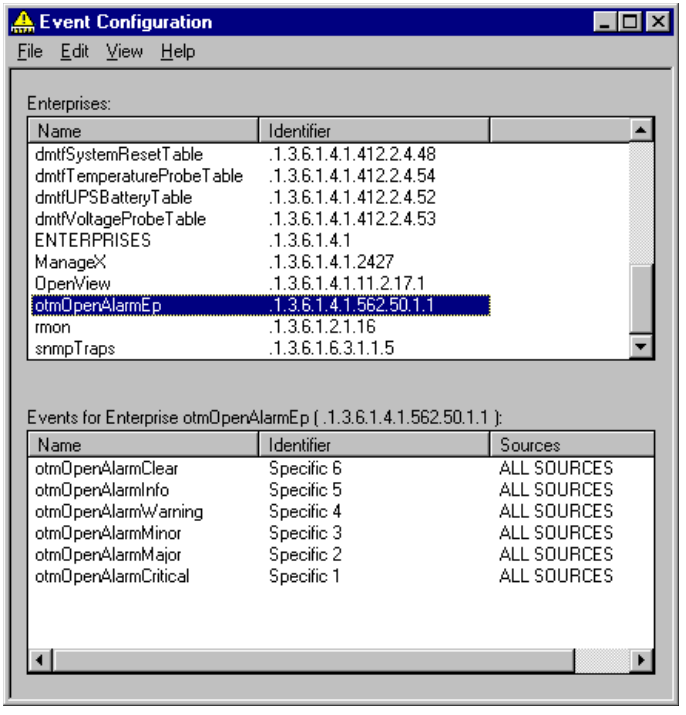
1 Select Options > Event Configuration (Figure 84).

Figure 84 NNM Main Menu - Event Configuration



2 Locate and select “otmOpenAlarmEp” from the list of Enterprises (Figure 85).

Figure 85 Event Configuration



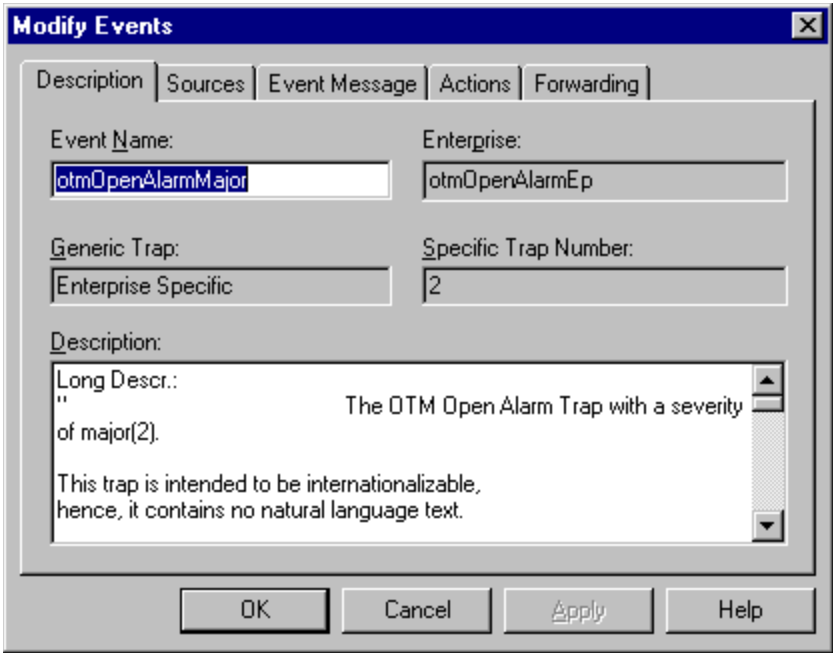
There are 6 events defined for the otmOpenAlarmEp Enterprise. For each event, you configure the desired actions to be taken if the event occurs.

Using the OTM Major Alarm event (otmOpenAlarmMajor, Specific 2) as an example:

1 Double-click on the corresponding entry on the list.

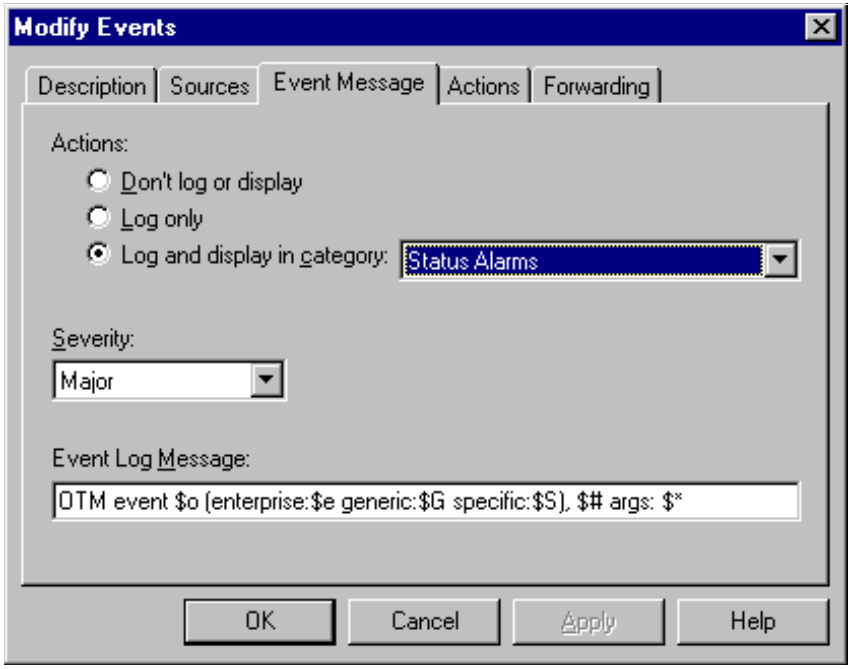
The Modify Events dialog box opens (Figure 86).

Figure 86 Modify Events - Description



2 Select the Event Message tab (Figure 13).

Figure 87 Modify Events - Event Message



3 Configure the following:

a Actions: Select Log and display in category: Status Alarms.

This will enable the display of the incoming event message in the NNM Alarm Browser.

b Severity: Select Major for this event.

c Event Log Message: Enter the following default text:

OTM event $o (enterprise:$e generic:$G specific:$S), $# args: $*

The message displayed will show the contents of the event message.

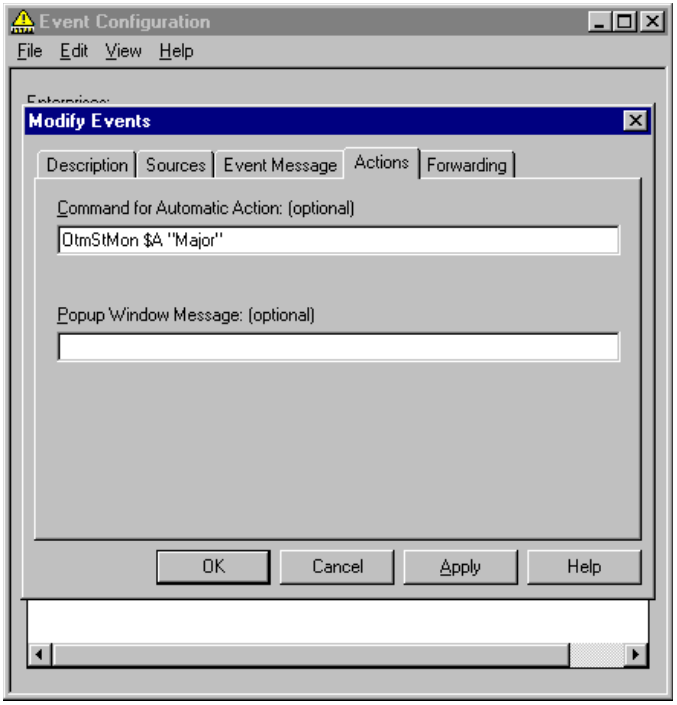
Note: You are allowed to display any message that you choose in the Alarm Browser

Table 6 Legend for $ variables in the Event Log Message

Variable	Action
$o	Print the name (object identifier) of the received event as a string of numbers.
$e	Print the trap enterprise as an Object ID string of numbers. This number is implied by the event object identifier for non-SNMPv1 events.
$G	Print the trap's generic-trap number. This number is implied by the event object identifier for non-SNMPv1 events.
$S	Print the trap's specific-trap number. This number is implied by the event object identifier for non-SNMPv1 events.
$#	Print the number of attributes in the event.
$*	Print all the attributes as seq name (type): value strings, where seq is the attribute sequence number.

If you also want the color of the object on the map to change to reflect the occurrence of the incoming event, you can also invoke the OTM Status Monitor (OtmStMon.exe) by specifying a call to it under the “Actions” item (Figure 14).

Figure 88 Modify Events > Actions



OTM Status Monitor

The OTM Status Monitor enables you to change the color of the OTM object on the Network Map to reflect the current status of the server. In addition, a message will also be logged onto the HP OV NNM Alarm Browser to indicate the status change.

OtmStMon is written in C and makes use of the HP OV ovevent application. OtmStMon takes in 2 parameters – an object's selection name and a textual representation of the new status, for example 'Critical' or 'Normal'. If ovevent cannot locate an object on the current Network Map with the specified selection name, an error message will be displayed. Therefore, if an OTM object is not defined in the Network Map, OtmStMon should not be invoked for an event.

The invocation format for OtmStMon is as follows:

OtmStMon <*selection_name*> <*object_status*>

Where

<selection_name> - HP OV NNM's unique selection name for an object item on the Network Map

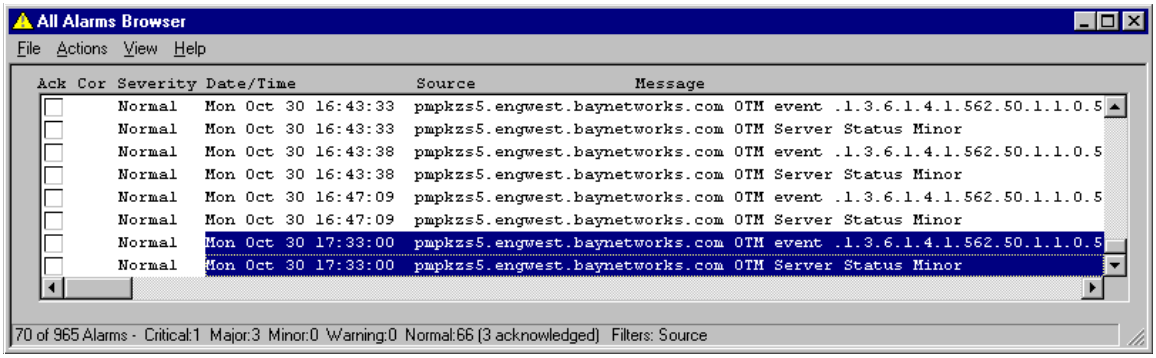
<object_status> - one of the following textual strings: "Unknown", "Normal", "Warning", "Minor", "Major", "Critical", "Restricted", "Testing", "Disabled", "Managed", "Unmanaged".

If the OTM Status Monitor is not called, then the color of the object displayed on the Network Map will not change for the incoming event.

Note: If no object is defined for the OTM Server on the Network Map, a call to OTM Status Monitor will result in an error. Therefore, do not specify calls to OtmStMon if there is no OTM Server defined on the Map.

Note: A call to the OTM Status Monitor will result in a message, in addition to the original incoming event message, being displayed in the NNM All Alarms Browser (Figure 89). This message is logged whenever the OTM Status Monitor changes the color of an object.

Figure 89 All Alarms Browser



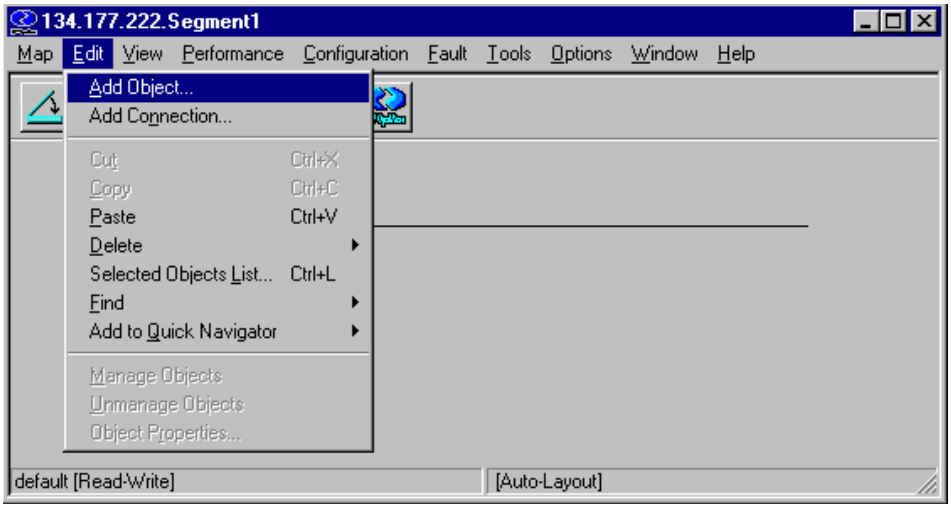
Note: Not every incoming OTM event necessitates the changing of the object's color. For example, a minor or info event may not need to alert the customer. In these cases, the customer might want to configure these events in such a way to simply log the incoming event message and not call OtmStMon.

Network Map Set-up

To set up an OTM Server object on the Network Map:

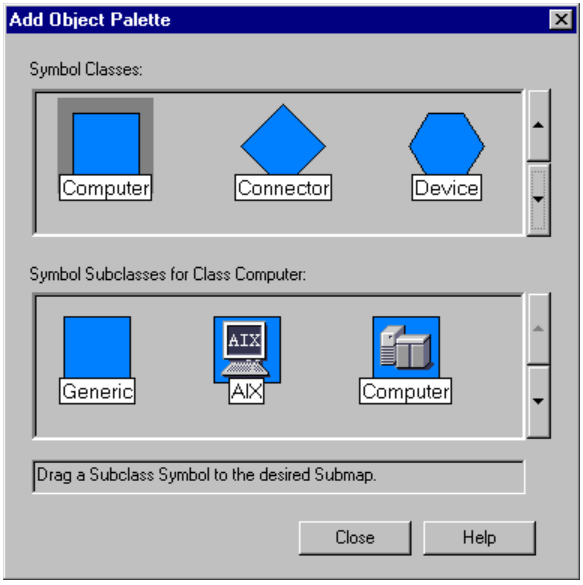
1. Locate the appropriate place in the Network Map for the OTM server.
2. Select Edit > Add Object (Figure 90).

Figure 90 NNM Edit > Add Object



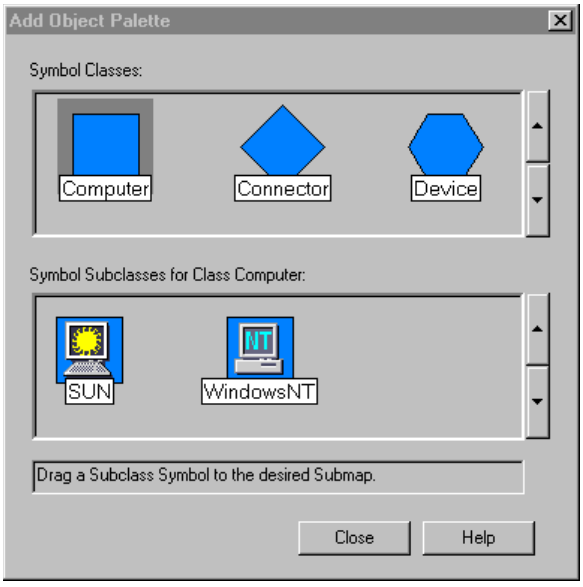
3 Select Computer from the Symbol Classes in the Add Object Palette dialog box (Figure 91).

Figure 91 Add Object Palette dialog box



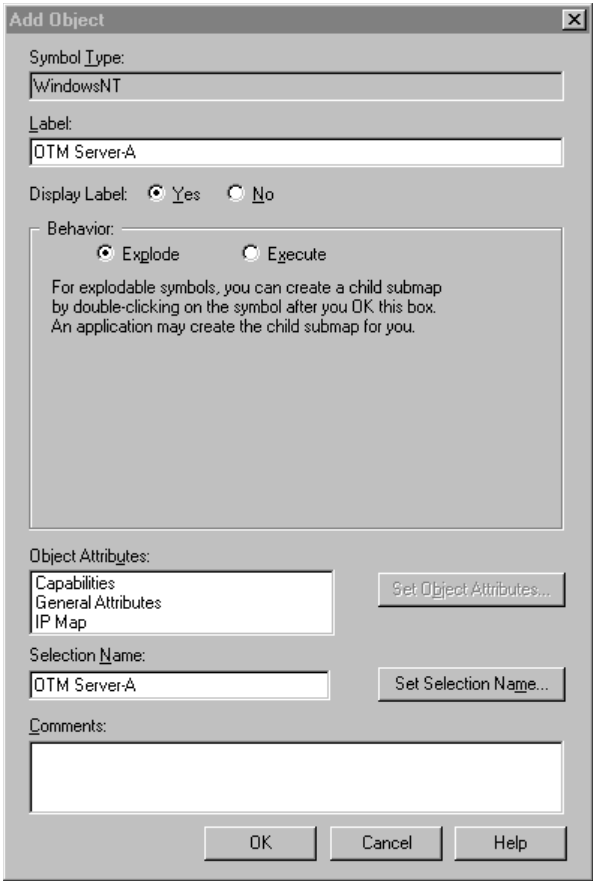
4 Select and Drag the standard WindowsNT icon from the Symbol Subclasses (Figure 92) onto the appropriate location on the Network Map.

Figure 92 Add Object Palette dialog box II



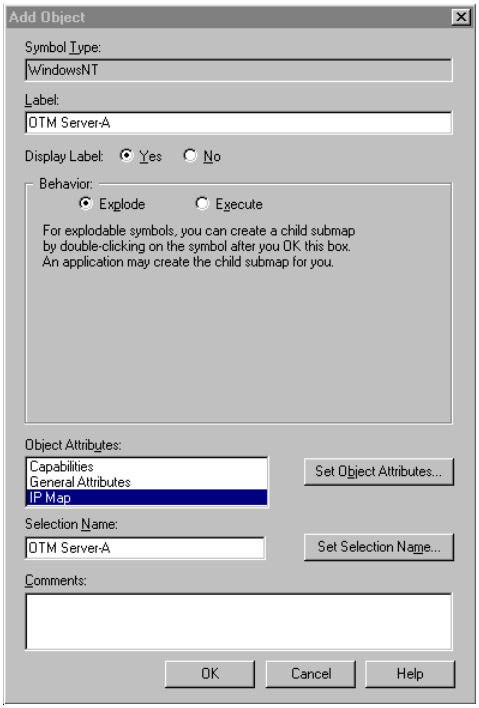
5 The Add Object dialog box will open. Fill in the Label field, OTM Server-A in this example (Figure 93).

Figure 93 Add Object dialog box



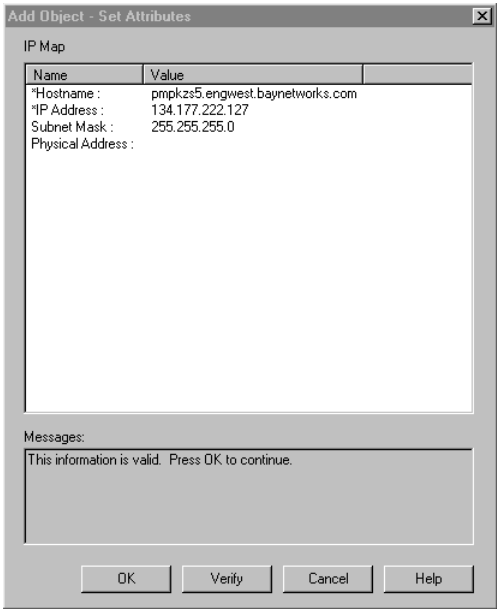
6 Select IP Map under Object Attributes and click the Set Object Attributes button (Figure 94).

Figure 94 Add Object > IP Map



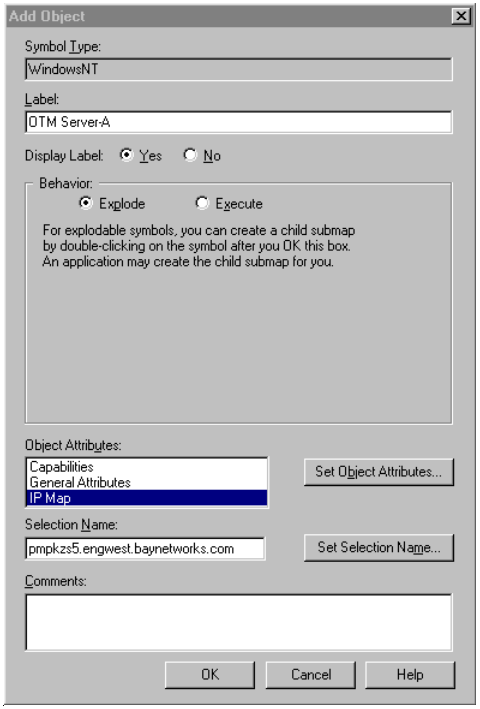
7 Select and fill in the entries for Hostname, IP Address and Subnet Mask (Figure 95).

Figure 95 Add Object - Set Attributes dialog box



8 Click OK. You are returned to the Add Object dialog box. In the Selection Name field, enter the same value as that of the Hostname in the previous step, pmpkzs5.engwest.baynetworks.com in this example (Figure 96).

Figure 96 Add Object > Selection Name



9 Click the OK button. The object is created on the Network Map.

Warning: The value for Hostname must be the domain name server (DNS) representation of the IP address (if the IP address can be resolved locally). Use the command *nslookup* to retrieve the DNS representation if you do not already know it (Figure 97). If the IP address cannot be interpreted locally, then enter the dotted decimal representation.

Figure 97 nslookup command

10 If you want to indicate the status of the OTM Server through the color of the object on the map, be sure to set the Status Source under Symbol Properties to Object (Figure 98, Figure 99).

Figure 98 NNM Main Menu > Symbol Properties

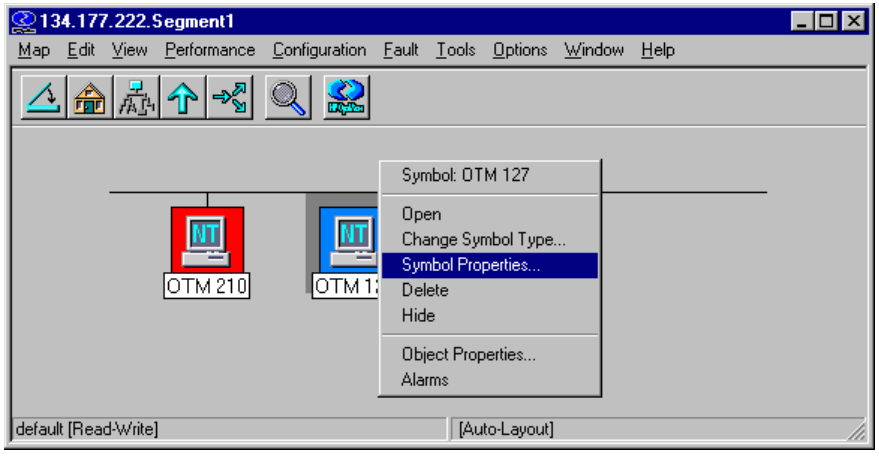
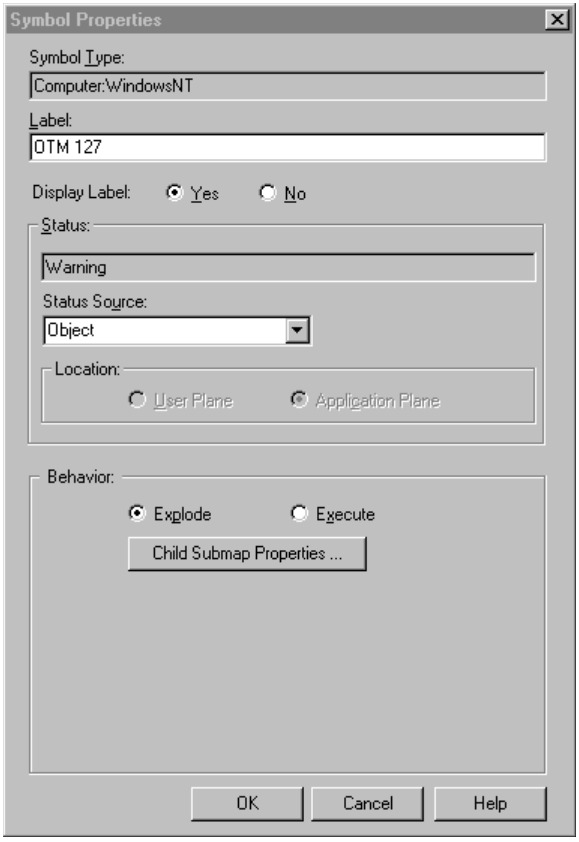


Figure 99 Symbol Properties dialog box



OTM Web Server Access Configuration

You can also configure the Management URL to access the OTM Server (Figure 100, Figure 101).

For an object on the Network Map, under General Attributes in the Object Properties dialog box:

1. Enter the address (IP address or the DNS name) of the OTM Server in the ManagementURL field.
2. Set isHTTPSupported to True.

Figure 100 Object Properties dialog box

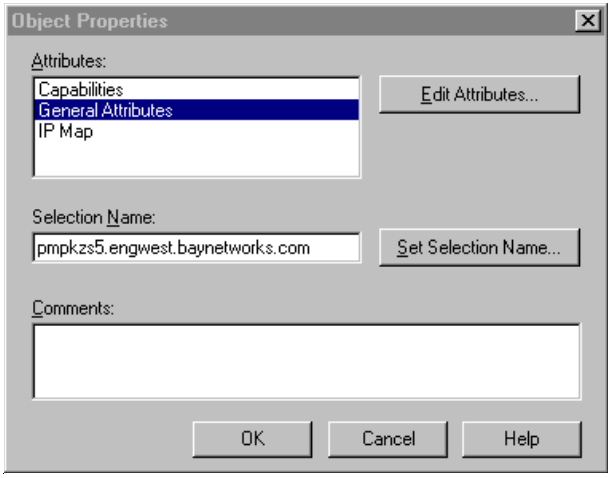
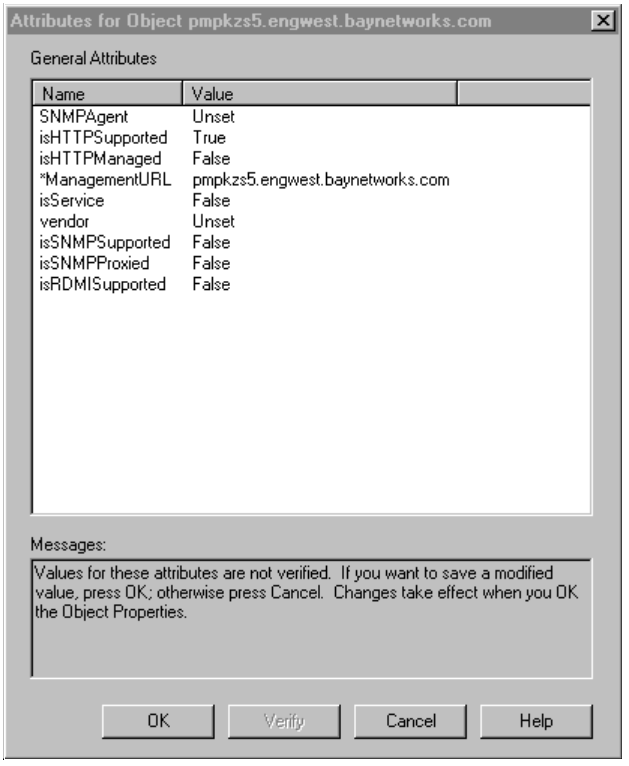


Figure 101 Attributes for Object dialog box



OTM configuration (OTM PC)

Refer to the Alarm Management chapter in *Using Optivity Telephony Manager* (553-3001-330) for information on configuring the OTM server to forward SNMP traps to HP OV NNM or other remote systems.

Chapter 3
Windows NT reference

This chapter provides reference information related to the Windows NT operating system. The following topics are presented:

Installing Windows NT

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.

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, Chapters 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 C-LAN card driver and follow the previous step to install the C-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 102. 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,

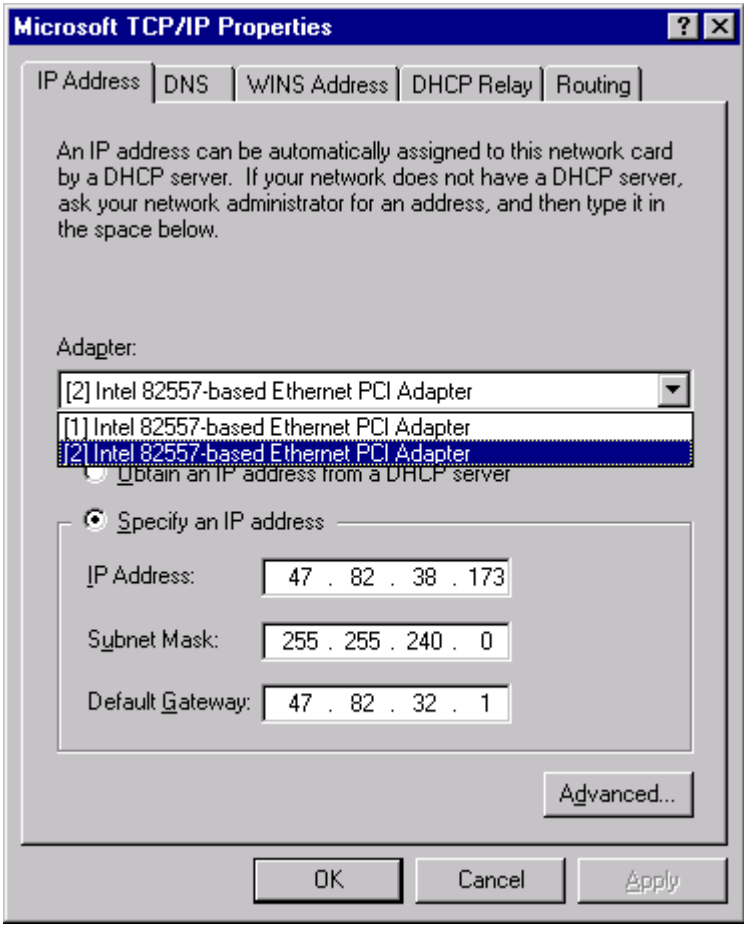
- Select adapter “[1]…” and enter the IP Address, Subnet Mask and Default Gateway for the Customer LAN (C-LAN) connection,
- Select adapter “[2]…” and enter the IP Address, Subnet Mask and Default Gateway for the Embeded LAN (E-LAN) connection.
- Click OK to continue.

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 102 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.
10. Select “Configure…” to choose “Dial out and Receive Calls” as Port Usage. Click OK.
11. Select “Network…” to configure “TCP/IP”. Click OK.
12. 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”.
13. In the “Remote Access Service has been successfully installed” screen, click OK.
14. In the “Network” screen, click OK. Click Close.

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.

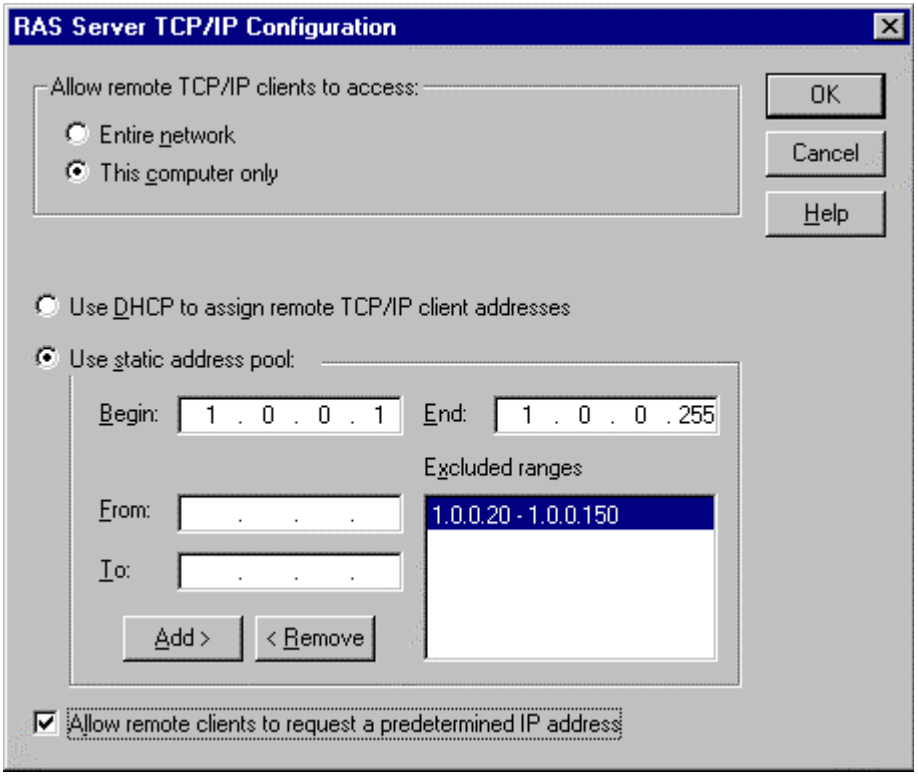
Caution: For security reasons, we recommend allowing the incoming call to access "The computer only," which is the RAS server itself.

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.

As shown in Figure 103, 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), or
- 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.

Figure 103 RAS Server TCP/IP Configuration window



Grant Permission

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

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 104, 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.

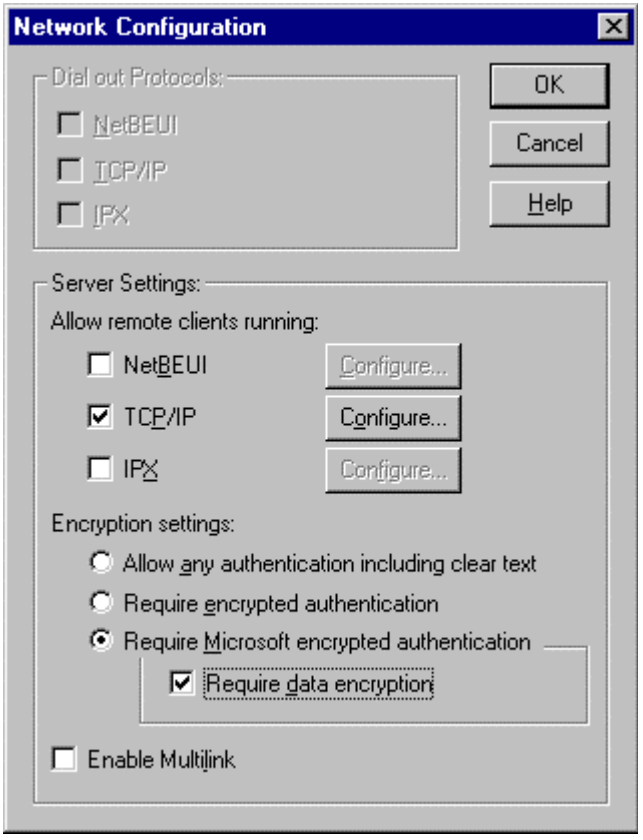
To use Multilink, both the server and client must have Multilink enabled.

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 104 Network Configuration window



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

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 5.01 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.

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 95/98/2000 TCP/IP protocol and routing table on the Meridian 1 or Succession CSE 1000 system, so that one Windows 95/98/2000 PC in a subnet is able to communicate with a Meridian 1 or Succession CSE 1000 system in a 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 or Succession CSE 1000 system, 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 and Succession CSE 1000 systems

- 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, 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, 192.168.40.11.

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 and Succession CSE 1000 TCP/IP Configuration

The first NIC address you enter will be your Meridian 1 or Succession CSE 1000 system's default gateway. Use Overlay 117 to add the new gateway address into the Meridian 1 or Succession CSE 1000 system's routing table. This will allow the system 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 Meridian 1 or Succession CSE 1000 system.

   ```
   >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 M1INACTIVEIP
   ```

3. Configure the subnet mask.

   ```
   >CHG MASK 255.255.255.0
   ```

4. Configure a default gateway for the Meridian 1 or Succession CSE 1000 system 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 that the computer is able to communicate with 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 messages similar to those below, where <*###.###.###.###*> represents the router address the packets crossed:

```
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.
```

If you receive messages similar to those in the following two examples, there must be a problem or configuration error at one of the routers on the network. Consult 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.

Security guidelines for Windows NT

This section 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 section 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 section:

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 primary domain controller (PDC).
- 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 and Windows 2000 provide 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 a 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 and Windows 2000 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 directory permissions specified in Table 7.

Table 7 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. Table 8 lists the services that can run on a secure IIS server.

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

Table 8 Services that can run on a secure IIS server (Sheet 1 of 2)

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)[1]	ClipBook Server
License Logging Service	FTP Publishing Service Web services run on different servers)	Computer Browser
MSDTC	FTP Publishing Service[1]	DHCP Client
Protected Storage	NNTP Service (required if using NNTP Service)[1]	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

Table 8 Services that can run on a secure IIS server (Sheet 2 of 2)

Required	May Be Required	Probably Not Required
Windows NT Server or Windows NT Workstation	RPC Locator (required if doing remote administration)	Network DDE & Network DDE DSDM Front Page extensions
Windows NTLM Security Support Provider	FTP Publishing Service Web services run on different servers)[1]	Network Monitor Agent
Workstation	FTP Publishing Service[1]	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)

1 Not required by the OTM Server nor recommended by Nortel Networks.

Nortel Networks strongly recommends that the OTM administrator does not store any installation application software on the OTM server or workstation, other than Nortel approved software.

Chapter 4
Uninstall OTM

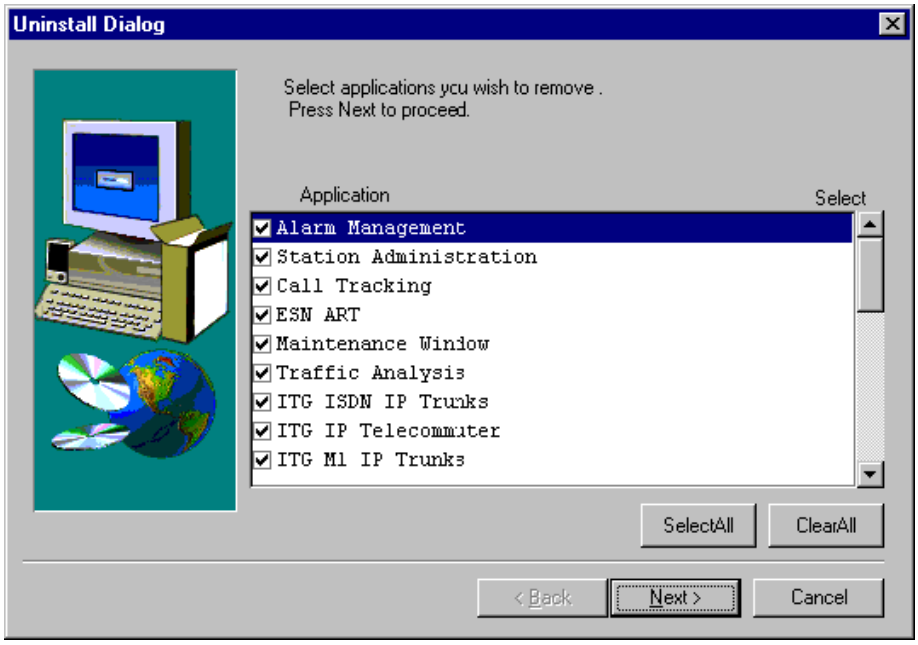
Use Uninstall to remove software that is no longer needed, or that has become damaged or was incorrectly installed.

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.

      or

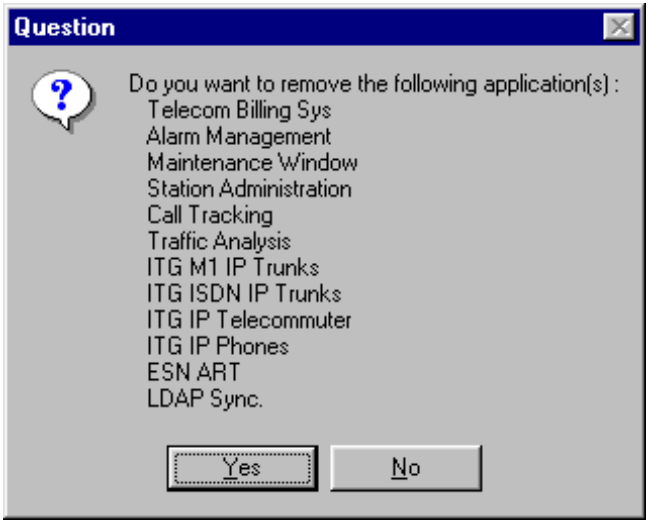
   b. In the Software Installation Wizard, select Uninstall in the Setup Choices dialog box. See "Setup Choices" on page 39.
2. The Uninstall dialog box displays a list of OTM applications which are currently installed. See Figure 105. Use the check boxes to select the applications you want to remove. Click Next to continue the uninstall process.

Figure 105 Uninstall dialog box



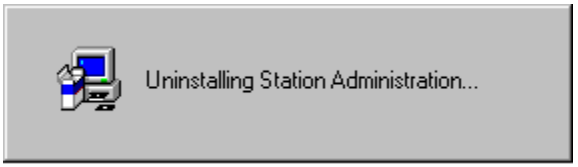
3 The dialog box shown in Figure 106 appears asking for confirmation that you want to delete the applications that you selected in the previous step. Click Yes to continue.

Figure 106 Uninstall Confirmation dialog box



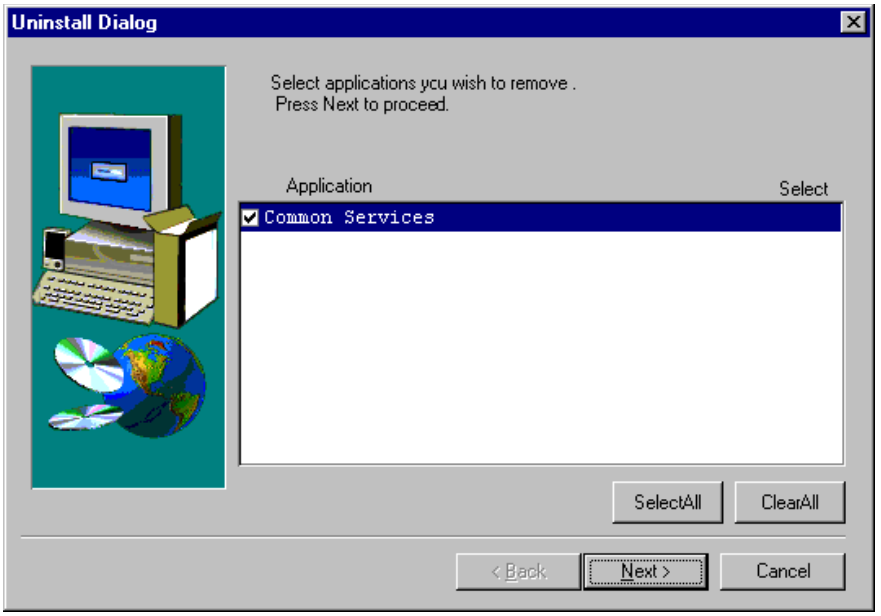
4 The status box, shown in Figure 107, provides a visual indicator of the progress of the uninstall process.

Figure 107 Uninstall status box



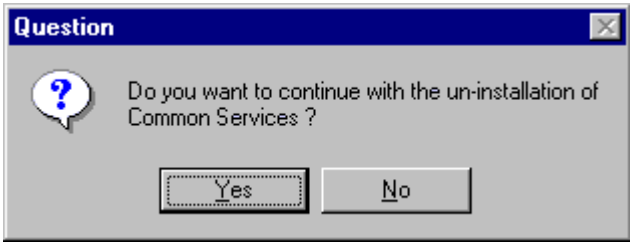
5 Common Services is always the last application to be uninstalled. After all other applications have been uninstalled, select Common Services from the Uninstall Dialog box as shown in Figure 108. Click Next.

Figure 108 Uninstall Common Services dialog box



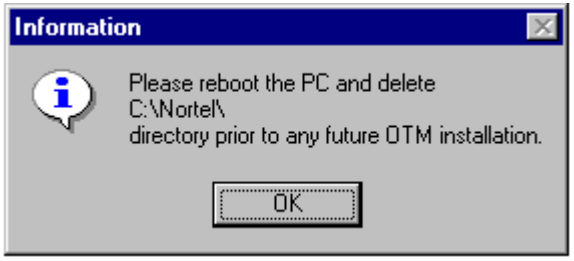
6 The dialog box shown in Figure 109 appears asking for confirmation that you want to continue with the uninstall. Click Yes to confirm that you want to remove Common Services.

Figure 109 Uninstall confirmation question box



7 The dialog box shown in Figure 110 appears requesting that you reboot the PC and reminding you to delete the OTM directory. Click OK.

Figure 110 Uninstall complete information box



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

Appendix A
OTM engineering guidelines

This appendix provides a set of guidelines to help you determine the configuration and distribution of OTM servers within a network to efficiently manage Meridian 1 and Succession CSE 1000 systems.

This appendix includes the following sections:

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. In order to simplify analysis, only those features are highlighted here that impact these resources.

- Web and OTM Clients and their impact on OTM Server Resources

- Web-based Station Administration Write capability (i.e. performing Station updates over the Web) and its impact on the OTM Server
- Meridian 1 and Succession CSE 1000 and their impact on OTM Server Resources
- Communications between the OTM Server and Meridian 1 systems, Succession CSE 1000 systems, OTM/Web Clients, LDAP Server, etc. and their impact on the network to which they are connected

Note: The GCAS and CRS Billing applications will result in processor load which is not possible to predict. The exact impact depends on several factors including types of reports being generated and quantity of data being merged. It is not possible to derive a general formula to predict the impact of these applications. Nortel Networks recommends that these applications be run during off-hours and that they not be run in parallel with other resource-intensive applications.

Based upon this analysis, recommendations are made as to:

- The resources required on the OTM Server
- The number of Clients and Meridian 1 or Succession CSE 1000 systems 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 standalone mode. The resource calculations presented herein are centered around the OTM Server, running on a Windows NT Server Platform.

Table A-5 on page A-22 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.

Sample walk-through of computations

This section provides a sample walk-through of computations used to determine how many Meridian 1 or Succession CSE 1000 systems 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 or Succession CSE 1000 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, General, Enhanced, and Premium).

Example 1:

Configuration
Station, ITG, Maintenance Windows, and other applications

Example 2:

Configuration and Alarms Management, MDECT configuration

Example 3:

Configuration and Alarms Management with Web/OTM Client Access and LDAP Service and Web Station Write configured for End Users (Full OTM System)

Example 4:

Alarms Management, Data Buffering & Access (DBA), Traffic Analysis, 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 A-3 on page A-26.

- 512 MB of physical memory
- ATAPI Hard Disk
- 2 OTM Windows and/or Web Clients active at the same time at peak usage
- Option 11C averaging 400 lines per system
  - — Averaging 1 call records/second generated (peak is 6)
- Option 81 with CP4 averaging 2000 lines per system
  - — 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 A-4 on page A-16 are:

  - — Station Add/Move/Change from server
  - — Station Add/Move/Change from OTM Client
  - — Station Web access
  - — Web Desktop Services Write capability for End Users
  - — Alarms monitoring
  - — CDR and Traffic Collection
- Normal operations are performed daily during normal working hours, for example from 8:00 AM to 5:00 PM every day. The default value is the peak six hours of the day (9:00 AM - 12:00 PM and 1:00 PM - 4:00 PM). Daily activities are based on the following assumptions:
  - — Percentage of lines changes by the network administrator per day is 1%. For example, a system with 2000 lines would have 20 lines changes by the network administrator during a normal work day.
  - — Number of lines changed by End Users through the Web Desktop Services is 0.25%. For example, a system with 2000 lines will have approximately 5 lines changes by End Users during a normal work day provided that the Web Desktop Services Write feature is configured.
- Off-hours operations can use 100% of the CPU, and will be limited as follows (from Table A-4):
  - — Station retrieve/reconcile will be performed once a week, or twice a month, on the weekend. The maximum period of time reserved for this activity will theoretically be 48 hours. For these examples, reserve the time from 9 p.m. on Sunday to 6 a.m. Monday, or 9 hours.
  - — Station transmit will be scheduled and performed during peak six hours, for example, from 9:00 AM - 12:00 PM and 1:00 PM - 4:00 PM.
  - — Assume, for Option 11C that OTM can run Station update for two Meridian 1 or Succession CSE 1000 devices simultaneously (based upon processor speed and CPU usage figures).
  - — CDR Reports will be performed once a day. For these examples, off-hours are from 12:00 AM (midnight) to 6:00 AM., or 6 hours.
  - — LDAP Sync will be performed once a week; on the weekend. For these examples, reserve the time from 9:00 PM Sunday to 6:00 AM Monday, or 9 hours.

Table A-1 and Table A-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 A-1 Maximum configuration for an Option 11C or Succession CSE 1000 network averaging 400 lines per system

Configuration Example	Number of Meridian 1 or Succession CSE 1000 systems	Number of Lines*	Number of simultaneous OTM Clients
1	26	10,800	
2	26	10,800	
3	26	10,800	20
4	6	2,600	

* Assumes two simultaneous systems.

Table A-2 Maximum configuration for an Option 81 network averaging 2000 lines per system

Configuration Example	Number of Meridian 1 systems	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 81 = 5 Meridian 1 systems or 10,800 lines:

- Routine operation:
  - — If administration is done primarily through the OTM Windows interface:

Adds/Moves/Changes = approximately 23.8%

— If administration is done primarily through the OTM Web interface:

Adds/Moves/Changes = approximately 36%

- 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/2000 lines per system = approximately 5 Meridian 1 systems
- Network bandwidth:
  - — Station (peak) operations = 80kb/second
  - — Network = 100 Mb/second
  - — % usage per system = 80 Kb/second / 100 Mb/second = approximately 0.1%
  - — 35% allowed usage / 0.1% per system = approximately 350 Meridian 1 systems

Option 11C = 26 Meridian 1 or Succession CSE 1000 systems or 10,800 lines

- Routine operation:
  - — If administration is done primarily through the OTM Windows interface:

    Adds/Moves/Changes = approximately 23.8%

  - — If administration is done primarily through the OTM Web interface:

    Adds/Moves/Changes = approximately 36%
- 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 system * 2 simultaneous systems = approximately 26 Meridian 1 or Succession CSE 1000 systems
- Network bandwidth:
  - — Station (peak) operations = 40 Kb/second
  - — Network = 100 Mb/second

— % usage per system = 40 Kb/second / 100 Mb/second = approximately 0.05%

— 35% allowed usage / 0.05% per system = approximately 700 Meridian 1 or Succession CSE 1000 systems

Example 2

The average alarms and MDECT usage are so small that their impact on routine, off-hour and network bandwidth is negligible. Therefore, use the results calculated in Example 1.

Example 3

Option 81 = 3 Meridian 1 systems or 6,480 lines:

- Routine operation:
  - — If administration is done primarily through the OTM Windows interface:

    If Web Desktop Services Write for End Users is not configured, then Adds/Moves/Changes = approximately 14.28%

    If Web Desktop Services Write for End Users is configured, then Adds/Moves/Changes = approximately 17.88%
  - — If administration is done primarily through the OTM Web interface:

    If Web Desktop Services Write for End Users is not configured, then Adds/Moves/Changes = approximately 21.6%

    If Web Desktop Services Write for End Users is configured, then Adds/Moves/Changes = approximately 25.2%
  - — OTM Client usage on OTM Server = approximately 4% per Client
    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 records = approximately 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 system =approximately 3 Meridian 1 systems

- Network bandwidth:
  - — Station (peak) operations = 80kb/second
  - — LDAP Sync operation = 720kb/second
    Percent usage of network = approximately 0.7%
  - — Network = 100 Mb/second
  - — Percent usage per system = 80 Kb/second / 100 Mb/second = approximately 0.1%
  - — 35% allowed usage / 0.1% per system = approximately 350 Meridian 1 systems

Option 11C = 26 Meridian 1 or Succession CSE 1000 systems or 10,800 lines:

- Routine operation:
  - — If administration is done primarily through the OTM Windows interface:

    If Web Desktop Services Write for End Users is not configured, then Adds/Moves/Changes = approximately 23.8%

    If Web Desktop Services Write for End Users is configured, then Adds/Moves/Changes = approximately 29.8%
  - — If administration is done primarily through the OTM Web interface:

    If Web Desktop Services Write for End Users is not configured, then Adds/Moves/Changes = approximately 36.0%

    If Web Desktop Services Write for End Users is configured, then Adds/Moves/Changes = approximately 42.0%
  - — OTM Client usage on OTM Server = approximately 4% per Client
    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/second
    For 100,000 records = approximately 2.8 hours
  - — 9 hours = 32,400 seconds
  - — 32,400 seconds * 1 record/6 seconds = 5,400 records (lines)
  - — 5,400 lines/400 lines per system * 2 simultaneous systems = approximately 26 Meridian 1 or Succession CSE 1000 systems

- Network bandwidth:
  - Station (peak) operations = 40 Kb/second
  - LDAP Sync operation = 720kb/second
    Percent usage of network = approximately 0.7%
  - Network = 100 Mb/second
  - Percent usage per system = 40 Kb/second / 100 Mb/second = approximately 0.05%
  - 35% allowed usage / 0.05% per system = approximately 700 Meridian 1 or Succession CSE 1000 systems

Example 4 configuration calculations

Option 81 = 2 Meridian 1 systems or 4,400 lines:

- Routine Operation:
  - CDR plus traffic = approximately 3.5% per system
  - If administration is done primarily through the OTM Windows interface:

    Adds/Moves/Changes = approximately 9.7%
  - If administration is done primarily through the OTM Web interface:

    Adds/Moves/Changes = approximately 14.67%
- 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/system = 194,400 call records per system
  - 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 system = approximately 2 Meridian 1 systems
- Network bandwidth:
  - CDR plus traffic (peak) operations = 118kb/second
  - Network = 100 Mb/second
  - Percent usage per system = 118 Kb/second / 100 Mb/second = approximately 0.1%

— 35% allowed usage / 0.1% per system = approximately 350 Meridian 1 systems

Option 11C = 6 Meridian 1 or Succession CSE 1000 systems or 2,600 lines

- Routine operation:
  - — If administration is done primarily through the OTM Windows interface:

    Adds/Moves/Changes = approximately 5.73%
  - — If administration is done primarily through the OTM Web interface:

    Adds/Moves/Changes = approximately 8.67%
- 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/system = 64,800 call records per system
  - — 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/system = approximately 6 Meridian 1 or Succession CSE 1000 systems
- Network bandwidth:
  - — CDR plus traffic (peak) operations = 59 Kb/second
  - — Network = 100 Mb/second
  - — Percent usage per system = 59 Kb/second / 100 Mb/second = approximately 0.05%
  - — 35% allowed usage / 0.05% per system = approximately 700 Meridian 1 or Succession CSE 1000 systems

Software Limits

Hard-coded Limits

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

- Data Buffering & Access (DBA)
  - — Connect to 256 Meridian 1 or Succession CSE 1000 systems

    DBA can perform all functions, CDR, Traffic, Backup and restore, etc. using one connection per Meridian 1 or Succession CSE 1000 system.
- 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 system without losing alarm information.
  - — Starting with Release 25 of Meridian 1 system software and in all releases of Succession CSE 1000 system software, there is the capability of filtering traps, on the system 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 Meridian 1 and Succession CSE 1000 systems that can be connected to greatly increases. However, when a single Meridian 1 or Succession CSE 1000 system 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 system, assuming that alarms from the other systems are minimal.

Operational Limits

Table A-4 lists those OTM features that have a significant impact on the performance of the OTM Server PC. Each feature the table lists their CPU utilization and elapsed time statistics, as appropriate, when connected to a single Meridian 1 or Succession CSE 1000 system.

OTM Web interface

Using the OTM Web interface has the advantages of not requiring installation of the OTM Client and providing the ability to access the OTM Server from any PC with a Web browser. However, using the Web interface will place a heavier workload on the OTM Server. The Web Desktop Services Write capability was introduced in OTM 1.1, and provides End Users as well as Administrators with the ability to configure telephones using a Web interface. After a telephone's configuration has been changed and scheduled, the job is placed into the queue of the scheduler. Currently, OTM supports only the "Schedule Now" capability which only allows the execution of one job at a time even for jobs involving different Meridian 1 or Succession CSE 1000 systems.

The scheduler executes the jobs in the queue one by one. This impacts the throughput of the system. There is a delay between the time that the job is scheduled and the time that the job is finished. While the job is being executed, the peak CPU usage may approach 100% causing a performance degradation to other applications.

Note: The slowness of DECT and other Web-based application responses is due to inherent limitations of the Web server software provided on Windows NT Workstation and Windows 2000 Professional. The Personal Web Server* software provides very slow responses and limits Web connections to ten simultaneous users.

Web Desktop Services

Web Desktop Services Write capability requires more OTM Server resources that earlier versions of OTM without this capability. For example, a station change performed through the Web interface would take up to 48 seconds of CPU time (2 seconds for finding, 24 seconds for changing, and 22 seconds for transmitting), while a change through the Windows Station Administration application requires

on 23.8 seconds of CPU time (1 second for finding, 0.8 seconds for changing, and 22 second for transmitting). If you schedule a job to run during off-hours, then the total CPU time is only 1.8 seconds for a change using the Windows Station Administration application.

Performing station administration activities primarily through the Web interface using the "Schedule Now" function places a larger workload on the OTM Server. For example, in a system with 10,800 lines and a daily change rate of 1%, Add/Move/Change activity through the Web interface would consume up to 36.0% of CPU usage compared to only 23.8% if performed using the Windows interface.

Web Desktop Services for end users

Configuring Web Desktop Services Write for end users also places an higher workload on the OTM Server. For example, in a system with 10,800 lines and an end user daily change rate of 0.25% (approximately 27 telephones), enabling Web Desktop Services Write for end users increases CPU usage for Add/Move/Change activity from 23.8% to 29.8%. Note that the ability for end users to make changes should decrease the need for the network administrator to make changes; so, the impact of configuring Web Desktop Services Write for end users may not be significant.

Web support on Server and Workstation platforms

Table A-3 outlines the differences observed in Web support when OTM is running on server grade platforms (Windows 2000 Server, Windows NT Server) and Workstation platforms. Additional differences between the Windows NT Server and Windows NT Workstation platforms are given in Table A-5 on page A-22.

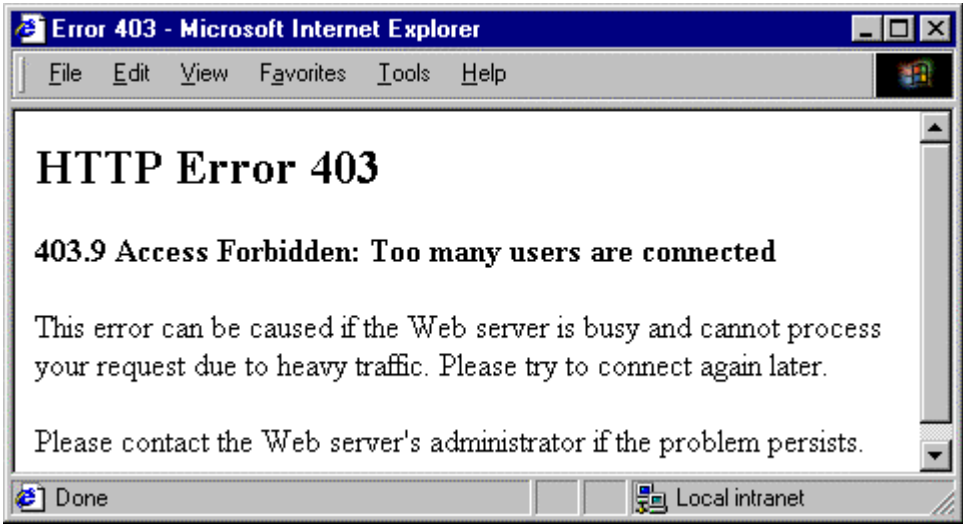
Table A-3 Web support on Servers and Workstations

	IIS on Windows NT Server or Windows 2000 Server	PWS on Windows NT Workstation or Windows 2000 Professional
Concurrent Internet Explorer sessions	Only limited by application capacity	5
Concurrent Netscape Navigator sessions	Only limited by application capacity	2
Restricted Access by IP address and domain name	Yes	No

Peer Web Server (PWS) is only intended to provide low volume Web publishing capability. Performance will degrade with increased traffic and complex Web pages or Java applications. The number of sessions supported by PWS ia based on a ten connection limit. Internet Explorer uses two connections per session while Netscape Navigator uses between four and six connections depending on the size of the Web page.

When additional clients attempt to access Web Services and there are no available connections, the error message shown in Figure A-1 is displayed.

Figure A-1 Too many users are connected error message



Modems

A modem connection between the OTM Client and the OTM Server is used for the command line interface (CLI) and Web applications. The OTM Server can operate as a terminal server, and the OTM Client uses the CLI to access the Meridian 1 or Succession CSE 1000 system. Nortel Networks recommends that you migrate to Web applications and access OTM features in a Client/Server configuration using a modem connection.

Operational testing

The test setup was:

- A 450 MHz Pentium II/III with 256 MB of memory and ATAPI hard disk interface
- A Meridian 1 Option 61C/81C, and assumes that 1% of a total of 1000 lines are changed on a daily basis by the network administrator

  For an Option 11C or Succession CSE 1000 system decrease CPU usage by a factor of 2 and increase elapsed time by the same factor for those features that interact with the system, for example, Station Update, but not Cost Report.
- A 100 mb network

Table A-4 PC Performance by Application

Application	Real Time (CPU)		Elapsed Time
	Peak	Average	
Station Administration Add/Chg/Del		2.2%	
Station Reconcile with Meridian 1 system	100%		1 record / 3 seconds
Web Station Administration	100%		1 record / 48 seconds
Web Desktop Services Write for end users	100%		1 record / 48 seconds
Web Admin		Negligible	
Alarm Monitor	2%	Negligible	
DBA - CDR Collection	6%	3%	
DBA - Traffic Collection	1%	0.5%	
LDAP Sync*	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

* LDAP Sync testing was based upon the use of an LDAP server dedicated for this testing. Since OTM 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 A-17. Also, follow these guidelines using the information provided in sections "Physical Memory" on page A-19, "Hard Disk" on page A-20, and "Processor Speed" on page A-21:

- 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 A-20 for details.)
  - — Has a spare storage bay and power for adding an internal hard disk
  - — Can accommodate increasing the memory capacity to 512 MB or greater (Most PCs have 2 to 4 memory card slots that can accommodate 32 MB, 64MB, 128MB, 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 A-20 for details)
- 256 MB of RAM (refer to "Physical Memory" on page A-19 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 Telecom BIlling System)
- 2 GB hard drive with 500 MB of free space with IDE interface
- 64 MB of RAM (128 MB of RAM is recommended for improved performance and for the Billing Enhanced level applications)
- 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, Windows 2000, or 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 Telecom Billing System)
- 2 GB hard drive with 500 MB of free space with IDE interface
- 64 MB of RAM (128 MB of RAM is recommended for improved performance and for the Billing Enhanced level applications)
- 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, Windows 2000, or 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 or modem
- Windows-compatible mouse or positioning device
- Windows 95, Windows 98, Windows 2000, or 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 ~150MB without active features. The minimum server memory is 256MB.

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 256MB of memory installed.

The one exception to this is OTM Client access. Each OTM Client connection to the OTM Server requires an additional 3MB of memory. For large configurations, such as 100 Meridian 1 systems and 50 OTM Clients, an additional 150MB of memory would be required.

For maximum performance on the largest systems, a minimum of 512MB 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
- TBS 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 A-17 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.

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

  If the 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 approximately 900MB without OTM data or active features.

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

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

Station~ =500KB per 100 telephones. From the example Tables A-1 and A-2: Disk space = 500 KB/100 telephones*10,000 lines = 50 MB of disk space.

Directory~= 80 KB per 100 records. From the example Tables A-1 and A-2: Disk space = 80 KB/100 telephones * 10,000 lines = 8 MB 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 A-5 shows the differences between Windows NT Workstation and Windows NT Server.

Table A-5 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 A-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.

OTM Clients can dial up to the OTM Server and use CLI to access the Meridian 1 systems. For full access to OTM features, the OTM Client can also use OTM's Web interface. An OTM Client can connect to a standalone OTM Server using a remote access software package, for example pcANYWHERE*.

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

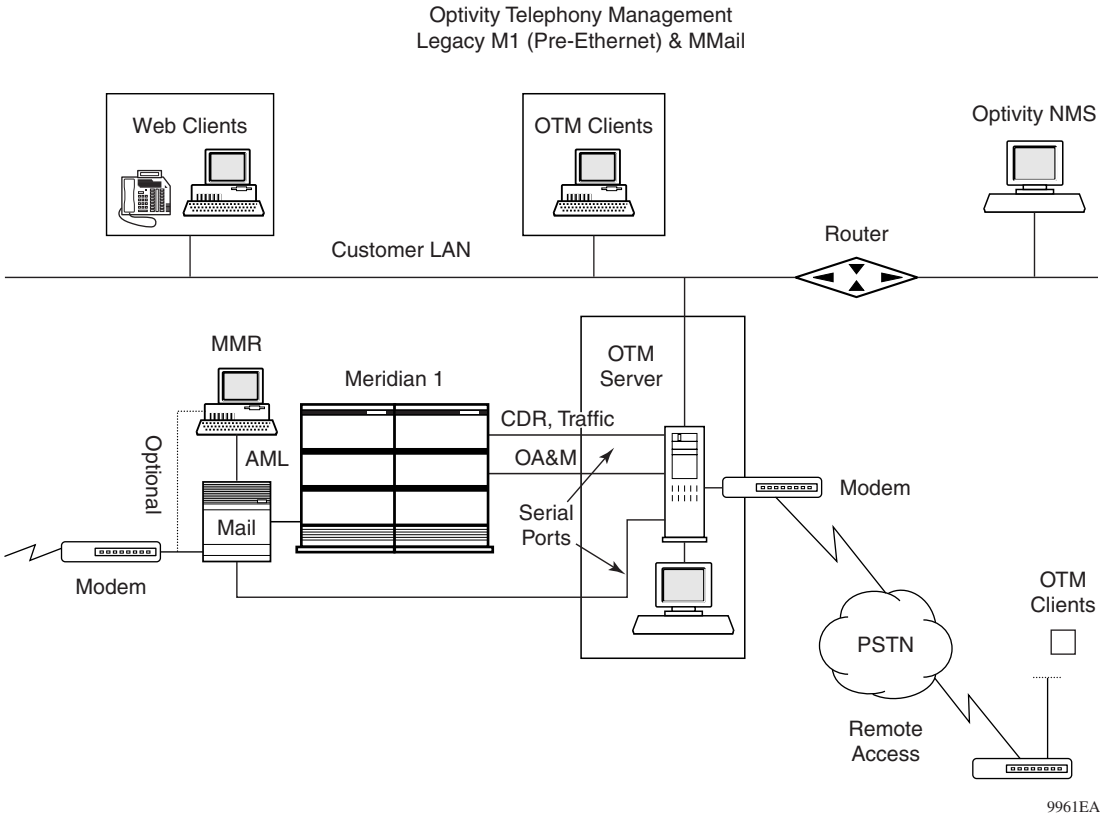
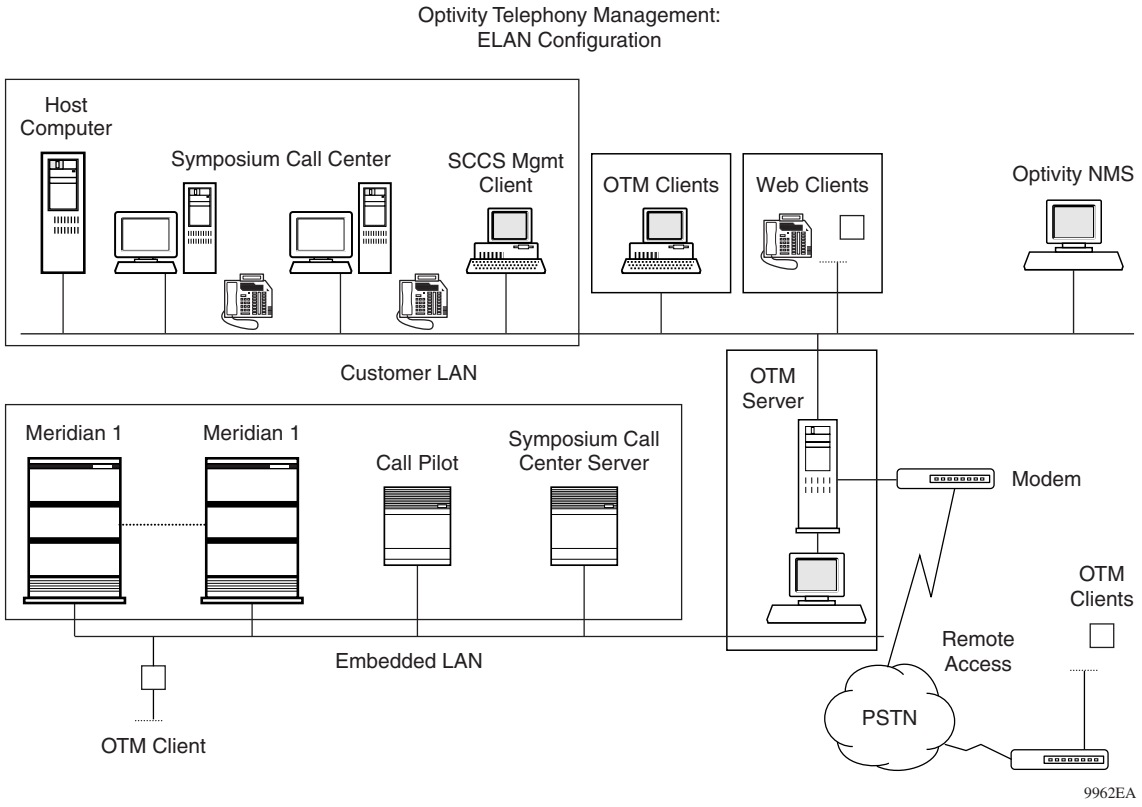


Figure A-2 represents how OTM would connect to Meridian Applications and to Meridian 1 and Succession CSE 1000 systems that are packaged with Ethernet. In this picture, OTM is connected to these systems via Ethernet using the Meridian 1 or Succession CSE 1000 system's ELAN (Embedded LAN). Meridian 1 and Succession CSE 1000 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.

Figure A-2 Connecting OTM to ELAN connected Meridian 1 and Succession CSE 1000 Systems

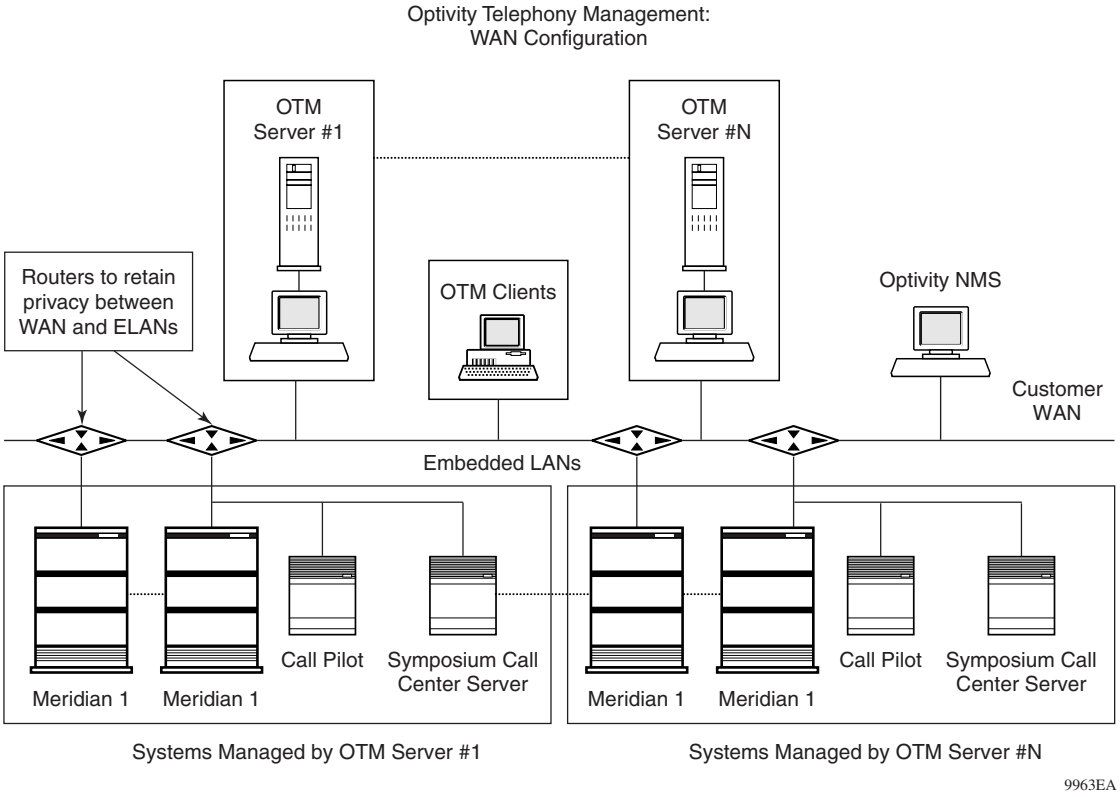


This configuration provides optimum performance, in that all communications between OTM and the Meridian 1 or Succession CSE 1000 systems are private. In this case, there is no impact to this communication due to Customer LAN traffic. It also meets the requirement of protecting the ELAN from the CLAN as required for Meridian 1and Succession CSE 1000 systems by having OTM act 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 A-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 Meridian 1 and Succession CSE 1000 systems, when these systems are geographically disperse, without requiring a separate network. It also permits OTM to be connected to a larger number of systems 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 A-3 Connecting OTM to CWAN connected Meridian systems



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's network may be impacted, but there is a savings on the number of OTMs 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 A-6 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 an Option 11C or Succession CSE 1000 system, divide the ELAN numbers by 2, except alarms. For the CPP CPU, multiply the ELAN numbers by 4, except for alarms.

Table A-6 Network Bandwidth Usage Per Meridian 1 System

OTM Activity	Transfer Rate (bits/second)	
	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