553-3001-230
October 2003

Optivity Telephony Manager Installation and Configuration

NORTEL NETWORKS™

Copyright © 2002, 2003 Nortel Networks

All rights reserved. October 2003.

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.

Novell and NetWare are trademarks of Novell, Inc.

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

October 2003

Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: Installing and Configuring Optivity Telephony Manager (553-3001-230).

Contents

Appendix A

Appendix B

About this document

Subject

Optivity Telephony Manager (OTM) is designed for managers of telecommunications equipment and authorized Nortel Networks* distributors. OTM provides a single point of access for management of Nortel Networks systems. OTM uses IP technology to target:

- Single point of connectivity to 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)
- Windows and Web-based management applications

Applicable systems

The document applies to all the following Succession 1000 systems.

Large system types

- Meridian 1 Option 61C CPII
- Meridian 1 Option 81C CPII
- Succession 1000M Single Group
- Succession 1000M Multi Group

Small system types

- Meridian 1 Option 11C Cabinet

- Meridian 1 Option 11C Chassis
- Succession 1000M Cabinet
- Succession 1000M Chassis.

In addition, for purposes of this document, the Call Processor in each Succession 1000 or Succession 1000M system is referred to generically as the " Call Server”.

System migration

When particular Meridian 1 systems are upgraded to run Succession 3.0 Software and configured to include a Succession Signaling Server, they become Succession 1000M systems. The table lists each Meridian 1 system that supports an upgrade path to a Succession 1000M system.

Table 1
Meridian 1 systems to Succession 1000M systems

This Meridian 1 system...	Maps to this Succession 1000M system
Meridian 1 Option 11C Chassis	Succession 1000M Chassis
Meridian 1 Option 11C Cabinet	Succession 1000M Cabinet
Meridian 1 Option 51C	Succession 1000M Half Group
Meridian 1 Option 61	Succession 1000M Single Group
Meridian 1 Option 61C	Succession 1000M Single Group
Meridian 1 Option 61C CP PII	Succession 1000M Single Group
Meridian 1 Option 81	Succession 1000M Multi Group
Meridian 1 Option 81C	Succession 1000M Multi Group
Meridian 1 Option 81C CP PII	Succession 1000M Multi Group

Note the following:

- When an Option 11C Mini system is upgraded to run Succession 3.0 Software, that system becomes a Meridian 1 Option 11C Chassis.
- When an Option 11C system is upgraded to run Succession 3.0 Software, that system becomes a Meridian 1 Option 11C Cabinet.

For more information, see one or more of the following NTPs:

- *Small System: Upgrade Procedures* (553-3011-258)
- *Large System: Upgrade Procedures* (553-3021-258)
- *Succession 1000 System: Upgrade Procedures* (553-3031-258)

Intended audience

This guide is intended for Succession 1000 and Meridian 1 system administrators using a Microsoft Windows*-based PC for management activities. It assumes that you have the following background:

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

Conventions

This document uses certain terminology, text conventions, and acronyms as explained here.

Terminology

In this document, the following systems are referred to generically as “system”:

- Meridian 1
- Succession 1000
- Succession 1000M

The following systems are referred to generically as “Small System”:

- Succession 1000M Chassis
- Succession 1000M Cabinet
- Meridian 1 Option 11C Chassis
- Meridian 1 Option 11C Cabinet

The following systems are referred to generically as “Large System”:

- Meridian 1 Option 51C
- Meridian 1 Option 61
- Meridian 1 Option 61C
- Meridian 1 Option 61C CP PII
- Meridian 1 Option 81
- Meridian 1 Option 81C
- Meridian 1 Option 81C CP PII
- Succession 1000M Half Group
- Succession 1000M Single Group
- Succession 1000M Multi Group

The call processor in Succession 1000 and Succession 1000M systems is referred to as the “Succession Call Server”.

Text conventions

The text conventions are:

angle brackets (< >)

Indicate that you must input some command text. 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, options, and text.

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
CLAN	customer local area network
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 information

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

- *Meridian 1 Integrated Telephony Gateway Trunk 1.0/Basic Per-Trunk Signaling: Description, Installation, and Operation* (553-3001-116)

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

- *Meridian 1 Integrated Telephony Gateway Line Card 1.0/IP Telecommuter: Description, Installation, and Operation* (553-3001-119)

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

- *Features and Services* (553-3001-306)

  Describes features associated with systems. For each feature, information is provided on feature implementation, feature operation, and interaction between features.

- *Software Input/Output: Administration* (553-3001-311)

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

- *Optivity Telephony Manager: System Administration* (553-3001-330)

  Provides information on using the applications and features available with Optivity Telephony Manager on systems.

- *Using Optivity Telephony Manager Release 2.1 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), Consolidated Reporting System (CRS), and Consolidated Call Cost Reports (CCCR).

- *IP Trunk: Description, Installation, and Operation* (553-3001-363)

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

- *IP Line: Description, Installation, and Operation* (553-3001-365)

  Describes configuration and maintenance of gateway cards.

- *Telephones and Consoles: Description* (553-3001-367)

  Describes telephones and related features. The telephones provide access to an OTM-generated Corporate Directory.

- *DECT: Description, Planning, Installation, and Operation* (553-3001-370)

  Provides an overview of OTM for MDECT systems.

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

  Describes the meaning of system messages.

- *Software Input/Output: Maintenance* (553-3001-511)

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

- *Large System: Installation and Configuration* (553-3021-210)

  Provides information on the Survivable IP Expansion (SIPE) feature for a Meridian 1 Large System.

- *Succession 1000 System: Installation and Configuration* (553-3031-210)

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

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

Online

To access Nortel Networks documentation online, click the **Technical Documentation** link under **Support** on the Nortel Networks home page:

http://www.nortelnetworks.com/

CD-ROM

To obtain Nortel Networks documentation on CD-ROM, contact your Nortel Networks customer representative.

Preparing for installation

This chapter contains information on the following topics:

- Installation tasks
- Supported systems
- Supported upgrade paths
- OTM hardware requirements
- OTM software requirements
- License management

Before installing OTM 2.1 software, please read all of this chapter.

About 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 later chapters for information on OTM/ Optivity NMS integration procedures and requirements.

For installation recommendations that will help to create a secure environment for your OTM data and users, see “Security Management” in the Common Services chapter of *Optivity Telephony Manager: System Administration* (553-3001-330).

To configure modems for use with OTM, refer to “Configuring a modem for OTM applications in Windows” on page 113.

When planning OTM installations, consider detailed hardware and software guidelines in Appendix A.

OTM installation tasks

Installing OTM involves performing tasks related to:

- New OTM server software
- New client software
- Upgrades
- Migrations
- Web Help
- License management

These tasks are covered in detail in the coming chapters.

Supported systems

OTM 2.1 supports the following systems:

- Succession 3.0 software
- Succession 1000M
- Succession 1000M Cabinet running X27 Releases 1 - 2
- Succession 1000M Chassis running X11 Releases 24.24 - 25.40
- Succession 1000M Single Group running X11 Releases 19 - 25.40
- Succession 1000M Multi Group running X11 Releases 19 - 25.40
- Meridian ITG Trunk 1.0 (IP Telephony/ M1 IP Trunks)
- Meridian ITG Line 1.0 (IP M1 Telecommuter)
- Meridian ITG Trunk 2.x (IP ISDN IP Trunks)
- Meridian ITG Line 2.x (IP Phones)
- MDECT (DMC8 card, and DMC4 with updated loadware)
- IP Trunk 3.0 on Meridian 1
- IP Line 3.0 on Meridian 1

Supported upgrade paths

OTM 2.1 supports a direct upgrade from OTM 1.20.26, the OTM 2.00 GA load and the OTM 2.01 GA load directly to OTM 2.1.

Direct upgrades are NOT supported for customers migrating from OTM releases prior to 1.20.26, or from MAT 6.67. A two-step upgrade is required, first to OTM 2.0 and then to 2.1.

Customers on MAT releases prior to 6.67 need to purchase and install OTM as a new installation.

OTM hardware requirements

Refer to Appendix A for more information on OTM Server hardware requirements.

Use correct information

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

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

Response-time testing is based upon the recommended configuration, not the minimum configuration. Response-time performance is only supported on the recommended configuration.

For the Windows Client, some of the variables include:

- The amount of RAM on the OTM Client PC
- The OS platform in use on the OTM Client PC
- The number of TNs being managed through the Station Administration application
- Other applications that may be running on the OTM Client PC, including those that run in the background such as antivirus software

- The amount of traffic on the LAN
- The NIC on the OTM Client PC
- Deployment in the network architecture (topology and placement of the OTM Client PC with respect to the OTM Server)

The minimum and recommended CPU and RAM configurations are specified. Some OTM applications can run with less than the recommended, but performance may be degraded.

The OTM Server requires the following minimum hardware specifications (Table 2).

Table 2: OTM hardware requirements (Part 1 of 2)

Requirement	Server configuration	Single (stand alone) configuration	Client configuration
Recommended CPU	Intel Pentium III Processor 600 MHz	Intel Pentium III Processor 400 MHz (600 MHz for XP)	Intel Pentium III Processor 400 MHz (600 MHz for XP)
Minimum CPU	Intel Pentium III Processor 400 MHz	Intel Pentium II Processor 233 MHz (PIII 400 MHz for XP)	Intel Pentium II Processor 233 MHz (PIII 400 MHz for XP)
Recommended RAM	512 MB	256 MB, 512 MB for Windows XP	256 MB, 512 MB for Windows XP
Minimum RAM	256 MB	128 MB 256 MB for billing applications, or for Windows XP	128 MB, 256 MB for Windows XP
Hard Drive Space	2 GB (1 GB plus customer data storage)	2 GB (1 GB plus customer data storage)	500 MB
SVGA Color Monitor and interface card	800 X 600 or higher Resolution	800 X 600 or higher Resolution	800 X 600 or higher Resolution
3 1/2-inch 1.44 MB floppy disk drive	Required	Required	Required

Table 2: OTM hardware requirements (Part 2 of 2)

CD-ROM drive	Required	Required	Required
Ethernet Network Interface Card	1 or 2	1	1
Hayes compatible modem is optional for connection to remote sites, required for polling configurations. Please note: WinModems *are incompatible and are not supported.*	56K BPS recommended	56K BPS recommended	56K BPS recommended
PC COM port with 16550 UART [1]	Required	Required	Required
Dongle or USB dongle	Required Supports one USB dongle only USB dongles are not supported through a USB hub USB dongles are not supported on Windows NT server	Required Supports one USB dongle only USB dongles are not supported through a USB hub	Not required
Parallel printer port (configured) or USB port (required for dongle)	Required	Required	Required
Two-button Windows compatible mouse or positioning	Required	Required	Required

For external modems or direct connection the PC must have an available serial port (i.e., one not being used by a mouse or other serial device). The number of on-board PC COM ports required depends on the number of external modem or direct connections required.

OTM Software requirements

Novell

The OTM Server is not supported on a Novell server. TCP/IP communication is supported. IPX/SPX communication is not supported.

Important restrictions on Windows XP Professional

Restrictions on Windows XP Professional when operating OTM are:

- Multi-session is not supported. Two users cannot be concurrently logged into the same PC at the same time and have OTM running.
- A Windows XP Professional default is that “EveryOne” has no rights on the drive level. To ensure that “Everyone” has full-control access rights to the NTFS drive, override the default access rights to the drive in which OTM is installed. This is a requirement for OTM web applications.
- An install time check is made to ensure the NTFS drive has the required access rights set. If not set, the user is asked to have OTM to change the required access rights. This check will proceed immediately after the check for IIS installation.

Operating System and application requirements for OTM PC Configurations

These tables list the required and supported software that run on OTM PC configuration types.

Table 1 OTM configuration OS requirements

	OTM PC Configuration		
OS Software	**Server**	**Single (stand alone)**	**Windows Client**
Windows XP Professional	Not applicable	Service Pack 1 required	Not applicable
Windows 2000 Professional	Not applicable	Service Pack 3 required	Not applicable
Windows 2000 Server	Service Pack 3 required	Not applicable	Supports Windows XP Professional or Windows 2000 Professional
Windows NT 4.0 Server	Service Pack 6a and Option Pack 4.0 required	Not applicable	Supports Windows XP or Windows 2000 Professional
Windows NT 4.0 Workstation	Not supported	Not supported	Not supported
Windows 95/98/ME	Not supported	Not supported	Not supported

Table 2 Application software requirements (Part 1 of 2)

	OTM PC configuration		
Application software	**Server**	**Single (stand alone)**	**Windows Client**
Internet Explorer 6.0 SP 1 (Windows only) Netscape Communicator 4.79 (UNIX only)	Required	Required	Required
Netscape 6.x or later, Netscape Navigator 4.08	Not supported	Not supported	Not supported
TCP/IP Protocol	Required	Required	Required
RAS (Remote Access Service)	Required	Required	Required
Javga 1.4.2 runtime environment	Required	Required	Required
NT Server 4.0, Service Pack 6a, and Option Pack 4 (for Windows NT)	Required: components: Internet Information Server (IIS) 4.0 or above Microsoft Transaction Server Microsoft Data Access Components (MDAC) Microsoft Management Console (NMC) NT Option Pack Common Files	Not applicable	Not applicable
Microsoft Active Server Page (ASP)	Required	Required	Required

Table 2 Application software requirements (Part 2 of 2)

Succession 1000 Element Manager	Supported	Supported	Supported
Novell NetWare Client 4.8	Supports Windows XP Professional or Windows 2000 Professional	Supports Windows XP Professional or Windows 2000 Professional	Supports Windows XP Professional or Windows 2000 Professional
IIS	IIS 4.0 required for Windows NT 4.0 Server	IIS 5.0 required for Windows 2000l IIS 5.1 required for Windows XP Professional	

System software release and package requirements

Table 3 lists OTM software releases and required packages for OTM applications.

Table 3 Meridian 1 X11 system software release and packages (Part 1 of 2)

OTM application	Minimum X11 release required	X11 pkgs required
Alarm Management	X11 R22 or later	Pkg 164, 242, 243, and 296
Additional packages 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 3 Meridian 1 X11 system software release and packages (Part 2 of 2)

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

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

Installing OTM server software

This chapter contains information on:

- Installation program features and restrictions
- What to do if there is a problem
- Installing new OTM servers

An installation checklist is provided in Appendix B.

See the chapter titled Windows NT and Windows 2000 Reference for detailed information on installing and configuring Windows NT for use with OTM.

You must install OTM Web Help separately. A separate chapter covers the installation procedure for OTM Web Help.

Installation program features

The OTM software installation program uses a standard Windows “Wizard” method of user interaction.

Installation messages and log

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.

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” (for example, “Service Pack 6a is not installed”).

Users and groups

During the installation process, OTM adds the Default, EndUser and HelpDesk user groups to the server. User groups cannot have the same name as a local user on the OTM Server. If the installation program detects a local user with the same name as one of the user groups that it is attempting to add, you are given the option of renaming or deleting the local user or canceling the creation of the user group.

Restriction

DO NOT install OTM on a Microsoft Windows NT or Windows 2000 system that is configured as a primary domain controller (PDC).

DO NOT install OTM in the default directory when also installing CallPilot. You must install OTM in a directory other than the default folder (C:\Nortel). During OTM Uninstall, OTM prompts you to delete the whole C:\Nortel directory, including CallPilot.

If there is a problem

If a major problem occurs in the middle of an OTM installation, an unstable system could prevent successful completion. If a problem does occur:

1. Delete OTM Navigator and Pervasive shortcuts from the StartUp folder.
2. Reboot.
3. Delete the OTM directory, e.g. C:\Nortel\OTM.
4. Run regedit and delete the "HKEY_LOCAL_MACHINE\SOFTWARE\Normat" key.
5. Reboot.
6. Re-install OTM.Execute the setup file. To do this, double-click the *Setup.exe* file on the OTM CD-ROM.

Procedure for new OTM server installations

Use this procedure for new OTM installations.

1 Configure Windows for OTM installation by completing the following steps:

- **a** Log on to Windows as an Administrator.
- **b** For network installations, close all OTM Client sessions. This includes both Windows and Web clients.
- **c** Exit all Windows programs and disable any virus detection software.
- **d** Install the latest Windows critical security updates from Microsoft at http://www.microsoft.com/technet/. The OTM installation wizard does not install the index server, but other applications can install an index server.
- **e** Install security patches (such as Code Red Worm IIS patches) as advised through Product Bulletins available on the Partner Information Center Web site.
- **f** Ensure that a drive labeled “C” exists on the server. Although the OTM software can be installed on any drive, there are some dependencies on the C drive. In particular, the directory C:\dbcnv is created during installation and removed at the end of the installation process.
- **g** Install RAS. RAS (Remote Access Service) is required for certain modules of OTM that support dial-up connectivity such as PPP connectivity to a switch and ITG applications. During installation OTM checks for RAS. The RAS installation procedure is provided in the Windows reference chapter.
- **h** If present, remove the *MAT.exe* shortcut file in the *Start up* folder.
- **i** Ensure Distributed COM is enabled. For DCOM to work, the OTM client must be able to reach the OTM server by its actual IP address. If Network Address Translation (NAT) is used on the server, the OTM client will not be able to reach the server.

For Windows 2000

1) Using the Component Services administrative tool, locate My Computer under the Computers folder of the Console tree and right-click on My Computer.

2) Select “Default Properties” tab, ensure “Enable Distributed COM on this computer” check box is selected.

3) Restart Windows Operating System.

For Windows NT

1) From the Start menu, run the command “dcomcnfg”.

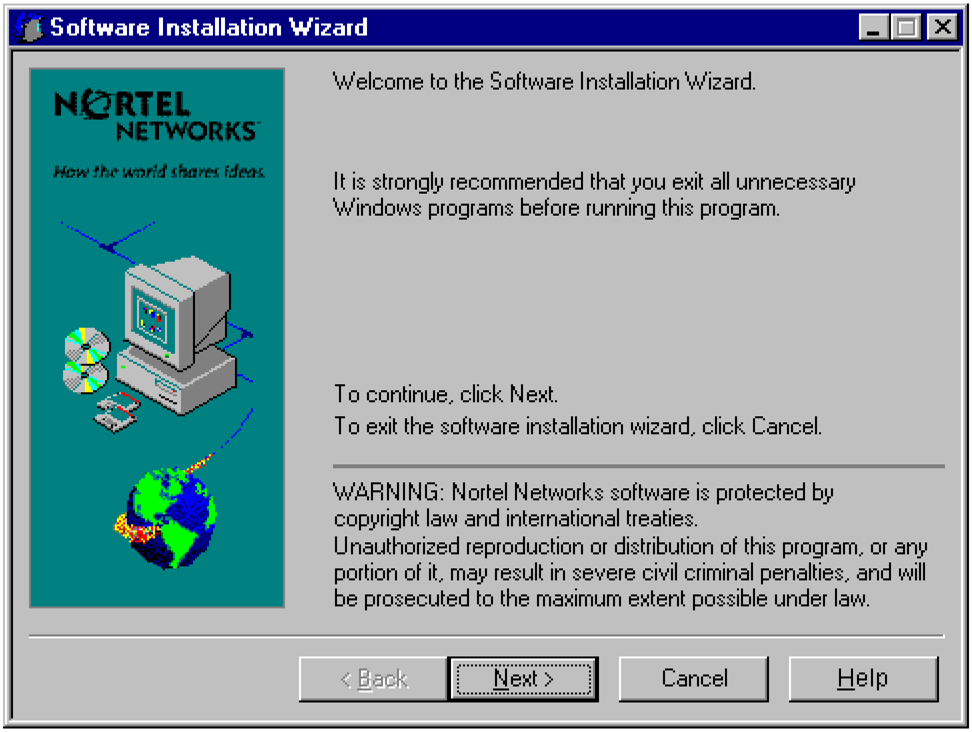
2) Select the “Default Properties” tab. Ensure “Enabled Distributed COM on this computer” check box is selected.

j On OTM Server, share the Nortel directory with the specific users or user groups using the OTM Client.

➡ **Warning:** Assign share permissions for the Nortel directory according to your corporate security standards.

k On the Client PC, map to the Nortel directory located on the OTM Server. The welcome screen appears (Figure 1).

Figure 1 Software Installation Wizard



Welcome to the Software Installation Wizard.

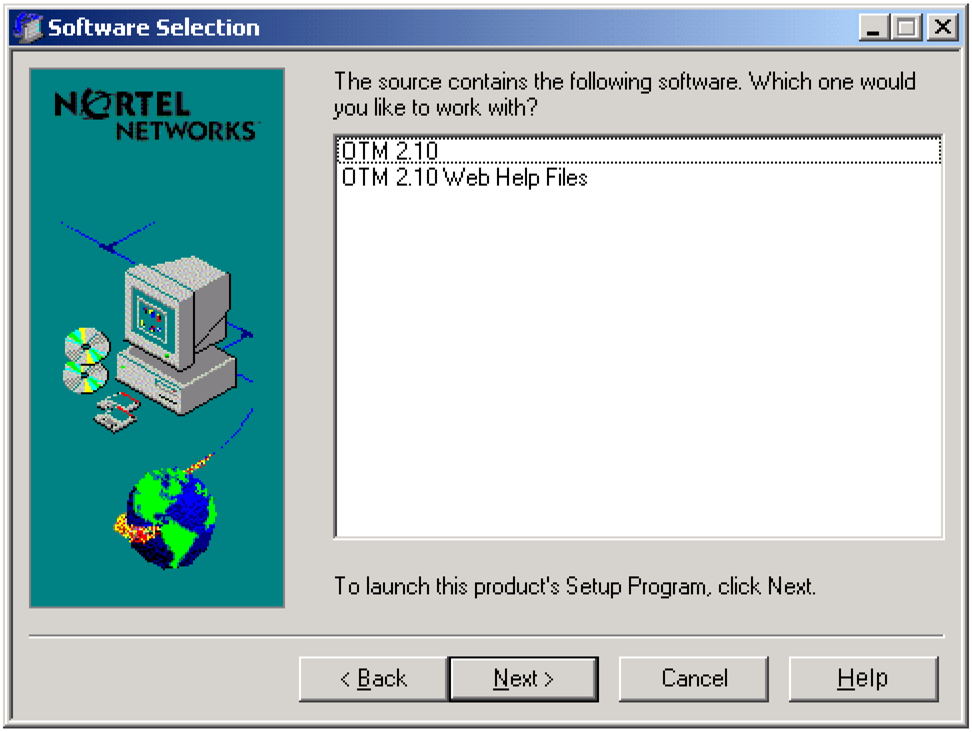
It is strongly recommended that you exit all unnecessary Windows programs before running this program.

To continue, click Next.
To exit the software installation wizard, click Cancel.

WARNING: Nortel Networks software is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil criminal penalties, and will be prosecuted to the maximum extent possible under law.

Click Next to continue. The Software Selection dialog box appears (Figure 2).

Figure 2 Software Selection dialog box



The source contains the following software. Which one would you like to work with?

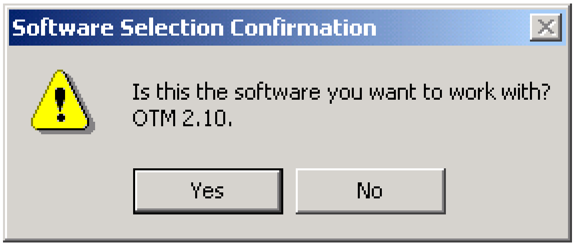
OTM 2.10
OTM 2.10 Web Help Files

To launch this product's Setup Program, click Next.

The Software Selection Confirmation dialog box (Figure 3) opens to request confirmation that OTM 2.10 is the software that you want to work with.

2 Click to select OTM 2.10. The other option is OTM Web Help files. You can install OTM Web Help once the OTM Application installation is complete. Click Next to continue.

Figure 3 Software Selection Confirmation dialog box

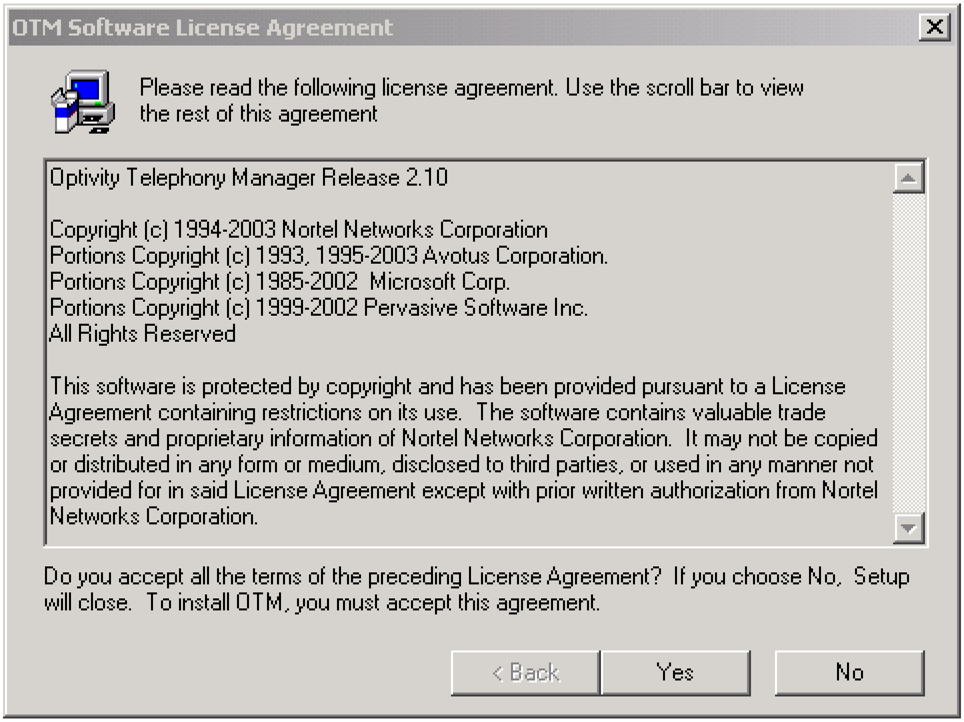


Is this the software you want to work with?
OTM 2.10.

Click Yes to continue.

3 The software license agreement opens (Figure 4). Read it. Click Yes to accept the agreement.

Figure 4 Software License Agreement



OTM Software License Agreement

Please read the following license agreement. Use the scroll bar to view the rest of this agreement

Optivity Telephony Manager Release 2.10

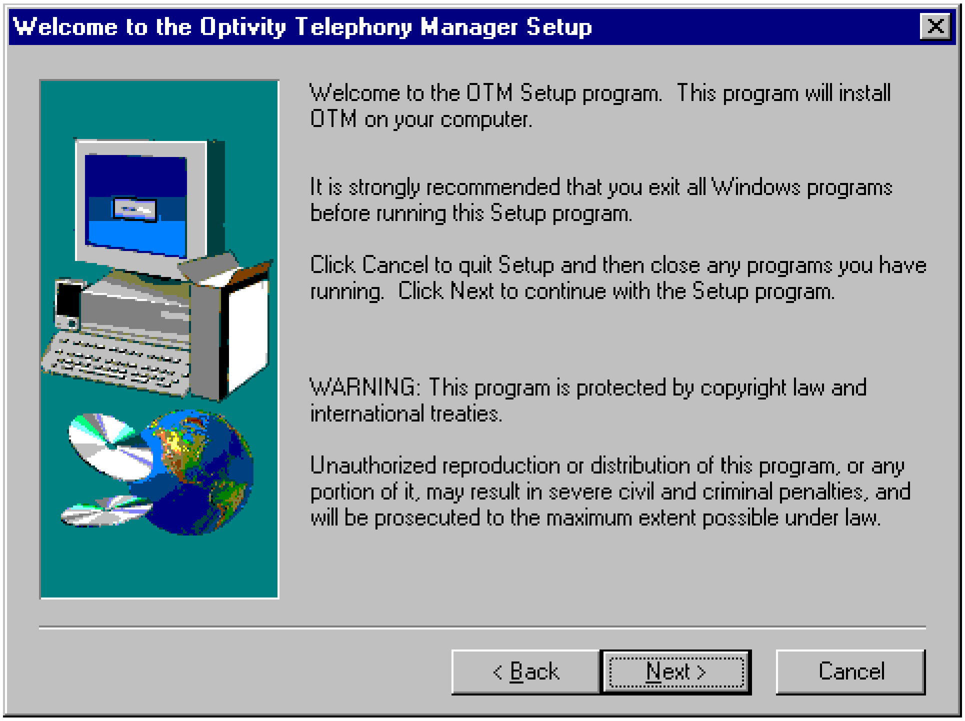
Copyright (c) 1994-2003 Nortel Networks Corporation
Portions Copyright (c) 1993, 1995-2003 Avotus Corporation.
Portions Copyright (c) 1985-2002 Microsoft Corp.
Portions Copyright (c) 1999-2002 Pervasive Software Inc.
All Rights Reserved

This software is protected by copyright and has been provided pursuant to a License Agreement containing restrictions on its use. The software contains valuable trade secrets and proprietary information of Nortel Networks Corporation. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not provided for in said License Agreement except with prior written authorization from Nortel Networks Corporation.

Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install OTM, you must accept this agreement.

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

Figure 5 Welcome



Welcome to the Optivity Telephony Manager Setup

Welcome to the OTM Setup program. This program will install OTM on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

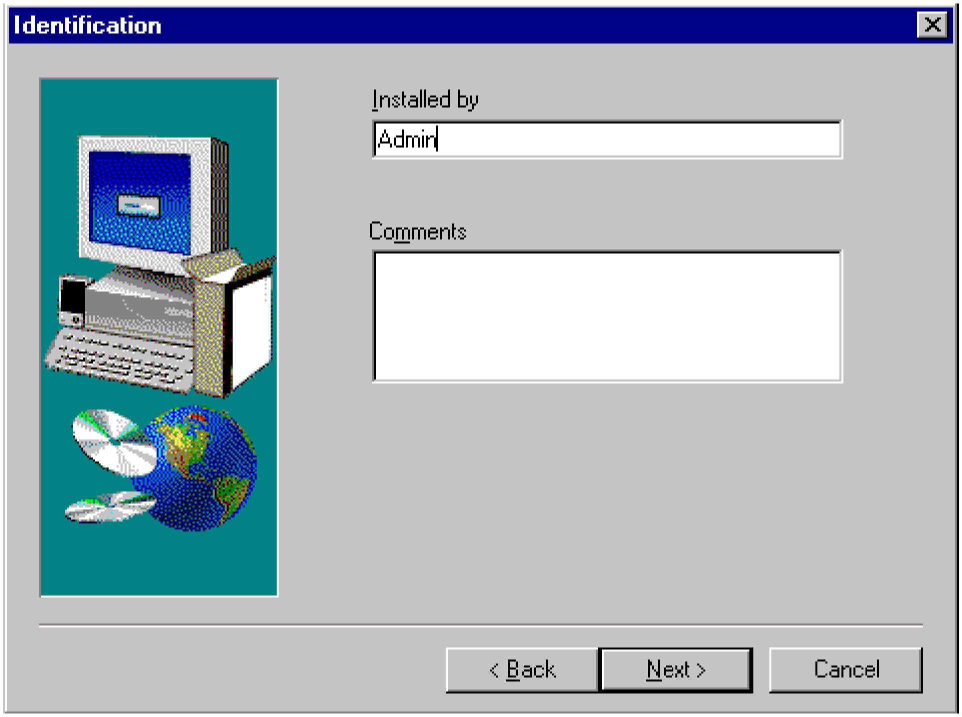
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

5 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



Identification

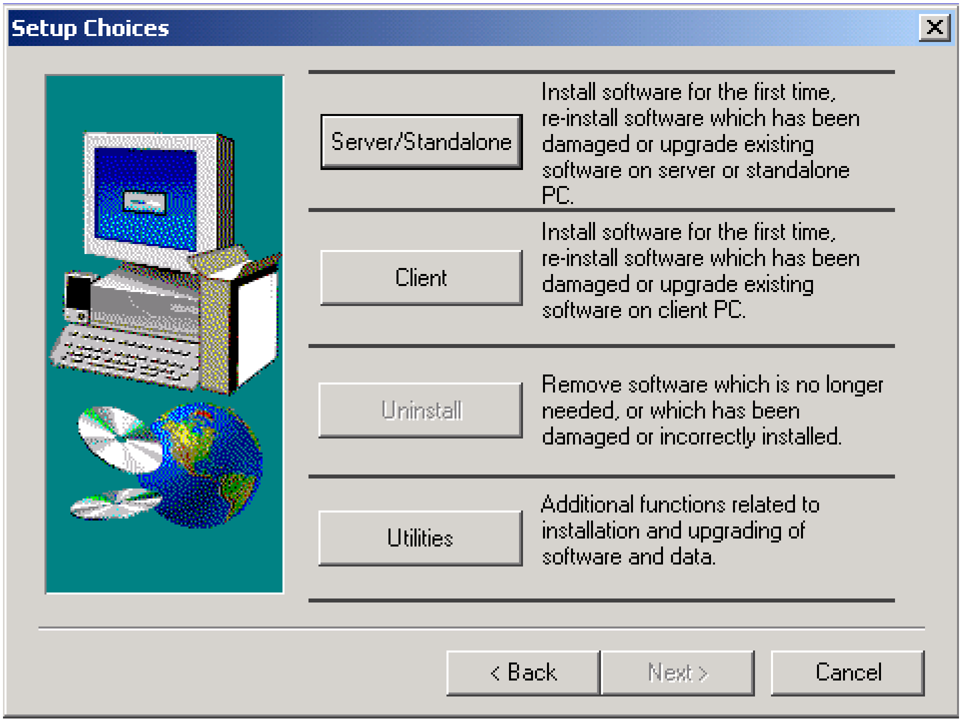
Installed by

Admin

Comments

6 Make setup choices. For installation on an OTM Server, select Server/ Standalone (Figure 7). For installation on a Client PC, select Client and see the chapter on OTM Client software installation.

Figure 7 Setup Choices



Install software for the first time, re-install software which has been damaged or upgrade existing software on server or standalone PC.

Install software for the first time, re-install software which has been damaged or upgrade existing software on client PC.

Remove software which is no longer needed, or which has been damaged or incorrectly installed.

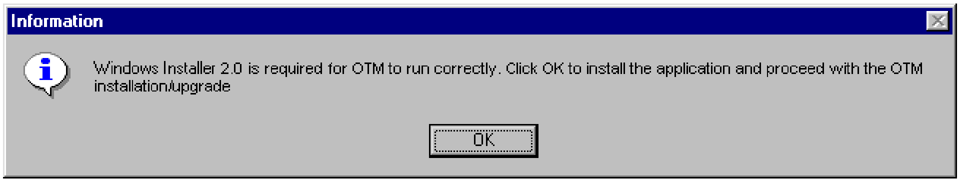
Additional functions related to installation and upgrading of software and data.

Note: Selecting Server/Standalone will not resolve problems with damaged software. To resolve a damaged software problem, back up your data files and perform an Uninstall. Next, perform an installation, and then restore your data. See See Table 5 on page 77.

Select Client to install an OTM client. The client has applications and executables, but uses the common data from the OTM Server. You must have the OTM Server software installed prior to installing the client software.

7 OTM requires Windows Installer 2.0. If the installation wizard detects that Windows Installer 2.0 is not installed, the information box shown in Figure 8 appears. Click OK. OTM installation continues after Windows Installer 2.0 installation has been completed, and the system has been rebooted.

Figure 8 Windows Installer 2.0 information box



Information

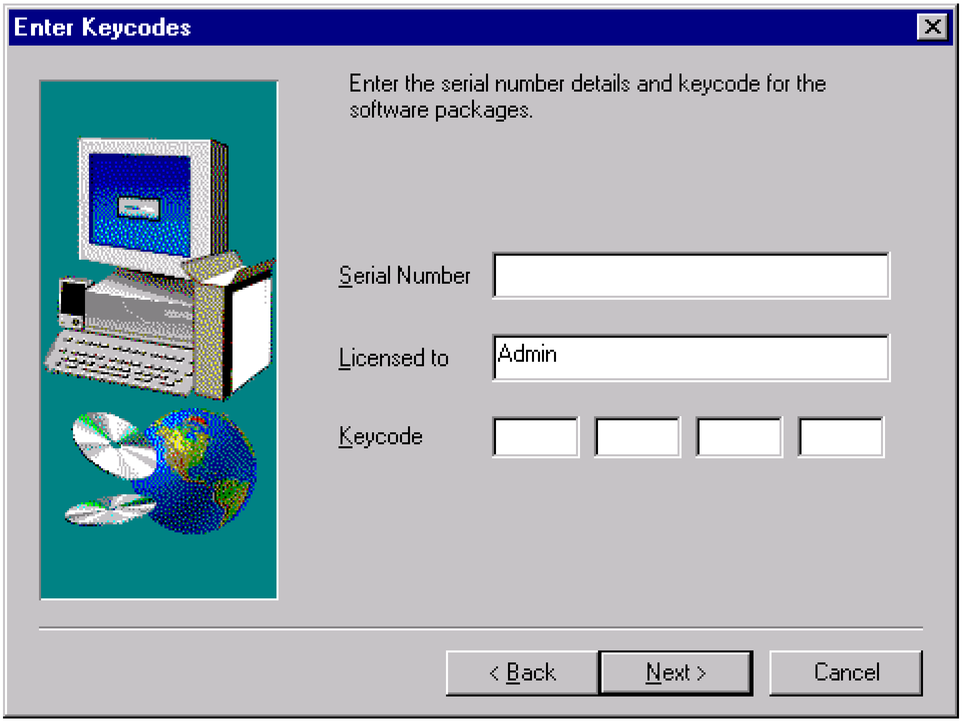
Windows Installer 2.0 is required for OTM to run correctly. Click OK to install the application and proceed with the OTM installation/upgrade

8 Enter the serial number and key code that you received with your OTM software package in the Enter Keycodes dialog box (Figure 9). T.

Previous OTM keycodes will not work. You must use the OTM keycode.

The serial number and key code determine which applications are installed during the software installation process. The serial number and key code 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, contact your OTM vendor. Click Next to continue.

Figure 9 Enter keycode



Enter Keycodes

Enter the serial number details and keycode for the software packages.

Serial Number

Licensed to: Admin

Keycode

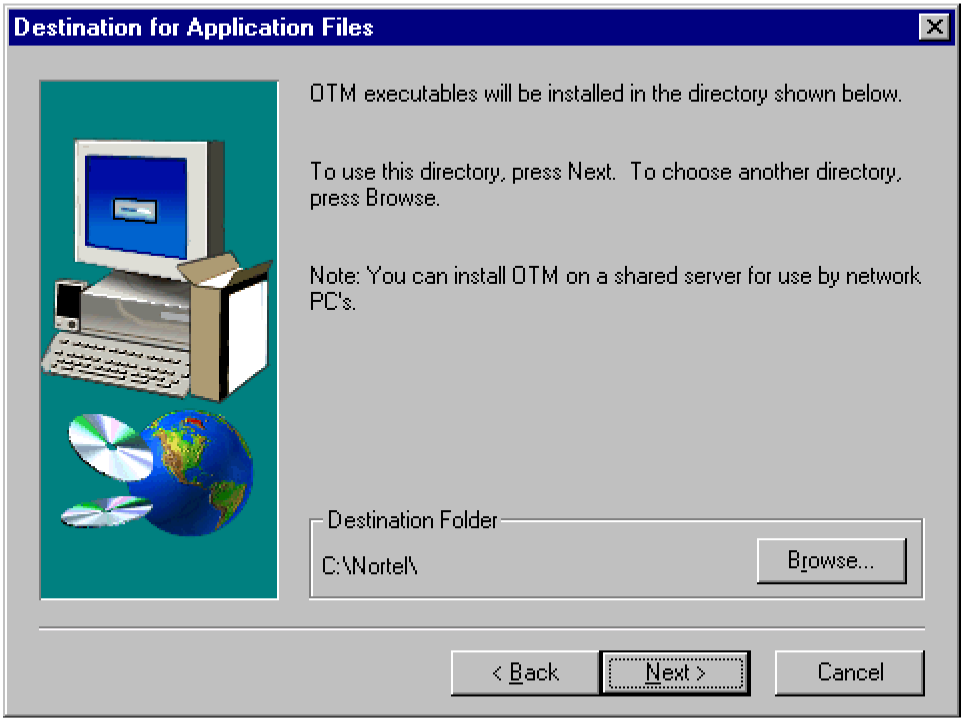
9 Specify a destination for application files. Specify the root directory for installing OTM Application files. Use the default directory or browse to specify a different location, as shown in Figure 10.

Caution: You must not install OTM in the root directory (for example, C:\). During the installation process, you must specify a folder (for example, C:\Nortel). If you install in the root directory, OTM uninstall attempts to delete everything on the drive.

Note: DO NOT install OTM in the default directory when also installing CallPilot. You must install OTM in a directory other than the default folder (C:\Nortel). During OTM Uninstall, OTM prompts you to delete the whole C:\Nortel directory, including CallPilot.

10 Click Next to continue.

Figure 10 Destination for Application Files



Destination for Application Files

OTM executables will be installed in the directory shown below.

To use this directory, press Next. To choose another directory, press Browse.

Note: You can install OTM on a shared server for use by network PC's.

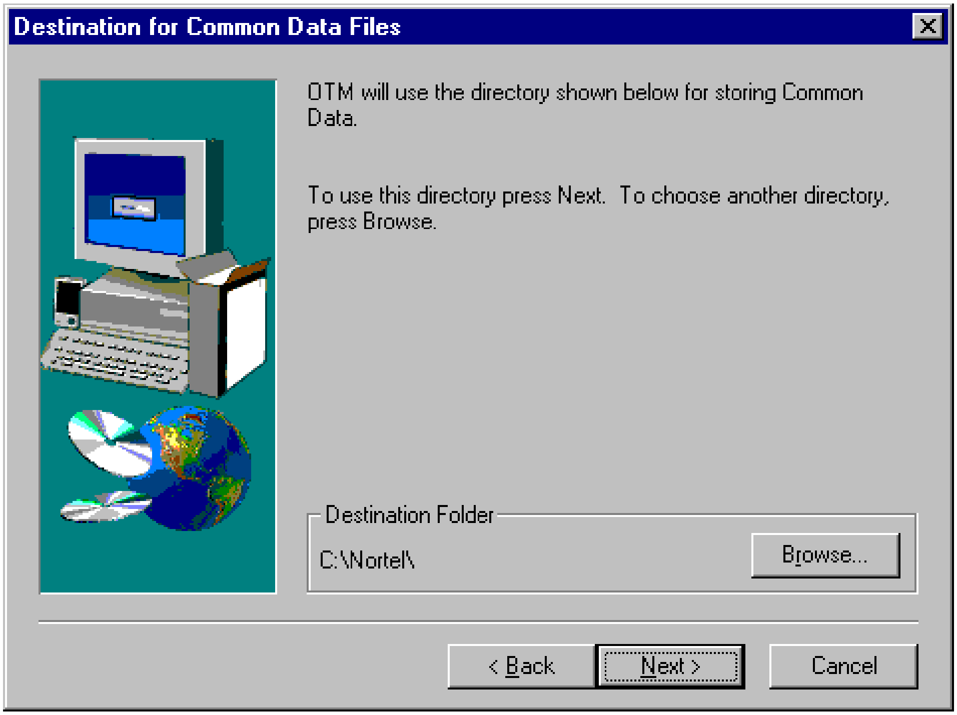
Destination Folder

C:\Nortel\

11 Specify a destination for common data files. Specify the root directory for installing OTM Common Data files (Figure 11). Use the default directory or browse to specify a different location. The directory defaults to the path defined in step . 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 checks your system and prevents you from specifying a networked drive.

Figure 11 Destination for Common Data Files dialog box



Destination for Common Data Files

OTM will use the directory shown below for storing Common Data.

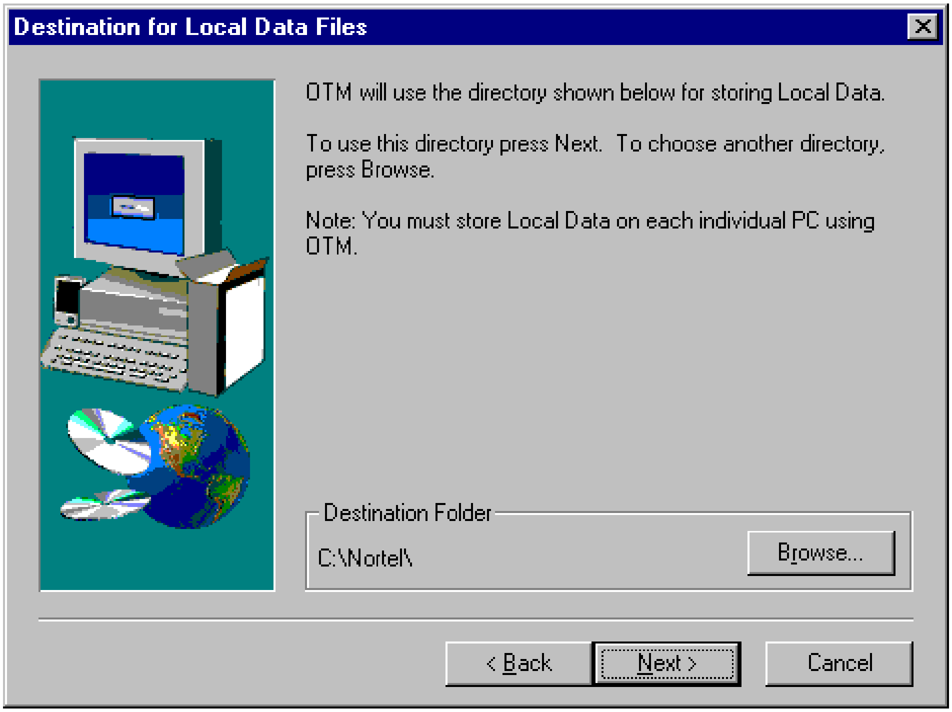
To use this directory press Next. To choose another directory, press Browse.

Destination Folder

C:\Nortel\

12 Specify a destination for local data files. Specify the root directory for installing OTM Local Data files (Figure 12). Use the default directory or browse to specify a different location. The directory defaults to the path defined in step. Click Next to continue.

Figure 12 Destination for Local Data Files dialog box



Destination for Local Data Files

OTM will use the directory shown below for storing Local Data.

To use this directory press Next. To choose another directory, press Browse.

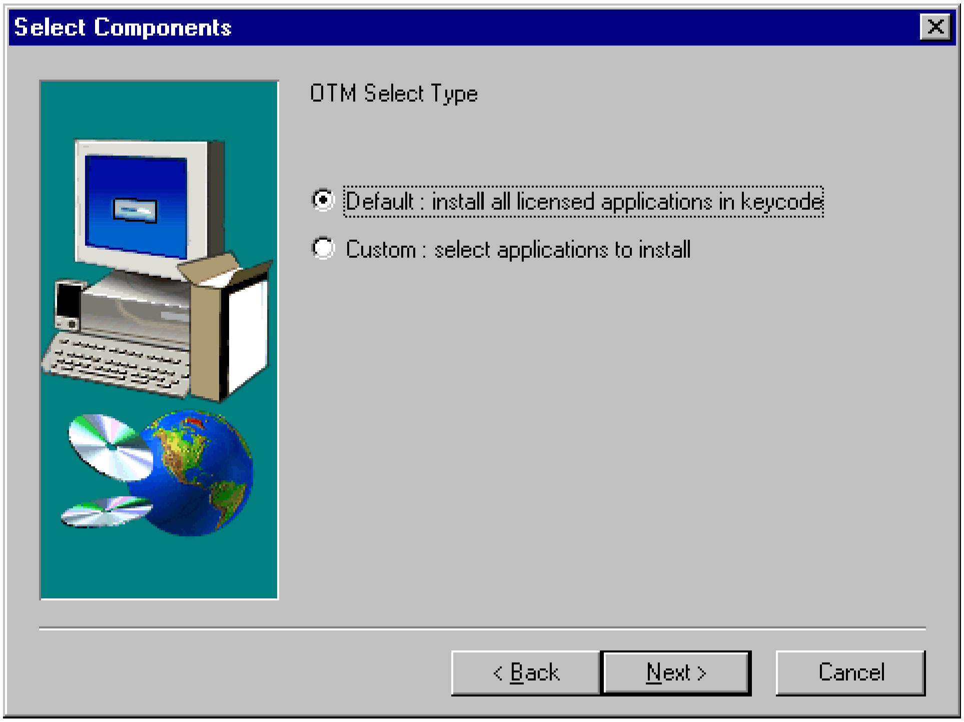
Note: You must store Local Data on each individual PC using OTM.

Destination Folder

C:\Nortel\

13 Specify installation options. 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 13).

Figure 13 Select Components



Select Components

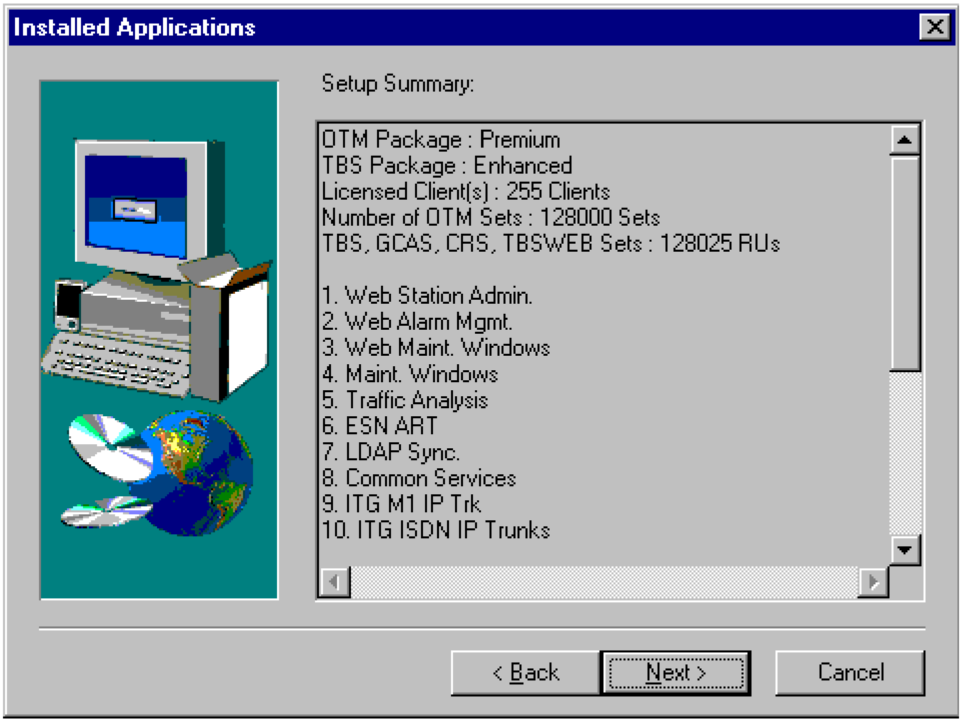
OTM Select Type

● Default : install all licensed applications in keycode

○ Custom : select applications to install

If you select Default, a summary of the default applications for the level of OTM that you have purchased appears (Figure 14).

Figure 14 Summary of default applications

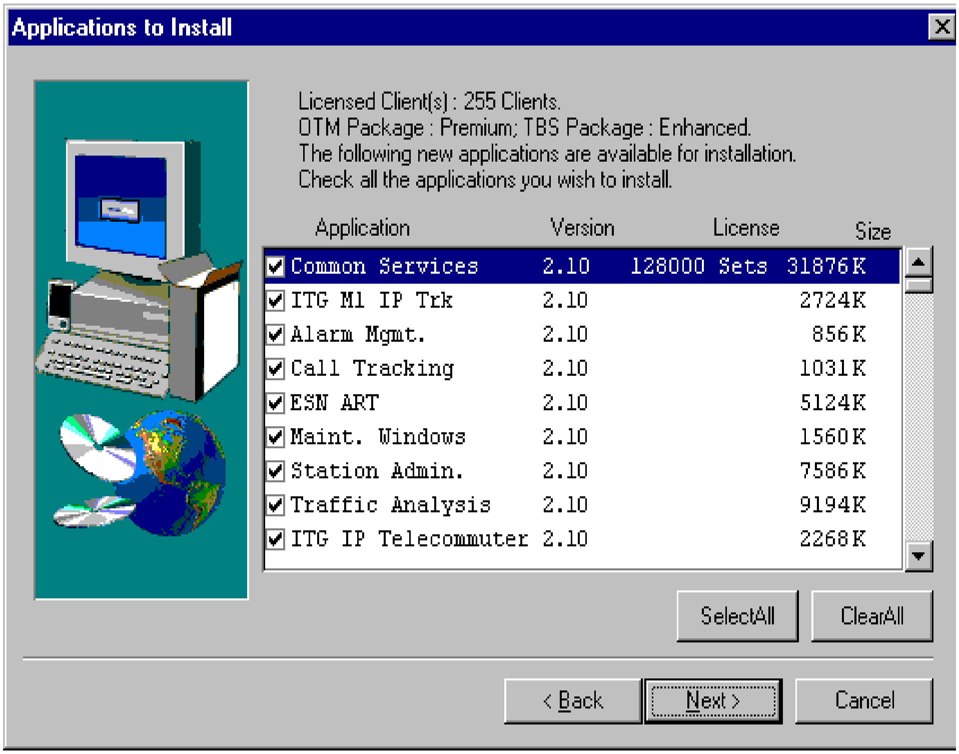


OTM Package : Premium
TBS Package : Enhanced
Licensed Client(s) : 255 Clients
Number of OTM Sets : 128000 Sets
TBS, GCAS, CRS, TBSWEB Sets : 128025 RUs

1. Web Station Admin.
2. Web Alarm Mgmt.
3. Web Maint. Windows
4. Maint. Windows
5. Traffic Analysis
6. ESN ART
7. LDAP Sync.
8. Common Services
9. ITG M1 IP Trk
10. ITG ISDN IP Trunks

14 Install applications. If you select Custom, you are given a list of applications to install (Figure 15). Check the appropriate applications.

Figure 15 Applications to Install



Applications to Install

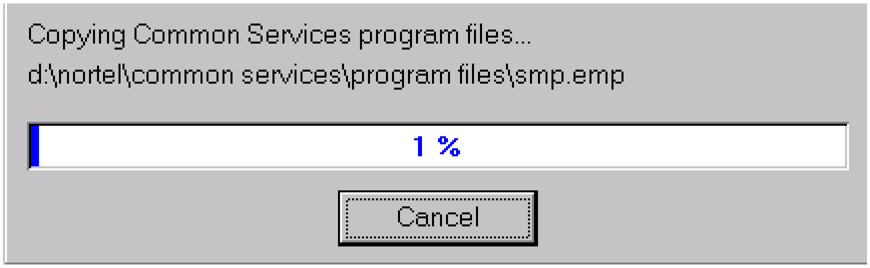
Licensed Client(s) : 255 Clients.
OTM Package : Premium; TBS Package : Enhanced.
The following new applications are available for installation.
Check all the applications you wish to install.

Application	Version	License	Size
☑ Common Services	2.10	128000 Sets	31876K
☑ ITG M1 IP Trk	2.10		2724K
☑ Alarm Mgmt.	2.10		856K
☑ Call Tracking	2.10		1031K
☑ ESN ART	2.10		5124K
☑ Maint. Windows	2.10		1560K
☑ Station Admin.	2.10		7586K
☑ Traffic Analysis	2.10		9194K
☑ ITG IP Telecommuter	2.10		2268K

Click Next to continue.

The Copy files dialog box displays the percentage status of OTM installation, which application files are being copied, and their locations (Figure 16).

Figure 16 Copy files



Copying Common Services program files...
d:\nortel\common services\program files\smp.emp

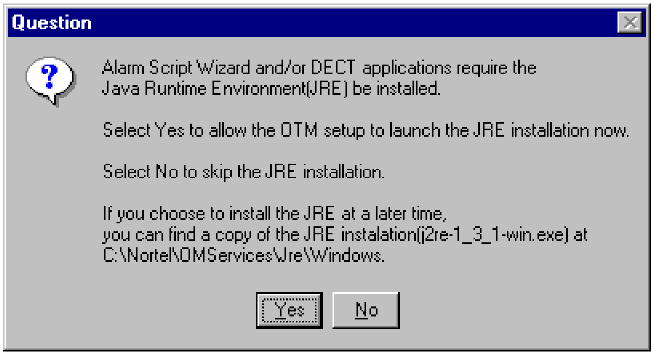
1 %

A Read Me dialog box prompts you to read the readme.txt file.

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

15 If you have installed applications that require Java* Runtime Environment (JRE), you are prompted to install JRE at this point (Figure 17). Click Yes if you want to install JRE now. It is required for the Alarm Script Wizard and the DECT application.

Figure 17 JRE Installation



Question

Alarm Script Wizard and/or DECT applications require the
Java Runtime Environment(JRE) be installed.

Select Yes to allow the OTM setup to launch the JRE installation now.

Select No to skip the JRE installation.

If you choose to install the JRE at a later time,
you can find a copy of the JRE instalation(j2re-1_3_1-win.exe) at
C:\Nortel\OMServices\Jre\Windows.

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

- For Windows: *C:\Nortel\OMServices\Jre\Windows\j2re-1_4_2-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, refer to http://java.sun.com/.

  JRE is required for the Alarm Script Wizard and the DECT application.

16 Restart the computer. A dialog box asks you to restart the computer or end the installation without restarting the computer. Select Yes, I want to restart my computer now, and then click OK.

17 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.

Installing OTM client software

This chapter contains information on installing OTM Client software.

OTM Client software installation is similar to the OTM Server installation. The steps are summarized below. See the previous chapter to view the installation screens that are common to both procedures.

Installing the software

1 Before installation:

a Exit all Windows programs and disable any virus detection software.

b Remove the MAT.exe shortcut file in the Start up folder, if present.

⚠ **Warning:** Assign share permissions for the Nortel directory according to your corporate security standards.

c Ensure Distributed COM is enabled. For DCOM to work, the OTM client must be able to reach the OTM server by its actual IP address. If Network Address Translation (NAT) is used on the server, the OTM client will not be able to reach the server.

For Windows 2000

1) From the Component Services administrative tool, locate and right-click on My Computer under the Computers folder of the Console tree.

2) Click on the Default Properties tab, ensure the “Enable Distributed COM on this computer” check box is selected.

For Windows NT

1) From the Start menu, run the command “dcomcnfg”.

2) Select the “Default Properties” tab. Ensure “Enabled Distributed COM on this computer” check box is selected.

d On the OTM Server, share the Nortel directory with the specific users or user groups that will be using the OTM Client.

e On the Client PC, map the Nortel directory located on the OTM Server.

2 Start the installation. To do this, double-click the *Setup.exe* file on the OTM CD-ROM.

3 Navigate through the OTM installation wizard. The following screens appear (for examples, see See Chapter , “Installing OTM server software,” on page 37).

a Welcome to the Software Installation Wizard

b Software selection

c OTM Software Licences Agreement

d Welcome to the Optivity Telephony Manager Setup

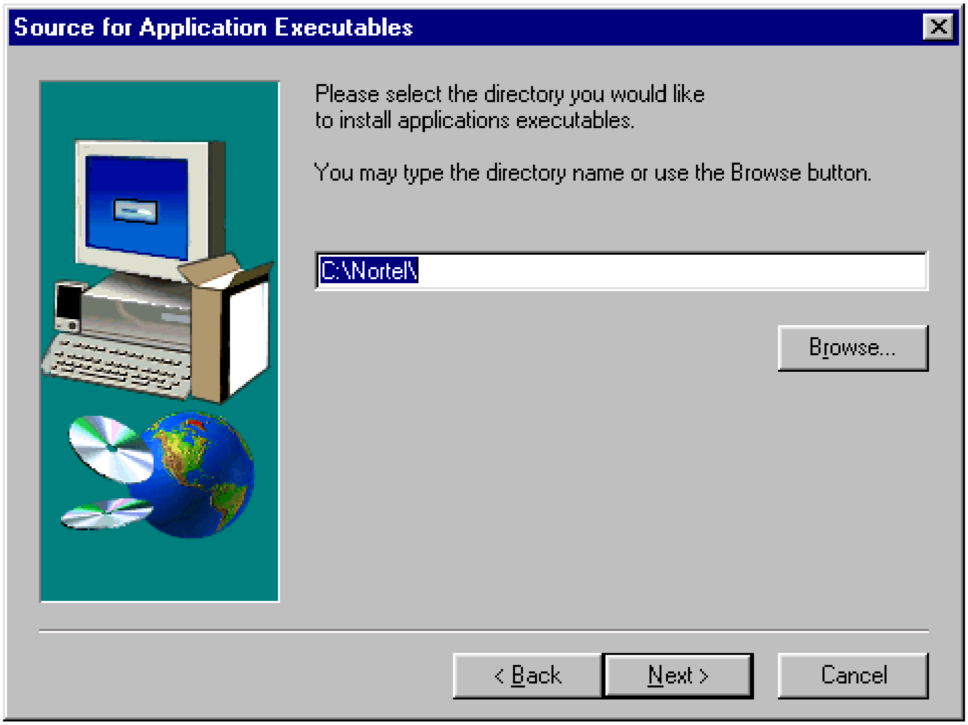
e Identification

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

4 In the Setup Choices dialog box, select Client.

5 Select the directory for the installation of the application executable as shown in Figure 18. You may browse and select a local directory on the Client PC, or you may browse and select the mapped OTM Server directory. Click Next to continue.

Figure 18 Source for Application Executables dialog box



Source for Application Executables

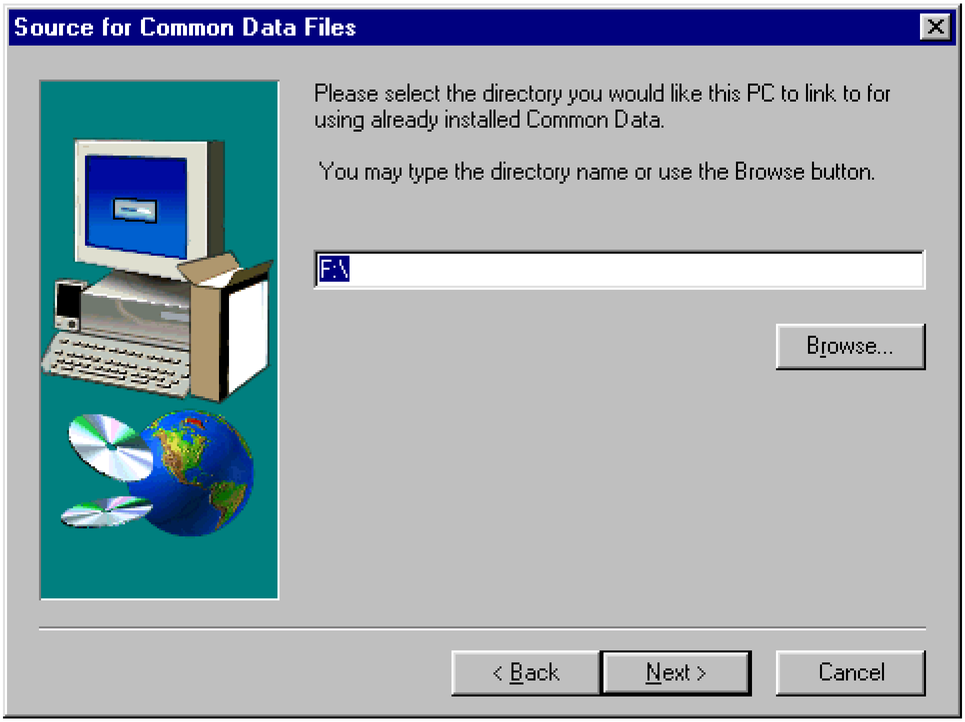
Please select the directory you would like to install applications executables.

You may type the directory name or use the Browse button.

C:\Nortel\

6 Select the directory on the OTM Server where the Common Data files are stored as shown in Figure 19. Click Next to continue.

Figure 19 Source for Common Data Files dialog box



Source for Common Data Files

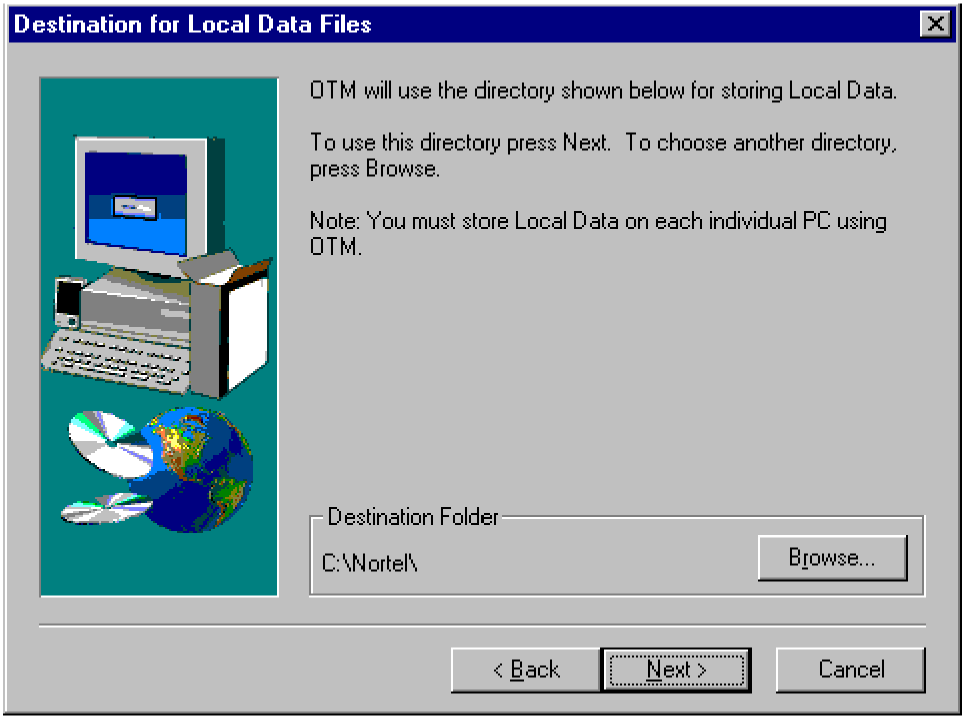
Please select the directory you would like this PC to link to for using already installed Common Data.

You may type the directory name or use the Browse button.

F:\

7 Select the destination on the Client PC for the local data files. See Figure 20. You must select a directory on the Client PC. Click Next to continue.

Figure 20 Destination for Local Data Files dialog box



Destination for Local Data Files

OTM will use the directory shown below for storing Local Data.

To use this directory press Next. To choose another directory, press Browse.

Note: You must store Local Data on each individual PC using OTM.

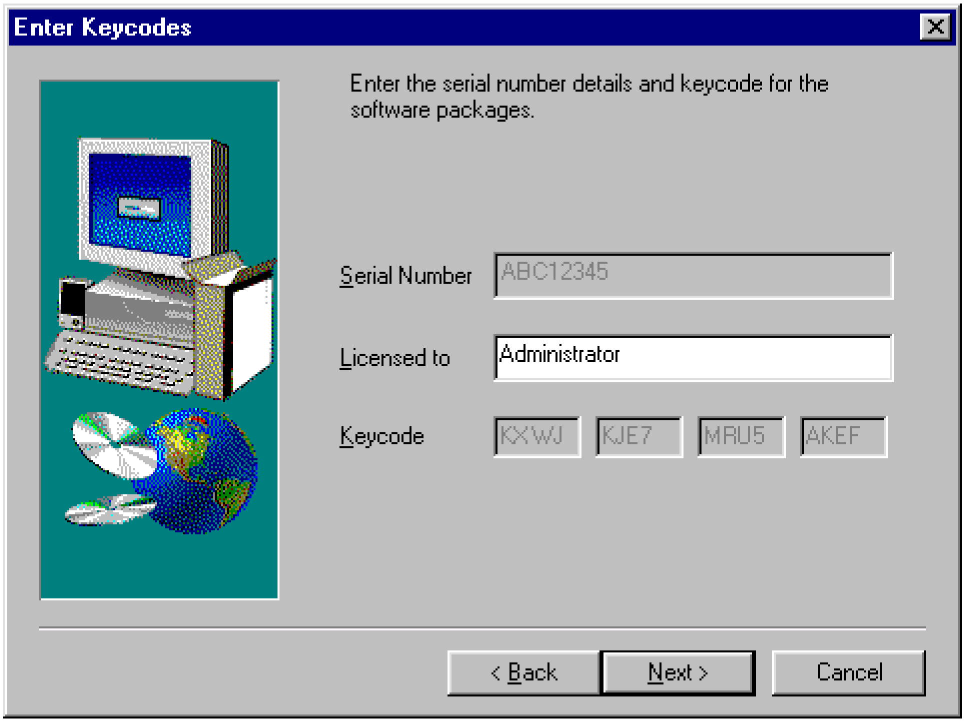
Destination Folder

C:\Nortel\

➡ **Note:** If it is not present on the PC, the setup program installs Microsoft Data Access Components (MDAC). Once installed, you must reboot the PC.

8 The Enter Keycodes dialog box appears. See Figure 21. The fields contain the data stored on the OTM Server. Click Next to continue.

Figure 21 Enter Keycodes dialog box



Enter Keycodes

Enter the serial number details and keycode for the software packages.

Serial Number: ABC12345

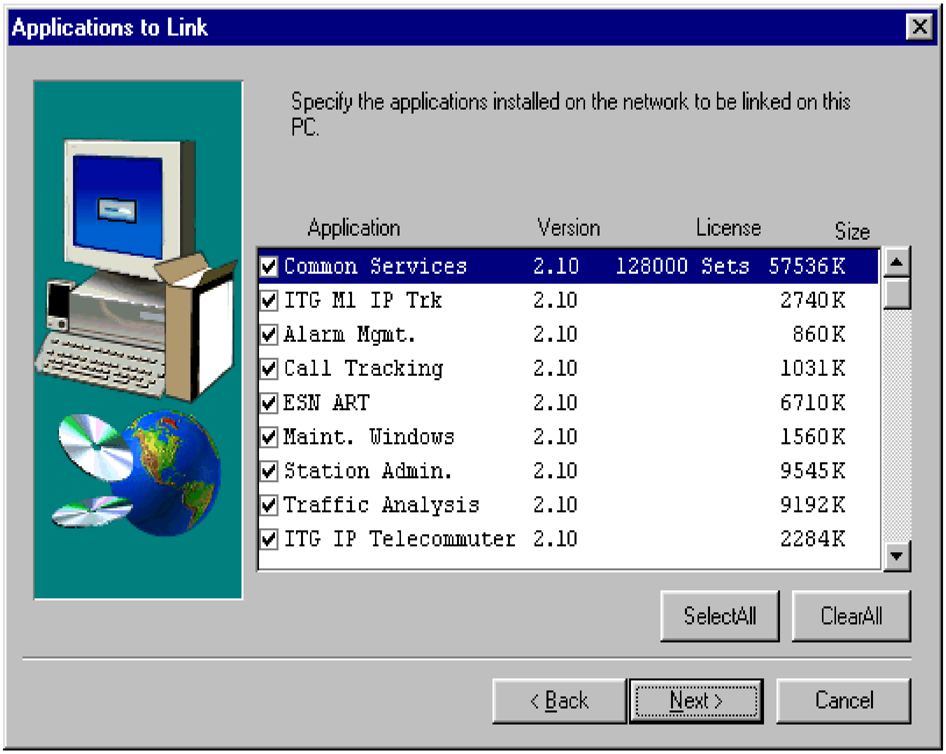
Licensed to: Administrator

Keycode: KXWJ KJE7 MRU5 AKEF

9 Choose one of the following:

- Select the applications to be installed to have the application executable installed on the Client PC.
- Select the applications to be linked to use the applications installed on the OTM Server. See Figure 22. Click Next to continue.

Figure 22 Applications to Link dialog box



Specify the applications installed on the network to be linked on this PC.

	Application	Version	License	Size
☑	Common Services	2.10	128000 Sets	57536K
☑	ITG M1 IP Trk	2.10		2740K
☑	Alarm Mgmt.	2.10		860K
☑	Call Tracking	2.10		1031K
☑	ESN ART	2.10		6710K
☑	Maint. Windows	2.10		1560K
☑	Station Admin.	2.10		9545K
☑	Traffic Analysis	2.10		9192K
☑	ITG IP Telecommuter	2.10		2284K

10 The Applications to Install window displays. see Figure 15. Click Next to continue.

11 After the installation is complete, you are given the option to view the Read Me file. Click Yes to view the Read Me file or No to skip the Read Me file.

12 When prompted, restart the computer.

The software installation is complete.

Performing upgrades

This section contains information on upgrading:

- OTM Server
- OTM PCs
- to a new release of 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 the OTM Server to the same release of OTM

Upgrade the OTM Server:

- To install OTM applications not previously installed
- To upgrade to another OTM package (for example, from General to Premium)
- To increase the maximum number of OTM clients or the maximum number of sets (telephones) supported by OTM

Upgrading OTM PCs from Windows 95

On an existing Windows 95 PC that is running OTM release 1.x, the OTM PC must first be upgraded to one of the supported PC platforms (See “OTM Software requirements” on page 30) before upgrading the software to OTM 2.1.

Procedure

1 Perform a backup of the OTM data by selecting Utilities > Backup in the Navigator window. Choose the Disaster Recovery option.

> **Note:** The following data is not backed up in OTM 1.x releases running on the Windows 95 platform:
>
> - Alarm Notification Run Options parameters and Control/Script files
> - Custom Help

2 Uninstall OTM 1.x.

3 Upgrade the PC to one of the platforms supported in OTM 2.1.

4 Reinstall OTM 1.x (the same release that was uninstalled in step 2).

5 Restore the OTM data by selecting Utilities > Restore in the Navigator window. Choose the backup file created in step 1.

6 Upgrade OTM to release 2.1.

Upgrading OTM PCs from Windows 98 or Windows NT

Before upgrading your PC, use the following procedure to upgrade OTM to release 2.1:

1 Upgrade OTM to release 2.1.

2 Perform a backup of the OTM data by selecting Utilities > Backup in the Navigator window. Choose the Full OTM Backup option.

> **Note:** The following data is not backed up in OTM 2.1:
>
> - Alarm Notification Run Options parameters and Control/Script files
> - Custom Help

3. Uninstall OTM 2.1.
4. Upgrade the PC to one of the platforms supported in OTM 2.1.
5. Reinstall OTM 2.1 (the same release that was uninstalled in step 3.
6. Restore the OTM data by selecting Utilities > Restore in the Navigator window. Choose the backup file created in step 2.

   When restoring users, if the user account no longer exists in the OS, then the user account will be created with the default password provided by the administrator during the restore process in step 6.

Upgrading to a new release of OTM

Perform this upgrade when installing a new release of OTM. Upgrade the OTM Server before performing OTM Windows 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 attempts to migrate your data from MAT to OTM. This causes a loss of data.

Upgrading from Meridian 1 releases

When a Meridian1 release is upgraded from 25 to 26 or higher, all the TNs configured on the PE/EPE shelves are disabled, if no Meridian Mail feature is configured.

Upon choosing “Update System Data” from System Window, the following message is logged to the “Event Log” if the Meridian1 release is 26 or higher.

This WARNING message is displayed per-user per-PC, and can be turned off after the first appearance per user per PC:

“X11 release 26 (and higher) software does not support TNs configured on PE/EPE shelves. Upgrading to release 26 (or higher) will permanently disable all TNs on PE/EPE and will not allow new TNs to be configured”.

No WARNING message is prompted from Web Station.

Client PC preparation

If the client PC is a Windows 95/98 or Windows NT computer 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 Server/Standalone option.

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.

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.

Procedure

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 windows appear (see "Procedure for new OTM server installations" on page 37 for examples):

   a Software Licences Agreement

   b Welcome

   c Identification

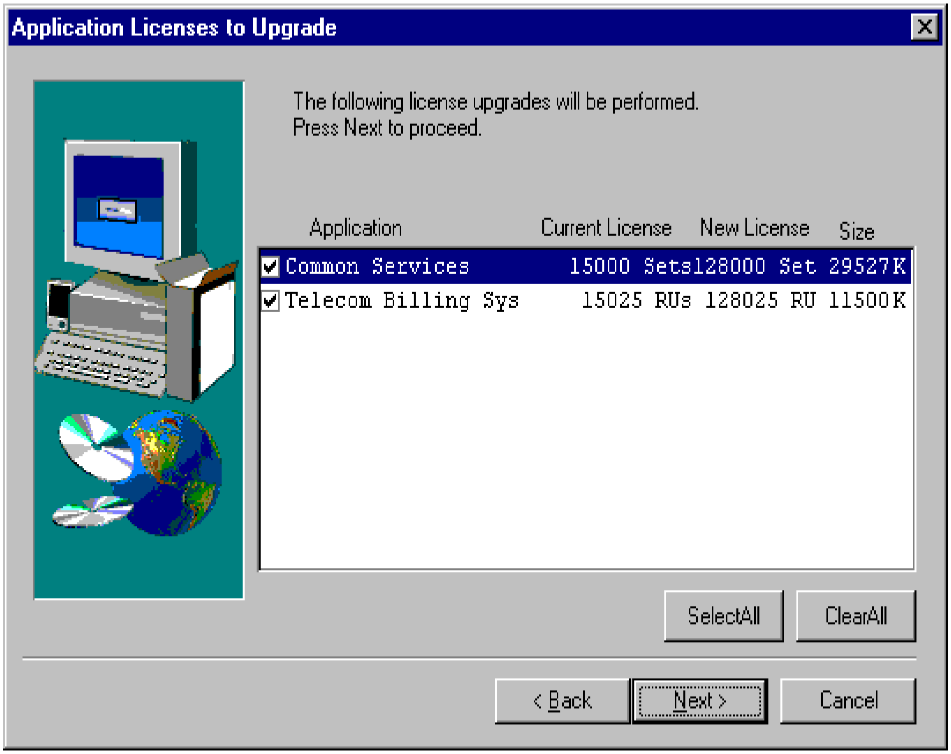
   d Setup Choices. Select Server/Standalone to upgrade the OTM Server, or select Client to upgrade an OTM Client.

   e Serial Number and Keycode

   f Destination for files

   g Application Licenses to Upgrade (Figure 23)

Figure 23 Application Licenses to Upgrade



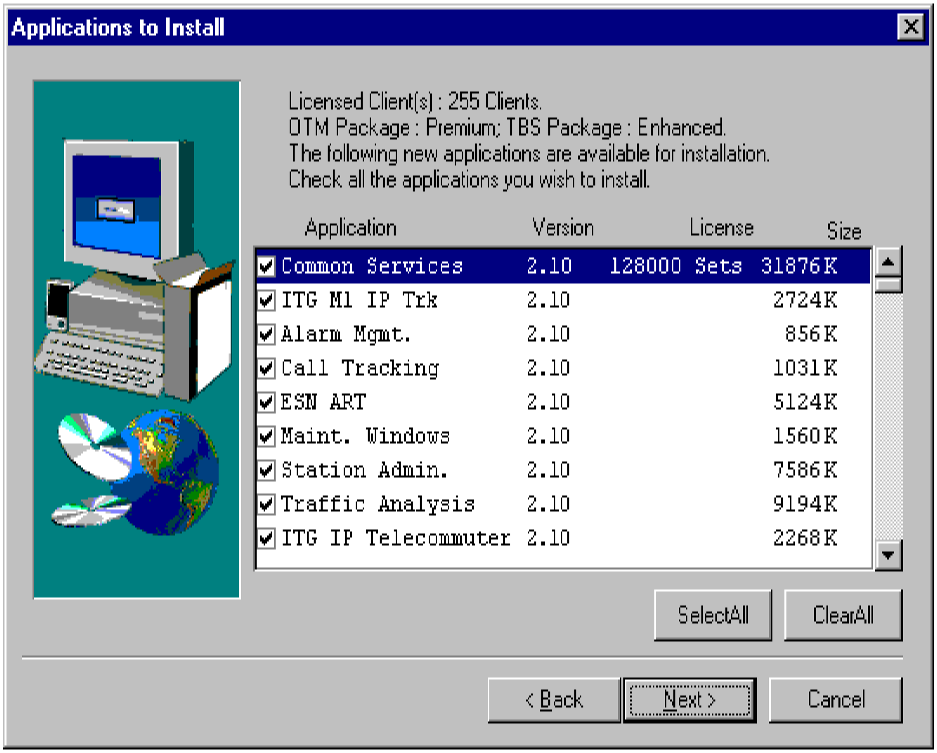
Application Licenses to Upgrade

The following license upgrades will be performed.
Press Next to proceed.

	Application	Current License	New License	Size
☑	Common Services	15000 Sets	128000 Set	29527K
☑	Telecom Billing Sys	15025 RUs	128025 RU	11500K

h New Applications to Install (Figure 24)

Figure 24 Applications to Install



Applications to Install

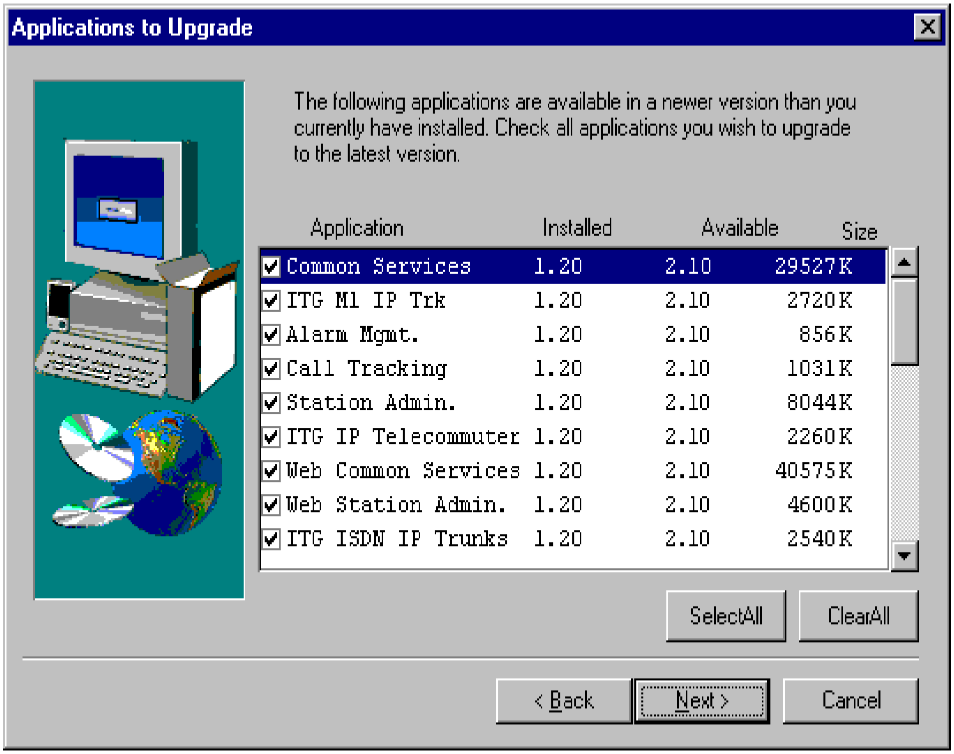
Licensed Client(s) : 255 Clients.
OTM Package : Premium; TBS Package : Enhanced.
The following new applications are available for installation.
Check all the applications you wish to install.

Application	Version	License	Size
☑ Common Services	2.10	128000 Sets	31876K
☑ ITG M1 IP Trk	2.10		2724K
☑ Alarm Mgmt.	2.10		856K
☑ Call Tracking	2.10		1031K
☑ ESN ART	2.10		5124K
☑ Maint. Windows	2.10		1560K
☑ Station Admin.	2.10		7586K
☑ Traffic Analysis	2.10		9194K
☑ ITG IP Telecommuter	2.10		2268K

i Applications to Upgrade (Figure 25)

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 25 Applications to Upgrade



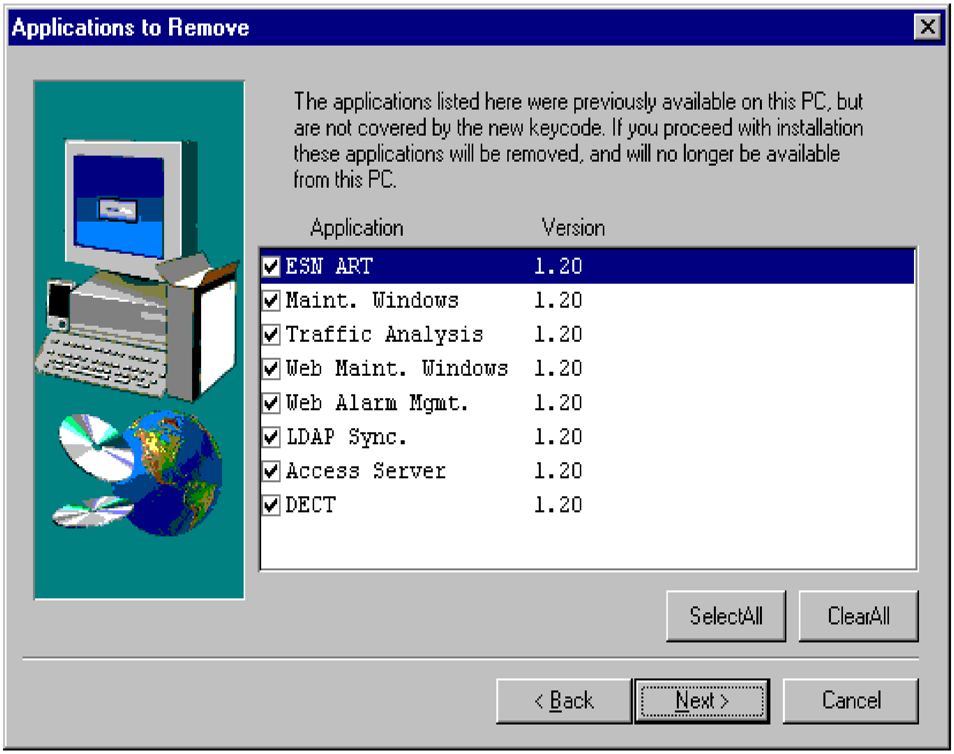
Applications to Upgrade

The following applications are available in a newer version than you currently have installed. Check all applications you wish to upgrade to the latest version.

	Application	Installed	Available	Size
☑	Common Services	1.20	2.10	29527K
☑	ITG M1 IP Trk	1.20	2.10	2720K
☑	Alarm Mgmt.	1.20	2.10	856K
☑	Call Tracking	1.20	2.10	1031K
☑	Station Admin.	1.20	2.10	8044K
☑	ITG IP Telecommuter	1.20	2.10	2260K
☑	Web Common Services	1.20	2.10	40575K
☑	Web Station Admin.	1.20	2.10	4600K
☑	ITG ISDN IP Trunks	1.20	2.10	2540K

j Applications to Remove. These are applications available in the old key code, but not available in the new key code (Figure 26).

Figure 26 Applications to Remove



The applications listed here were previously available on this PC, but are not covered by the new keycode. If you proceed with installation these applications will be removed, and will no longer be available from this PC.

Application	Version
☑ ESN ART	1.20
☑ Maint. Windows	1.20
☑ Traffic Analysis	1.20
☑ Web Maint. Windows	1.20
☑ Web Alarm Mgmt.	1.20
☑ LDAP Sync.	1.20
☑ Access Server	1.20
☑ DECT	1.20

k Copying files

After the installation is complete you are given the option to:

4 View the Read Me file.

5 Install JRE, if required.

6 Install OTM Web Help, if required.

7 Reboot the PC.

Performing migrations

This chapter contains information on:

- Migrating from MAT to OTM
- Migrating from OTM 1.2 or OTM 2.0x to OTM 2.1
- Migrating CDR data from MAT to OTM

Direct upgrades are NOT supported for customers migrating from OTM releases prior to 1.20.26, or from MAT 6.67. A two-step upgrade is required, first to OTM 2.0 and then to 2.1.

Before upgrading

Before upgrading to OTM, see "Migrating CDR data from MAT to OTM" on page 81 for information about transferring your Call Accounting data to OTM's Telecom Billing System (TBS) application. You may also want to print your Call Accounting reports before upgrading from MAT to OTM.

Migrating from MAT to OTM

Perform this upgrade when upgrading from MAT 6.67 or later to OTM. Customers on MAT releases prior to 6.67 will need to purchase and install OTM as a new installation.

The migration copies and converts existing MAT data to the OTM PC. This data includes:

- MAT Site and System data
- MAT Users and Templates
- Application data (Station, ESN, and so on)

Four scenarios

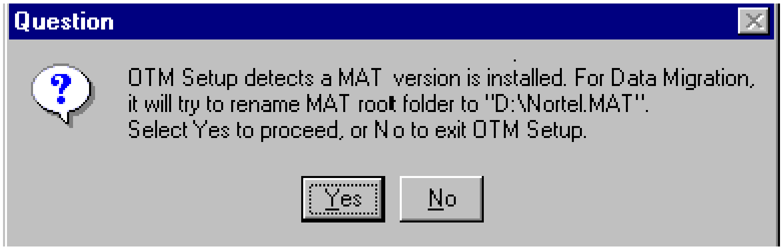
There are four scenarios:

1. Installing OTM on a Windows 98/NT Workstation on which MAT has been previously installed.
2. Installing OTM on a Windows NT server being used as a MAT file server.
3. Installing OTM on a clean Windows NT server and migrating the MAT data from another PC. See "Migrating data from MAT on one PC to OTM on another PC" on page 74.
4. Installing OTM on a MAT PC that is being upgraded to Windows 2000. See "Migrating data from MAT to OTM on a PC being upgraded to Windows 2000" on page 75.

Migrating data from MAT to OTM on the same PC

The migration is automatic if the setup program knows where MAT is installed (for example, installing OTM on a MAT PC) (Figure 27).

Figure 27 MAT Migration: OTM Setup dialog box



Question

OTM Setup detects a MAT version is installed. For Data Migration, it will try to rename MAT root folder to "D:\Nortel.MAT".
Select Yes to proceed, or No to exit OTM Setup.

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

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

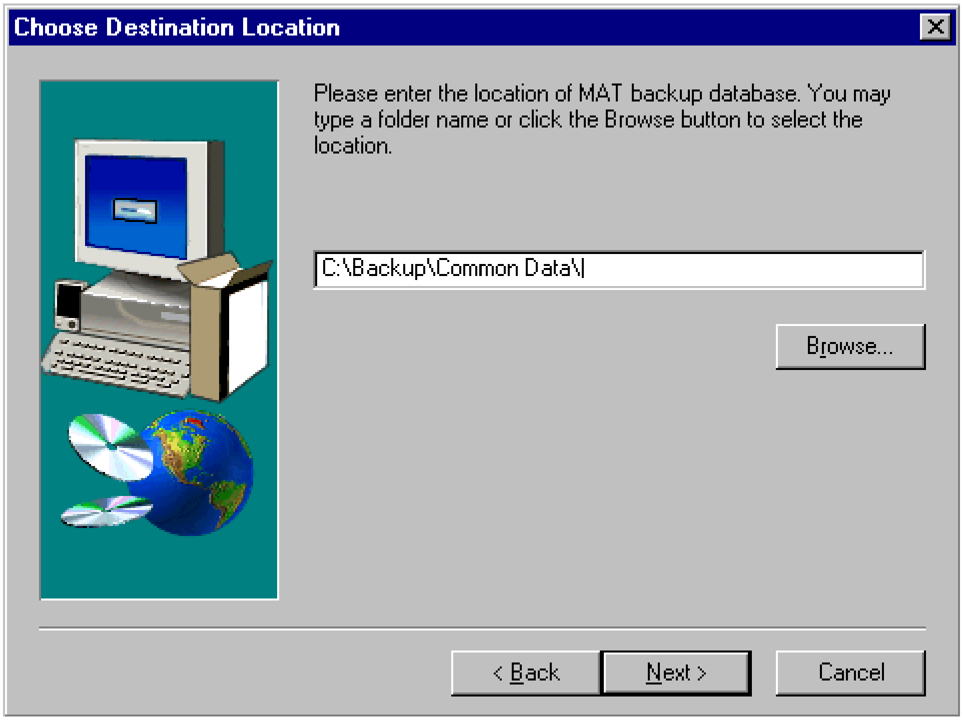
Installing OTM on a Windows NT server being used as a MAT file server

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 is *C:\Backup\Common Data*.

Caution: You must complete step 1 to prevent loss of data.

2. Install OTM.
3. Restart the PC.
4. In the Start menu, select Program Files > Optivity Telephony Manager > 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 Browse and locate the backup directory (Figure 28).

Figure 28 MAT Backup Database: Choose Destination Location


Choose Destination Location

Please enter the location of MAT backup database. You may type a folder name or click the Browse button to select the location.

C:\Backup\Common Data\

7 When asked to make a selection to rebuild data, click 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*).

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 > Optivity Telephony Manager > 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, click Rebuild All.

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

In this case, a current copy of MAT exists on the PC's hard drive.

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:

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 "Procedure for new OTM server installations" on page 37.
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.

For additional information on migrating the database from MAT to OTM, see "Migrating data from MAT to OTM on the same PC" on page 72.

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 "Procedure for new OTM server installations" on page 37.

4 Follow the procedure outlined in "Installing OTM on a Windows NT server being used as a MAT file server" on page 73, beginning with step 4, to migrate the data from MAT to OTM.

MAT/OTM migration summary

Table 4 and Table 5 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 stand-alone) shown in each table.

OTM in Windows NT server mode

Table 4 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 4 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

OTM in stand-alone mode

Table 5 summarizes the migration steps to use OTM in stand-alone mode.

Table 5 Migration for OTM in stand-alone mode

	MAT data migration for OTM in stand-alone mode:	
	Migrate data from MAT to OTM on same computer	Migrate data from MAT to OTM on different computer
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

Migrating from OTM 1.2 or OTM 2.0x to OTM 2.1

1 Back up files on existing OTM. If migrating to a new OS or a new PC then use the OtmOsMigrate tool described in the following section.

2 If migrating to a new OS or a new PC, then:

a Prepare the new PC

b Use the OtmOsMigrate tool described in the following section to restore existing version of OTM onto new PC. No OTM dongle is required for this step.

3 Install OTM 2.1 onto the PC. This migrates the existing OTM data from OTM 1.2/2.0x to OTM 2.1. A valid OTM 2.1 key code is required to be entered during this step. If changing dongle types and the new dongle has a different serial number, then it will also require a different key code. If changing dongles, enter the key code for the new dongle which is to be connected in the next step.

4 Ensure the dongle is connected to the PC. If migrating from a parallel port to USB dongle, switch dongles now. Note that USB dongles should not be attached until OTM 2.1 is installed.

5 Launch OTM 2.1

Windows NT/98 PC to Windows XP Pro/2000 Pro PC

These steps create a “Dummy OTM “on a WinXP Pro/Win2000 Pro machine.It appears to the installation program that there is an old OTM version installed, and this triggers the correct migration/upgrade logic. The utility backs up the installed OTM on the Win98/WinNT 4.0 Workstation, including executable, DLLs, data and registry, and restores them to the same location on a WinXP Pro/Win2000 Pro PC.

The OTM OS migration utility is included on the OTM 2.1 disk. This utility does not support OTM Windows Client Migration.

Migration paths

Migration paths supported by this utility are:

Table 6 Migration paths

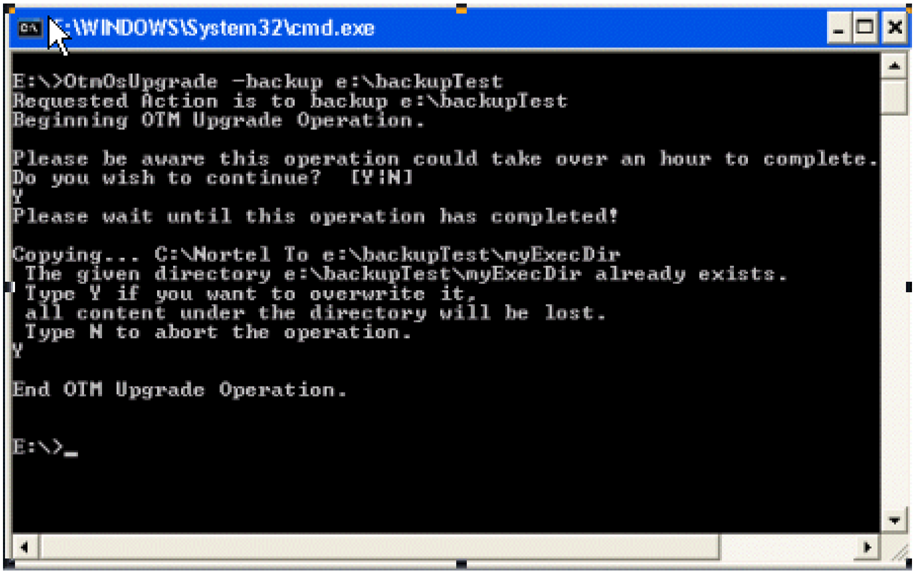
From	**To**
OTM 1.2 on Win95	OTM 2.1 on Win2000 Pro
OTM 1.2 on Win95	OTM 2.1 on WinXP Pro
OTM 1.2 on Win98	OTM 2.1 on Win2000 Pro
OTM 1.2 on Win98	OTM 2.1 on WinXP Pro
OTM 1.2 on WinNT 4.0 Workstation	OTM 2.1 on Win2000 Pro
OTM 1.2 on WinNT 4.0 Workstation	OTM 2.1 on WinXP Pro
OTM 2.0x on WinNT 4.0 Workstation	OTM 2.1 on Win2000 Pro
OTM 2.0x on WinNT 4.0 Workstation	OTM 2.1 on WinXP Pro

Win98/4.0 to WinXP/200Pro

With OTM 2.0 installed on WinNT 4.0 Workstation, the OTM user account from the local Windows NT account database cannot be migrated. OTM does not store the user password. You must re-create the local user account on the new PC. Once those local accounts (with the same name) are re-created, the OTM user /template relationship stay untouched. There is no need to recreate local user groups for each template.

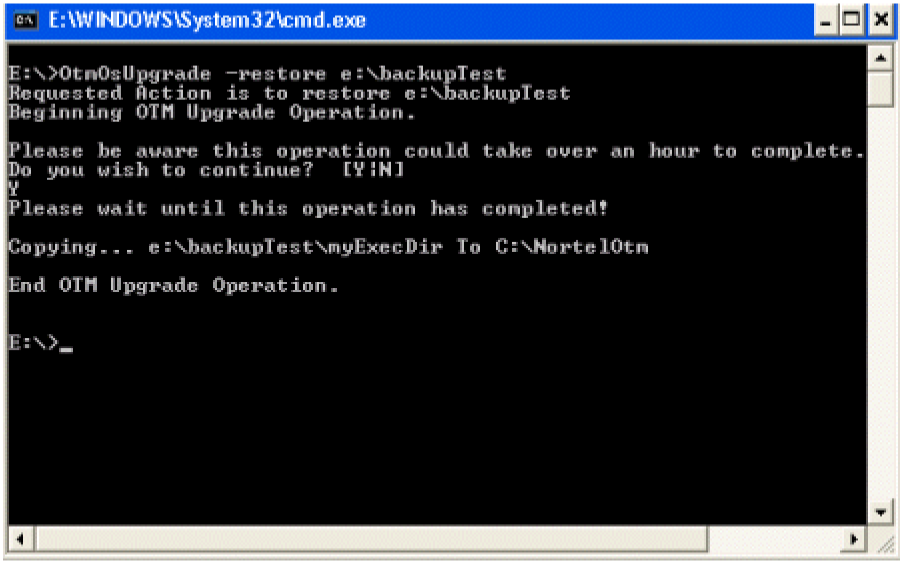
To move old OTM (data) from one PC running Win98/WinNT 4.0 Workstation to another PC running WinXP Pro/Win2000 Pro, complete these steps.

1 On the Win98/WinNT 4.0 Workstation machine, use the "-backup directoryPath [-batch]" option to back up all the OTM information. The directoryPath can be a shared folder to which you have read/write access.



```
E:\>OtmOsUpgrade -backup e:\backupTest
Requested Action is to backup e:\backupTest
Beginning OTM Upgrade Operation.

Please be aware this operation could take over an hour to complete.
Do you wish to continue?  [Y|N]
Y
Please wait until this operation has completed!

Copying... C:\Nortel To e:\backupTest\myExecDir
 The given directory e:\backupTest\myExecDir already exists.
 Type Y if you want to overwrite it,
 all content under the directory will be lost.
 Type N to abort the operation.
Y

End OTM Upgrade Operation.


E:\>_
```

2 On the WinXP Pro/Win2000 Pro machine, use the "-restore directoryPath [-batch]" option to restore all the OTM information from directoryPath.



```
E:\>OtmOsUpgrade -restore e:\backupTest
Requested Action is to restore e:\backupTest
Beginning OTM Upgrade Operation.

Please be aware this operation could take over an hour to complete.
Do you wish to continue?  [Y|N]
Y
Please wait until this operation has completed!

Copying... e:\backupTest\myExecDir To C:\NortelOtm

End OTM Upgrade Operation.


E:\>_
```

3 Install OTM 2.1 on the WinXP Pro/Win2000 Pro machine. The installation program detects the OTM 1.2 information and implements proper migration.

After migration, OTM 2.1 must be installed on exactly the same location as the old OTM version. For example, if an OTM 1.2 is installed on "c:\Nortel" on a Window NT 4.0 Workstation, after migrating to WinXP Pro, OTM 2.1 must be installed on the same location "c:\Nortel". The same limitation applies to migrating from OTM 1.2 to OTM 2.0.

4 Using the OtmOsUpgrade utility, back up directoryPath [-batch]. Back up all the OTM directories and OTM related registry information into the destinationPath. If -batch is given, no user input is required.

The OtmOsUpgrade utility is a CLI-based script written in Jscript and running inside Windows Script Host. The lowest version of Windows Script Host required by this utility is 2.0. IE 5.5 or higher must be installed on the PC before running the OtmOsUpgrade utility.

5 Restore directoryPath [-batch], restore the OTM registry information and OTM directories from directoryPath to the proper target location. If -batch is given, no user input is required.

Migrating CDR data from MAT to OTM

This section provides a procedure for migrating data from the MAT Call Accounting application to the OTM Telecom Billing System (TBS) application. The method outlined in this procedure takes advantage of the fact that the archived MAT Call Accounting data is in the same format as the data stored in an MDR 2000 buffer box.

Warning: CDR and MAT Call Accounting data do not include the year in their date formats. TBS includes the year, which it retrieves from the CPU clock setting. If you use the procedure outlined in this section to migrate data from MAT to OTM, the data must be from the same year as the computer's current clock setting; otherwise, all data will be assigned the wrong year.

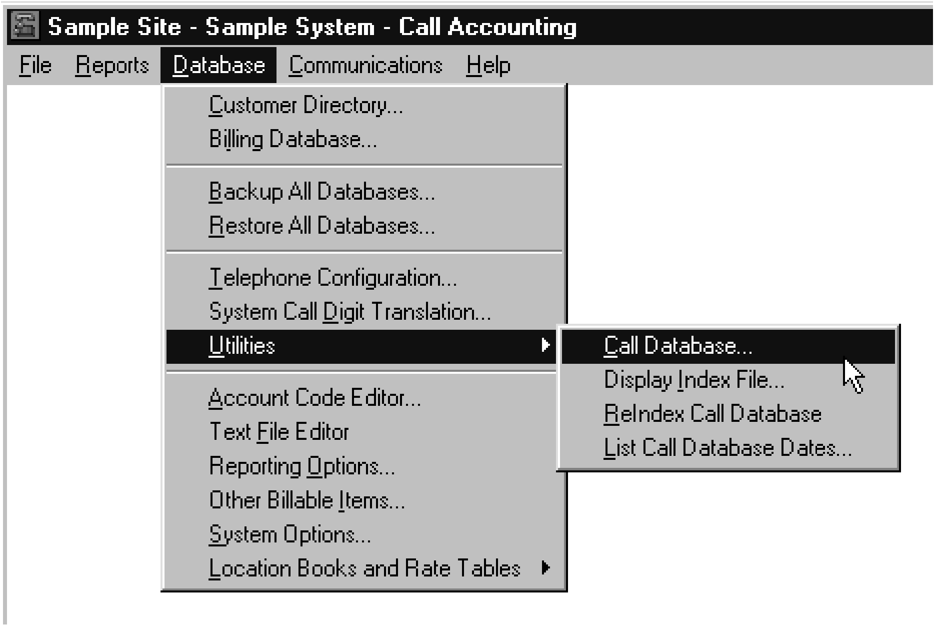
Archiving call data

Before upgrading from MAT to OTM, you should archive your call data.

To archive call data:

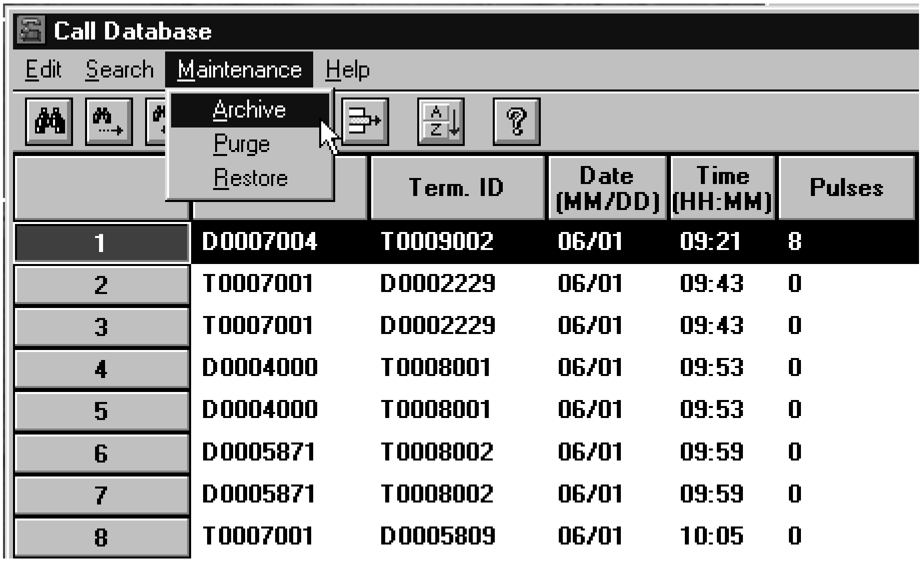
1 From the Call Accounting application for the site/system, launch the Call Database (Figure 29).

Figure 29 Launch Call Database



2 Select Archive from the Maintenance menu (Figure 30).

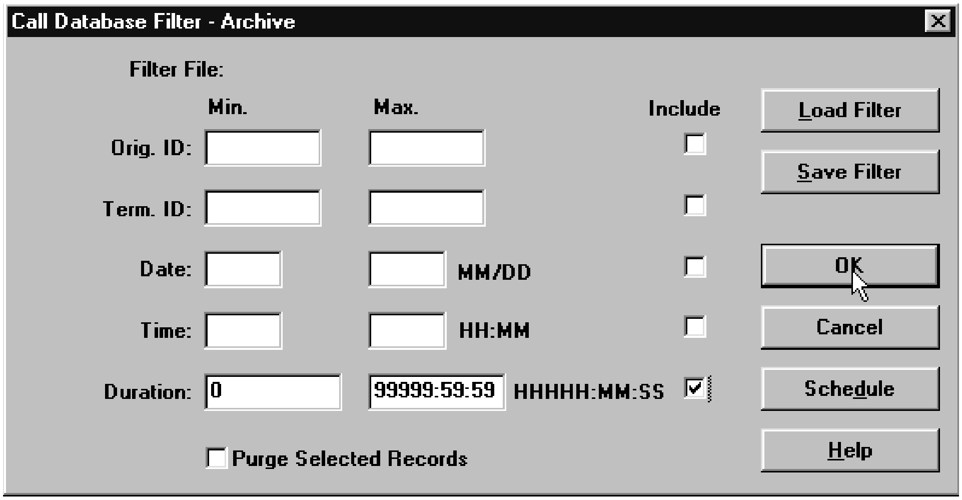
Figure 30 Launch Archive



		Term. ID	Date (MM/DD)	Time (HH:MM)	Pulses
1	D0007004	T0009002	06/01	09:21	8
2	T0007001	D0002229	06/01	09:43	0
3	T0007001	D0002229	06/01	09:43	0
4	D0004000	T0008001	06/01	09:53	0
5	D0004000	T0008001	06/01	09:53	0
6	D0005871	T0008002	06/01	09:59	0
7	D0005871	T0008002	06/01	09:59	0
8	T0007001	D0005809	06/01	10:05	0

3 Enter an appropriate filter, and then click OK. All calls are selected in the example shown in Figure 31.

Figure 31 Archive Filter dialog box



Call Database Filter - Archive

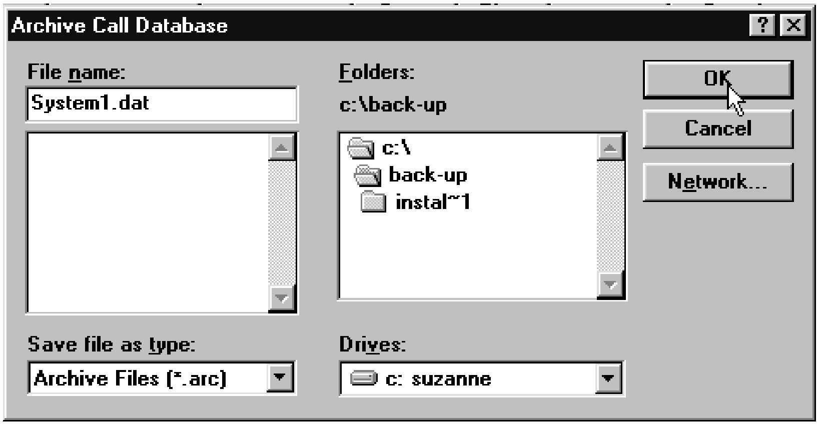
Filter File:

	Min.	Max.		Include
Orig. ID:				□
Term. ID:				□
Date:			MM/DD	□
Time:			HH:MM	□
Duration:	0	99999:59:59	HHHHH:MM:SS	☑

□ Purge Selected Records

4 Name your file and choose where you want to save the file (Figure 32), and then click OK.

Figure 32 Store the Archive file



Archive Call Database

File name: System1.dat

Folders: c:\back-up

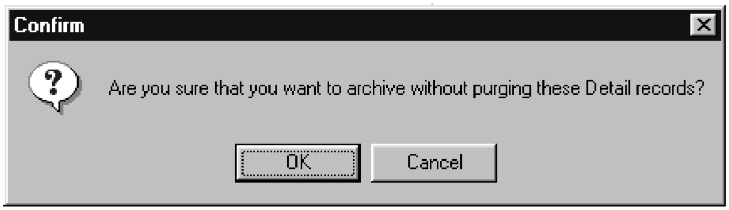
c:\
back-up
instal~1

Save file as type: Archive Files (*.arc)

Drives: c: suzanne

You can ignore the warning message (Figure 33). There is no reason to purge the data since the database will be obsolete after you upgrade from MAT to OTM.

Figure 33 Purge warning confirmation box



Confirm

Are you sure that you want to archive without purging these Detail records?

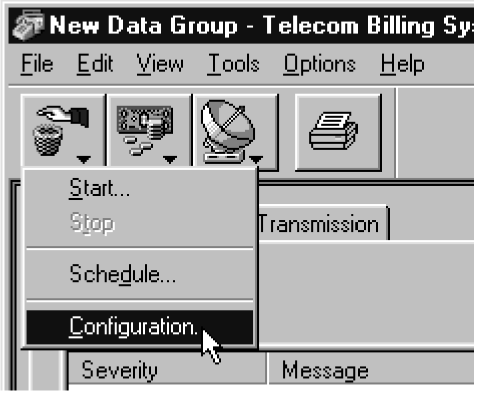
After you have upgraded from MAT to OTM, collect the archived Call Accounting data into the TBS application.

To collect the data into TBS:

1 Launch the TBS application for the desired site/system.

2 From the TBS application, launch the Collection Configuration editor (Figure 34).

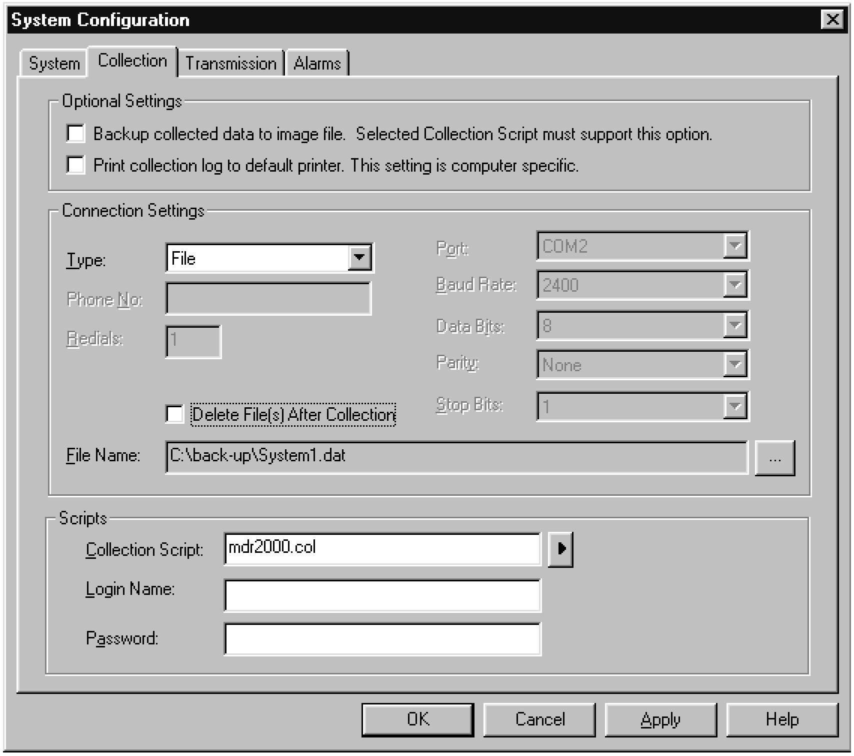
Figure 34 Launch Collection Configuration



New Data Group - Telecom Billing Sy
File Edit View Tools Options Help
Start...
Stop
Schedule...
Configuration...
Transmission
Severity
Message

The TBS System Configuration dialog box opens with the Collection tab selected (Figure 35).

Figure 35 TBS System Configuration—Collection tab



System Configuration

System | Collection | Transmission | Alarms

Optional Settings

☐ Backup collected data to image file. Selected Collection Script must support this option.

☐ Print collection log to default printer. This setting is computer specific.

Connection Settings

Type: File

Phone No:

Redials: 1

☐ Delete File(s) After Collection

Port: COM2

Baud Rate: 2400

Data Bits: 8

Parity: None

Stop Bits: 1

File Name: C:\back-up\System1.dat ...

Scripts

Collection Script: mdr2000.col

Login Name:

Password:

3 In the System Configuration—Collection dialog box:

  a Enter the File Name of the Call Accounting archive file. See step 4 on page 83.

  b For Collection Script, select *MDR2000.col.*

  c Uncheck the Delete File(s) After Collection check box to turn off the auto-delete option.

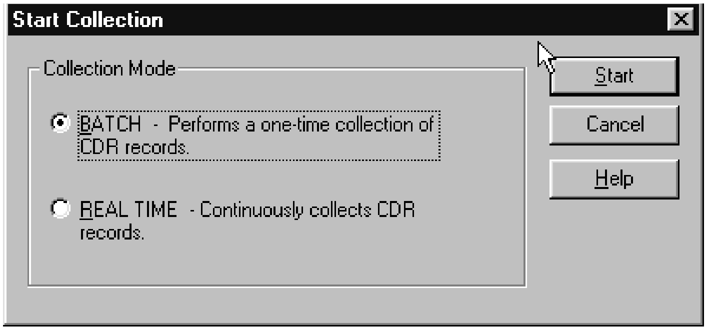
  d Click OK.

4 In the Start Collection dialog box (Figure 36):

  a Select BATCH to collect the data in the Call Accounting archive file.

  b Click Start.

Figure 36 Start Collection dialog box



Start Collection

Collection Mode

● BATCH - Performs a one-time collection of CDR records.

○ REAL TIME - Continuously collects CDR records.

You can now use the normal TBS procedure to cost the CDR data. You will also want to modify your Collection Configuration to collect data from your site/ system. See Chapter 2, “Telecom Billing System,” in *Using Optivity Telephony Manager Release 2.1 Telemanagement Applications* (553-3001-331) for information on TBS.

Installing Web Help

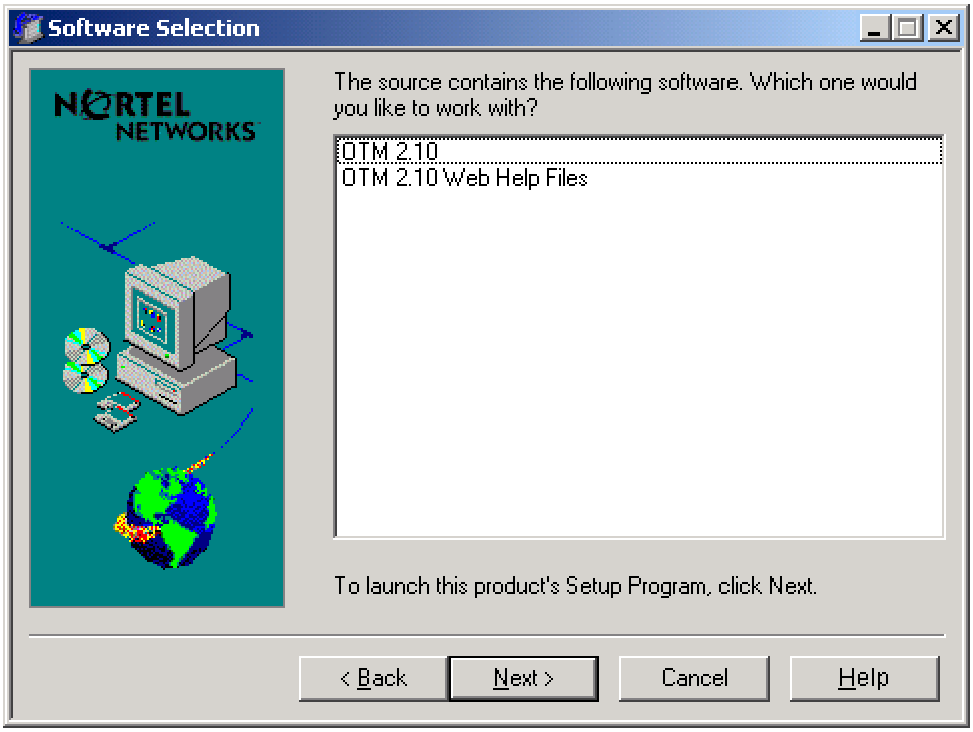
This chapter contains information on installing Web Help.

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 37).

1 Double-click the *Setup.exe* file to launch the Software Installation Wizard (Figure 1 on page 39).

2 Select the OTM Web Help Files option, and then click Next (Figure 37).

Figure 37 Software Selection: Web Help



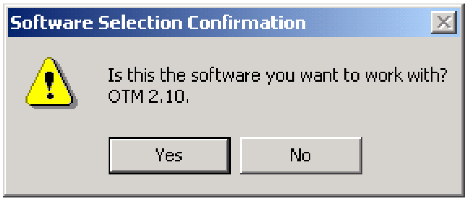
The source contains the following software. Which one would you like to work with?

OTM 2.10
OTM 2.10 Web Help Files

To launch this product's Setup Program, click Next.

The Software Selection Confirmation dialog box (Figure 38) opens to request confirmation that OTM 2.10 Web Help Files is the software that you want to work with.

Figure 38 Confirmation Dialog Box



Software Selection Confirmation

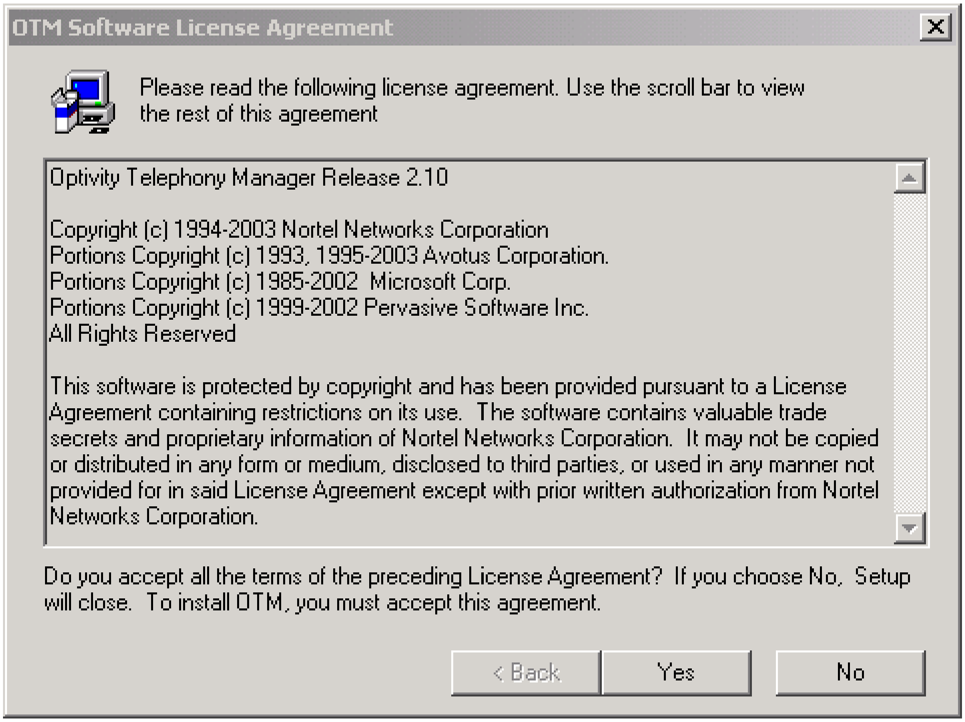
Is this the software you want to work with?
OTM 2.10.

Click Yes to continue.

3 The "Software License Agreement" is the first dialog box displayed when you launch the OTM installation program (Figure 39). Click Yes to accept the agreement.

The Select Components dialog box appears (Figure 40).

Figure 39 Help License



OTM Software License Agreement

Please read the following license agreement. Use the scroll bar to view the rest of this agreement

Optivity Telephony Manager Release 2.10

Copyright (c) 1994-2003 Nortel Networks Corporation
Portions Copyright (c) 1993, 1995-2003 Avotus Corporation.
Portions Copyright (c) 1985-2002 Microsoft Corp.
Portions Copyright (c) 1999-2002 Pervasive Software Inc.
All Rights Reserved

This software is protected by copyright and has been provided pursuant to a License Agreement containing restrictions on its use. The software contains valuable trade secrets and proprietary information of Nortel Networks Corporation. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not provided for in said License Agreement except with prior written authorization from Nortel Networks Corporation.

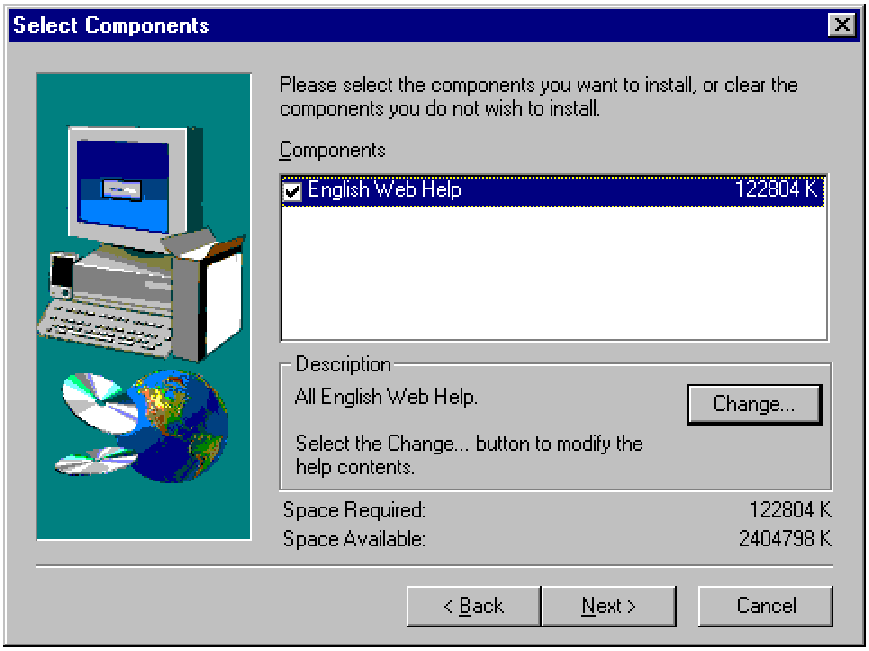
Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install OTM, you must accept this agreement.

4 In the Select Components dialog box, click Next to install all English Web Help, or click Change to select the sub-components that you want to install (Figure 41).

5 Click Continue in the Select Sub-components dialog box (Figure 41) to return to the Select Components dialog box (Figure 40).

6 Click Next to start the Web Help installation process.

Figure 40 Select Web Help components dialog box



Select Components

Please select the components you want to install, or clear the components you do not wish to install.

Components

☑ English Web Help 122804 K

Description

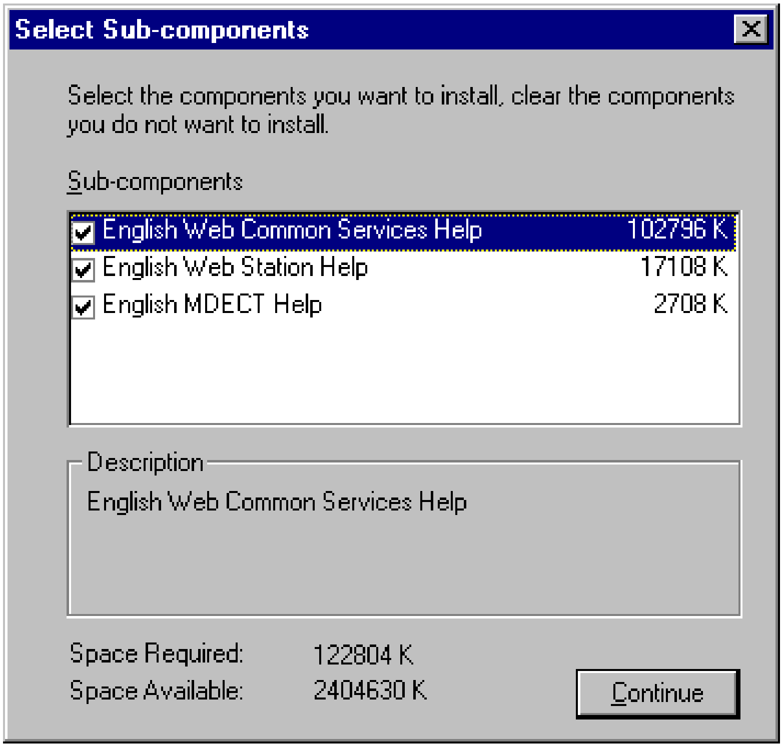
All English Web Help.

Select the Change... button to modify the help contents.

Space Required: 122804 K

Space Available: 2404798 K

Figure 41 Select Web Help sub-components dialog box



Select the components you want to install, clear the components you do not want to install.

Sub-components

☑	English Web Common Services Help	102796 K
☑	English Web Station Help	17108 K
☑	English MDECT Help	2708 K

Description

English Web Common Services Help

Space Required: 122804 K

Space Available: 2404630 K

License management

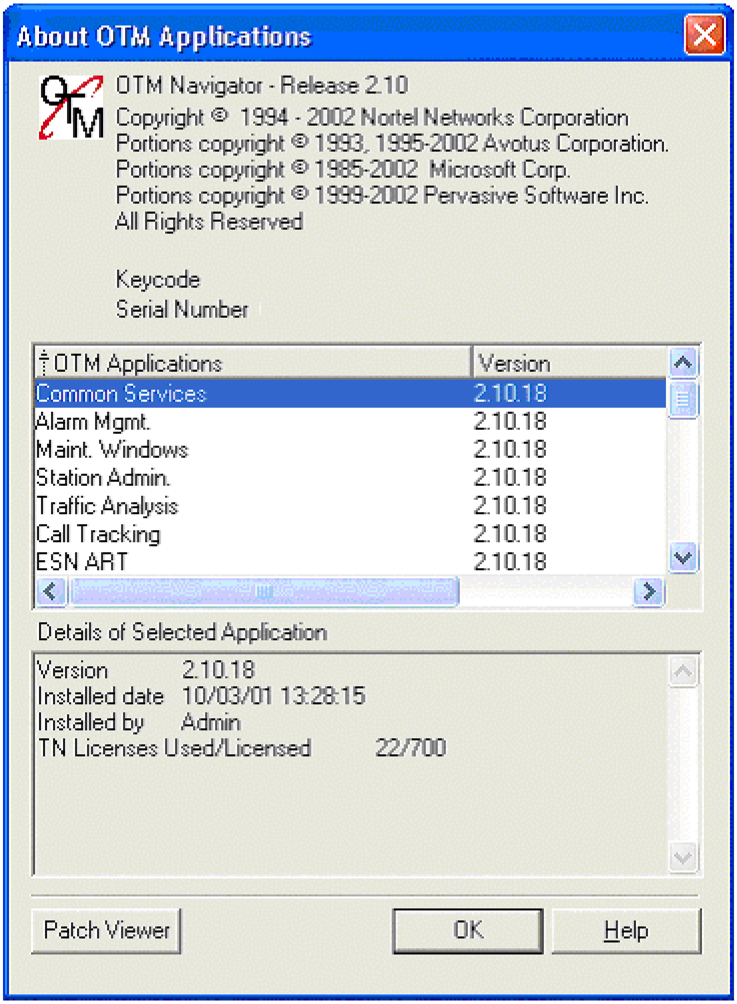
This chapter contains information on:

- Serial number and key code
- TN license
- RU license
- Client license
- Security device

Serial number and key code

Key codes supported on previous releases of OTM will not work in OTM 2.1

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, contact your OTM vendor.



OTM Navigator - Release 2.10
Copyright © 1994 - 2002 Nortel Networks Corporation
Portions copyright © 1993, 1995-2002 Avotus Corporation.
Portions copyright © 1985-2002 Microsoft Corp.
Portions copyright © 1999-2002 Pervasive Software Inc.
All Rights Reserved

Keycode
Serial Number

OTM Applications	Version
Common Services	2.10.18
Alarm Mgmt.	2.10.18
Maint. Windows	2.10.18
Station Admin.	2.10.18
Traffic Analysis	2.10.18
Call Tracking	2.10.18
ESN ART	2.10.18

Details of Selected Application

Version 2.10.18
Installed date 10/03/01 13:28:15
Installed by Admin
TN Licenses Used/Licensed 22/700

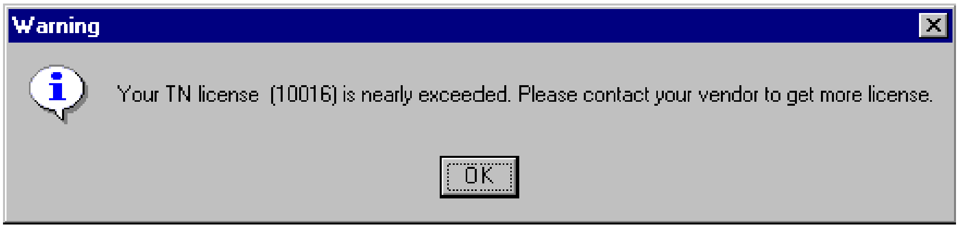
TN license

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 42 appears.

License exceeded

If your TN license has been exceeded, an error message appears. This message appears every 15 minutes. Contact your vendor to obtain a license for additional TNs.

Figure 42 TN license warning dialog box

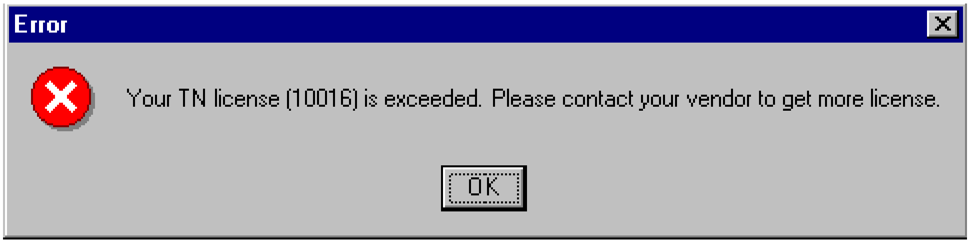


Your TN license (10016) is nearly exceeded. Please contact your vendor to get more license.

License re-use

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 becomes 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.

Figure 43 TN license error dialog box



Your TN license (10016) is exceeded. Please contact your vendor to get more license.

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 appears.

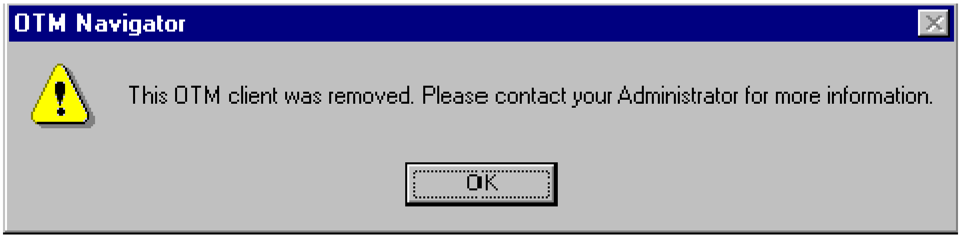
If your RU license has been exceeded, you receive an error message. The TBS application continues to collect data; however, you cannot cost the data and generate reports. The GCAS application launches, but you cannot generate reports. Contact your vendor to obtain a license for additional RUs.

See *Using Optivity Telephony Manager Release 2.1 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 checks the OTM database. If the OTM Client is not located in the database, the dialog box shown in Figure 44 appears.

Figure 44 Client removed dialog box



OTM Navigator

This OTM client was removed. Please contact your Administrator for more information.

This message appears if the OTM Client computer'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 computer 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, refer to *Optivity Telephony Manager: System Administration* (553-3001-330).

Security device (dongle or USB dongle)

Dongle

The process for checking the security device, commonly referred to as the "dongle". In OTM, the dongle attached to the OTM Server enables 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 5 minutes, once it has been reattached, for the OTM Client to recognize the dongle.

USB dongle

Server configuration

- supports one USB dongle only
- not supported through a USB hub
- not supported on Windows NT server

Stand alone configuration

- supports one USB dongle only
- not supported through a USB hub

PCI port limitations

PCI-based parallel ports may have problems on certain operating systems. Compaq Proliant DL360R01 running Windows 2000 Server using a Lava PCI Bus Enhanced Parallel Port card is one such system. OTM does not support this configuration.

Before configuring

Before configuring for OTM, test the connection between OTM and your equipment, using the sample site and system configuration. Follow the procedure in this chapter.

After connecting successfully, refer to "Adding sites and systems via the OTM Navigator window" on page 133 to configure your own sites and systems.

The complete list of OTM configuration procedures includes:

- "Configuring Secure Sockets Layer" on page 109
- "Configuring a modem for OTM applications in Windows" on page 113
- "Initial login" on page 121
- "Testing the connection" on page 100
- "Adding sites and systems via the OTM Navigator window" on page 133
- "Adding OTM Windows users via the OTM Windows Navigator" on page 185
- "Adding OTM Web Navigator users" on page 193
- "Setting up the Meridian 1 or Succession system" on page 215
- "Configuring Succession systems for survivability" on page 227
- "Setting up virtual terminal service" on page 233
- "Setting up FTP Server support for CDR Data Collection (Succession DCM)" on page 241
- "Setting up the Data Buffering and Access application" on page 245
- "Setting up the LDAP server" on page 247
- "Backing up and restoring OTM" on page 251
- "Installing OTM Web browser client" on page 257
- "Integrating OTM with Optivity NMS" on page 259
- "Integrating OTM with HP OpenView" on page 277

Testing the connection

Use the following procedures to test the connection between OTM and your equipment. For detailed instructions on adding sites and systems, see “Once the data is copied from the system into OTM, the test procedure is complete.” on page 108.

ELAN required

The Embedded LAN (ELAN) must be configured and devices must be connected to the ELAN before you can test the connection.

Setting up communications information

1 Double-click Sample Site in the OTM Navigator window.

2 Click Sample System, and then choose File > Properties.

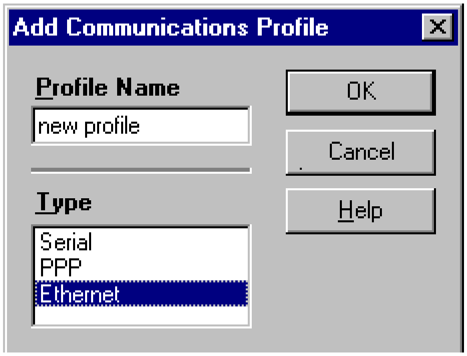
The System Properties dialog box appears with the General tab selected.

3 Click the Communications tab.

4 Click Add.

The Add Communications Profile dialog box appears (Figure 45).

Figure 45 Add Communications Profile dialog box



Profile Name
new profile

Type
Serial
PPP
Ethernet

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

6 Enter a Profile Name.

7 Click OK.

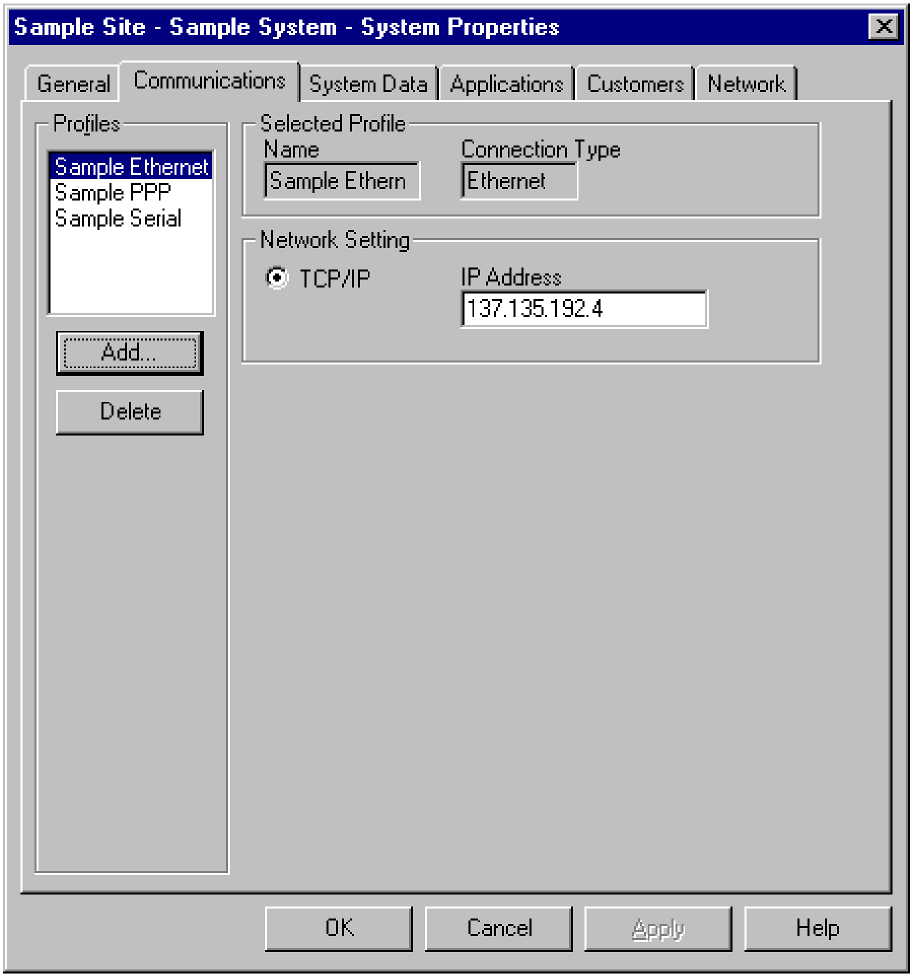
8 Enter the information in the System Properties—Communications dialog box for the connection type selected in step 5.

For an Ethernet connection type (Figure 46):

a Enter the IP address that you configured on the Meridian 1 or Succession 3.0 system.

b Click Apply.

Figure 46 System Properties dialog box—Communications tab—Ethernet Profile



Sample Site - Sample System - System Properties

Profiles: Sample Ethernet (selected), Sample PPP, Sample Serial

Selected Profile

Name: Sample Ethern

Connection Type: Ethernet

Network Setting

● TCP/IP

IP Address: 137.135.192.4

For a PPP connection type (Figure 47):

a Enter all modem parameters and dial-up information.

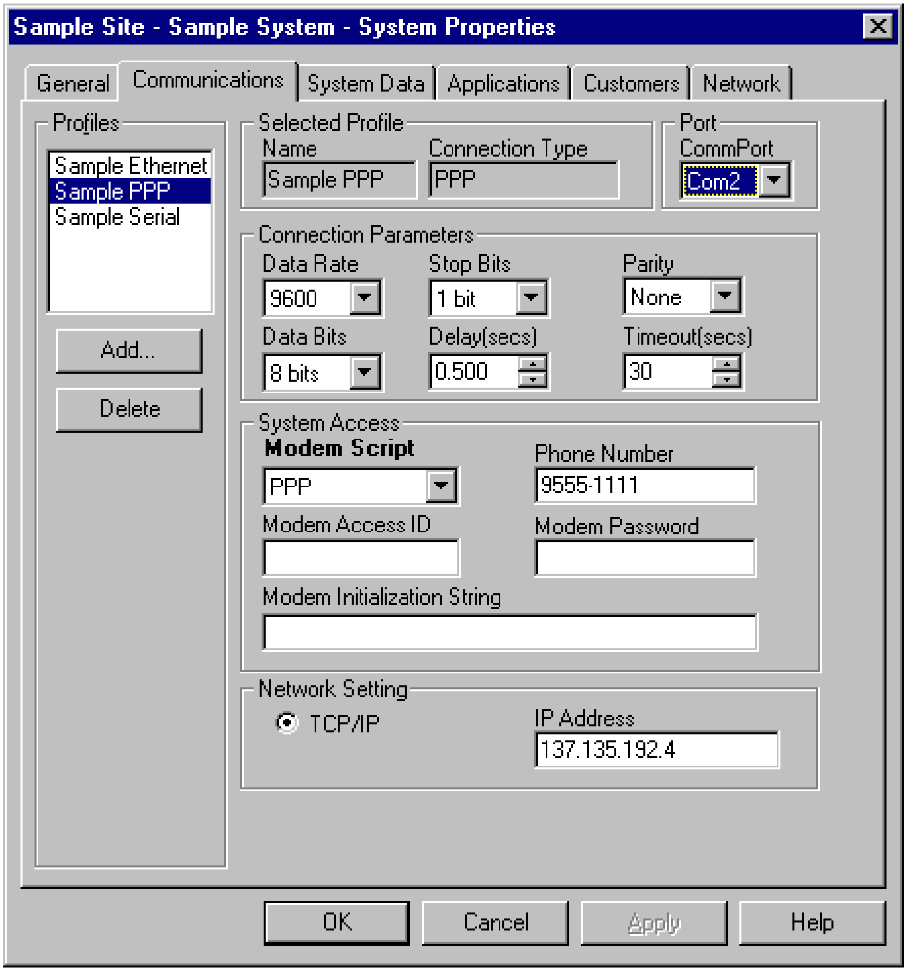
b Select PPP in the Modem Script text box and enter the phone number.

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 initialization string.

c Set the IP address to the local IP address, as configured on the Meridian 1 or Succession 3.0 system.

d Click Apply.

Figure 47 System Properties dialog box—Communications tab—PPP Profile



Sample Site - Sample System - System Properties

Selected Profile
Name: Sample PPP
Connection Type: PPP

Port
CommPort: Com2

Connection Parameters
Data Rate: 9600
Stop Bits: 1 bit
Parity: None
Data Bits: 8 bits
Delay(secs): 0.500
Timeout(secs): 30

System Access
Modem Script: PPP
Phone Number: 9555-1111
Modem Access ID:
Modem Password:
Modem Initialization String:

Network Setting
● TCP/IP
IP Address: 137.135.192.4

For a Serial connection type (Figure 48):

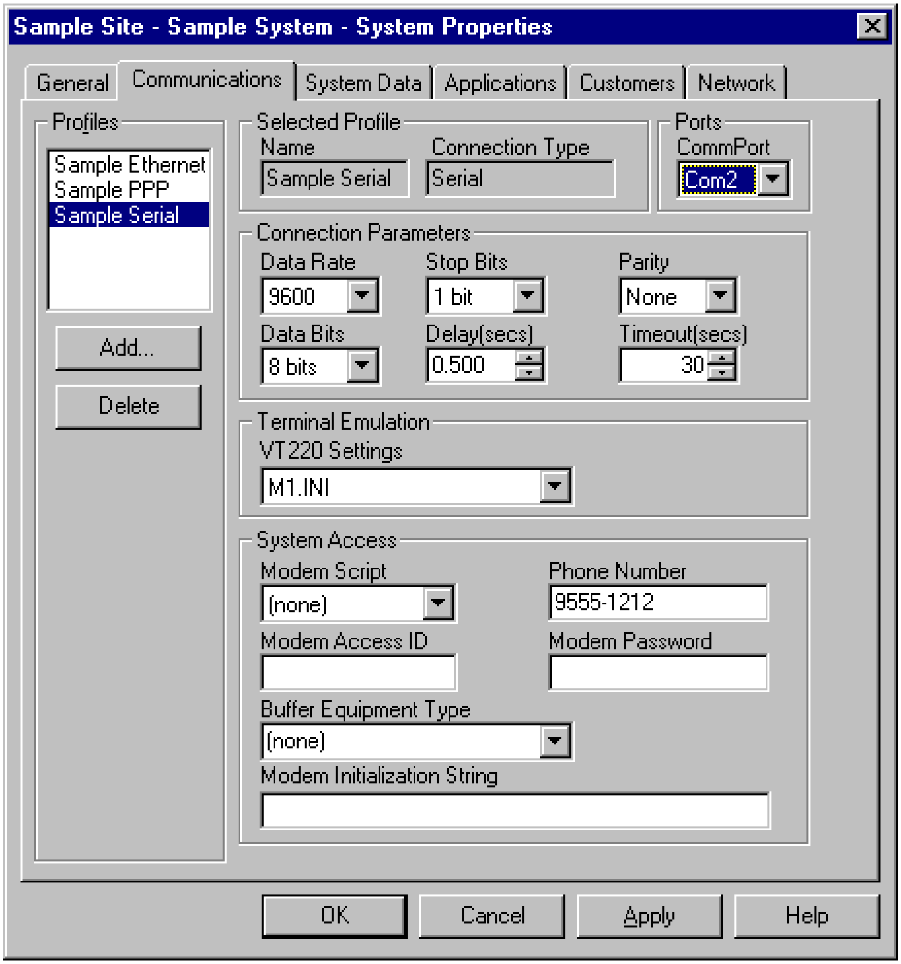
a Enter all modem parameters and dial-up information.

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

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

c Click Apply.

Figure 48 System Properties dialog box—Communications tab—Serial Profile



Sample Site - Sample System - System Properties

Profiles: Sample Ethernet, Sample PPP, Sample Serial

Selected Profile
Name: Sample Serial
Connection Type: Serial

Ports
CommPort: Com2

Connection Parameters
Data Rate: 9600
Stop Bits: 1 bit
Parity: None
Data Bits: 8 bits
Delay(secs): 0.500
Timeout(secs): 30

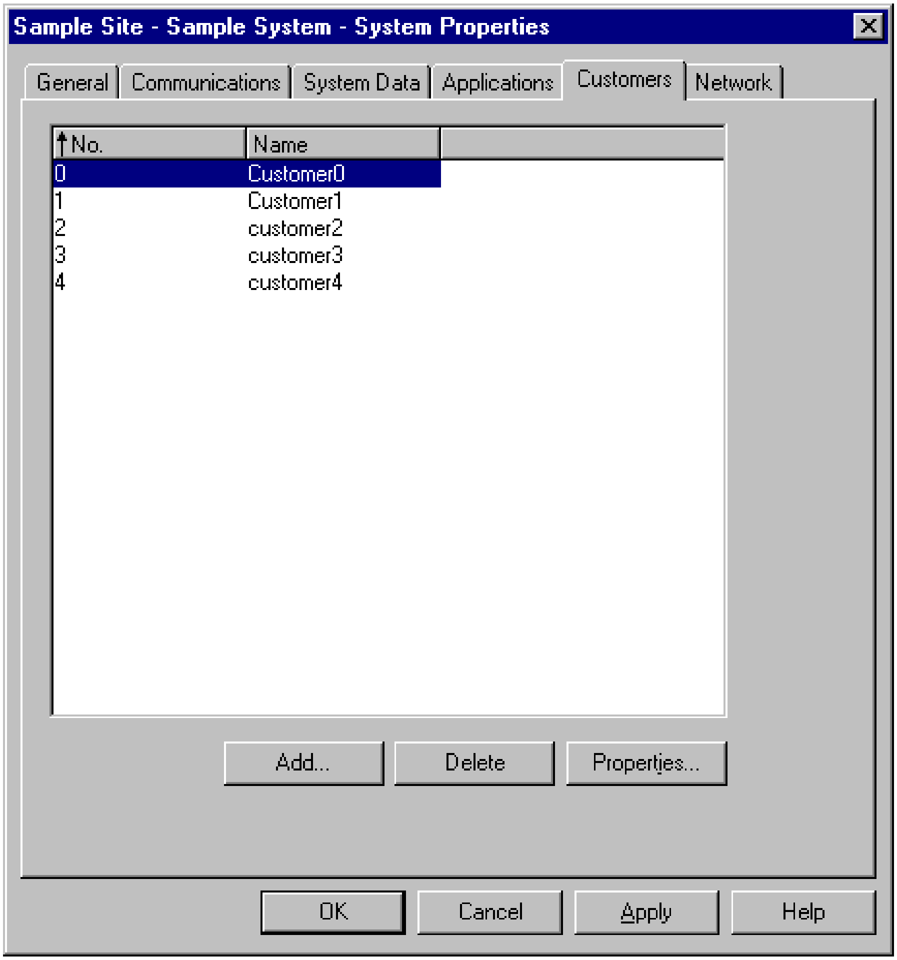
Terminal Emulation
VT220 Settings: M1.INI

System Access
Modem Script: (none)
Phone Number: 9555-1212
Modem Access ID:
Modem Password:
Buffer Equipment Type: (none)
Modem Initialization String:

Setting up customer information

1 Click the Customers tab (Figure 49).

Figure 49 System Properties dialog box—Customers tab

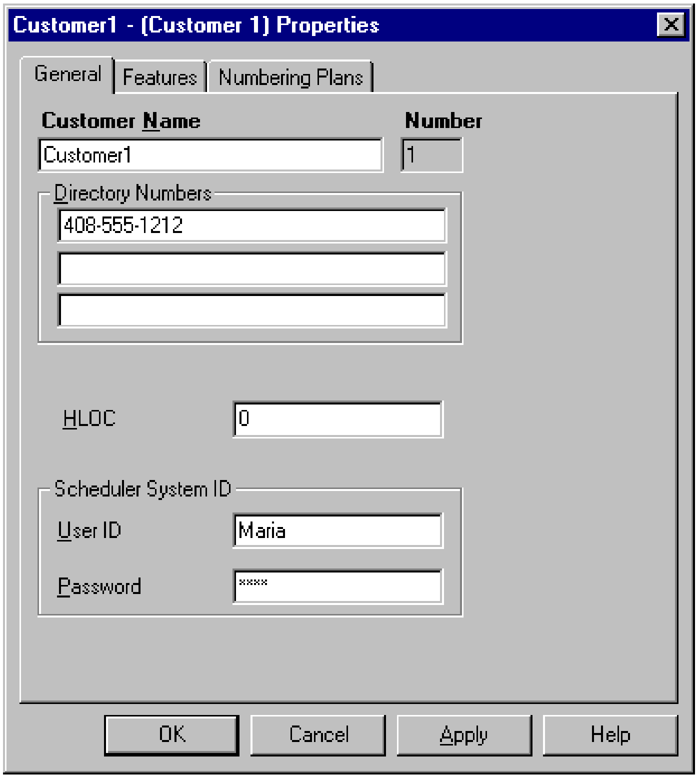


No.	Name
0	Customer0
1	Customer1
2	customer2
3	customer3
4	customer4

2 Click the Properties button.

The Customer Properties dialog box appears with the General tab selected (Figure 50).

Figure 50 Customer Properties dialog box—General tab



Customer1 - (Customer 1) Properties

Customer Name: Customer1

Number: 1

Directory Numbers: 408-555-1212

HLOC: 0

Scheduler System ID

User ID: Maria

Password: ****

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 system, and then click OK.

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

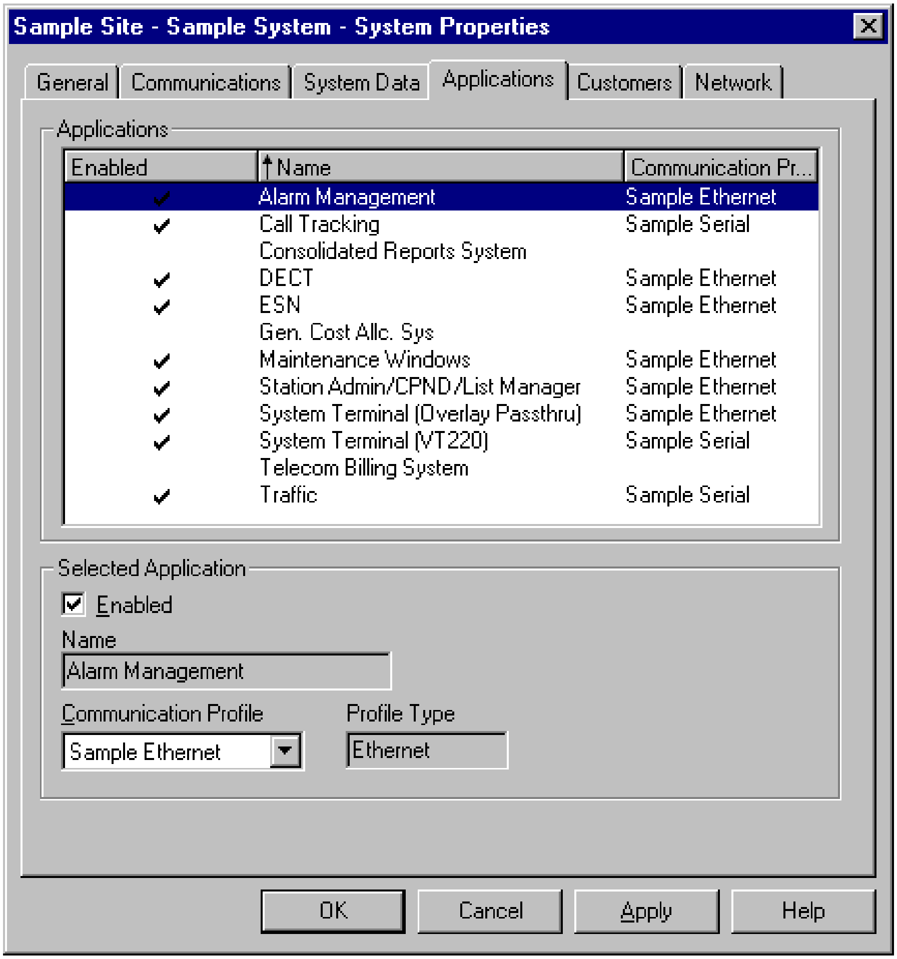
Setting up OTM applications

You must enable applications to make them available in the System window.

1 Click the Applications tab.

The System Properties dialog box—Applications tab appears (Figure 51).

Figure 51 System Properties dialog box—Applications tab



Applications

Enabled	Name	Communication Pr...
✓	Alarm Management	Sample Ethernet
✓	Call Tracking	Sample Serial
	Consolidated Reports System	
✓	DECT	Sample Ethernet
✓	ESN	Sample Ethernet
	Gen. Cost Allc. Sys	
✓	Maintenance Windows	Sample Ethernet
✓	Station Admin/CPND/List Manager	Sample Ethernet
✓	System Terminal (Overlay Passthru)	Sample Ethernet
✓	System Terminal (VT220)	Sample Serial
	Telecom Billing System	
✓	Traffic	Sample Serial

Selected Application

☑ Enabled

Name: Alarm Management

Communication Profile: Sample Ethernet

Profile Type: Ethernet

2 Enable each OTM Windows application:

a Select the application.

b 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 OK.

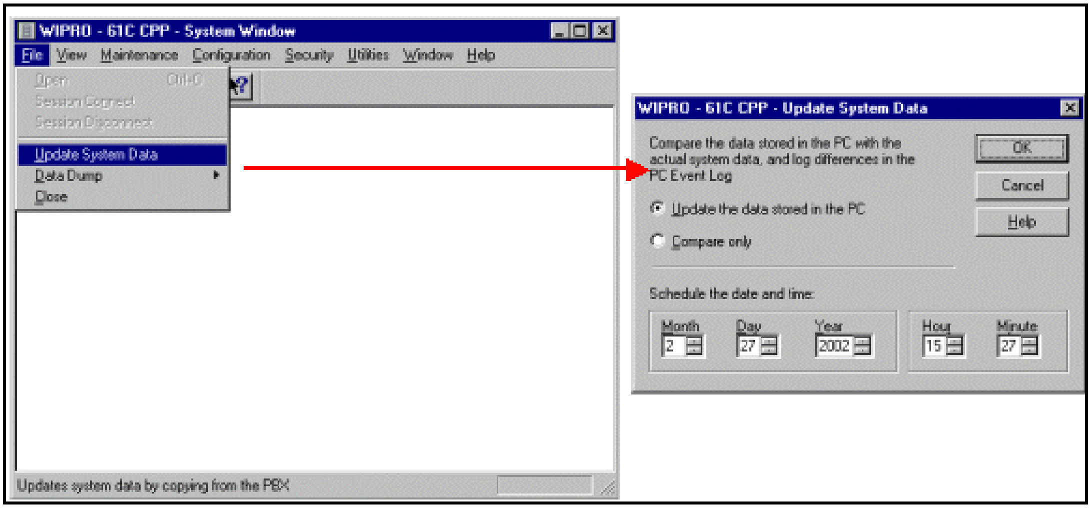
Setting up system data

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.`**

Figure 52 System Update.



Updates system data by copying from the PBX

Compare the data stored in the PC with the actual system data, and log differences in the PC Event Log

● Update the data stored in the PC

○ Compare only

Schedule the date and time:

Month	Day	Year	Hour	Minute
2	27	2002	15	27

4 Click OK.

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

Once the data is copied from the system into OTM, the test procedure is complete.

Configuring Secure Sockets Layer

Configuring Secure Sockets Layer protocol

Configuring Secure Sockets Layer (SSL) protocol on OTM involves:

- Configuring SSL on the OTM server platform
- Enabling SSL for OTM web login
- Setting up LDAP SSL

How SSL works in Internet Information Services (IIS)

To use SSL in Web applications, a Server Certificate must be installed in IIS. For the certificate to become valid, the key-storage file which contains both private and public keys and is password protected must be used. Private and public keys are used by the browser and IIS to negotiate encryption.

Installing a Server Certificate in IIS

OTM Server can be configured to use SSL to protect passwords in network transport during the login sequence. For the SSL transport to become fully operational, an SSL Server Certificate must be installed in IIS. You can obtain your own Server Certificate from a trusted authority (e.g. Verisign) or generate your own certificate using a Certificate Server. This document assumes you have already obtained a Server Certificate and only describes the steps required to install the certificate.

Configuring SSL on the OTM server platform

To install the Certificate from the Internet Services Manager application on a Windows 2000 Server, complete the following procedure:

1 Launch the application from Programs->Administrative Tools->Internet Services Manager.

2 From the left navigator pane, click to select the Default Web Site.

3 Right click on Default Web Site and select Properties.

4 From the Properties window, select the Directory Security tab and click on the Server Certificate button under Secure Communications. The Web Server Certificate Wizard then walks you through the installation of the certificate.

5 After the certificate installation has been completed, go to the Default Web Site Properties window and select the Web Site tab. Make sure the SSL Port is set to 443.

SSL is now available on the server.

Enabling SSL for OTM Web login

To enable SSL for OTM Web login, complete the following procedure:

1 From OTM Navigator (Windows or Web), launch the User Authentication application.

2 Enable the checkbox Use SSL for Web login authentication.

Importing OTM Root Certificate

Enabling SSL for OTM Web login may cause long delays before the login page is displayed. When IIS receives an incoming SSL request from a client, it attempts to build its certificate chain before sending its certificate information back to the client. During this time, if the IIS computer does not have the issuing Certificate

Authority's Root certificate installed locally, it tries to connect to the Certificate Authority directly to obtain it. This causes the server to try and resolve the certificate authority's machine name or fully qualified domain name to an IP address.

If the Certificate Authority (Certificate Server) is inaccessible from the IIS computer, then IIS continues to resolve the Certificate Authority's IP address until it times out. These name resolution queries cause SSL connection delays.

To resolve this, the client can import the OTM Root Certificate into the browser's certificate storage.

To import the OTM Root Certificate into Internet Explorer certificate storage, complete the following procedure:

1 Make the OTM Server Certificate available to the client PC.

2 From Internet Explorer, go to Tools->Internet Options.

3 Select the Content tab and click on Certificates button.

4 Select the Trusted Root Certification Authorities tab.

5 Click on the Import button. The Certificate Import Wizard will then walk you through the import.

Setting up LDAP SSL

To set up LDAP SSL, complete the following procedure:

1 Set up Netscape Communicator 4.79 or above, to trust Certificate Authorities used by LDAP Servers that have SSL enabled.

   If the LDAP Server Certificate is issued by well known Certificate Authorities such as VeriSign etc., the Certificate Authority may already be in the Netscape Communicator certificate database by default.

   a Verify the Certificate Authority is included in Netscape Communicator certificate database. To do this, open the Communicator menu, choose Tools, then Security Info, then click Signers on the left side.

b If the Certificate Authority is not included in the database, please consult your System Administrator for importing a private Certificate Authority.

2 Locate the certificate database files used by the Netscape Communicator:

a From C:\Netscape\userName directory (UserName is the current log-in user name), select cert7.db, key3.db, and secmod.db.

b Copy the three files to the OTM Common Data directory (usually under c:\Nortel\Common Data).

3 Set up the LDAP SSL connection in OTM Server:

a Open OTM Windows Navigator, choose Utilities, then LDAP Setup & Logs.

b Set the port number to be 636 or the specific SSL port number configured by corresponding LDAP Server.

c Check the option "Use SSL for authentication and synchronization".

4 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 *Optivity Telephony Manager: System Administration* (553-3001-330).

Configuring a modem for OTM applications in Windows

This section contains information on:

- Using installation tools
- Installing high-speed modems
- Troubleshooting modem installation

Using installation tools

To ensure 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 automatically searches for and detects a connected modem, and then stores 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 then sets up the Run-Time-Container (RTC) with the modem-initialization string and communication-profile settings for the application to make its connection to the system.

Limitations

You must take into account some limitations with this process when configuring the modems:

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

OTM software always uses the first modem found in the registry configured for the specified COM port in the communications profile. To ensure proper modem operation, configure only one modem or communication device on a given COM port.

- A factory modem-initialization (INIT) string is stored in the Windows registry. OTM applications use this INIT string 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 occurs and the dial-up attempt is aborted. Use the registry editor (regedit) to change the factory INIT string to use verbal (V1) result code. 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 is found during the search and the RTC only contains the communication-profile settings. To correct this problem, use the registry editor (regedit) to add this “AttachedTo” string value of the COM port configured for the PCMCIA modem. See the Microsoft Windows documentation for detailed instructions on how to use the registry editor, or use the instructions below.

Configuring high-speed smart-modems

As modem technology progresses, the new generation of high-speed modems provides 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.

SDI port

The modem configured on the SDI port needs extra attention. In most cases, the modem attached to the SDI port is configured to run in dumb mode at the same speed for which the Meridian 1 or Succession 3.0 SDI port is configured (at 9600 bps or less). This locks the modem into a specific mode of operation, preventing it from being run in command mode (echo input) or from connecting at a different baud rate than is configured for the Meridian 1 or Succession 3.0 SDI port.

Prevent lockup

When a high-speed smart modem is used on the OTM PC to dial up the Meridian 1 or Succession 3.0 modem, the PC modem always attempts to connect at its highest possible speed. The Meridian 1 or Succession 3.0 system's modem, however, can only connect at the configured speed. Therefore, during the modem online handshaking period, the PC modem sends out different tones to negotiate the speed and protocol, and the switch modem connects at its configured speed and ignores additional attempts.

Once the switch modem is connected, any additional handshaking tones sent by PC modem are translated into data (garbage under this condition) and forwarded to Meridian 1 or Succession 3.0 SDI port. These garbage characters may eventually lock up the Meridian 1 or Succession 3.0 port. The two modems may still be connected, but access to the Meridian 1 or Succession 3.0 overlay input is no longer possible.

To avoid this type of problem, the key is to maintain modem compatibility. To avoid potential problems and increase the connection success rate:

- Configure the PC modem to match the switch modem's settings.
- The speed between the Meridian 1 or Succession 3.0 SDI port and Meridian 1 or Succession 3.0 system's modem is locked to the Meridian 1 or Succession 3.0 SDI port's baud rate if a high-speed modem is installed on the 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).

When increasing the value of the S9 register, you may need to do some timing adjustments on some of the modem/buffer equipment scripts.

Troubleshooting modem connections

Here are approaches to the most common troubles.

Modem does not dial

Verify that your modem is configured on the correct COM port:

1. From the Start menu, select Settings > Control Panel.
2. Open the Modems file and click Properties.

Test the COM port to which your modem is connected by launching HyperTerminal:

1. From the Start menu, select Programs > Accessories > HyperTerminal.

   HyperTerminal prompts you for a connection name and presents you with the phone number dialog box.
2. 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.
3. Once you are in the terminal, type the command AT.

   The modem should respond with OK.

If your modem does not respond, you may be using the wrong COM port. To verify that you are using the correct COM port:

1. In the File/Properties menu, select Direct to COM *Y,* where *Y* is a different COM port.
2. 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.
3. Click the communication tab, and then select PPP or Serial from the communication profile list.

4 Verify that the COM port you selected for this profile is the COM port on which you located your modem using HyperTerminal.

5 Verify that the baud rate matches the settings for the Meridian 1 or Succession 3.0 port into which you will dial.

If the modem still does not dial:

1 Follow the steps in the procedure "Test the COM port to which your modem is connected by launching HyperTerminal:" on page 116 to establish a HyperTerminal connection.

2 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 3.0 system.

3 Listen to determine whether the modem dials and connects:

   a If you do not hear the modem dialing and connecting at this point, verify that your phone line and modem cables are connected correctly.

   b If the modem dials and connects, verify that you have dial-up networking installed along with a dial-up-adapter.

Scripting fails

In this scenario, the modem dials and connects but the Connection Details button reveals that scripting failed while waiting for a prompt.

In the Communications profile, 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:

   a Right-click on the desired system in the Navigator window.

   b Select Properties from the pop-up menu, and then click the Communications tab in the Properties dialog box.

Modem dials but does not connect

1 Verify that the phone number you are dialing is not busy.

2 Verify that you have included all necessary digits in the phone number.

3 Check the PPP or Serial Communications profiles for the system to which you wish to connect.

To view the Communications profiles for a system:

a Right-click on the desired system in the Navigator window.

b Select Properties from the pop-up menu, and then click the Communications tab in the Properties dialog box.

Session fails

In this scenario, the modem dials and connects and the scripting is completed successfully, but the Connection Details button reveals that the session failed.

1 Verify that the IP address that you assigned to the local PPP interface on the Meridian 1 or the Succession3.0 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:

a Right-click on the desired system in the Navigator window.

b Select Properties from the pop up menu, and then click the Communications tab in the Properties dialog box.

2 If possible, verify that you can make an Ethernet connection to the same system:

a After establishing a PPP connection, but before canceling the connection dialog, open a DOS command prompt: From the Start menu select Programs > MS-DOS Prompt.

b Run the ping command by typing **`ping`** ***`47.1.1.10`*** where ***`47.1.1.10`*** is the Meridian 1 or Succession 3.0 system's local IP address. See "Setting up the Meridian 1 or Succession system" on page 215 for information on configuring Ethernet and PPP on the Meridian 1 or Succession 3.0 system.

c Verify that the data lights on your modem flash as the ping data is sent to the Meridian 1 or Succession 3.0 system.

If you do not receive a response from the Meridian 1 or Succession 3.0 system, verify that the IP address is the same as the one that you assigned to the local PPP interface on the Meridian 1 or Succession 3.0 system. To verify the IP address, go to the System Properties—Communication, PPP Connection Type dialog box, and confirm that the IP address that appears in the address field is correct.

COM port error

In this scenario, the modem dials and connects but you receive the error message “Error writing to COM port” or “Error reading from COM port”.

1 Verify that the modem you installed in the Control Panel matches your modem type.

2 Remove your installed modem driver and install a generic modem driver in its place:

a From the Start menu, select Settings > Control Panel.

b Double-click Modems.

c Click the Remove button to remove your modem from the installed list.

d Click Add to add a new modem driver.

e Click the check box that says “Don’t detect my modem; I will select it from a list”, and then click Next.

f Select the standard modem driver matching your modem’s baud rate (for example, Standard 28 800 bps Modem), and then click Next.

g Select the COM port to which your modem is connected, and then click Next.

h Click Finish to complete the modem installation.

i Restart the system, and try to establish a PPP or Serial connection.

Initial login

Windows NT and Windows 2000 users are authenticated using either a local account on the OTM Server, a Windows domain account, or LDAP. There is no default Login Name and Password for these systems.

Any user account (for example, Administrator) that is a member of the local Administrators group will always be able to log in to OTM. In a new OTM installation, use any local Administrators group account for your initial log in.

After logging in to OTM for the first time, you can set up additional users and user groups. To add user groups, select Security > User Groups from the OTM Navigator window, and then select Configuration > Add User Group... from the User Groups window. See “Creating a user group” on page 186 for detailed instructions on adding OTM user groups. To add users, select Security > Users from the OTM Navigator window, and then select Configuration > Add User... from the OTM Users window. See “Adding a user” on page 188 for detailed instructions on adding OTM users.

Users that are not created from within OTM do not appear in the OTM Users window.

Testing the connection

Use the following procedures to test the connection between OTM and your equipment. For detailed instructions on adding sites and systems, see "Once the data is copied from the system into OTM, the test procedure is complete." on page 131.

ELAN required

The Embedded LAN (ELAN) must be configured and devices must be connected to the ELAN before you can test the connection.

Setting up communications information

1 Double-click Sample Site in the OTM Navigator window.

2 Click Sample System, and then choose File > Properties.

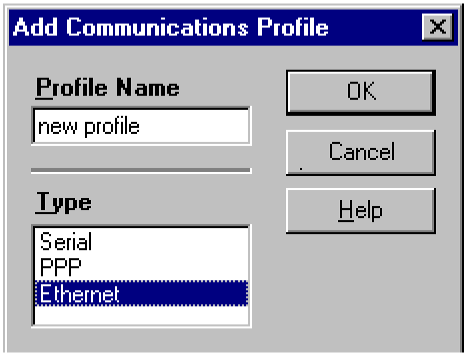
The System Properties dialog box appears with the General tab selected.

3 Click the Communications tab.

4 Click Add.

The Add Communications Profile dialog box appears (Figure 53).

Figure 53 Add Communications Profile dialog box



Add Communications Profile

Profile Name: new profile

Type: Serial, PPP, Ethernet (Ethernet selected)

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

6 Enter a Profile Name.

7 Click OK.

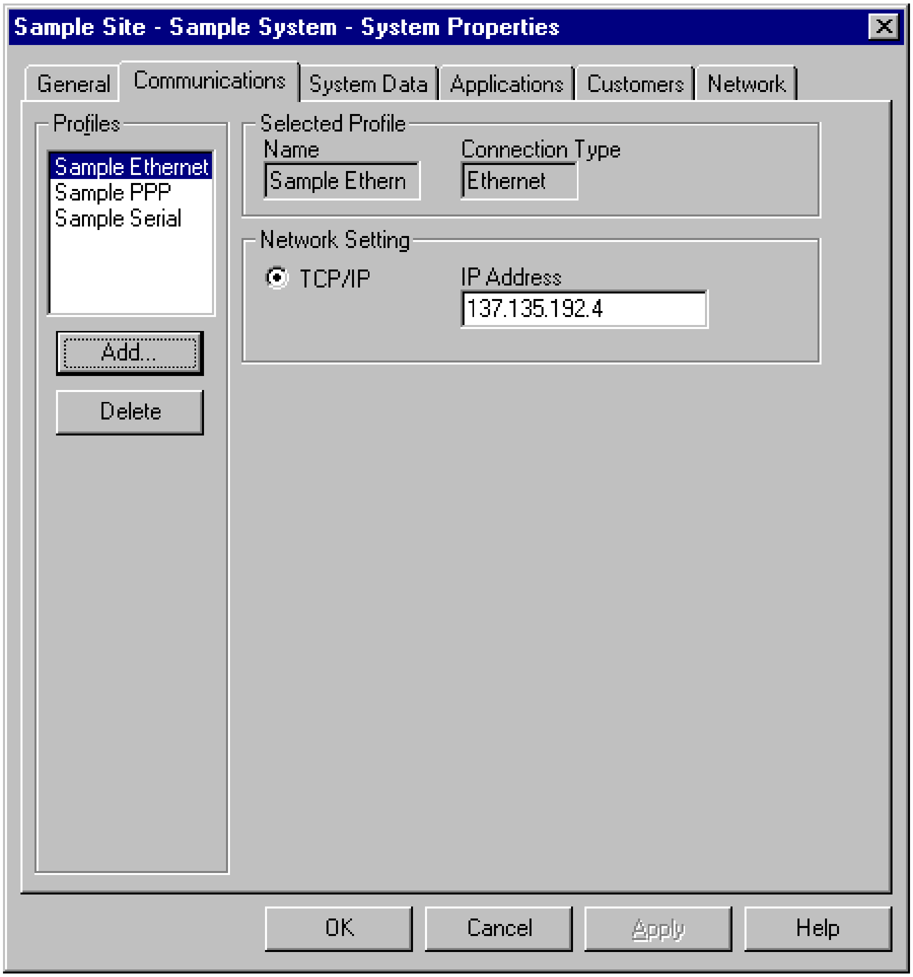
8 Enter the information in the System Properties—Communications dialog box for the connection type selected in step 5.

For an Ethernet connection type (Figure 54):

a Enter the IP address that you configured on the Meridian 1 or Succession 3.0 system.

b Click Apply.

Figure 54 System Properties dialog box—Communications tab—Ethernet Profile



Sample Site - Sample System - System Properties

General | Communications | System Data | Applications | Customers | Network

Profiles: Sample Ethernet, Sample PPP, Sample Serial

Selected Profile
Name: Sample Ethern
Connection Type: Ethernet

Network Setting
● TCP/IP
IP Address: 137.135.192.4

For a PPP connection type (Figure 55):

a Enter all modem parameters and dial-up information.

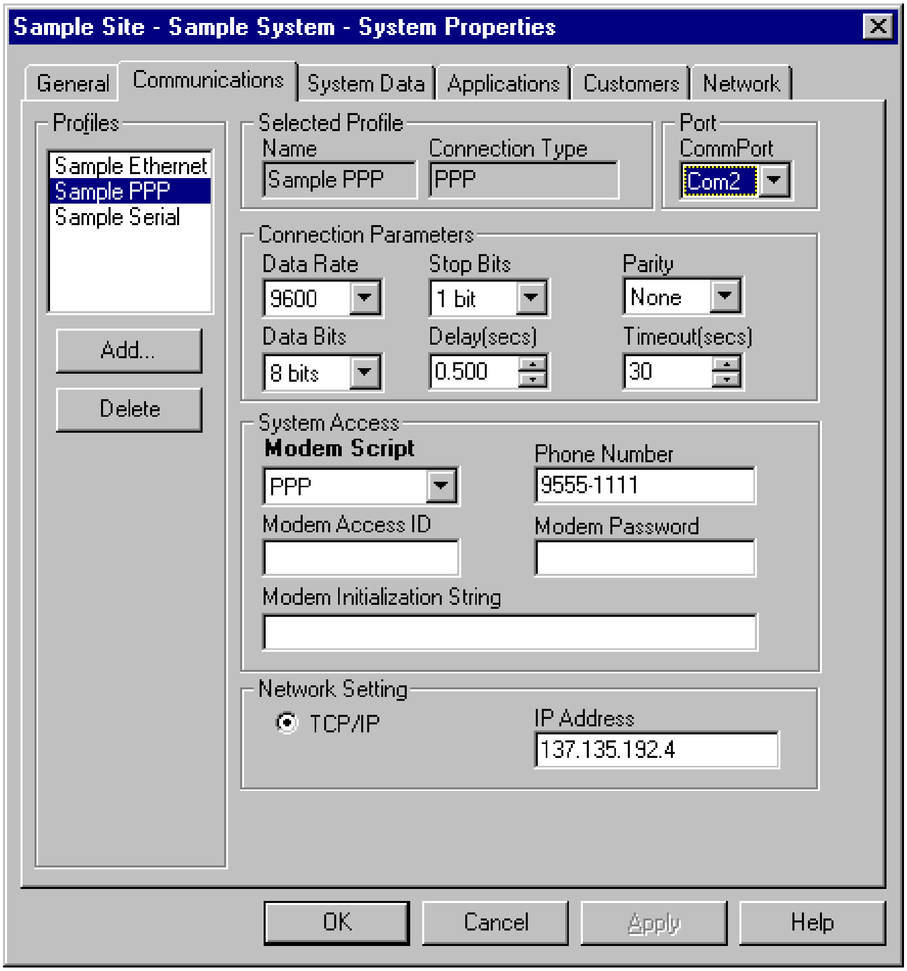
b Select PPP in the Modem Script text box and enter the phone number.

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 initialization string.

c Set the IP address to the local IP address, as configured on the Meridian 1 or Succession 3.0 system.

d Click Apply.

Figure 55 System Properties dialog box—Communications tab—PPP Profile



Sample Site - Sample System - System Properties

General | Communications | System Data | Applications | Customers | Network

Profiles: Sample Ethernet, Sample PPP, Sample Serial

Add... Delete

Selected Profile — Name: Sample PPP; Connection Type: PPP

Port — CommPort: Com2

Connection Parameters — Data Rate: 9600; Stop Bits: 1 bit; Parity: None; Data Bits: 8 bits; Delay(secs): 0.500; Timeout(secs): 30

System Access — **Modem Script**: PPP; Phone Number: 9555-1111; Modem Access ID: ; Modem Password: ; Modem Initialization String:

Network Setting — ● TCP/IP; IP Address: 137.135.192.4

OK | Cancel | Apply | Help

For a Serial connection type (Figure 56):

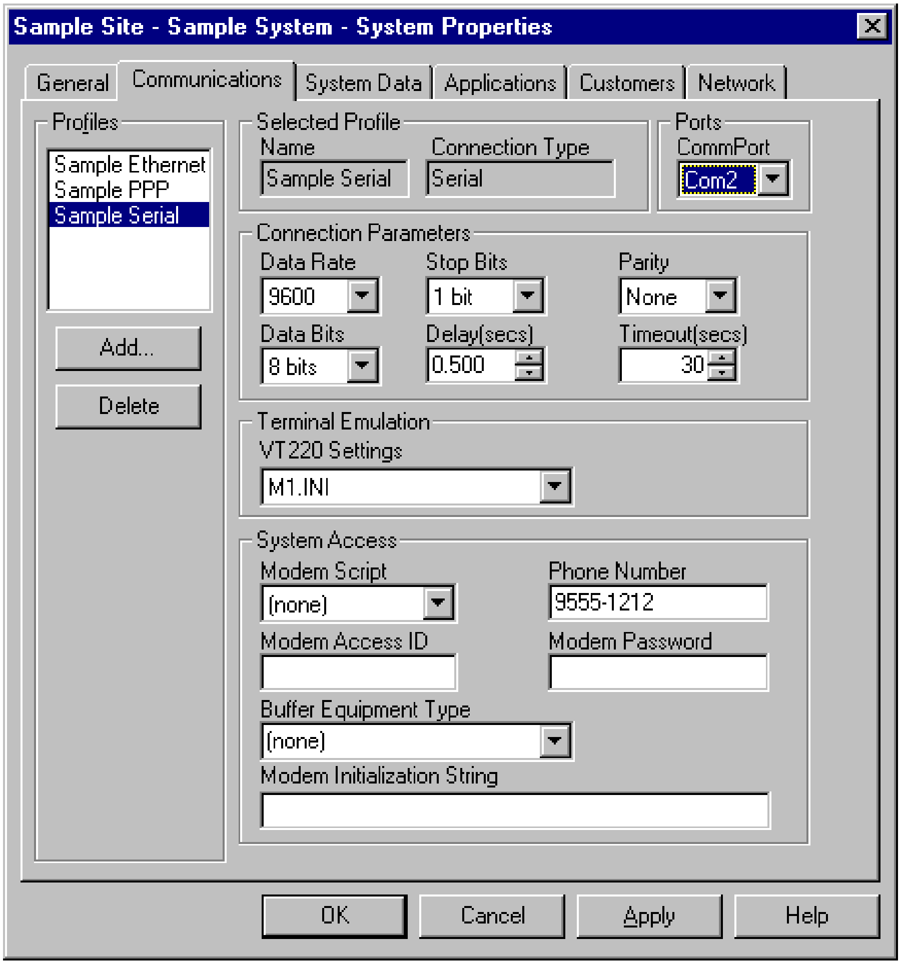
a Enter all modem parameters and dial-up information.

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

This is commonly “None” unless a specific value is defined for your system.

c Click Apply.

Figure 56 System Properties dialog box—Communications tab—Serial Profile



Sample Site - Sample System - System Properties

Profiles

- Sample Ethernet
- Sample PPP
- Sample Serial

Selected Profile

Name: Sample Serial

Connection Type: Serial

Ports

CommPort: Com2

Connection Parameters

Data Rate: 9600

Stop Bits: 1 bit

Parity: None

Data Bits: 8 bits

Delay(secs): 0.500

Timeout(secs): 30

Terminal Emulation

VT220 Settings: M1.INI

System Access

Modem Script: (none)

Phone Number: 9555-1212

Modem Access ID:

Modem Password:

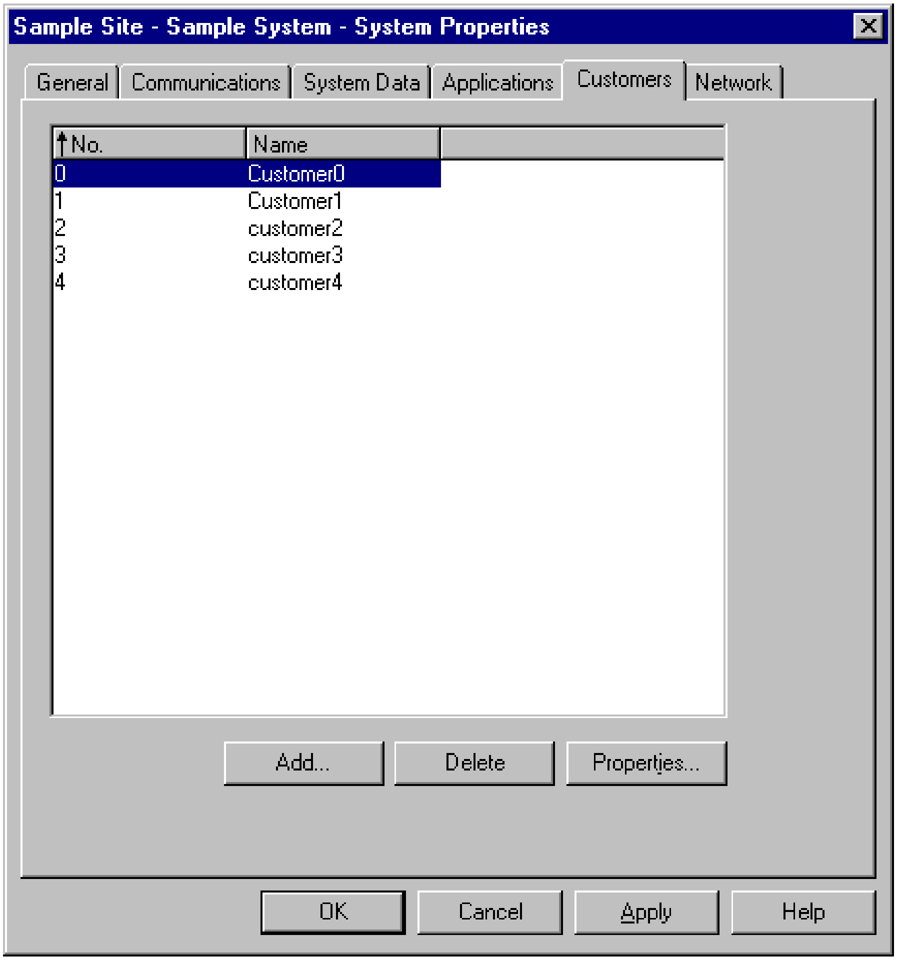
Buffer Equipment Type: (none)

Modem Initialization String:

Setting up customer information

1 Click the Customers tab (Figure 57).

Figure 57 System Properties dialog box—Customers tab

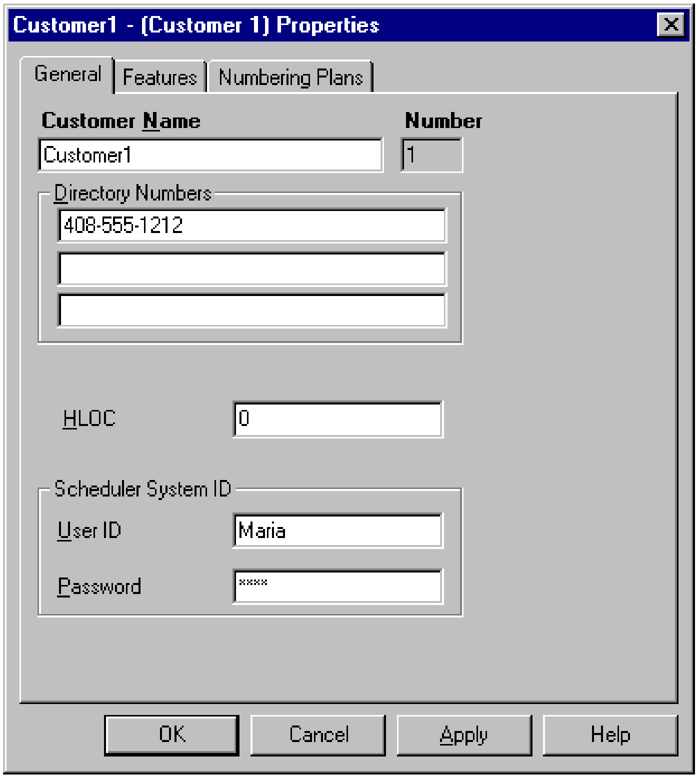


No.	Name
0	Customer0
1	Customer1
2	customer2
3	customer3
4	customer4

2 Click the Properties button.

The Customer Properties dialog box appears with the General tab selected (Figure 58).

Figure 58 Customer Properties dialog box—General tab



Customer1 - (Customer 1) Properties

Customer Name: Customer1

Number: 1

Directory Numbers: 408-555-1212

HLOC: 0

Scheduler System ID

User ID: Maria

Password: ****

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 system, and then click OK.

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

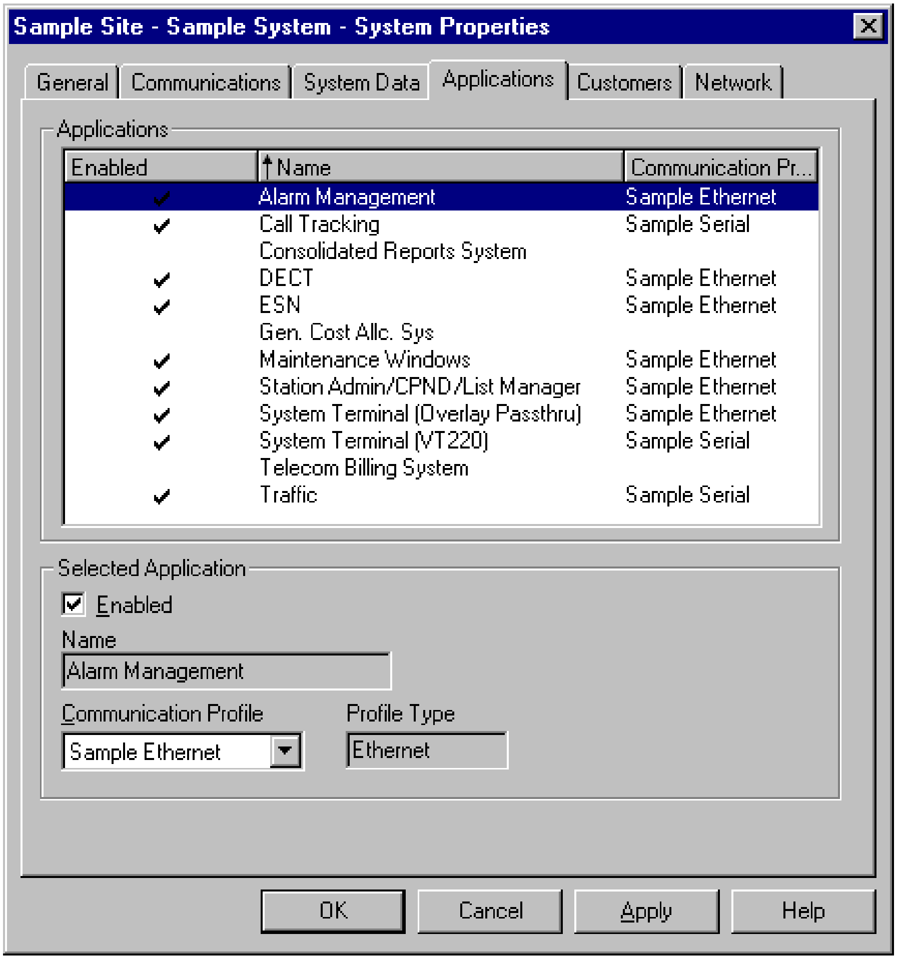
Setting up OTM applications

You must enable applications to make them available in the System window.

1 Click the Applications tab.

The System Properties dialog box—Applications tab appears (Figure 59).

Figure 59 System Properties dialog box—Applications tab



Sample Site - Sample System - System Properties

Applications

Enabled	Name	Communication Pr...
✓	Alarm Management	Sample Ethernet
✓	Call Tracking	Sample Serial
	Consolidated Reports System	
✓	DECT	Sample Ethernet
✓	ESN	Sample Ethernet
	Gen. Cost Allc. Sys	
✓	Maintenance Windows	Sample Ethernet
✓	Station Admin/CPND/List Manager	Sample Ethernet
✓	System Terminal (Overlay Passthru)	Sample Ethernet
✓	System Terminal (VT220)	Sample Serial
	Telecom Billing System	
✓	Traffic	Sample Serial

Selected Application

☑ Enabled

Name: Alarm Management

Communication Profile: Sample Ethernet

Profile Type: Ethernet

2 Enable each OTM Windows application:

   a Select the application.

   b 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 OK.

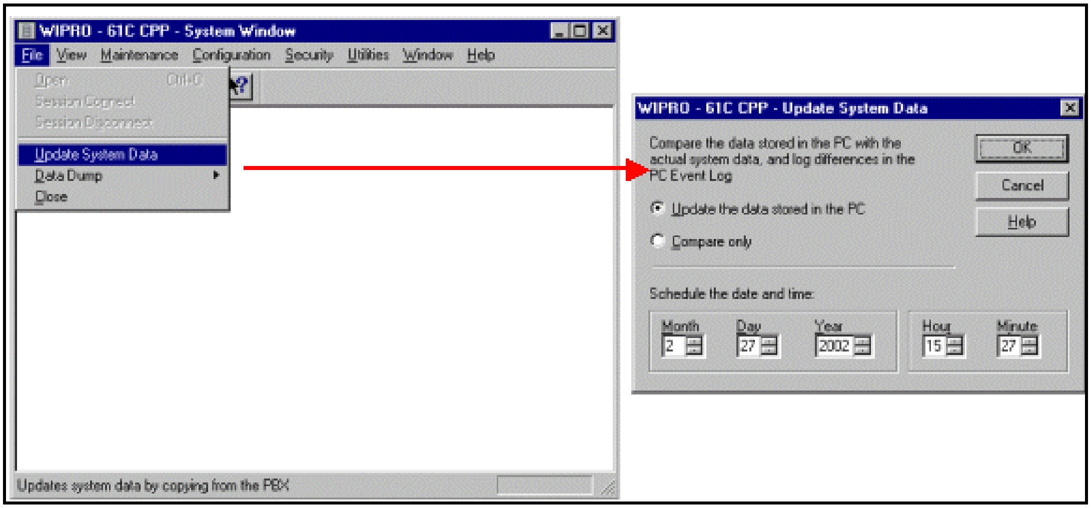
Setting up system data

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.`**

Figure 60 System Update.



Compare the data stored in the PC with the actual system data, and log differences in the PC Event Log

● Update the data stored in the PC

○ Compare only

Schedule the date and time:

Month 2 Day 27 Year 2002 Hour 15 Minute 27

Updates system data by copying from the PBX

4 Click OK.

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

Once the data is copied from the system into OTM, the test procedure is complete.

Adding sites and systems via the OTM Navigator window

This section contains information on adding:

- Sites
- Meridian 1 or Succession CSE 1000 Release 1.x systems
- Succession systems
- Generic systems or devices

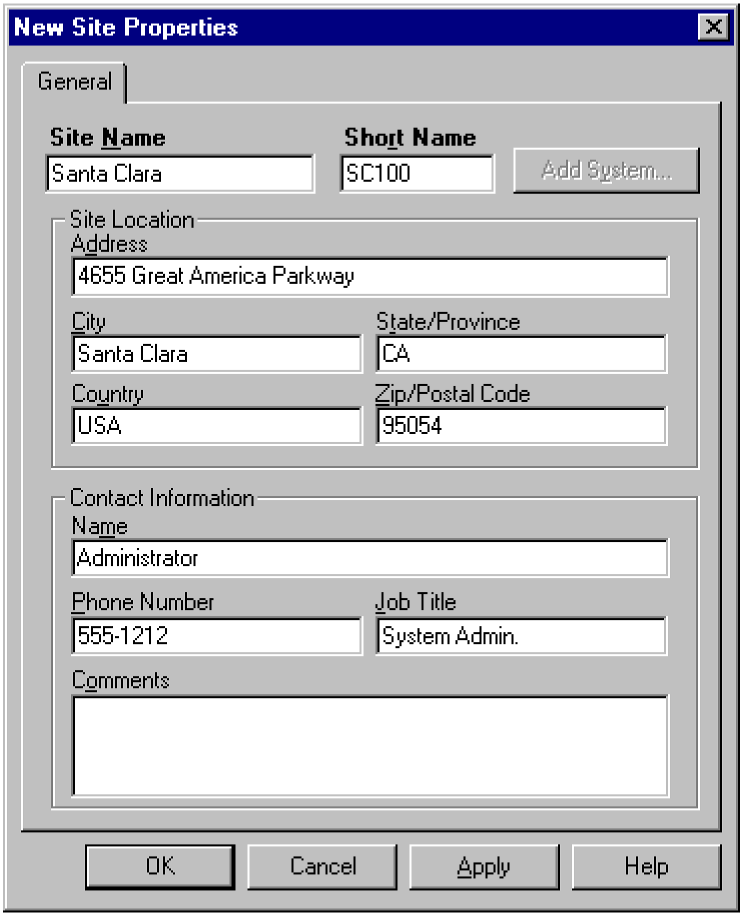
Adding a site

You can add up to 3000 sites to the OTM Navigator window.

1 In the OTM Navigator window, choose Configuration > Add Site.

The New Site Properties dialog box appears (Figure 61).

Figure 61 New Site Properties dialog box



New Site Properties

General

Site Name: Santa Clara

Short Name: SC100

Site Location

Address: 4655 Great America Parkway

City: Santa Clara

State/Province: CA

Country: USA

Zip/Postal Code: 95054

Contact Information

Name: Administrator

Phone Number: 555-1212

Job Title: System Admin.

Comments:

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

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

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

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

5 To add a new system to this site:

a Click Add System.

b Follow the instructions for "Adding a Meridian 1 or Successon CSE 1000 Release 1.x system" on page 135, "Adding a Succession system" on page 153, or "Adding a Generic system or device" on page 180.

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

- OK adds the site and closes the property sheet.
- Apply adds the site and leaves the property sheet open allowing you to add another system to this site. Repeat step 5 to add another system.
- Cancel closes the dialog box without adding the site.

Adding a Meridian 1 or Successon CSE 1000 Release 1.x system

You can add up to 256 systems (including non-Meridian 1 systems) to a site. You must have administrator privileges to add a system.

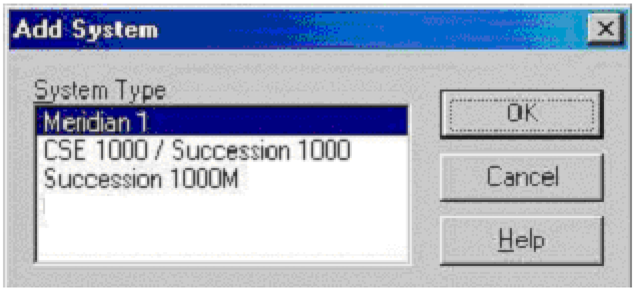
1 In the Navigator window, select the desired site.

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

2 Choose Configuration > Add System or use the right mouse button pop-up menu.

The Add System dialog box appears (Figure 62).

Figure 62 Add System dialog box—Meridian 1



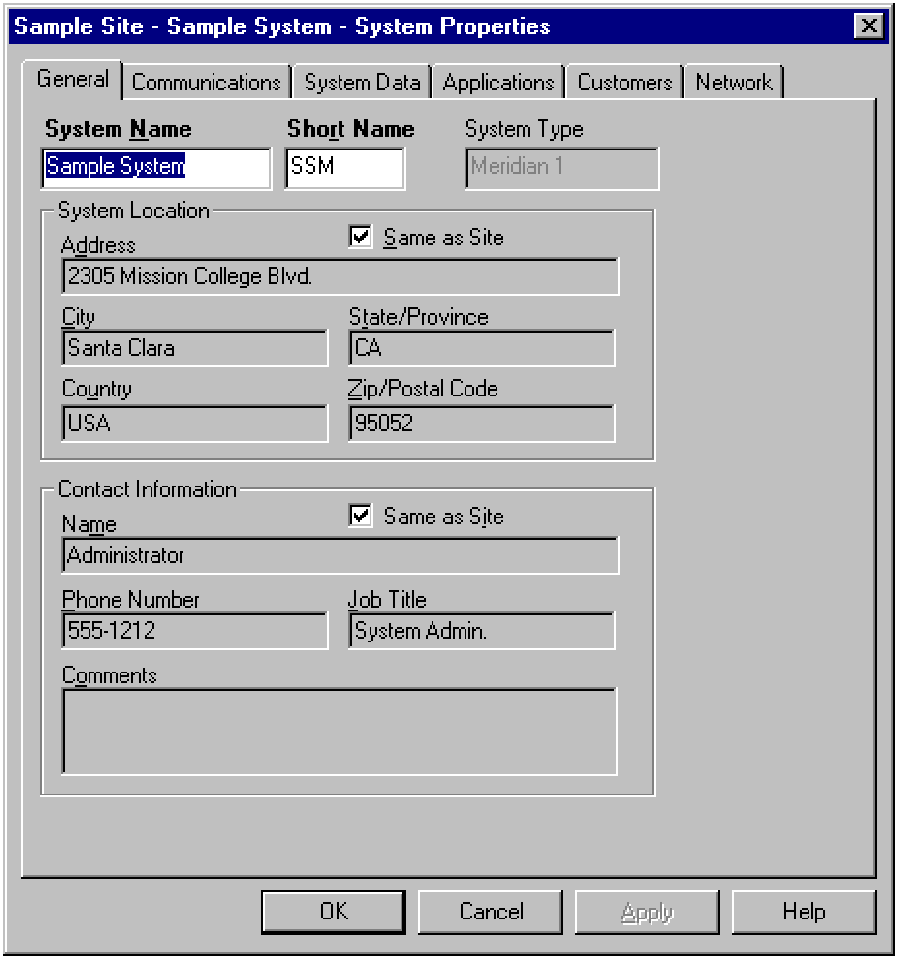
3 In the Add System dialog box, select Meridian 1 and click OK

You must select Meridian 1 as the system type for Succession systems prior to Succession CSE 1000 Release 2.0.

You may need to install additional software to enable other system types not listed in Figure 62. Follow the installation instructions included with your order.

4 The System Properties dialog box appears with the General tab selected (Figure 63).

Figure 63 System Properties dialog box—General tab



Sample Site - Sample System - System Properties

System Name: Sample System

Short Name: SSM

System Type: Meridian 1

System Location

☑ Same as Site

Address: 2305 Mission College Blvd.

City: Santa Clara

State/Province: CA

Country: USA

Zip/Postal Code: 95052

Contact Information

☑ Same as Site

Name: Administrator

Phone Number: 555-1212

Job Title: System Admin.

Comments:

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

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

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.

6 To add a new communications profile, click the System Properties dialog box—Communications tab.

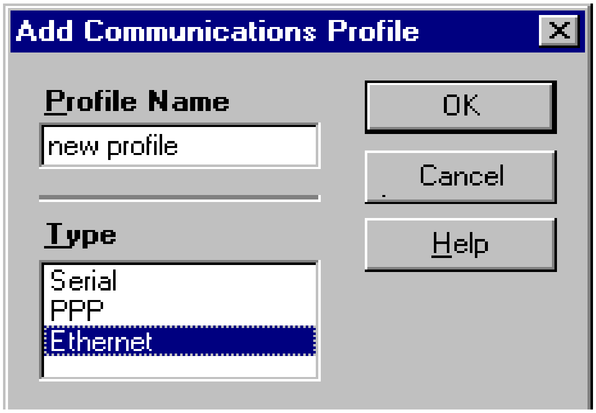
This tab defines the types of communications profiles that may be applied to system applications (one profile may be used for multiple applications).

OTM is shipped with a default communication profile. The Default profile is an Ethernet profile, and it cannot be deleted.

Click Add.

The Add Communications Profile dialog box appears (Figure 64).

Figure 64 Add Communications Profile dialog box



Add Communications Profile

Profile Name: new profile

Type:
- Serial
- PPP
- Ethernet (selected)

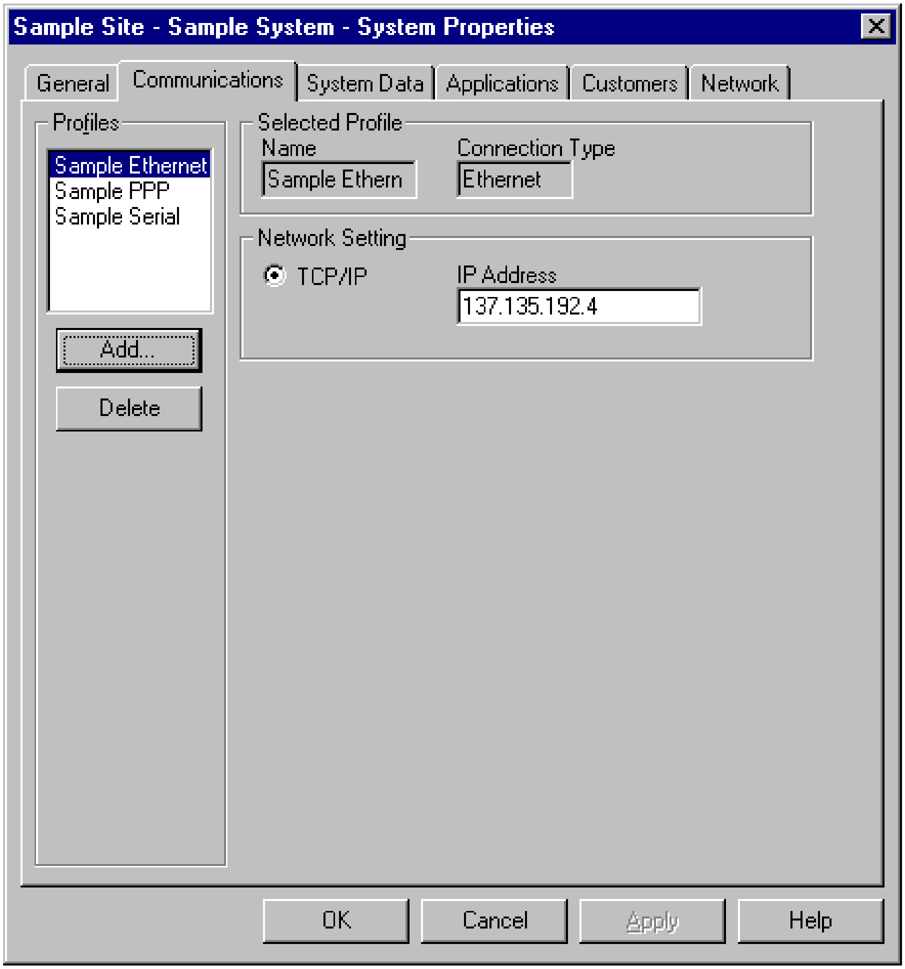
Select a communications type from the Type box and enter a Profile Name. Then click OK to go back to the Communications tab.

7 Fill in the communications information for the new profile:

- For Ethernet (Figure 65):
  - — Select the appropriate network protocol.
  - — Enter the IP address that you configured on the Meridian 1 or Succession CSE 1000 system.

— Click Apply.

Figure 65 System Properties dialog box—Communications tab—Ethernet Profile



Sample Site - Sample System - System Properties

Profiles: Sample Ethernet, Sample PPP, Sample Serial

Selected Profile

Name: Sample Ethern

Connection Type: Ethernet

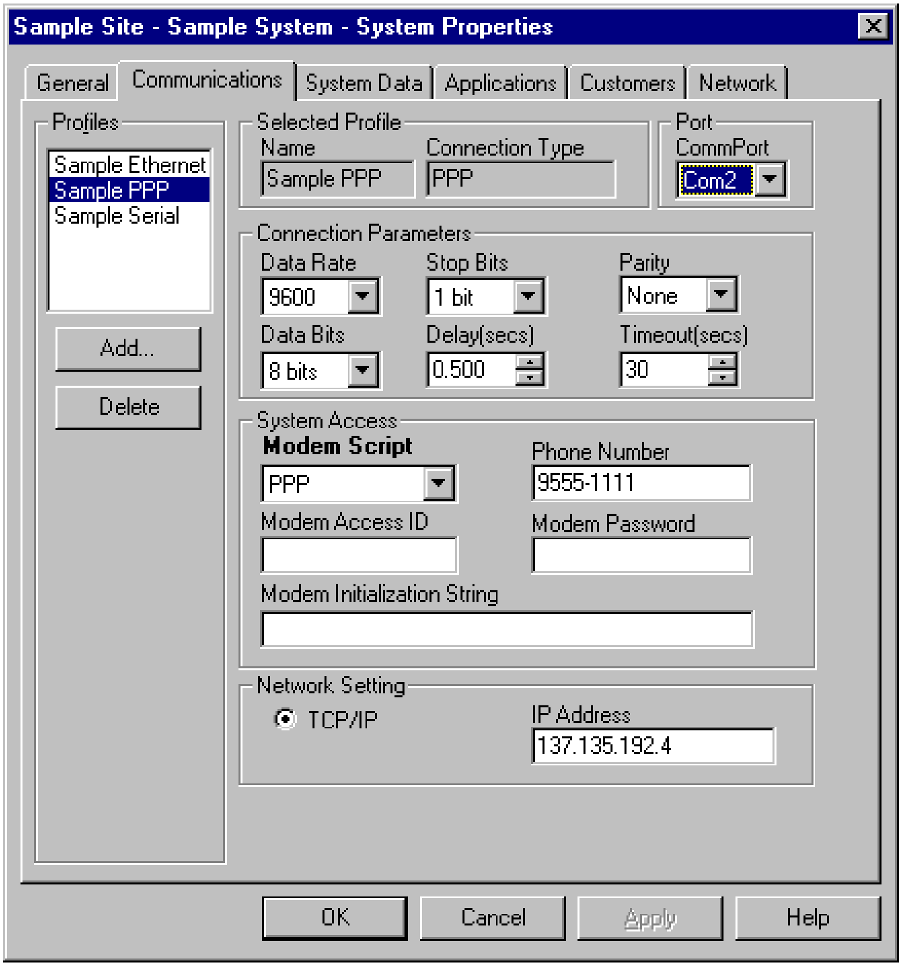
Network Setting

● TCP/IP

IP Address: 137.135.192.4

- For PPP (Figure 66):
  - — Enter all modem parameters and dialup information.
  - — Select PPP in the Modem Script text box.
  - — Set the IP address to the local IP address, as configured on the Meridian 1 or Succession CSE 1000 system.
  - — Click Apply.

Figure 66 System Properties dialog box—Communications tab—PPP Profile



Sample Site - Sample System - System Properties

Profiles: Sample Ethernet, Sample PPP, Sample Serial

Selected Profile
Name: Sample PPP
Connection Type: PPP

Port
CommPort: Com2

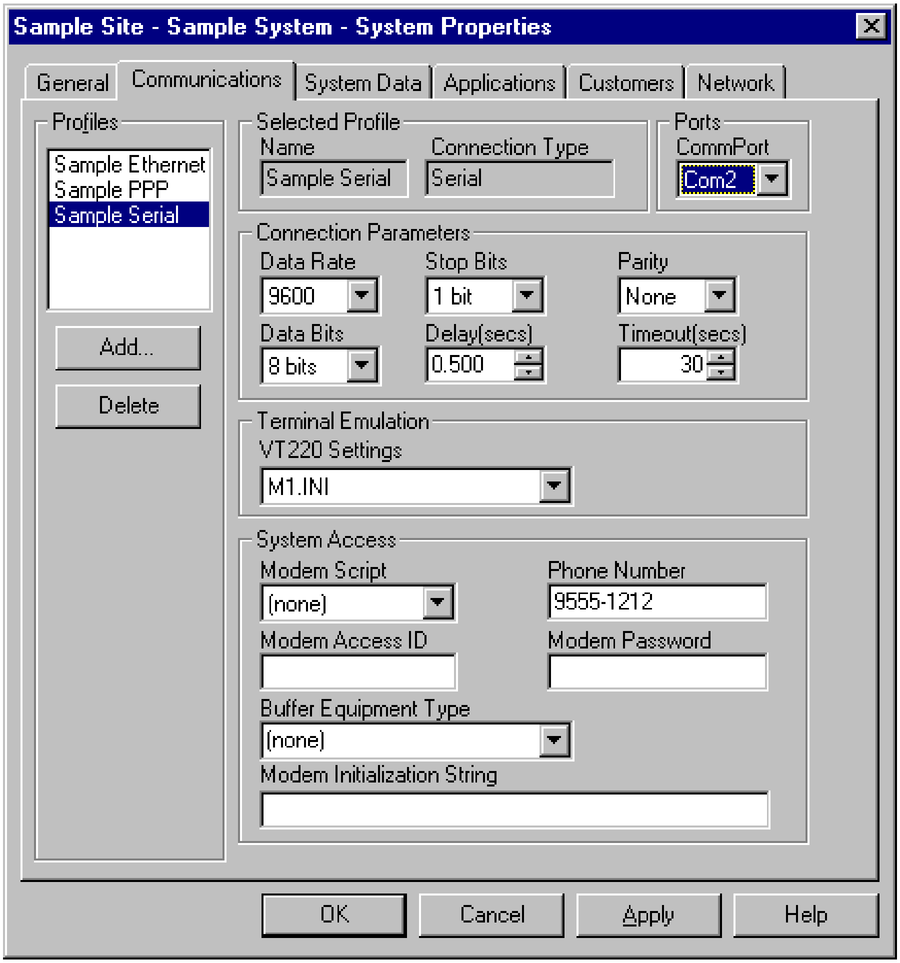
Connection Parameters
Data Rate: 9600
Stop Bits: 1 bit
Parity: None
Data Bits: 8 bits
Delay(secs): 0.500
Timeout(secs): 30

System Access
Modem Script: PPP
Phone Number: 9555-1111
Modem Access ID:
Modem Password:
Modem Initialization String:

Network Setting
● TCP/IP
IP Address: 137.135.192.4

- For Serial (Figure 67):
  - — Enter all modem parameters and dial-up information.
  - — Select the appropriate value in the Modem Script drop-down box. This is usually None unless a specific value is defined for your system.
  - — Click Apply.

Figure 67 System Properties dialog box—Communications tab—Serial Profile



Sample Site - Sample System - System Properties

Profiles: Sample Ethernet, Sample PPP, Sample Serial

Selected Profile — Name: Sample Serial; Connection Type: Serial

Ports — CommPort: Com2

Connection Parameters — Data Rate: 9600; Stop Bits: 1 bit; Parity: None; Data Bits: 8 bits; Delay(secs): 0.500; Timeout(secs): 30

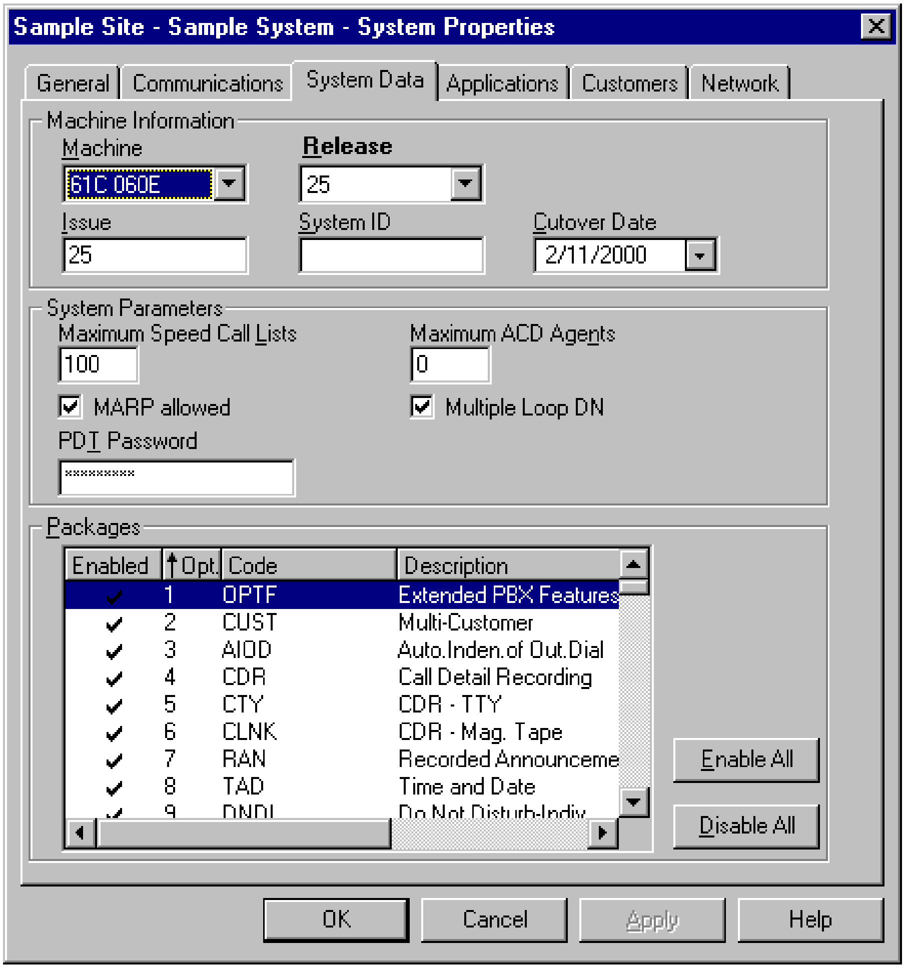
Terminal Emulation — VT220 Settings: M1.INI

System Access — Modem Script: (none); Phone Number: 9555-1212; Modem Access ID: ; Modem Password: ; Buffer Equipment Type: (none); Modem Initialization String:

8 Enter the system data. Click the System Data tab.

The System Properties dialog box—System Data tab appears (Figure 68). Enter the machine or system type and release version for the system, and enable or disable feature packages. For example, if your Meridian 1 is an Option 61C running X11 Release 25.25 software, use the drop-down boxes to select 61C in the Machine field and 25 in the Release field, and enter **25** in the Issue field.

Figure 68 System Properties dialog box—System Data tab



Sample Site - Sample System - System Properties

Machine Information

Machine: 61C 060E

Release: 25

Issue: 25

System ID:

Cutover Date: 2/11/2000

System Parameters

Maximum Speed Call Lists: 100

Maximum ACD Agents: 0

☑ MARP allowed

☑ Multiple Loop DN

PDT Password: *********

Packages

Enabled	Opt.	Code	Description
✓	1	OPTF	Extended PBX Features
✓	2	CUST	Multi-Customer
✓	3	AIOD	Auto.Inden.of Out.Dial
✓	4	CDR	Call Detail Recording
✓	5	CTY	CDR - TTY
✓	6	CLNK	CDR - Mag. Tape
✓	7	RAN	Recorded Announceme
✓	8	TAD	Time and Date
✓	9	DNDI	Do Not Disturb-Indiv.

For a Succession CSE 1000 Release 1.x system, select 11C as the machine type. Early versions of these systems are configured as Meridian 1 Option 11C systems, and their Media Gateways are configured as Survivable IP Expansion (SIPE) Cabinets.

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

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.

When you have finished entering the information in the System Data tab, click Apply.

9 Click the Applications tab.

The System Properties dialog box—Applications tab appears (Figure 69).

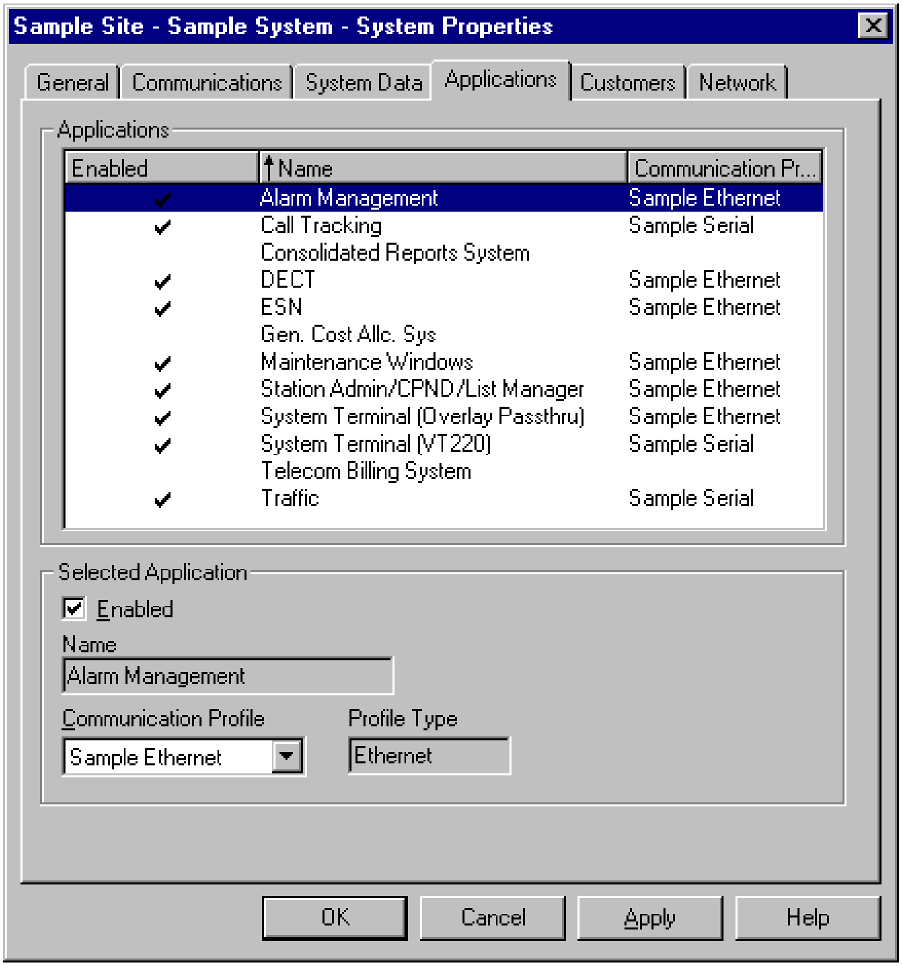
This tab defines the OTM applications that will appear in the System window and the communications profile to be used with each application.

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

Communication profile settings are defined on a site/system basis and are shared by the OTM Server and its Clients. Consequently, if you define a serial communication profile for the Station Administration application, then the OTM Server and OTM Client PCs must have a physical serial connection to the system. An OTM Client PC cannot use the COM ports of the OTM Server. Any communication task uses the resources of the PC on which it is running.

10 Enable or disable applications.

Figure 69 System Properties dialog box—Applications tab



Sample Site - Sample System - System Properties

Applications

Enabled	Name	Communication Pr...
✓	Alarm Management	Sample Ethernet
✓	Call Tracking	Sample Serial
	Consolidated Reports System	
✓	DECT	Sample Ethernet
✓	ESN	Sample Ethernet
	Gen. Cost Allc. Sys	
✓	Maintenance Windows	Sample Ethernet
✓	Station Admin/CPND/List Manager	Sample Ethernet
✓	System Terminal (Overlay Passthru)	Sample Ethernet
✓	System Terminal (VT220)	Sample Serial
	Telecom Billing System	
✓	Traffic	Sample Serial

Selected Application

☑ Enabled

Name: Alarm Management

Communication Profile: Sample Ethernet

Profile Type: Ethernet

To enable:

a Select the application in the Applications tab dialog box.

b Select a Communications 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:

a Select the application in the Applications tab dialog box.

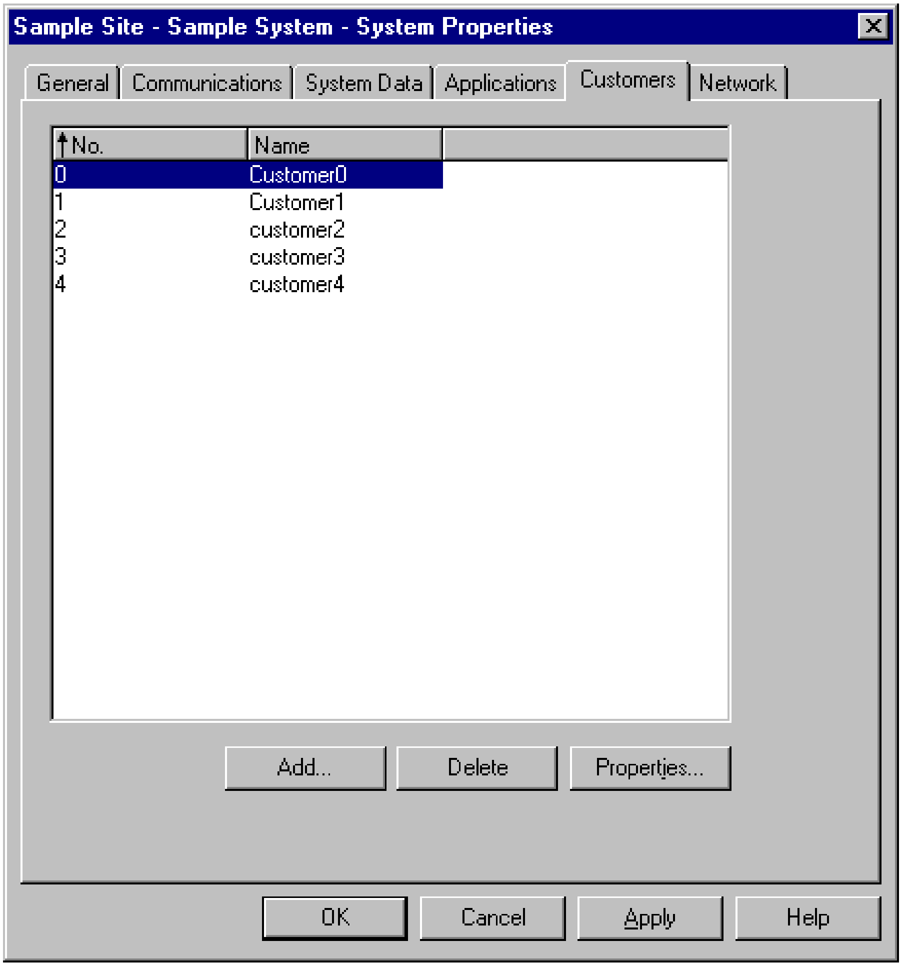
b In the Selected Application box, click the "Enabled" check box to remove the check mark.

When you have finished entering the information in the Applications tab, click Apply.

11 Click the Customers tab.

The System Properties dialog box—Customers tab appears (Figure 70).

Figure 70 System Properties dialog box—Customers tab



Sample Site - Sample System - System Properties

No.	Name
0	Customer0
1	Customer1
2	customer2
3	customer3
4	customer4

This tab lists the customers currently defined for this Meridian 1 system. You can add new customers, delete customers, or review the properties of a selected customer. When you add a new customer, you configure the Meridian 1 features and numbering plans that are available to the customer. This information is not automatically updated on the Meridian 1 system and must be updated by using the LD 15 customer overlay. LD 15 is the overlay interface that allows customers to configure their systems on the Meridian 1. For more information on overlay interfaces, see the System online Help.

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

12 To add a customer:

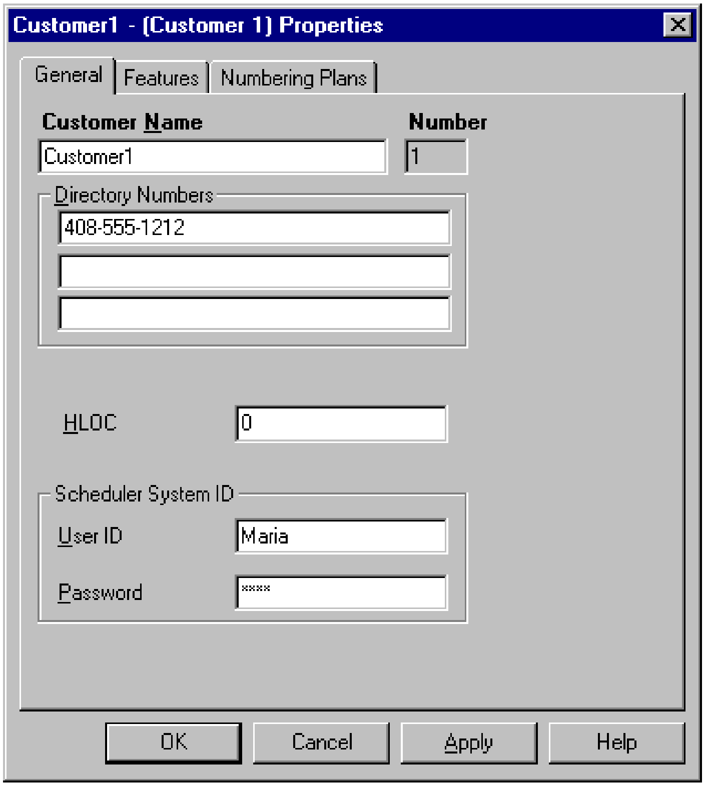
a Click Add in the System Properties dialog box—Customers tab.

b Select a Customer number.

c Click OK.

The Customer Properties dialog box appears with the General tab selected (Figure 71).

Figure 71 Customer Properties dialog box—General tab



Customer Name: Customer1

Number: 1

Directory Numbers: 408-555-1212

HLOC: 0

User ID: Maria

Password: ****

d Fill in the general information for the customer

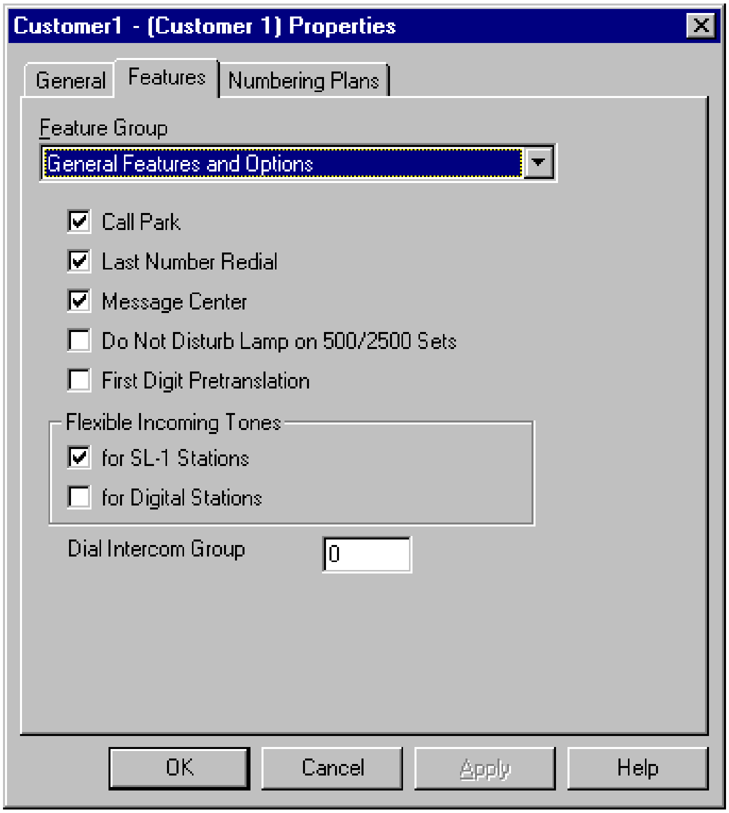
You can copy this data directly from an installed switch by scheduling an upload using File > Update System Data in the System window. Update System Data uses the communication profile for station administration. However, you should configure the release number here first to allow available applications to show up properly in the Applications tab.

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 Analysis.

e Click the Features tab.

The Features dialog box appears (Figure 72).

Figure 72 Customer Properties dialog box—Features tab


Customer1 - [Customer 1] Properties

Feature Group: General Features and Options

☑ Call Park

☑ Last Number Redial

☑ Message Center

☐ Do Not Disturb Lamp on 500/2500 Sets

☐ First Digit Pretranslation

Flexible Incoming Tones

☑ for SL-1 Stations

☐ for Digital Stations

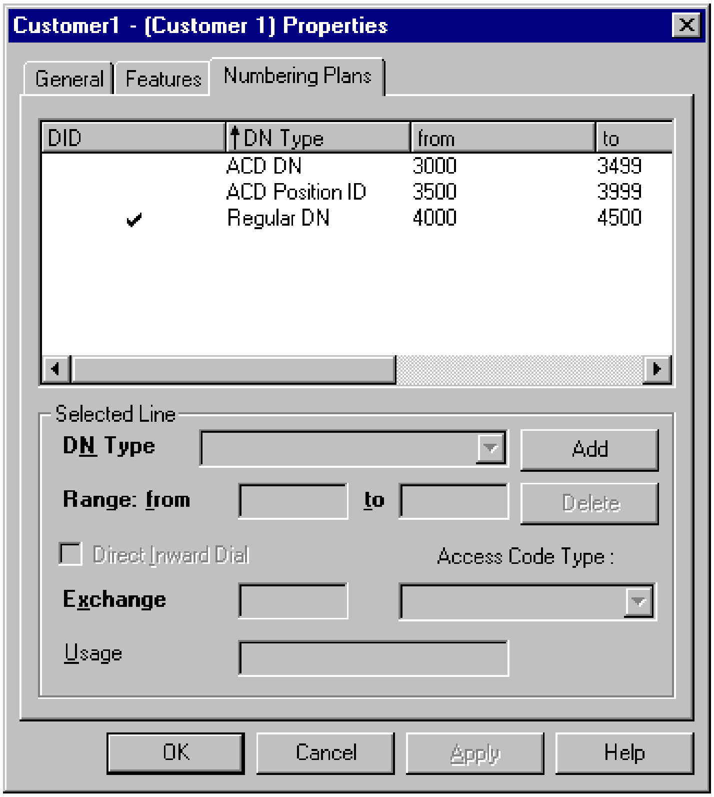
Dial Intercom Group: 0

f Fill in the feature information for the customer.

g Click the Numbering Plans tab.

The Numbering Plans dialog box appears (Figure 73).

Figure 73 Customer Properties dialog box—Numbering Plans tab



DID	DN Type	from	to
	ACD DN	3000	3499
	ACD Position ID	3500	3999
✓	Regular DN	4000	4500

h Fill in the numbering plan information for the customer.

13 When you have finished entering the customer information, click one of the following buttons to save the information:

- OK adds the customer and returns you to the System properties sheet.
- Cancel closes the dialog box without adding the customer.
- Apply adds the customer and leaves the Customer properties open so that you can add other information for this customer.

14 To delete a customer, click Delete in the System Properties dialog box—Customers tab. A delete confirmation box appears. Click OK.

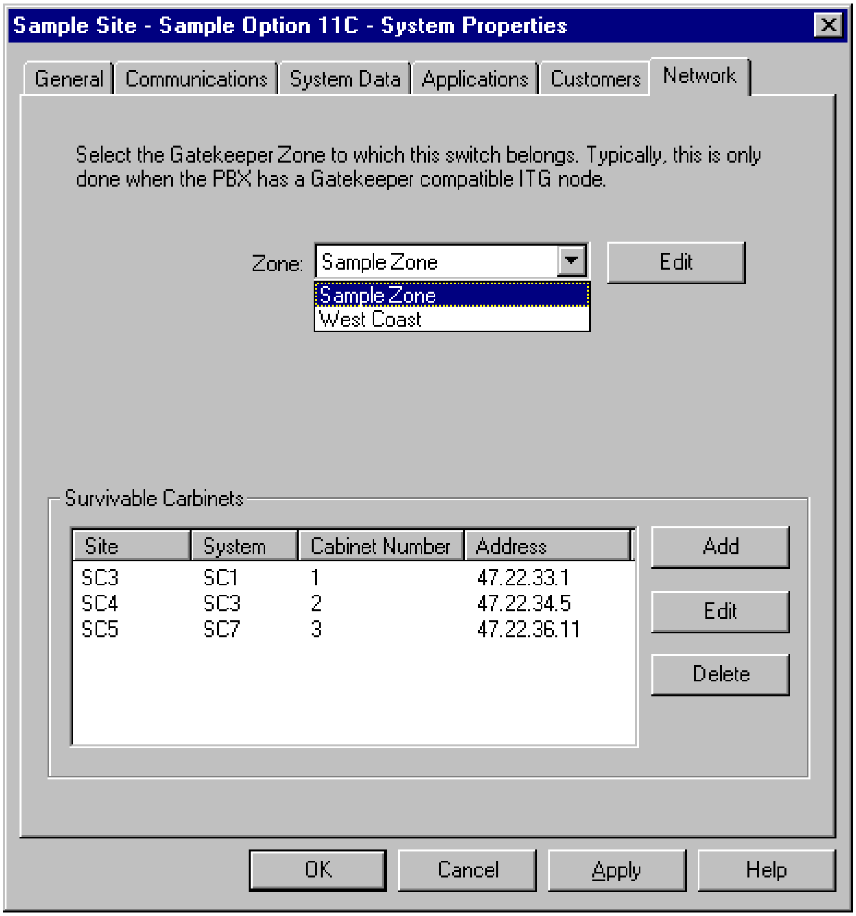
15 To modify customer information, click Properties in the System Properties dialog box—Customers tab. The Customer Properties dialog box appears with the General tab selected. Modify information in the appropriate tabs and click OK.

16 Click the Network tab.

The System Properties dialog box—Network tab appears (Figure 74).

The Network tab is used to both add and delete Survivable IP Expansion Cabinets and Survivable Media Gateways. On Meridian 1 systems, all Survivable IP Expansion Cabinets must be deleted before the main Meridian 1 system can be deleted.

Figure 74 System Properties dialog box—Network tab



Sample Site - Sample Option 11C - System Properties

Select the Gatekeeper Zone to which this switch belongs. Typically, this is only done when the PBX has a Gatekeeper compatible ITG node.

Zone: Sample Zone

Sample Zone
West Coast

Survivable Carbinets

Site	System	Cabinet Number	Address
SC3	SC1	1	47.22.33.1
SC4	SC3	2	47.22.34.5
SC5	SC7	3	47.22.36.11

a If the system is a Succession CSE 1000 Release 1.x system or a Meridian 1 with a Gatekeeper-compatible ITG Trunk node, select the Gatekeeper Zone from the drop-down list.

If the system does not contain a Gatekeeper-compatible ITG Trunk node and you continue, you add the system to a Gatekeeper Zone for display in the OTM Windows and Web Navigators only.

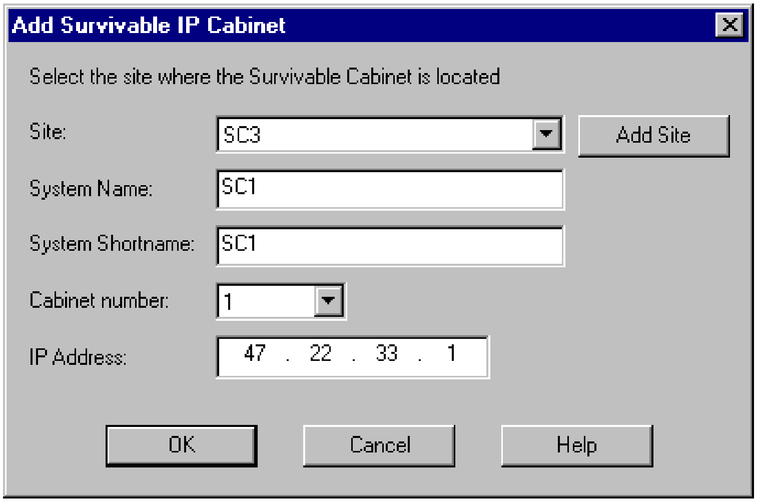
For information on managing gatekeeper zones, see "Managing gatekeeper zones" on page 178.

b If the system is not a Succession CSE 1000 Release 1.x system with Survivable Media Gateways or a Meridian 1 Option 11C with Survivable IP Expansion cabinets, go to step 17.

c If the system is Succession CSE 1000 Release 1.x system or a Meridian 1 Option 11C that is being configured to support Survivable IP Expansion cabinets or Media Gateways, click Add to add a cabinet.

The Add Survivable IP Cabinet dialog box appears (Figure 75).

Figure 75 Add Survivable IP Cabinet dialog box



Add Survivable IP Cabinet

Select the site where the Survivable Cabinet is located

Site: SC3

System Name: SC1

System Shortname: SC1

Cabinet number: 1

IP Address: 47 . 22 . 33 . 1

d Select the site and cabinet number from the drop-down lists, and enter the system name, system shortname, and IP address for this cabinet.

For additional information on Option 11C survivable expansion cabinets, see *Large System: Installation and Configuration* (553-3021-210).

For additional information on the Succession Media Gateway, see *Large System: Installation and Configuration* (553-3021-210).

e Click OK.

A new System Properties dialog box appears.

The Applications tab settings are copied from the Main Cabinet system properties. If the *Default* Ethernet communication profile is selected for the applications on the Main Cabinet that are likely to be used by the Survivable IP Expansion Cabinets, you can click OK to add the SIPE Cabinet and return to the System Properties dialog box—Network tab for the Main Cabinet (step 16b).

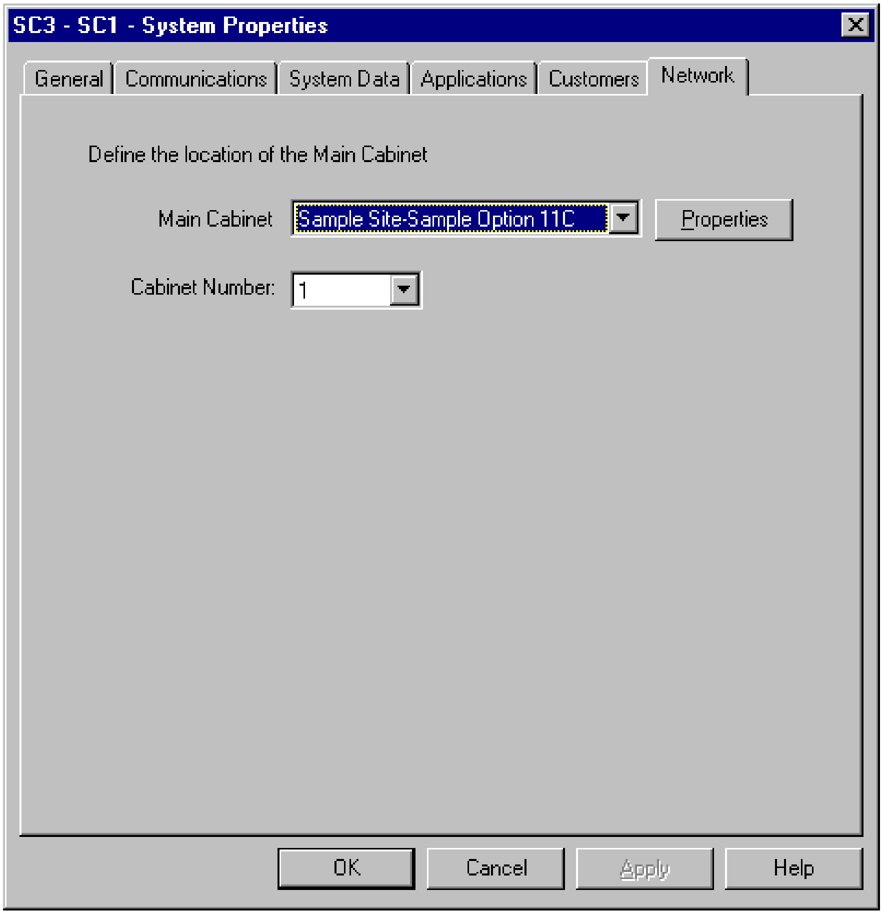
f Enter the requested information for the General and Communications tabs (see steps 5 through 7 in this procedure).

The IP address entered in the Add Survivable IP Cabinet dialog box is copied into the default Ethernet communication profile.

The System Data and Customers tabs are read-only. These contain the information from the main cabinet.

g Click the Network tab. The System Properties dialog box—Network tab appears (Figure 76).

Figure 76 Survivable Cabinet System Properties dialog box—Network tab



Define the location of the Main Cabinet

Main Cabinet: Sample Site-Sample Option 11C

Cabinet Number: 1

h Select the Main Cabinet and the Cabinet Number from the drop-down lists.

i Click OK to close the System Properties dialog box for the Survivable IP Expansion cabinet and return to the System Properties dialog box—Network tab for the Main Cabinet.

17 In the System Properties dialog box, click one of the following buttons:

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

The new system is added to the tree under the selected site.

Adding a Succession system

Pre-Release 2.0 Succession CSE 1000 systems that were added in an earlier version of OTM cannot be converted to a Succession 3.0 release. You must delete the pre-Release 2.0 system and add a new Succession 3.0 system.

You can add up to 256 systems (including non-Succession systems) to a site. You must have administrator privileges to add a system.

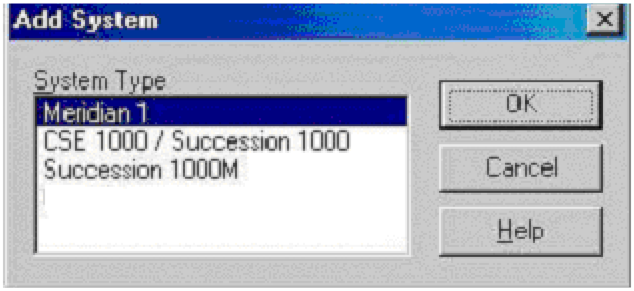
1 In the Navigator window, select the desired site.

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 use the right mouse button pop-up menu.

The Add System dialog box opens (Figure 77).

Figure 77 Add System dialog box



Add System

System Type

Meridian 1
CSE 1000 / Succession 1000
Succession 1000M

3 In the Add System dialog box, select one of the following systems:

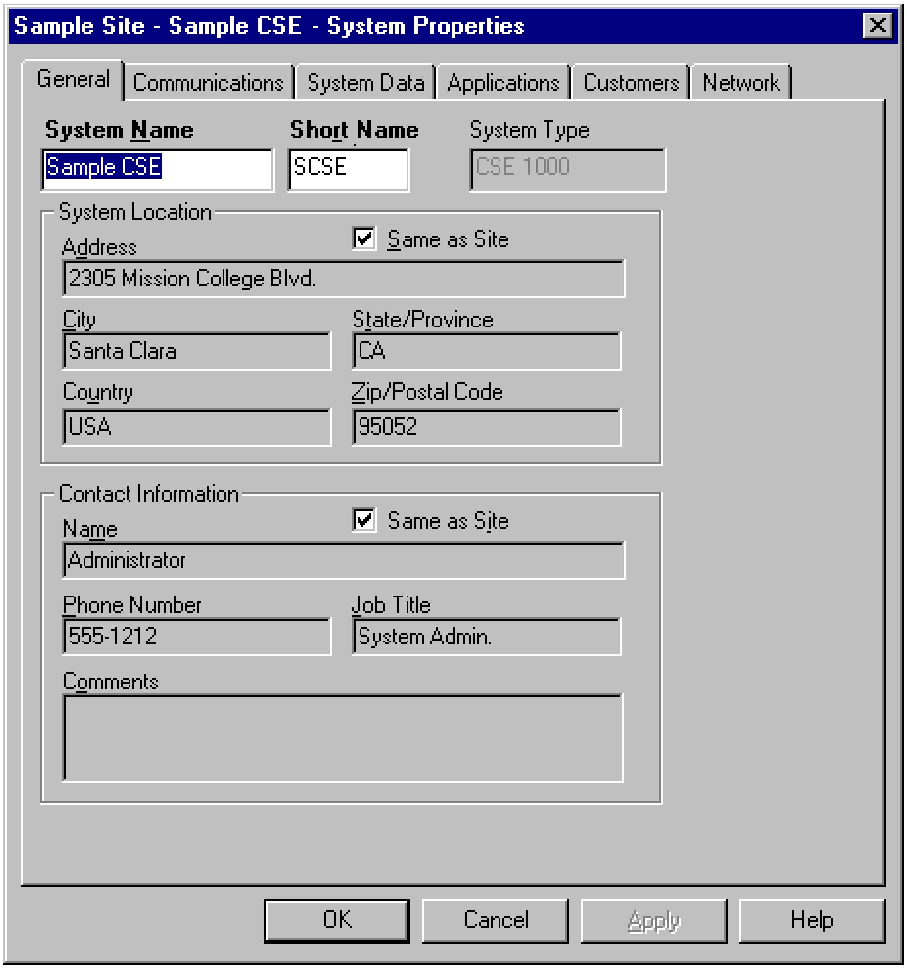
- 'Meridian 1' for a Meridian 1 system running any X11 release for running Succession release 3.0 without signaling server.
- 'CSE 1000 / Succession 1000' for a CSE system running X21 release 2.0 or Succession 3.0
- 'Succession 1000M' for a Meridian1 system running Succession 3.0 with signaling server.
- Generic

- Succession BCM

You may need to install additional software to enable other system types not listed in Figure 77. Follow the installation instructions included with your order.

The System Properties dialog box opens with the General tab displayed.

Figure 78 System Properties dialog box—General tab



Sample Site - Sample CSE - System Properties

System Name: Sample CSE
Short Name: SCSE
System Type: CSE 1000

System Location
☑ Same as Site
Address: 2305 Mission College Blvd.
City: Santa Clara
State/Province: CA
Country: USA
Zip/Postal Code: 95052

Contact Information
☑ Same as Site
Name: Administrator
Phone Number: 555-1212
Job Title: System Admin.
Comments:

4 Enter the system name and short name (required fields) and other information as needed. Click Apply.

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

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. Click the arrow to select from the list. For more detailed information, refer to the online Help.

5 To add a new communications profile, click the System Properties dialog box—Communications tab.

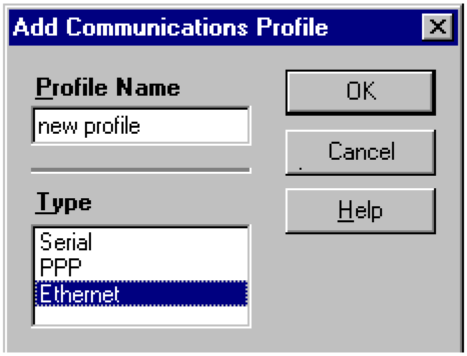
This tab defines the types of communications profiles that can be applied to system applications. One profile can be used for multiple applications.

OTM is shipped with a default communication profile. The Default profile is an Ethernet profile, and it cannot be deleted.

6 Click Add.

The Add Communications Profile dialog box appears (Figure 79).

Figure 79 Add Communications Profile dialog box



Add Communications Profile

Profile Name: new profile

Type: Serial / PPP / Ethernet (selected)

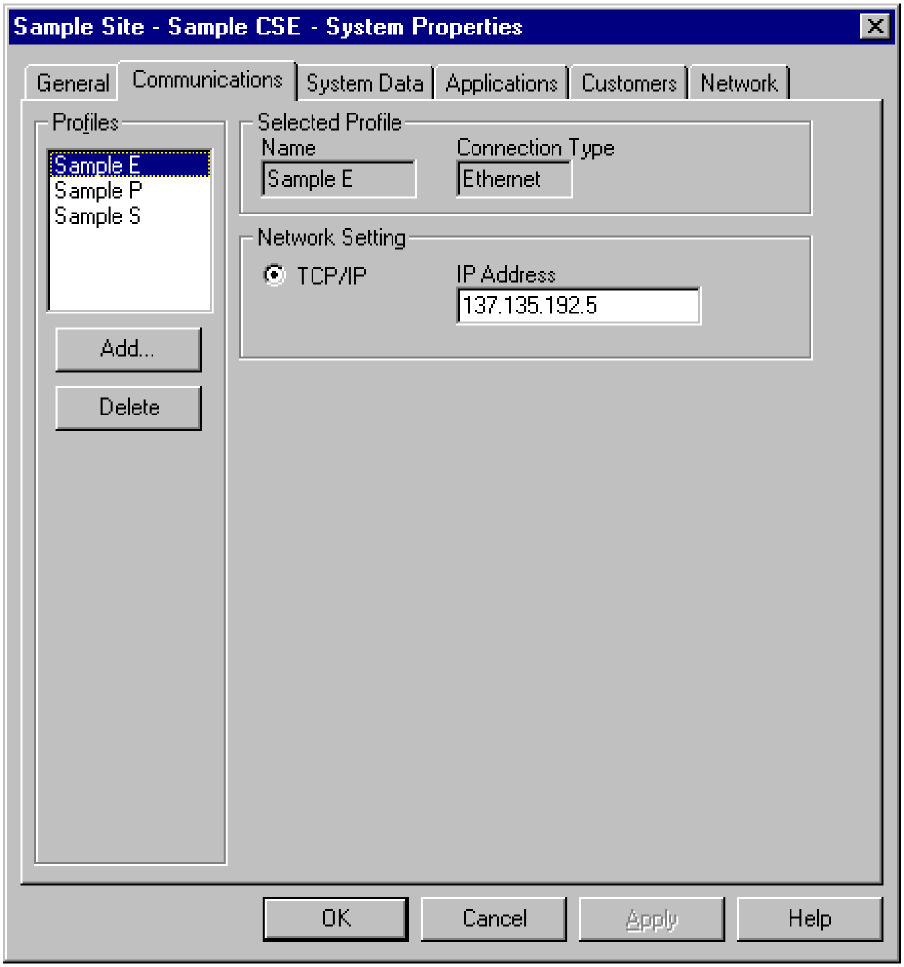
Select a communications type from the Type box, enter a profile name, and then click OK to return to the Communications tab.

7 Fill in the communications information for the new profile:

Ethernet (Figure 80):

- **a** Select the appropriate network protocol.
- **b** Enter the IP address that you configured on the Succession system.
- **c** Click Apply.

Figure 80 System Properties—Communications tab—Ethernet Profile



Sample Site - Sample CSE - System Properties

Profiles: Sample E, Sample P, Sample S

Selected Profile
Name: Sample E
Connection Type: Ethernet

Network Setting
● TCP/IP
IP Address: 137.135.192.5

PPP (Figure 81):

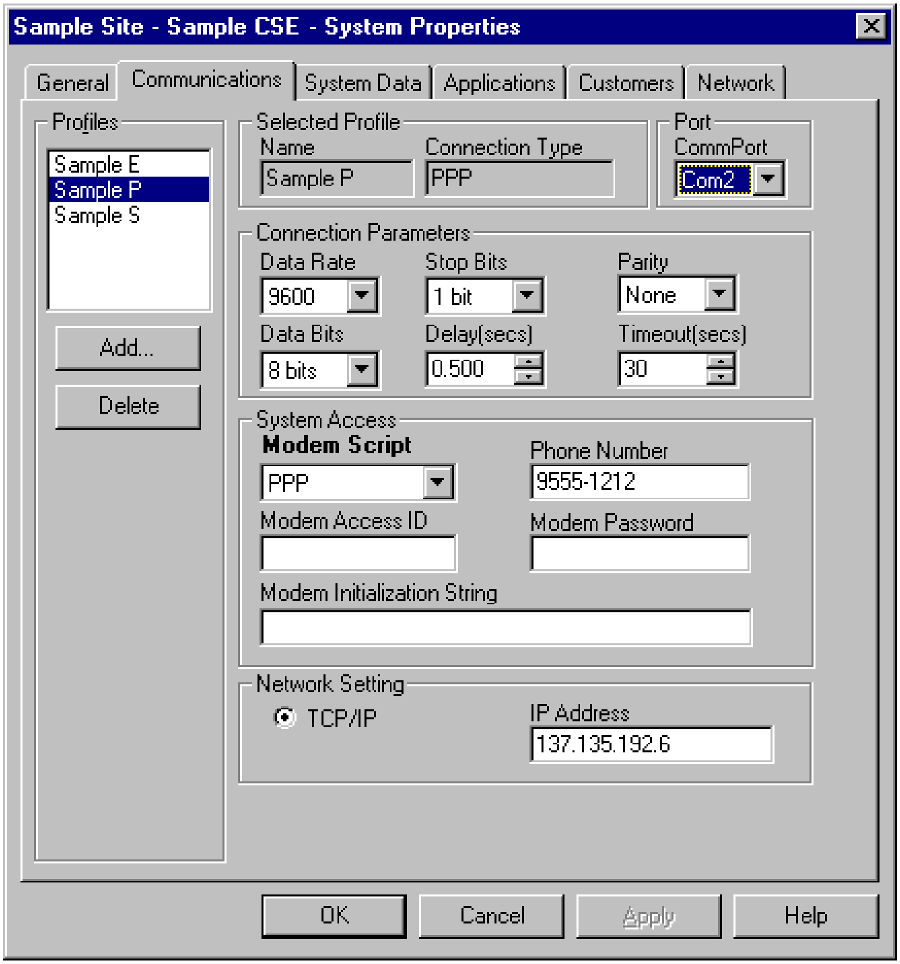
a Enter all modem parameters and dial-up information.

b Select PPP in the Modem Script text box.

c Set the IP address to the local IP address, as configured on the Succession system.

d Click Apply.

Figure 81 System Properties—Communications tab—PPP Profile



Sample Site - Sample CSE - System Properties

Profiles: Sample E, Sample P, Sample S

Selected Profile
Name: Sample P
Connection Type: PPP

Port
CommPort: Com2

Connection Parameters
Data Rate: 9600
Stop Bits: 1 bit
Parity: None
Data Bits: 8 bits
Delay(secs): 0.500
Timeout(secs): 30

System Access
Modem Script: PPP
Phone Number: 9555-1212
Modem Access ID:
Modem Password:
Modem Initialization String:

Network Setting
● TCP/IP
IP Address: 137.135.192.6

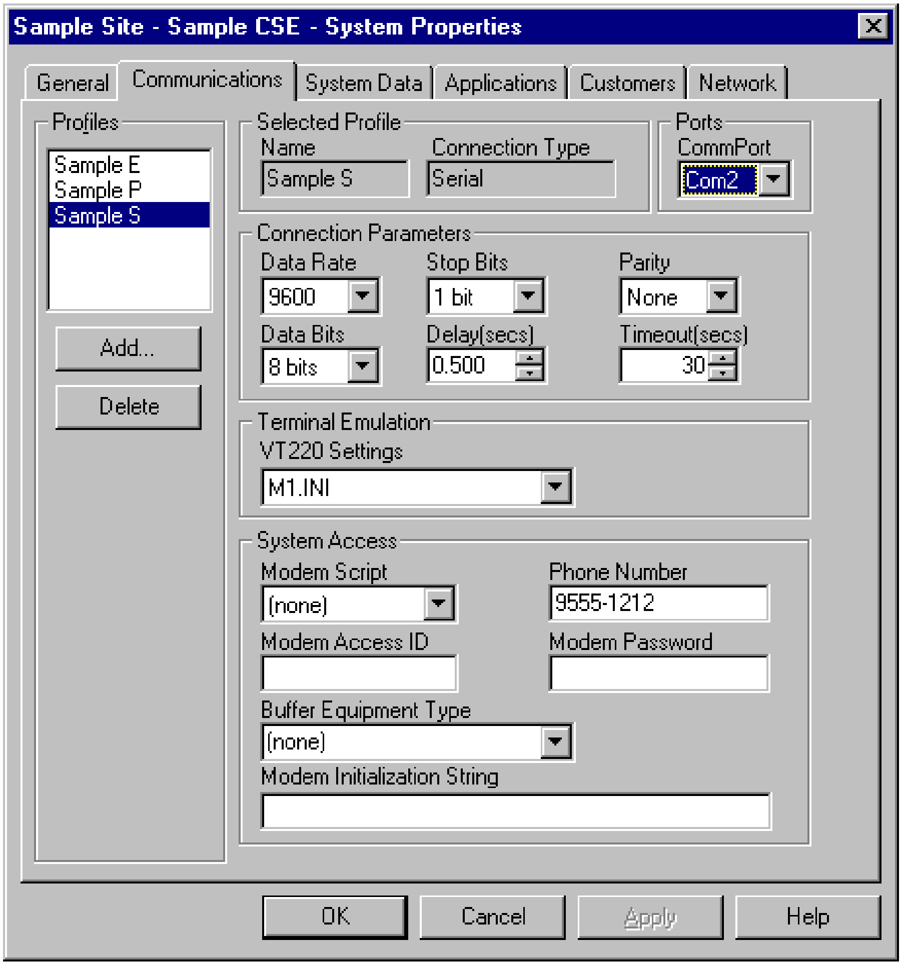
Serial (Figure 82):

a Enter all modem parameters and dial-up information.

b Select the appropriate value in the Modem Script drop-down box. This is usually “None” unless a specific value is defined for your system.

c Click Apply.

Figure 82 System Properties—Communications tab—Serial Profile



Sample Site - Sample CSE - System Properties

Profiles
Sample E
Sample P
Sample S

Selected Profile
Name: Sample S
Connection Type: Serial

Ports
CommPort: Com2

Connection Parameters
Data Rate: 9600
Stop Bits: 1 bit
Parity: None
Data Bits: 8 bits
Delay(secs): 0.500
Timeout(secs): 30

Terminal Emulation
VT220 Settings: M1.INI

System Access
Modem Script: (none)
Phone Number: 9555-1212
Modem Access ID:
Modem Password:
Buffer Equipment Type: (none)
Modem Initialization String:

8 Click the System Data tab. The System Properties dialog box—System Data tab appears (Figure 83).

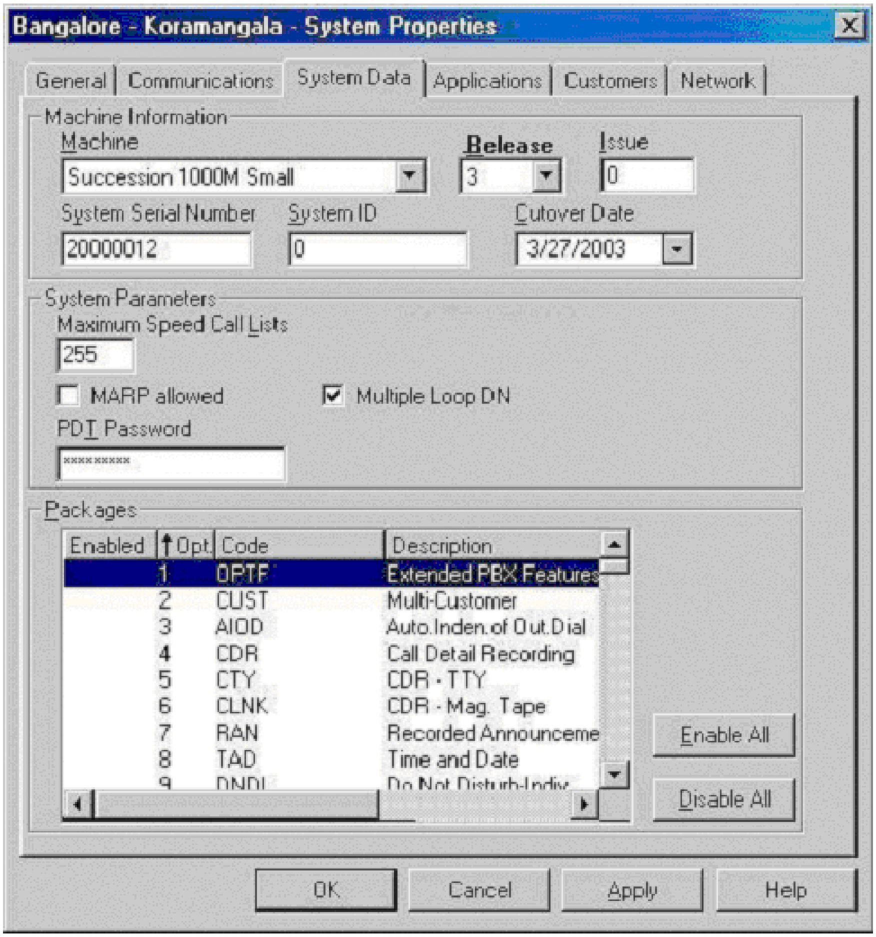
You can copy this data directly from an installed switch by scheduling an upload using File > Update System Data in the System window. Update System Data uses the communication profile for station administration. However, you should configure the release number in the System Data tab first to allow available applications to show up properly in the Applications tab.

The 'Release' combo box in 'System Data' page displays only for Succession 3.0. The entries for X11 software releases (25, 24, 23 and so on) are not displayed.

It is the user's responsibility to add proper system in OTM Navigator.

OTM can not differentiate between a 11C/Mini/CSE system based on the OVLY 22 values received during update system data.

Figure 83 The System Properties dialog box—System Data tab



Bangalore - Koramangala - System Properties

Machine Information

Machine: Succession 1000M Small

Release: 3

Issue: 0

System Serial Number: 20000012

System ID: 0

Cutover Date: 3/27/2003

System Parameters

Maximum Speed Call Lists: 255

□ MARP allowed

☑ Multiple Loop DN

PDT Password: xxxxxxxxxx

Packages

Enabled	Opt	Code	Description
	1	OPTF	Extended PBX Features
	2	CUST	Multi-Customer
	3	AIOD	Auto.Inden.of Out.Dial
	4	CDR	Call Detail Recording
	5	CTY	CDR - TTY
	6	CLNK	CDR - Mag. Tape
	7	RAN	Recorded Announceme
	8	TAD	Time and Date
	9	DNDI	Do Not Disturb-Indiv

a Select the machine/system type and release version for the system

Machine names are associated with the presence or absence of a signaling server. Checking the Signaling Server box in the Network tab changes the Machine names display.

b Set the system parameters.

In the System Parameters box, the PDT Password edit box lets you 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.

c Enable or disable feature packages.

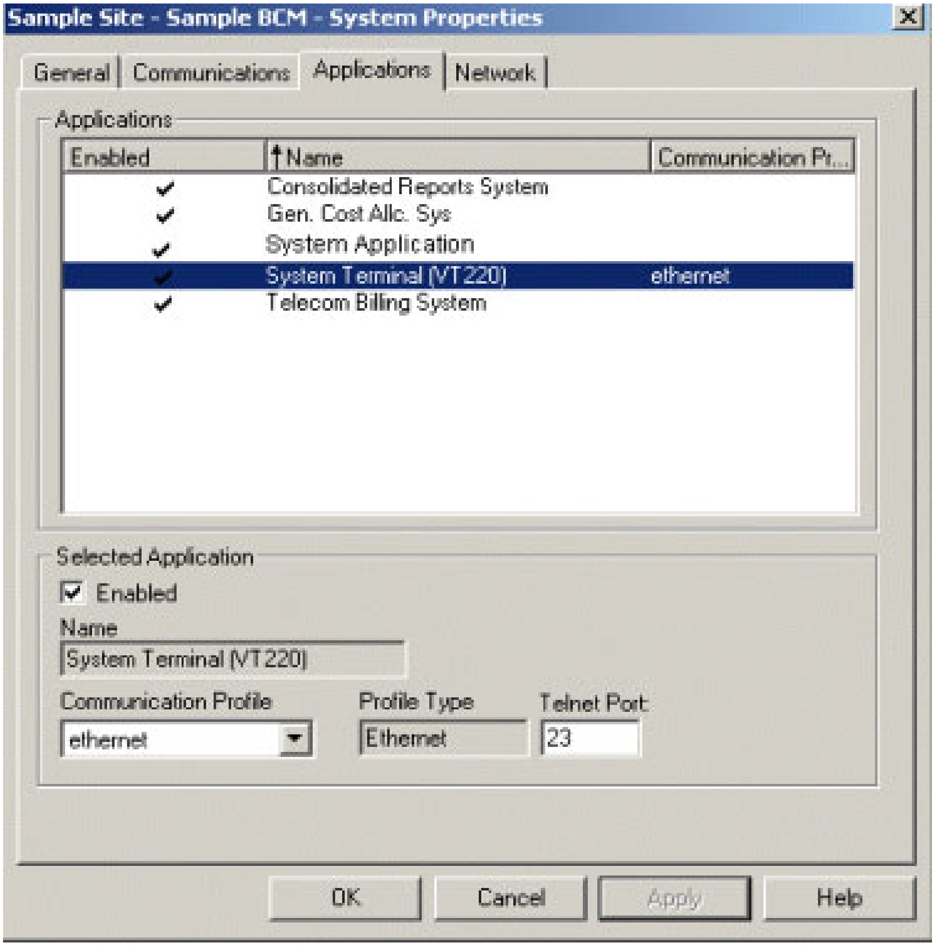
d Click Apply.

9 Define the OTM applications that appear in the System window and the communications profile to be used with each application.

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

Communication profile settings are defined on a site/system basis and are shared by the OTM Server and its Clients. Consequently, if you define a serial communication profile for an OTM application, then the OTM Server and OTM Client PCs must have a physical serial connection to the site/system. An OTM Client PC cannot use the COM ports of the OTM Server. Any communication task uses the resources of the PC on which it is running.

Figure 84 System Properties dialog box—Applications tab



Enabled	Name	Communication Pr...
✓	Consolidated Reports System	
✓	Gen. Cost Allc. Sys	
✓	System Application	
✓	System Terminal (VT220)	ethernet
✓	Telecom Billing System	

☑ Enabled

Name: System Terminal (VT220)

Communication Profile: ethernet

Profile Type: Ethernet

Telnet Port: 23

To enable an application:

a Select the application in the Applications tab dialog box.

For Succession BCM:

By default, when added to the system for the first time, the System Application is enabled with Web URL, populated as 'http://<default IP address>:6800". The Web URL path can be changed.

The System Terminal requires a communication profile. If ethernet profile type is selected, then enter the telnet port number. The Telnet edit control is disabled if serial profile type is selected.

The Telecom Billing System, General Cost Allocation System and Consolidated Reports System do not require a communication profile.

---

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.

c Click Apply and OK.

To disable an application:

a Select the application in the Applications tab dialog box.

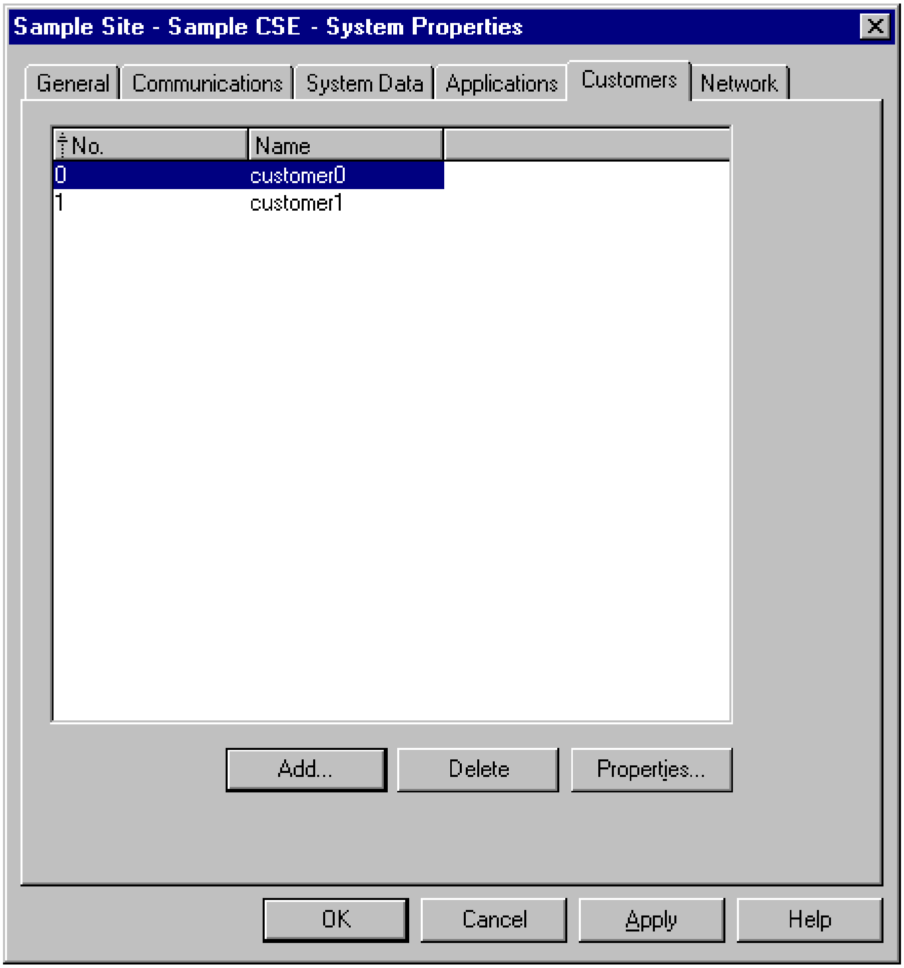
b In the Selected Application box, click the Enabled check box to remove the check mark.

When you have finished entering the information in the Applications tab, click Apply.

10 If applicable, click the Customers tab.

The System Properties dialog box—Customers tab appears (Figure 85).

Figure 85 System Properties dialog box—Customers tab



No.	Name
0	customer0
1	customer1

This tab lists the customers currently defined for this system.

Manual update:

This information is not automatically updated and must be updated by using the LD 15 customer overlay.

LD 15 is the overlay interface that enables customers to configure their systems on the Succession CSE 1000. For more information on overlay interfaces, see the System online help.

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

11 To add a customer:

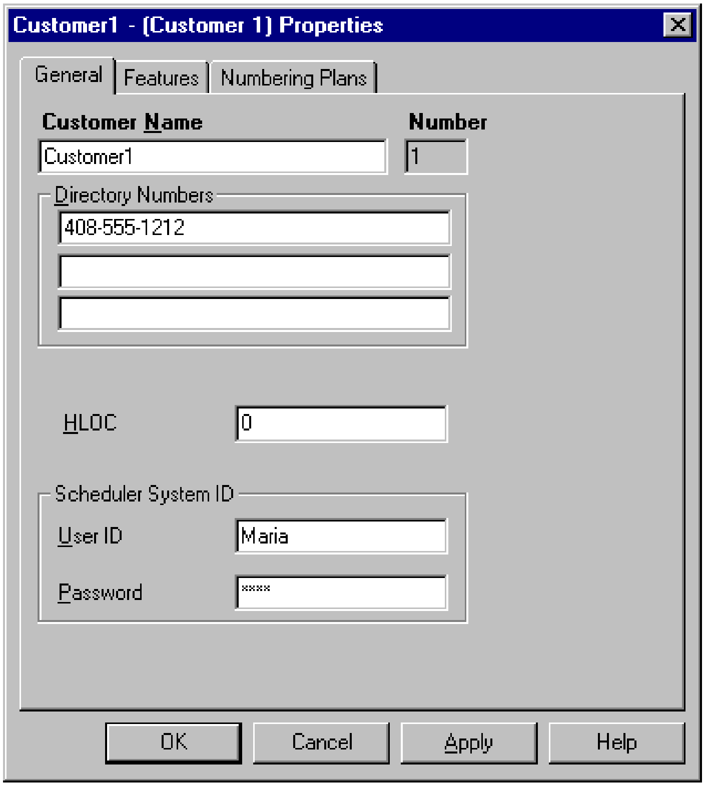
a Click Add in the System Properties dialog box—Customers tab.

b Select a Customer number.

c Click OK.

The Customer Properties dialog box opens with the General tab displayed (Figure 86).

Figure 86 Customer Properties dialog box—General tab



Customer1 - [Customer 1] Properties

Customer Name: Customer1

Number: 1

Directory Numbers: 408-555-1212

HLOC: 0

Scheduler System ID

User ID: Maria

Password: ****

d Fill in the general information for the customer.

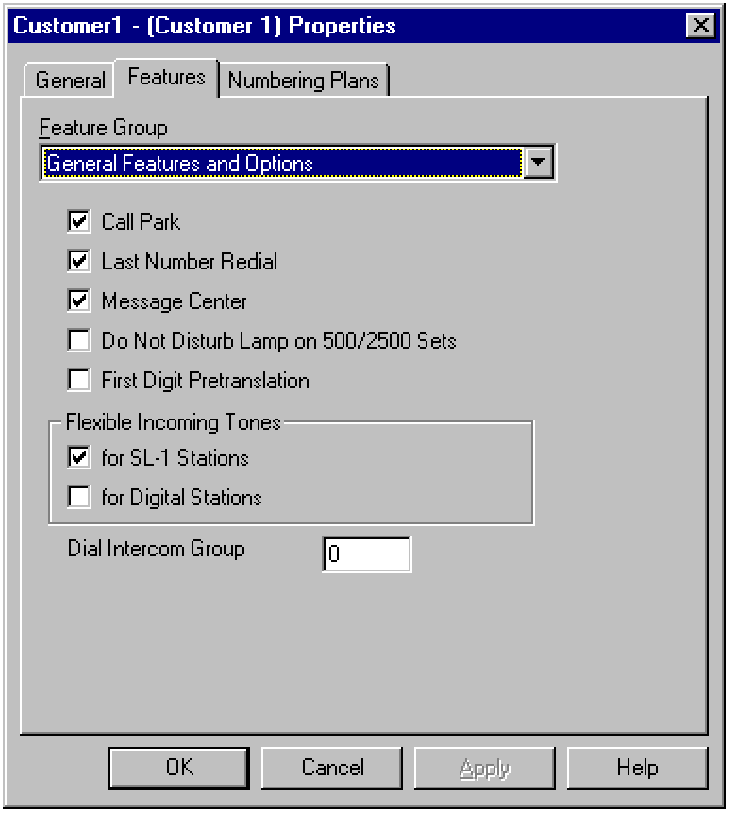
You can copy this data directly from an installed switch by scheduling an upload using File > Update System Data in the System window. Update System Data uses the communication profile for station administration. However, you should configure the release number here first to allow available applications to show up properly in the Applications tab.

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 Analysis.

e Click the Features tab.

The Customer Properties dialog box—Features tab appears (Figure 87).

Figure 87 Customer Properties dialog box—Features tab



Feature Group: General Features and Options

☑ Call Park
☑ Last Number Redial
☑ Message Center
□ Do Not Disturb Lamp on 500/2500 Sets
□ First Digit Pretranslation

Flexible Incoming Tones
☑ for SL-1 Stations
□ for Digital Stations

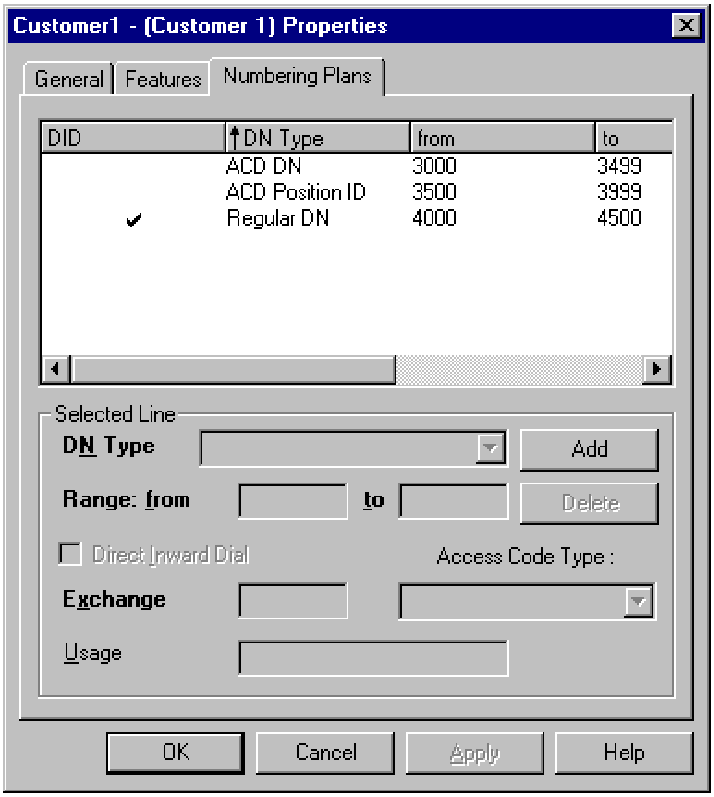
Dial Intercom Group: 0

f Fill in the feature information for the customer.

g Click the Numbering Plans tab.

The Customer Properties dialog box—Numbering Plans tab appears (Figure 88).

Figure 88 Customer Properties dialog box—Numbering Plans tab



Customer1 - (Customer 1) Properties

DID	DN Type	from	to
	ACD DN	3000	3499
	ACD Position ID	3500	3999
✓	Regular DN	4000	4500

h Fill in the numbering plan information for the customer.

The numbering plan information is used to validate DNs in station administration.

12 Click one of the following buttons to save the information:

- OK adds the customer and returns to the System Properties sheet.
- Cancel closes the dialog box without adding the customer.
- Apply adds the customer and leaves the Customer Properties dialog box open so that you can add other information for this customer.

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

14 To modify customer information, click Properties in the System Properties dialog box—Customers tab. The Customer Properties dialog box opens with the General tab displayed. Modify information in the appropriate tabs and click OK.

15 Click the Network Tab.

The Network page display depends on the type and size of the system added:

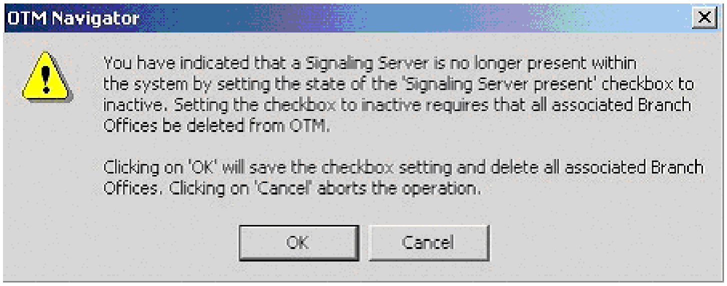
Succession 1000M -'Signaling Server present' is checked by default.

Meridian 1 -'Signaling Server present' checkbox is un-checked by default.

CSE 1000 / Succession 1000- system is added

16 Choose a system. See below for the specific instructions for your system.

IMPORTANT: If there is at least one Branch Office associated with the a Succession 3.0 Large System, you can confirm the deletion of associated Branch Offices. Do this by clicking on the OK/Apply button after un-checking the 'Signaling Server present' checkbox. It displays the following Warning dialog box.



OTM Navigator

You have indicated that a Signaling Server is no longer present within the system by setting the state of the 'Signaling Server present' checkbox to inactive. Setting the checkbox to inactive requires that all associated Branch Offices be deleted from OTM.

Clicking on 'OK' will save the checkbox setting and delete all associated Branch Offices. Clicking on 'Cancel' aborts the operation.

Click OK to delete all associated Branch Offices.

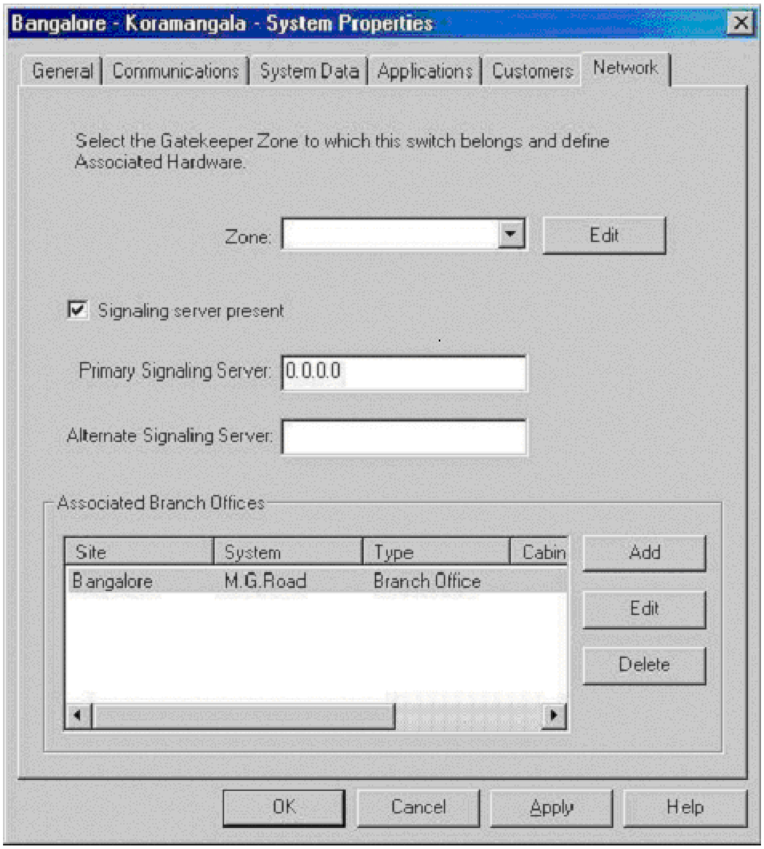
Click the Cancel button to re-select the 'Signaling Server present' check box and not delete associated Branch Offices.

Succession 3.0 Large System - 'Signaling server present' checked

The Primary Signaling Server and Alternate Signaling Server controls are enabled with the following associated values:

- The Add button within Associated Branch Offices is enabled.
- The Release combo box in the System Data page displays only Succession 3.0. The entries for X11 software releases (25, 24, 23 etc.) are not displayed.

Figure 89 Succession 3.0 Large System - 'Signaling server present' checked



Select the Gatekeeper Zone to which this switch belongs and define Associated Hardware.

Zone:

☑ Signaling server present

Primary Signaling Server: 0.0.0.0

Alternate Signaling Server:

Associated Branch Offices

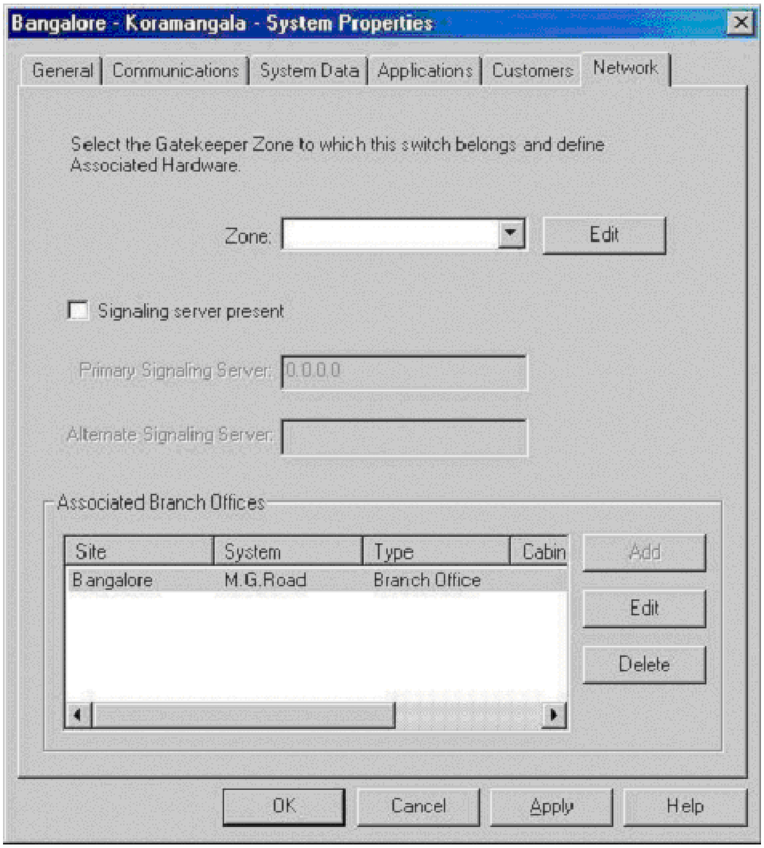
Site	System	Type	Cabin
Bangalore	M.G.Road	Branch Office	

Succession 3.0 Large System - 'Signaling server present' unchecked

The Primary Signaling Server and Alternate Signaling Server controls are disabled with the following associated values.

- The Add button within Associated Branch Offices is disabled.
- The Release combo box in System Data page displays all applicable Succession and X11 software releases.

Figure 90 Succession 3.0 Large System - 'Signaling server present' unchecked



Bangalore - Koramangala - System Properties

Select the Gatekeeper Zone to which this switch belongs and define Associated Hardware.

Zone:

☐ Signaling server present

Primary Signaling Server: 0.0.0.0

Alternate Signaling Server:

Associated Branch Offices

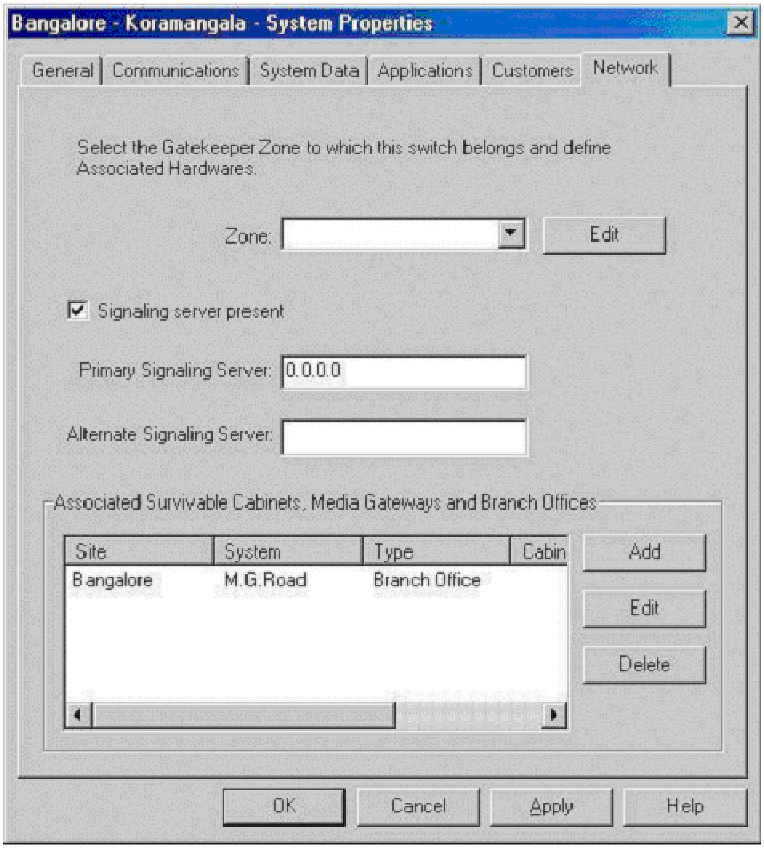
Site	System	Type	Cabin
Bangalore	M.G.Road	Branch Office	

Succession 3.0 Small System - 'Signaling server present' checked

The Primary Signaling Server and Alternate Signaling Server controls are enabled with the following associated values:

- The Add button for Survivable Cabinets, Media Gateways and Branch Offices is enabled.
- The Release combo box in the System Data page displays only Succession 3.0. The entries for X11 software releases (25, 24, 23, and so on) are not displayed.

Figure 91 Succession 3.0 Small System - 'Signaling server present' checked



Select the Gatekeeper Zone to which this switch belongs and define Associated Hardwares.

Zone:

☑ Signaling server present

Primary Signaling Server: 0.0.0.0

Alternate Signaling Server:

Associated Survivable Cabinets, Media Gateways and Branch Offices

Site	System	Type	Cabin
Bangalore	M.G.Road	Branch Office	

17 For a Succession 3.0 Small System with Signalling Server checked, select one of the following:

To add a Gatekeeper:

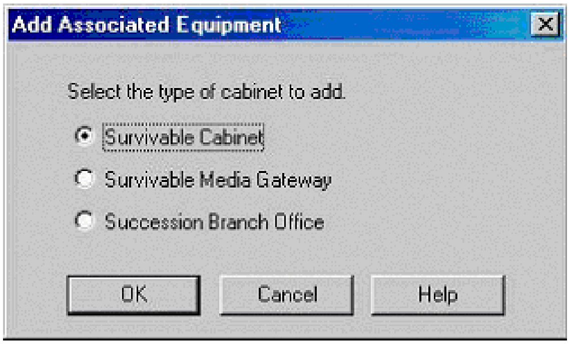
From the drop-down list, select the Gatekeeper Zone and enter the IP address or host name for the Primary Signaling Server. You can also define an Alternate (redundant) Signaling Server.

For information on managing Gatekeeper Zones, see "Managing gatekeeper zones" on page 178.

To add Survivable Cabinets, Survivable Media Gateways, or Succession Branch Office:

a Click on the Add button. The Add Associated Equipment window displays. (Figure 92)

Figure 92 Add Associated Equipment dialog box



Select the type of cabinet to add.

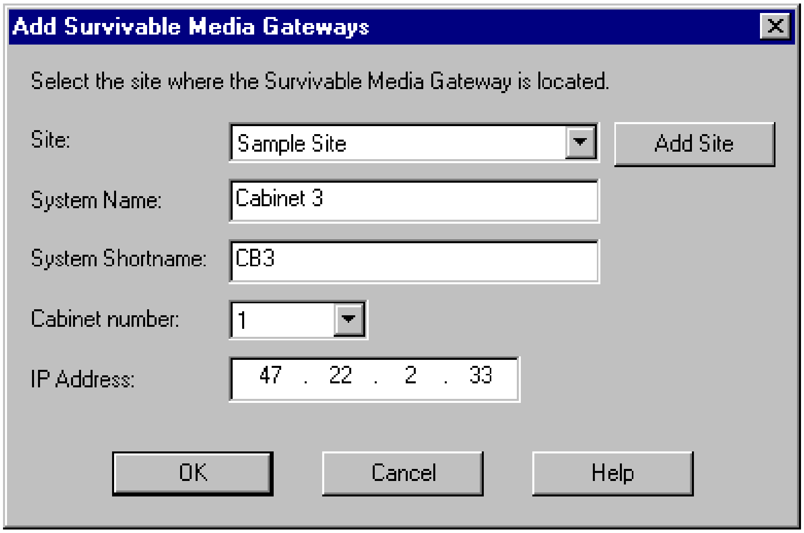
● Survivable Cabinet
○ Survivable Media Gateway
○ Succession Branch Office

b Select one of the following:

- **Survivable Cabinet**: Click OK. The Survivable Cabinet dialog box opens.
- **Survivable Media Gateway**: Click OK.

  The Add Survivable Media Gateways dialog box opens (Figure 93).

Figure 93 Add Survivable Media Gateways dialog box



Add Survivable Media Gateways

Select the site where the Survivable Media Gateway is located.

Site: Sample Site

System Name: Cabinet 3

System Shortname: CB3

Cabinet number: 1

IP Address: 47 . 22 . 2 . 33

Select the Site and Cabinet number from the drop-down lists, and enter the System Name, System Shortname, and IP Address for this Media Gateway. Click OK.

- **Succession Branch Office**:

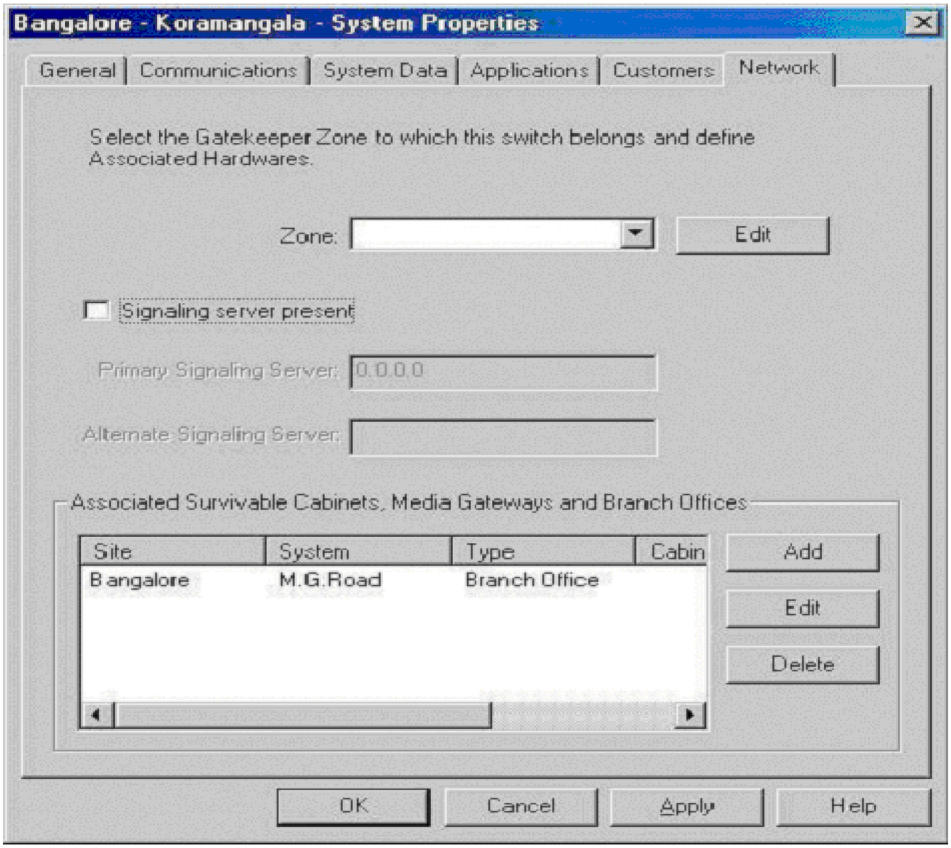
  Proceed to “Configuring a Branch Office for Meridian 1” on page 175.

Succession 3.0 Small System - 'Signaling server present' unchecked

The Primary Signaling Server and Alternate Signaling Server controls are disabled with the following associated values.

- The Add button for Survivable Cabinets, Media Gateways and Branch Offices is enabled.
- The Release combo box in System Data page displays all applicable Succession and X11 software releases.

Figure 94 Succession 3.0 Small System - 'Signaling server present' unchecked



Bangalore - Koramangala - System Properties

Select the Gatekeeper Zone to which this switch belongs and define Associated Hardwares.

Zone:

☐ Signaling server present

Primary Signaling Server: 0.0.0.0

Alternate Signaling Server:

Associated Survivable Cabinets, Media Gateways and Branch Offices

Site	System	Type	Cabin
Bangalore	M.G.Road	Branch Office	

18) For a Succession 3.0 Small System with Signalling Server unchecked, select one of the following:

To add a Gatekeeper:

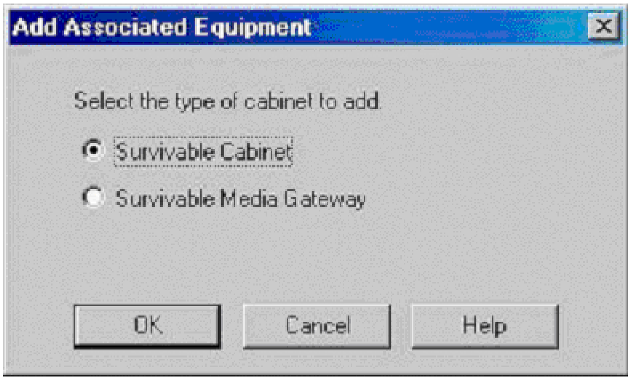
Select the Gatekeeper Zone from the drop-down list, and enter the IP address or host name for the Primary Signaling Server. You can also define an Alternate (redundant) Signaling Server.

For information on managing Gatekeeper Zones, see “Managing gatekeeper zones” on page 178.

To add Survivable Cabinets or Survivable Media Gateways:

a Click on Add button. The Add Associated Equipment window displays (Figure 92).

Figure 95 Add Associated Equipment dialog box


Add Associated Equipment

Select the type of cabinet to add.

● Survivable Cabinet

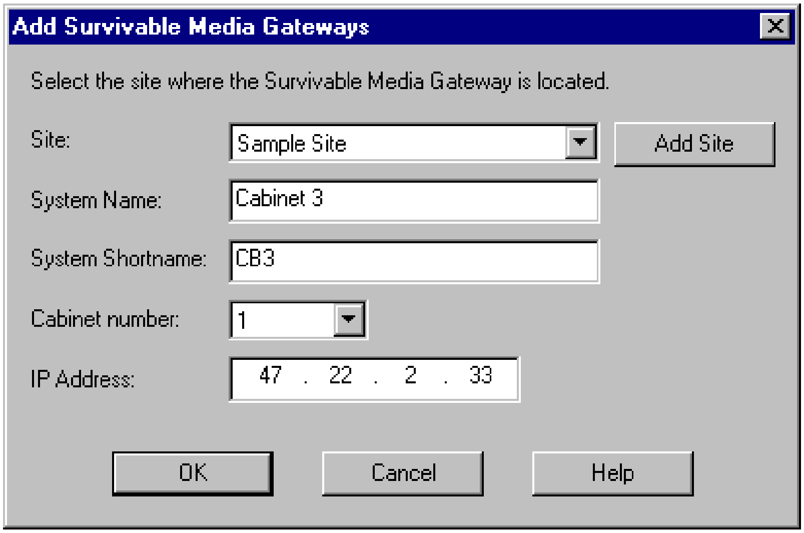
○ Survivable Media Gateway

b Select one of the following:

- **Survivable Cabinet**: Click OK. The Survivable Cabinet dialog box opens.
- **Survivable Media Gateway**: Click OK.

  The Add Survivable Media Gateways dialog box opens (Figure 96).

Figure 96 Add Survivable Media Gateways dialog box



Add Survivable Media Gateways

Select the site where the Survivable Media Gateway is located.

Site: Sample Site

System Name: Cabinet 3

System Shortname: CB3

Cabinet number: 1

IP Address: 47 . 22 . 2 . 33

Select the Site and Cabinet number from the drop-down lists, and enter the System Name, System Shortname, and IP Address for this Media Gateway.

Click OK.

For additional information on the Succession Media Gateway, see *Succession 1000 System: Installation and Configuration* (553-3031-210).

Configuring a Branch Office for Meridian 1

A Branch Office contains a call processor for connection to the local PSTN and for analog devices such as FAX machines. IP telephones are located at the Branch Office; however, under normal conditions, call processing for these telephones is handled by the Call Server at the main office. The Branch Office and the Main Office are connected by IP Trunks, Virtual Trunks, or through trunks to the PSTN.

For additional information on the Branch Office feature, see *Branch Office* (553-3001-214).

Requirements

IP telephones must be configured on both the Main Office and the Branch Office. Use Station Administration to add the telephones to both systems. You can copy and paste a telephone from one system to the other.

A Branch Office must be associated with a Succession Main Office and both must be in the same Gatekeeper Zone.

Enter the information in the System Properties dialog box—General, Communications, System Data, Applications, and Customers tabs as outlined in steps 5 through 15 of this procedure.

Unlike a Media Gateway, a Branch Office has its own copy of call processing code, and may be running a different version of system software. For this reason, you need to configure the System Data and Applications tabs as you do for a Call Server.

OTM 2.1 supports Branch Office for Large and Small Systems.

The feature BUID and MOTN are made available for configuring Internet telephones on the Branch office, only if the package 390 (SBO) is enabled. These features are not available for Internet telephone configuration, if package 390 is disabled.

OTM 2.1 MOTN accepts both LSCU as TN format for Large systems and CU format for small systems. Any other input results in the TN validation failure.

Update System Data should be tested during integration testing.

Procedure

To a configure a Meridian 1 Branch Office, choose one of the following from System Features:

a Select BUID and press Select button

b Enter the Large or Small System information and press OK

OR

a Select Branch Office Features and press Select.

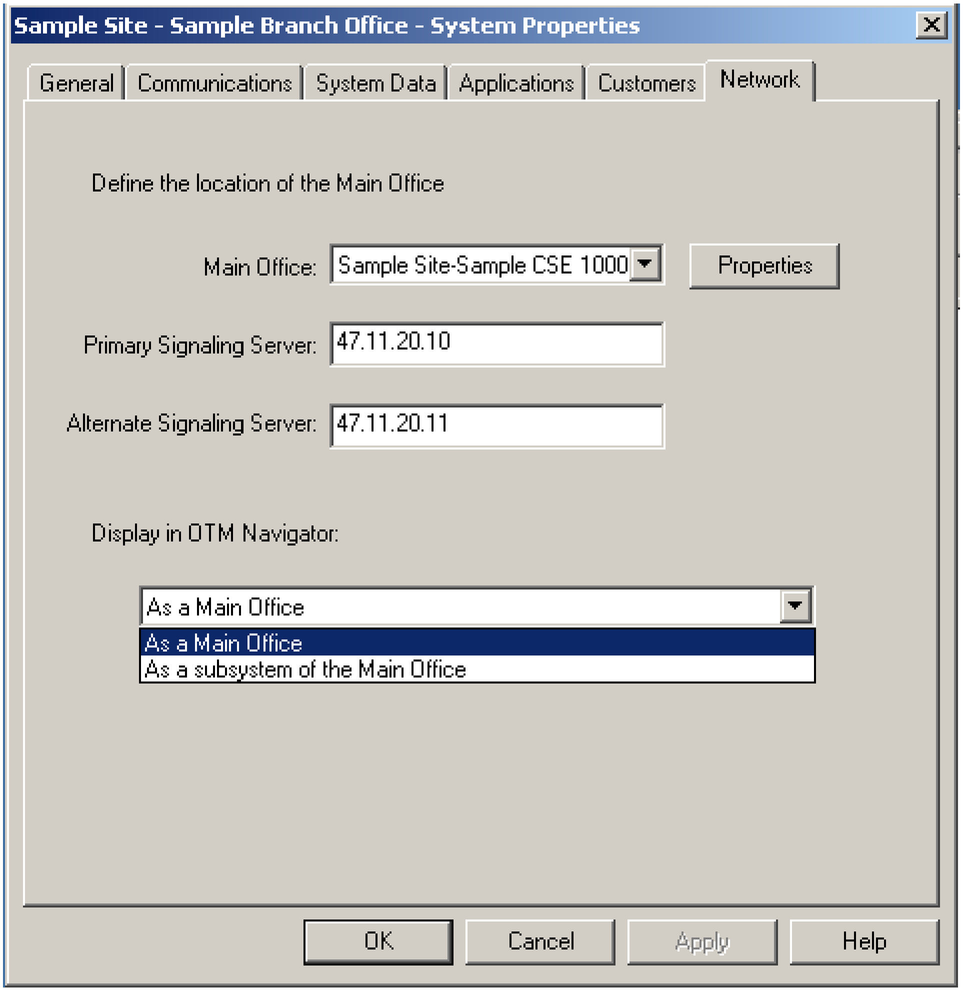
b Enter the Large or Small System information and press OK

1 In the Add Associated Equipment dialog box (Figure 92 on page 171), select Succession Branch Office and click OK. A new System Properties dialog box opens (Figure 78).

2 Click the Network tab.

The System Properties dialog box—Network tab appears (Figure 97).

Figure 97 Branch Office System Properties dialog box—Network tab



Sample Site - Sample Branch Office - System Properties

Define the location of the Main Office

Main Office: Sample Site-Sample CSE 1000

Primary Signaling Server: 47.11.20.10

Alternate Signaling Server: 47.11.20.11

Display in OTM Navigator:

As a Main Office

As a Main Office

As a subsystem of the Main Office

Select the Main Office from the drop-down list. You can click Properties to display the System Properties of the selected Main Office.

Use the drop-down list to select whether to display this Branch Office as a Main Office or as a subsystem of the Main Office.

Click OK.

3 In the System Properties dialog box, click one of the following buttons:

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

The new system is added to the tree under the selected site.

Managing gatekeeper zones

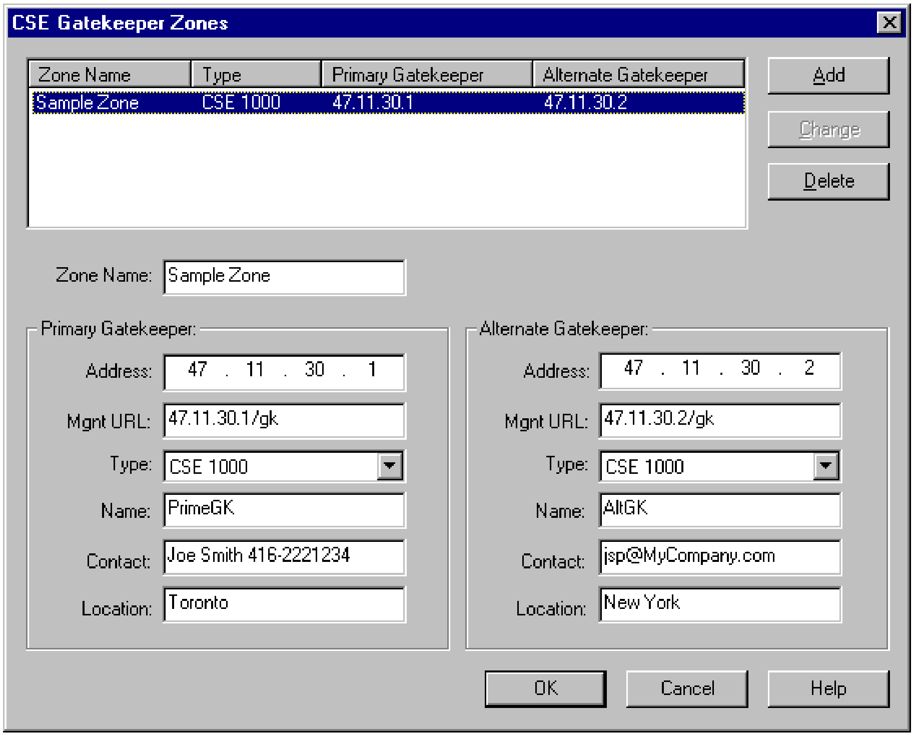
Use the Gatekeeper Zones dialog box to add, delete, and change gatekeeper zones.

To add a gatekeeper zone:

1 In the System Properties dialog box—Network tab for a Meridian 1 system (Figure 74), or a Succession CSE 1000 Call Server (Figure 97), click Edit located next to the Gatekeeper Zone drop-down list.

The Gatekeeper Zones dialog box appears (Figure 98).

Figure 98 Gatekeeper Zones dialog box



Zone Name	Type	Primary Gatekeeper	Alternate Gatekeeper
Sample Zone	CSE 1000	47.11.30.1	47.11.30.2

Zone Name: Sample Zone

Primary Gatekeeper:

Address: 47 . 11 . 30 . 1
Mgnt URL: 47.11.30.1/gk
Type: CSE 1000
Name: PrimeGK
Contact: Joe Smith 416-2221234
Location: Toronto

Alternate Gatekeeper:

Address: 47 . 11 . 30 . 2
Mgnt URL: 47.11.30.2/gk
Type: CSE 1000
Name: AltGK
Contact: jsp@MyCompany.com
Location: New York

2 Enter a Zone Name. The Zone Name is required and must be unique. The Zone Name appears in the Windows and Web Navigators.

3 Enter the IP address of the Primary Gatekeeper.

4 Enter the management URL for the Primary Gatekeeper.

5 Use the drop-down list to select the type of gatekeeper:

- CSE 1000 - for a Succession CSE 1000 call server
- CS 3000 - for a Succession CS 3000
- Other - for a third-party non-Nortel Networks gatekeeper

6 Enter a Name, Contact, and Location for the gatekeeper. These fields each have a maximum length of 30 characters. The Gatekeeper Name is required. The Contact and Location fields are optional.

7 If desired, you can assign an optional Alternate Gatekeeper to the zone by repeating steps 2 through 6 for the Alternate Gatekeeper.

8 Click Add to add the new gatekeeper zone to the list.

9 Click Close to close the Gatekeeper Zones dialog box and return to the System Properties dialog box—Network tab.

To modify the information on a gatekeeper zone:

1 In the System Properties dialog box—Network tab for a Meridian 1 system (Figure 74 on page 149) or a Succession 3.0 Call Server, click Edit located next to the Gatekeeper Zone drop-down list.

The Gatekeeper Zones dialog box appears (Figure 98).

2 Select a gatekeeper zone from the list.

3 Edit the fields as desired.

4 Click Change.

5 Click Close to close the Gatekeeper Zones dialog box and return to the System Properties dialog box—Network tab.

To delete a gatekeeper zone:

1 In the System Properties dialog box—Network tab for a Meridian 1 system (Figure 74 on page 149) or a Succession 3.0 Call Server (Figure 89 on page 168), click Edit located next to the Gatekeeper Zone drop-down list.

The Gatekeeper Zones dialog box appears (Figure 98 on page 179).

2 Select a gatekeeper zone from the list.

3 Click Delete.

4 Click Close to close the Gatekeeper Zones dialog box and return to the System Properties dialog box—Network tab.

Adding a Generic system or device

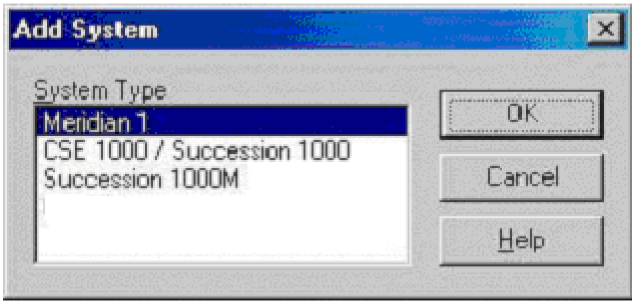
You can add as many as 256 systems (including non-Meridian 1 systems) to a site. You must have administrator privileges to add a system.

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 appears (Figure 99).

Figure 99 Add System dialog box—Generic



Note: You may need to install additional software to enable other system types not listed in Figure 99. Follow the installation instructions included with your order.

3 Select Generic in the System Type box.

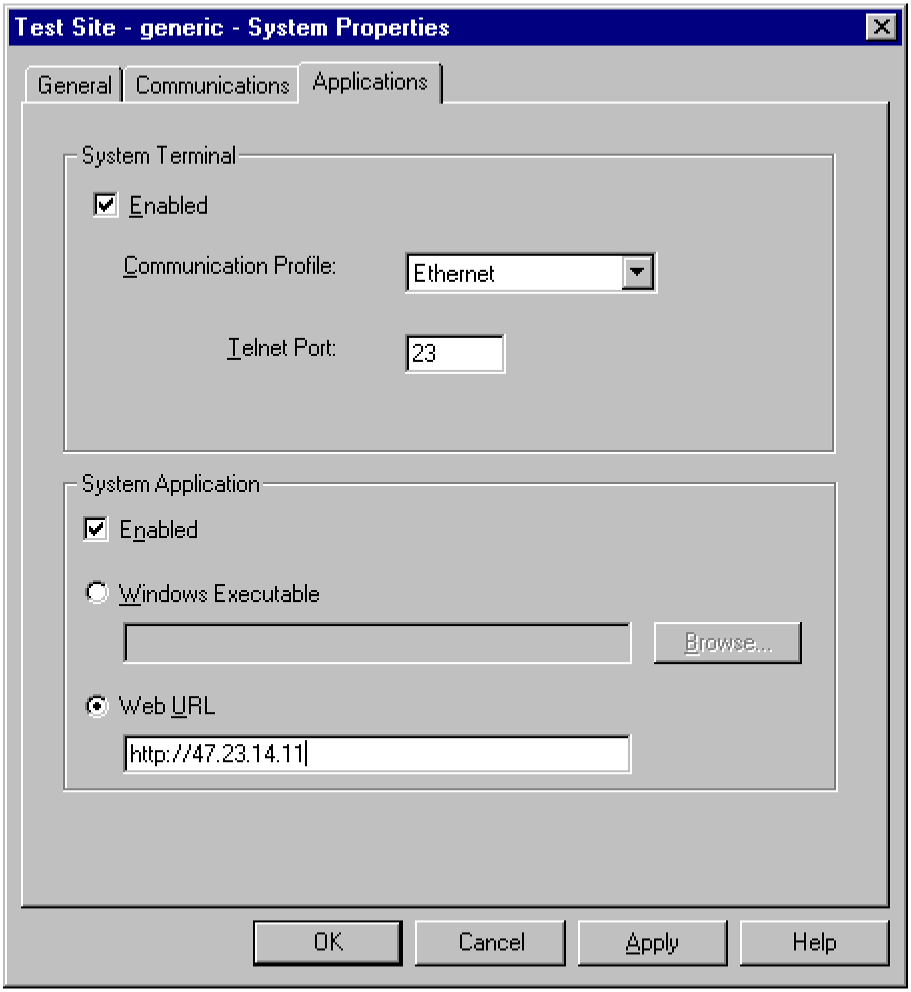
4 Click OK.

5 Complete the System Properties dialog box—General and Communications tabs as you would for a Meridian 1 or Succession CSE 1000 system. See "Adding a Meridian 1 or Successon CSE 1000 Release 1.x system" on page 135, or "Adding a Succession system" on page 153.

6 Click the Application tab.

The System Properties dialog box—Applications tab for non-Meridian 1 devices appears (Figure 100).

Figure 100 System Properties dialog box—Applications tab for non-Meridian 1 devices



Test Site - generic - System Properties

System Terminal

☑ Enabled

Communication Profile: Ethernet

Telnet Port: 23

System Application

☑ Enabled

○ Windows Executable

● Web URL

http://47.23.14.11

7 In the System Properties dialog box—Applications tab define the applications available for the device as follows:

- In the System Terminal section, select a Communication Profile. Typically, this is the Ethernet profile. Once defined, the user can double-click on the system in the Windows Navigator to launch the Windows System Terminal, or open a Web-based terminal window from the OTM Web Navigator Systems page, or both.

- 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, or Web site depends on the device.

Adding OTM Windows users via the OTM Windows Navigator

This section covers:

- Creating user groups
- Adding users
- Authenticating users

OTM allows you to create User Groups to speed the process of adding users by accessing the OTM Windows Navigator and certain OTM Web-based applications. In the User Group Properties dialog box, you define most aspects of certain kinds of users, such as their level of access to sites and systems and automatic connection to particular systems. You can create as many User Groups as you need. You assign individual users to a User Group when you add users to the OTM database.

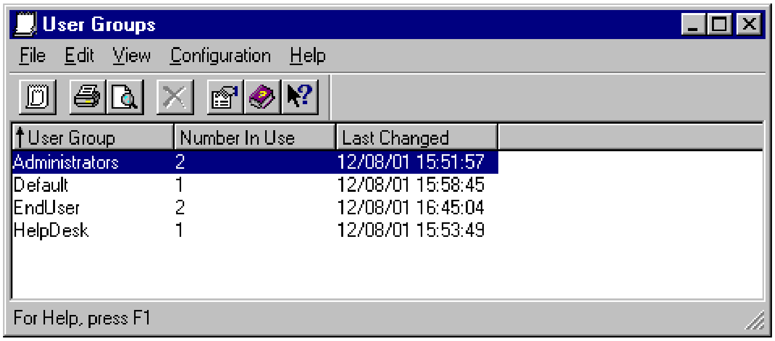
There are two types of users: local users and remote users. Local users have accounts on the OTM Server. When you add a new local user, an OTM user account and a local user account are created, and the account is assigned to the specified User Group. Deletion of a user removes the user account from the account list as well as from all relevant database tables. Remote users have accounts that exist on a domain controller or in an LDAP-compliant directory. For these users, OTM is used to assign the user ID for the account to an OTM user group.

Access to OTM Web Services is provided through the server. A Windows NT domain account or an LDAP-compliant directory can also be used to authenticate OTM users for Web Services. Refer to “Authenticating users” on page 190.

Creating a user group

1 In the Navigator window, choose Security > User Groups to display the User Groups window (Figure 101).

Figure 101 User Groups window

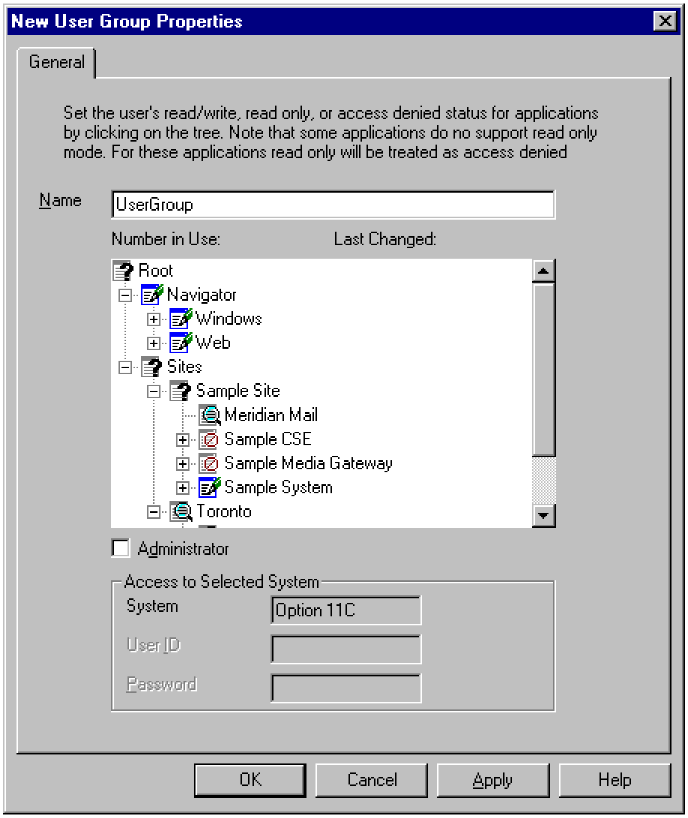


User Group	Number In Use	Last Changed
Administrators	2	12/08/01 15:51:57
Default	1	12/08/01 15:58:45
EndUser	2	12/08/01 16:45:04
HelpDesk	1	12/08/01 15:53:49

2 Choose Configuration > Add User Group. The new user group is created with the same access privileges as the highlighted user group. The New User Group Properties dialog box opens (Figure 102).

The Administrators, Default, EndUser, and HelpDesk User Groups are always available and cannot be deleted. You can modify all groups except for Administrators. The Administrators User Group has access to all Windows-based and Web-based OTM applications.

Figure 102 New User Group Properties dialog box



New User Group Properties

General

Set the user's read/write, read only, or access denied status for applications by clicking on the tree. Note that some applications do no support read only mode. For these applications read only will be treated as access denied

Name UserGroup

Number in Use:

Last Changed:

☐ Administrator

Access to Selected System

System Option 11C

User ID

Password

3 Enter a name for this User Group.

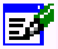
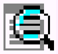
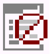
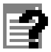
For each site, system, and application in the tree, use the right mouse button to assign user privileges (Read-write, Read-only, or No Access). Each click of the right mouse button causes the access privileges and corresponding icon to change (Table 7). Select the Administrator box, if appropriate. The site and system icons change to reflect the access level.

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

The question mark icon indicates that the sub-items belonging to the item displaying the question mark icon have mixed access settings.

4

Table 7 Access privilege icons

Icon	Explanation
	Read and write access
	Read only access
	No access
	Indicates that the access privileges in the branch are mixed between one or more of the above levels

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

6 Click OK to save changes and close the User Group Properties dialog box.

Adding a user

User accounts should be added here rather than through the Windows NT or Windows 2000 user management tools.

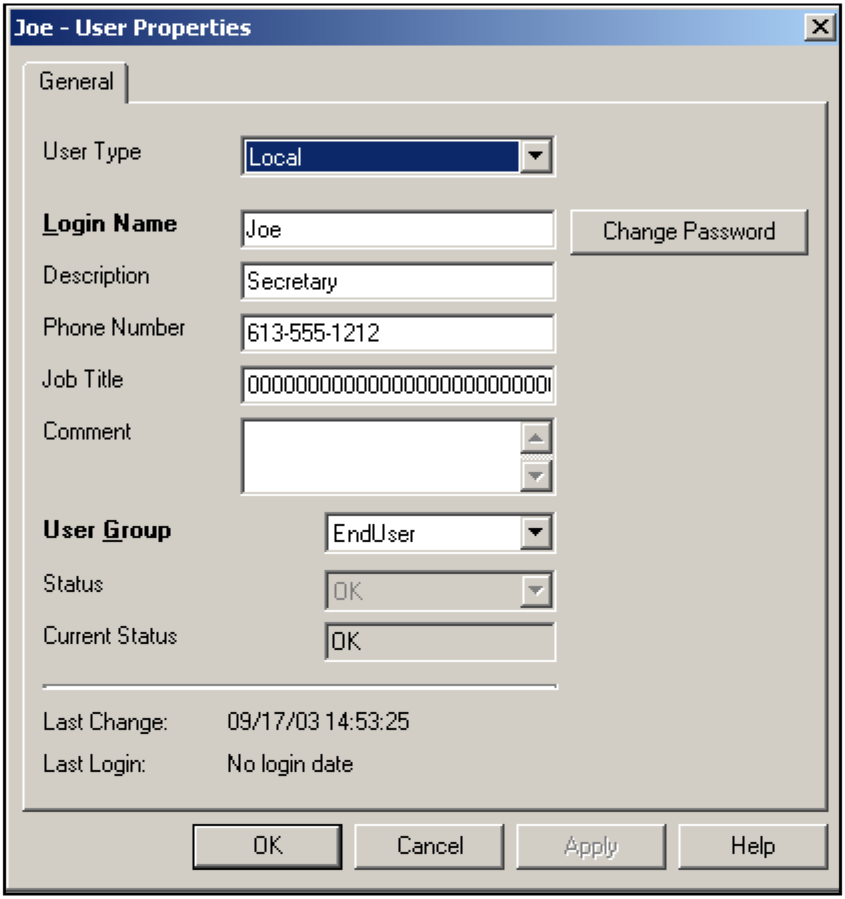
The “Administrator” user account for the Windows NT or Windows 2000 OS does not appear in the OTM Users window. This is to prevent users from changing the Administrator account password from within OTM.

Even though it is not listed in the Users window, the OS Administrator account can always be used to log in to OTM.

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

The User Properties dialog box opens (Figure 103).

Figure 103 User Properties dialog box



Joe - User Properties

General

User Type: Local

Login Name: Joe

Description: Secretary

Phone Number: 613-555-1212

Job Title: 000000000000000000000000000

Comment:

User Group: EndUser

Status: OK

Current Status: OK

Last Change: 09/17/03 14:53:25

Last Login: No login date

2 Select a User Type from the drop-down list:

- Local - Users who are authenticated using an account on the OTM Server.
- Remote - Users who are authenticated using either a Windows NT Domain account or LDAP.

When Remote is selected, the Change Password button as well as the Status and Current Status controls are disabled.

3 Enter a User ID.

4 From the User Group drop-down list, select the group that you will use as the basis for this user definition.

5 Fill in other data as required.

6 Click Apply. OTM prompts you to enter a password.

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

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

Authenticating users

You can select any of the following three methods or combination of these methods to authenticate OTM users:

- Local OTM Server account
- Windows NT Domain account
- LDAP authentication

The Administrator account will always be authenticated through the local server account because it is a default account on all supported Windows platforms.

The default authentication method is the Local OTM Server account. This method provides the best login performance because there is no requirement to search the OTM directory for the user's assigned User Group.

Procedure

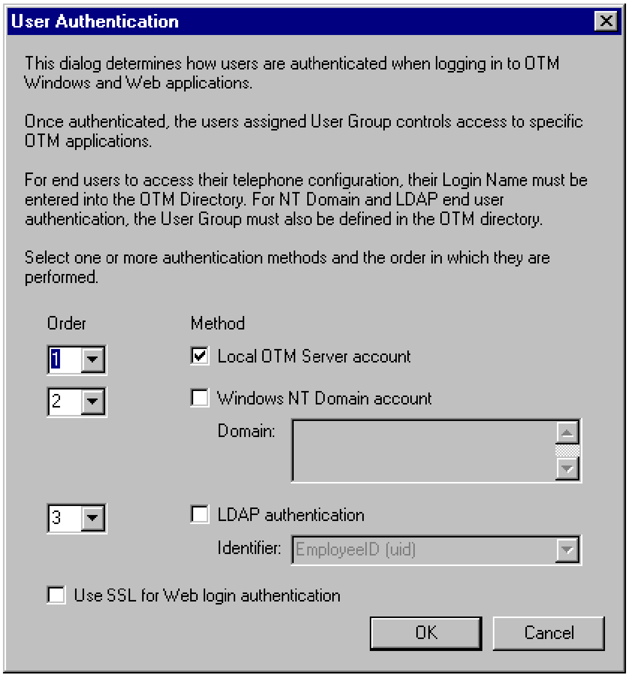
To configure authentication:

1 From the OTM Windows Navigator, select Security > User Authentication.

The User Authentication dialog box appears (Figure 104).

Authentication methods can also be configured using the Web navigator. See "User authentication" on page 197.

Figure 104 User Authentication dialog box



User Authentication

This dialog determines how users are authenticated when logging in to OTM Windows and Web applications.

Once authenticated, the users assigned User Group controls access to specific OTM applications.

For end users to access their telephone configuration, their Login Name must be entered into the OTM Directory. For NT Domain and LDAP end user authentication, the User Group must also be defined in the OTM directory.

Select one or more authentication methods and the order in which they are performed.

Order	Method
1	☑ Local OTM Server account
2	☐ Windows NT Domain account Domain:
3	☐ LDAP authentication Identifier: EmployeeID (uid)

☐ Use SSL for Web login authentication

2 Use the check boxes to select one or more of the available authentication methods.

a If you select Windows NT Domain account, enter one or more domains in the Domain text box.

Note: You must separate the domain names with a comma. Do not use any spaces.

b If you select LDAP authentication, use the drop-down list to choose either EmployeeID (uid), or EMail (email).

3 Use the drop-down lists to assign the order in which the authentication methods are performed.

If you choose multiple authentication methods, OTM respects the configured order; however, it should be noted that the best performance is achieved by using the Local OTM Server account method.

4 To use the secure socket layer (SSL) during the authentication process, the OTM Server must have the required certificate installed as described in *\Nortel\Common Services\Program Files\SSL\Setting SSL on OTM*

Server.doc. Click the “Use SSL for Web login authentication” check box after installing the certificate.

If the OTM Server has the required certificate installed, setting the check box causes OTM to use SSL encrypted transport during authentication. In this case, Web login is performed using https:// rather than http://, and the traffic is encrypted. The OTM Server automatically switches to non-SSL transport once the user is successfully authenticated.

5 The selected method(s) are used to authenticate users on all OTM platforms: OTM Server, OTM Client, and OTM Web Client.

Adding OTM Web Navigator users

This section contains information on:

- Web Navigator capabilities
- User login and security
- Access permissions
- User authentication
- User groups
- Desktop services

Access to the OTM Web Navigator is set up using the users and groups functionality in Windows NT and Windows 2000. User authentication can also be accomplished using Windows NT domain accounts or LDAP. Domain accounts and LDAP authentication are normally used for end users who will be accessing Web Desktop Services to administer their telephones.

Capabilities

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, and so on) on Meridian 1 or Succession CSE 1000 system hardware
- OTM Web configuration pages (login access, LDAP sync reports, and so on)

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

User login and security

Users log 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 computer.

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 user's access to only some of the OTM Web-based functionality. The OTM Web Navigator controls access to applications by shielding Web links to which the user does not have access. 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 "User Groups" on page 199.

Precaution

As a security precaution, with any upgrade or reinstallation of OTM software, access profiles for all user groups except Administrator are reset. By 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 plug-ins.

Plug-ins

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 the user's hard disk, and then it installs itself onto the computer.

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

Default URL

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 set up on the OTM Server.

Administrator Group access permissions

Persons belonging to the Administrators user group on the OTM Server can log in 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.

French or German OS

Important advice for localized operating systems — The name of the administrators user group in the French and German operating systems is not Administrators. These names are localized by Microsoft in the regional operating system software. In a default French installation of Windows NT or Windows 2000, the local administrators user group is Administrateurs. In the German version this user group is Administratoren. When installed on a French or German OS, the OTM predefined administrators user group will be named Administrateurs or Administratoren to match the OS.

User group access rights

You, the network administrator, log in to the OTM Administration Web site and assign access rights to the other user 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 User Groups 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. For new groups, the Administrator must assign access rights for Web applications before any users from that group can log in. For information about setting user access, refer to "User Groups" on page 199.

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. User may belong to other groups, but if they belong to the Administrators group, the Administrators profile overrides 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 can result in members of the user group being denied access to the Web site.

User authentication

You can select any of the following three methods or combination of these methods to authenticate OTM users:

- Local OTM Server account
- Windows NT Domain account
- LDAP authentication

The Administrator account is always authenticated through the local server account because it is a default account on all supported Windows platforms.

The default authentication method is the Local OTM Server account. This method provides the best login performance because there is no requirement to search the OTM directory for the user's assigned User Group.

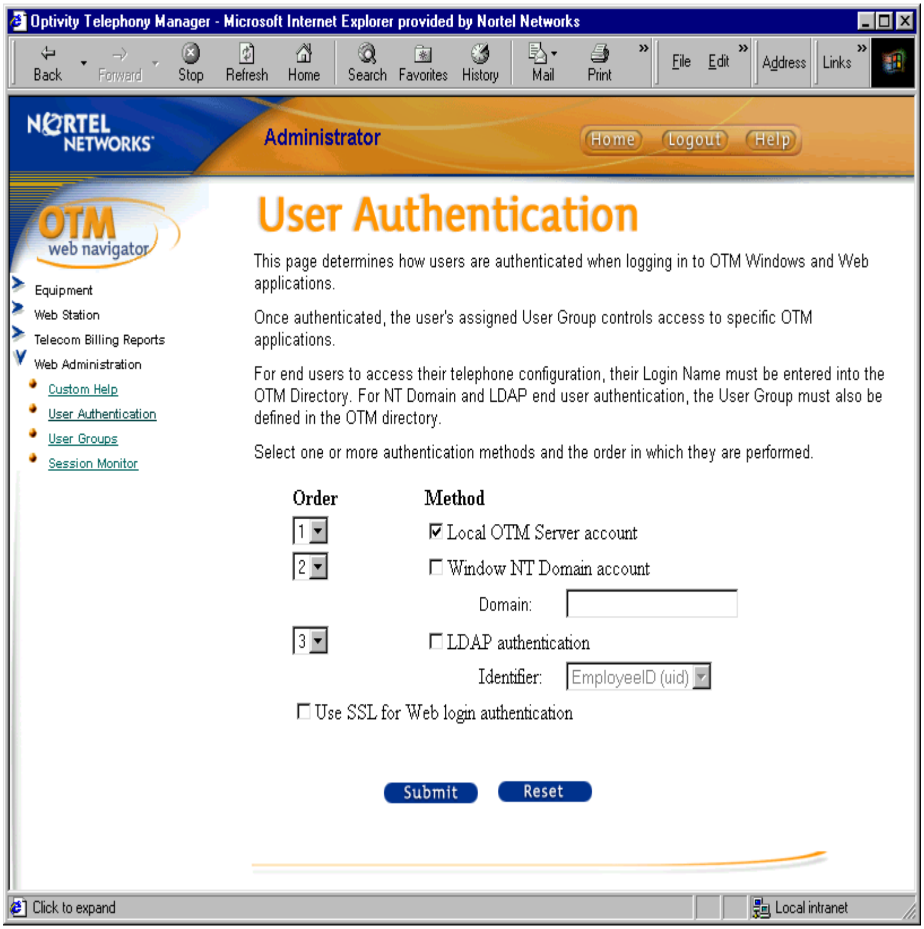
Procedure

To configure authentication:

1. Under Web Administration in the OTM Web Navigator tree, select User Authentication.

   The User Authentication page appears (Figure 105).

Figure 105 User Authentication page



User Authentication

This page determines how users are authenticated when logging in to OTM Windows and Web applications.

Once authenticated, the user's assigned User Group controls access to specific OTM applications.

For end users to access their telephone configuration, their Login Name must be entered into the OTM Directory. For NT Domain and LDAP end user authentication, the User Group must also be defined in the OTM directory.

Select one or more authentication methods and the order in which they are performed.

Order	Method
1	☑ Local OTM Server account
2	☐ Window NT Domain account
	Domain:
3	☐ LDAP authentication
	Identifier: EmployeeID (uid)

☐ Use SSL for Web login authentication

2 Use the check boxes to select one or more of the available authentication methods.

  a If you select Windows NT Domain account, enter one or more domains in the Domain text box.

Note: You must separate the domain names with a comma. Do not use any spaces.

  b If you select LDAP authentication, use the drop-down list to choose either EmployeeID (uid), or EMail (email).

3. Use the drop-down lists to assign the order in which the authentication methods are performed.

   If you choose multiple authentication methods, OTM respects the configured order; however, it should be noted that the best performance is achieved by using the Local OTM Server account method.

4. To use the secure socket layer (SSL) during the authentication process, the OTM Server must have the required certificate installed as described in *\Nortel\Common Services\Program Files\SSL\Setting SSL on OTM Server.doc*. Click the “Use SSL for Web login authentication” check box after installing the certificate.

   If the OTM Server has the required certificate installed, setting the check box causes OTM to use SSL encrypted transport during authentication. In this case, Web login is performed using https:// rather than http://, and the traffic is encrypted. The OTM Server automatically switches to non-SSL transport once the user is successfully authenticated.

5. The selected method(s) are used to authenticate users on all OTM platforms: OTM Server, OTM Client, and OTM Web Client.

For information on configuring users for desktop access, see “Enable Web desktop access in the OTM Directory” on page 210.

Authentication methods can also be configured using the Windows navigator. See “User authentication” on page 197.

User Groups

Navigator access is controlled by user group. A user’s User Group assignment determines which features are available on the Telephone features page. You also use the User Groups page to indicate which users are permitted to make changes to the General and Keys pages.

User groups must be added and deleted in the OTM Windows Navigator. See “Creating a user group” on page 186.

OTM is shipped with the following User Groups and corresponding access rights:

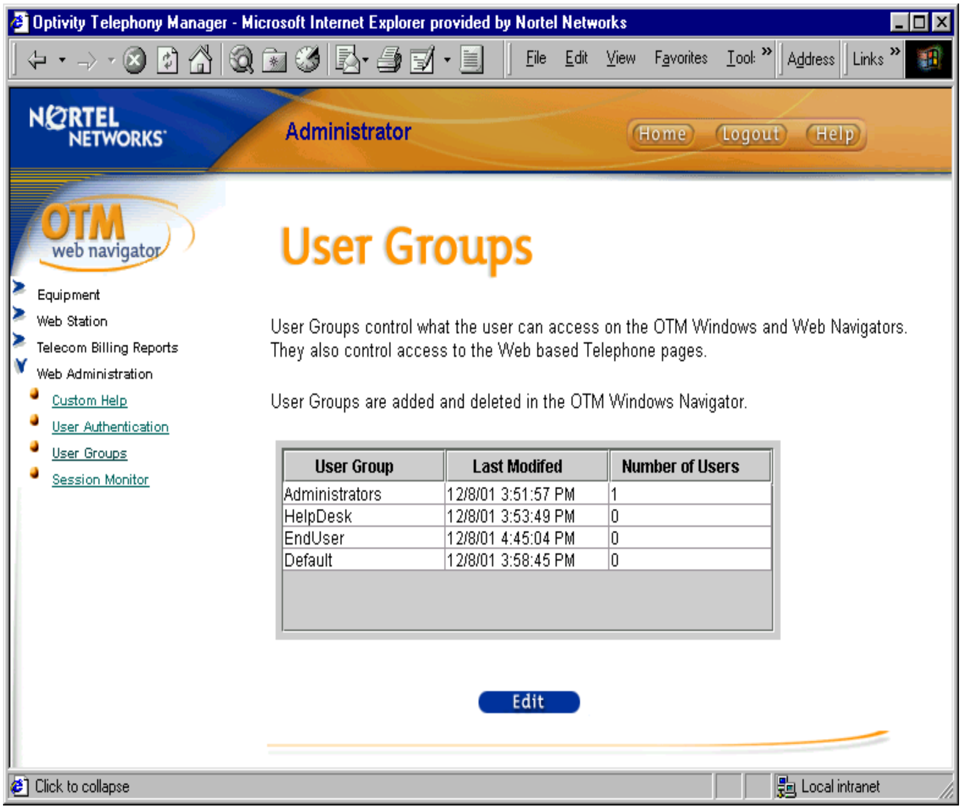
- Administrators

  - — Full read/write access rights. Access rights cannot be changed for this user group.
- HelpDesk
  - — Full access to all Web Navigator tree items except those under Web Administration.
  - — Full access to Web Desktop Services, including read/write and synchronization capabilities.
  - — Full access to Windows Navigator applications with the exception of ITG Services.
- EndUser
  - — No access to Web or Windows Navigator applications.
  - — Web Desktop Services is read only. Only 21 features are available; the rest are hidden.
- Default
  - — No access.

To view the available User Groups, click the User Groups link located under Web Administration in the OTM Web Navigator tree.

The User Groups page appears (Figure 106).

Figure 106 User Groups page



User Groups

User Groups control what the user can access on the OTM Windows and Web Navigators. They also control access to the Web based Telephone pages.

User Groups are added and deleted in the OTM Windows Navigator.

User Group	Last Modifed	Number of Users
Administrators	12/8/01 3:51:57 PM	1
HelpDesk	12/8/01 3:53:49 PM	0
EndUser	12/8/01 4:45:04 PM	0
Default	12/8/01 3:58:45 PM	0

Navigator access

Access to the sites, systems, and applications available in both the Windows and Web Navigators is controlled on a user-group basis through the User Group Properties Java application.

When the user group name is entered into the User Group field in an OTM user’s Directory record, the entry must match the user group name exactly. This is primarily a concern when OTM is operating in a language other than English. In this case, the access profile name “HelpDesk” may have been translated into the local language.

To modify the access rights of a user group:

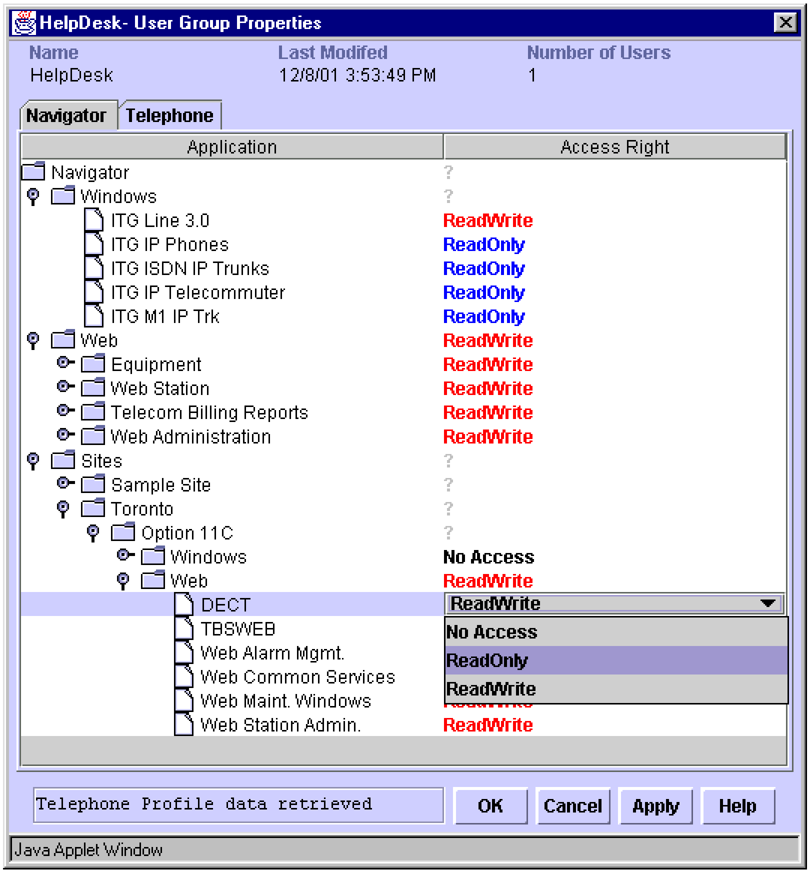
1 Click to select a User Group.

2 Click Edit.

The User Group Properties Java application launches, and the User Group Properties dialog box for the selected user group appears (Figure 107).

Alternatively, you can double-click the user group to display the User Group Properties dialog box for the selected user group.

Figure 107 User Group Properties dialog box—Navigator tab



HelpDesk- User Group Properties

Name	Last Modifed	Number of Users
HelpDesk	12/8/01 3:53:49 PM	1

Application	Access Right
Navigator	?
Windows	?
ITG Line 3.0	ReadWrite
ITG IP Phones	ReadOnly
ITG ISDN IP Trunks	ReadOnly
ITG IP Telecommuter	ReadOnly
ITG M1 IP Trk	ReadOnly
Web	ReadWrite
Equipment	ReadWrite
Web Station	ReadWrite
Telecom Billing Reports	ReadWrite
Web Administration	ReadWrite
Sites	?
Sample Site	?
Toronto	?
Option 11C	?
Windows	No Access
Web	ReadWrite
DECT	ReadWrite
TBSWEB	
Web Alarm Mgmt.	
Web Common Services	
Web Maint. Windows	
Web Station Admin.	ReadWrite

Telephone Profile data retrieved

Java Applet Window

The Access Right column lists the level of access allowed for each site, system, and application. This is the same tree structure and performs the same function as the Windows-based New User Group Properties dialog box (Figure 102 on page 187).

The question mark indicates that the sub-items belonging to the item displaying the question mark have mixed access settings.

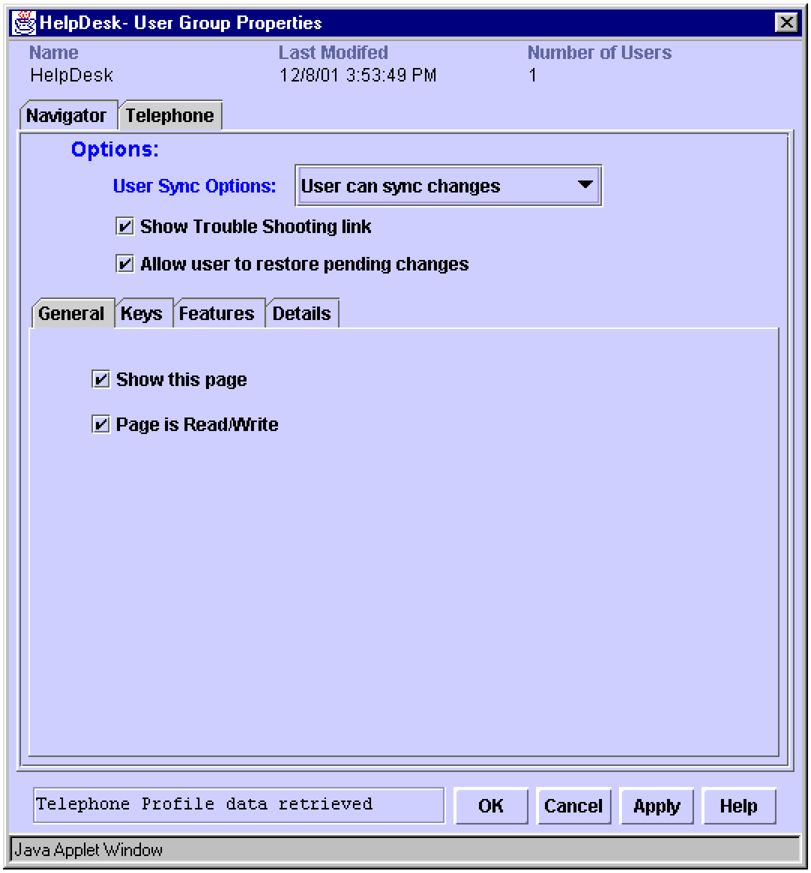
To modify access rights:

1. Use the drop-down list to select ReadWrite, ReadOnly, or No Access for each item in the tree.
2. Click Apply.

Telephone access

The Telephone tab in the User Group Properties dialog box is used to control access to the telephone pages on the Web for each user group (Figure 108).

Figure 108 Telephone access properties dialog box—General Tab



HelpDesk- User Group Properties

Name: HelpDesk
Last Modifed: 12/8/01 3:53:49 PM
Number of Users: 1

Navigator | Telephone

Options:

User Sync Options: User can sync changes

☑ Show Trouble Shooting link

☑ Allow user to restore pending changes

General | Keys | Features | Details

☑ Show this page

☑ Page is Read/Write

Telephone Profile data retrieved

The options that are configured in the upper section of this dialog box are applicable to all of the tabs in telephone pages. These options include:

- Allowing or denying this group the ability to synchronize changes with the system. If synchronization is denied, you must manually synchronize the changes with the system using Station Administration.
- Determining whether the troubleshooting link appears at the top of the telephone page for members of this group.

- Allowing or denying this group the ability to restore changes that have been made to a telephone.

To configure telephone access options:

1. Use the drop-down list to select either “User can sync changes” or “User cannot sync changes.”
2. Click the “Show Trouble Shooting link” check box to enable this option.

   For EndUsers, clicking the link displays the Telephone Troubleshooting Help page which includes a reset button.

   For Web Navigator users, clicking the link displays the maintenance page for the telephone with all of the available commands.
3. Click the “Allow users to restore pending changes” check box to permit the users in this group to restore the changes made to a telephone.
4. Click Apply to apply your changes.

General tab

In the General tab, you use check boxes to determine whether the Telephone—General page will appear for this user group and whether the users in this group will be able to make changes to this Telephone page. The Telephone—General page contains information such as site, system, location, and TN, which may not be appropriate for or valuable to end users.

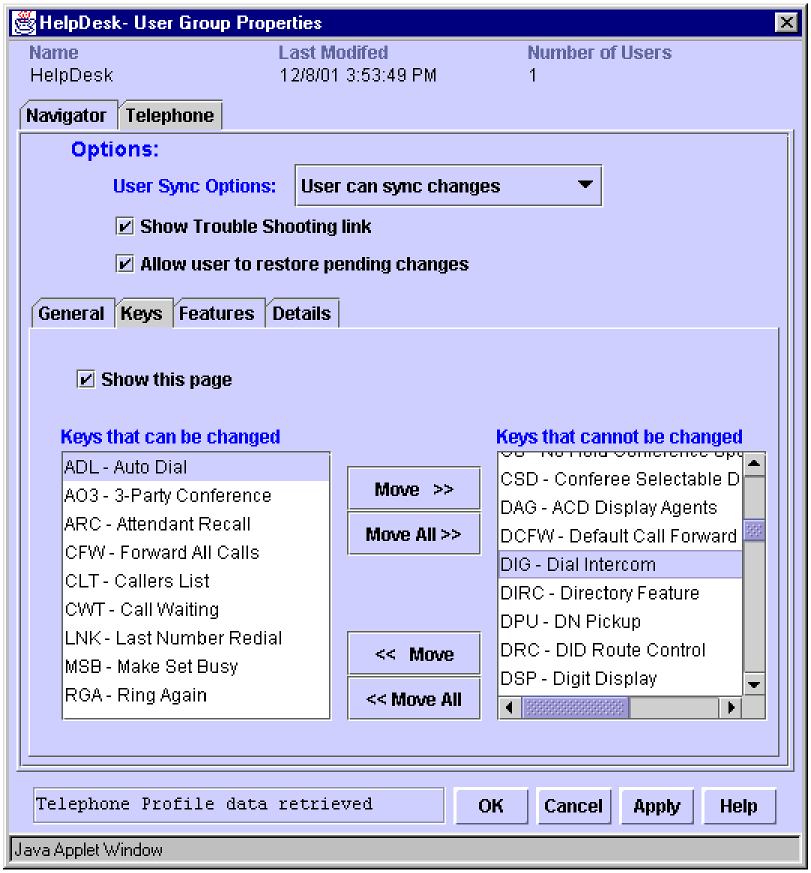
To configure the Telephone—General page:

1. Click the “Show this page” check box to allow this user group to be able to view the Telephone—General page.
2. Click the “Page is Read/Write” check box to allow users in this group to make changes to the information that appears in this telephone page.
3. Click Apply to apply your changes.

Keys tab

In the Keys tab (Figure 109), you use the check box and lists of key-based features to determine whether the Telephone—Keys page appears and, if so, which keys the users in this group can to change.

Figure 109 Telephone access properties dialog box—Keys tab



HelpDesk- User Group Properties

Name: HelpDesk
Last Modifed: 12/8/01 3:53:49 PM
Number of Users: 1

Options:

User Sync Options: User can sync changes

☑ Show Trouble Shooting link

☑ Allow user to restore pending changes

☑ Show this page

Keys that can be changed:

ADL - Auto Dial
AO3 - 3-Party Conference
ARC - Attendant Recall
CFW - Forward All Calls
CLT - Callers List
CWT - Call Waiting
LNK - Last Number Redial
MSB - Make Set Busy
RGA - Ring Again

Keys that cannot be changed:

CSD - Conferee Selectable D
DAG - ACD Display Agents
DCFW - Default Call Forward
DIG - Dial Intercom
DIRC - Directory Feature
DPU - DN Pickup
DRC - DID Route Control
DSP - Digit Display

Telephone Profile data retrieved

To configure the Telephone—Keys page:

1. Click the “Show this page” check box to allow this user group to be able to view the Telephone—Keys page.

2. Use the Move and Move All buttons to move the key-based features that this user group can change into the left column.

   By putting keys into the left column, users in this group can interchange these key types and change the key parameters.

   If the user selects a key that is not in the left-hand column while viewing the Telephone—Keys page, the Change button does not appear.

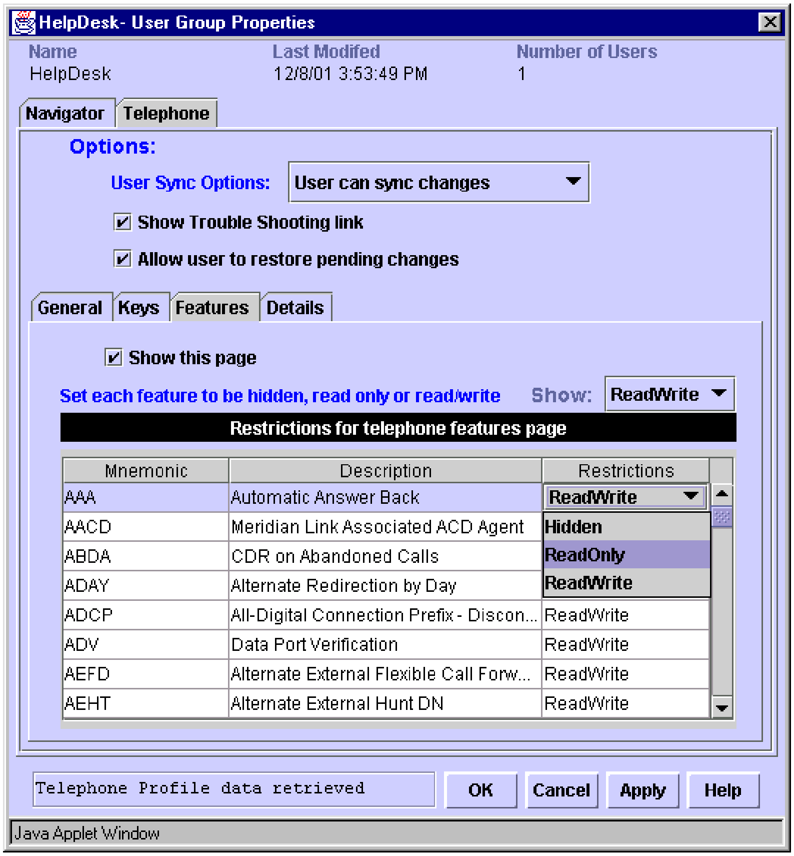
   Click Apply to apply your changes.

Features tab

In the Features tab (Figure 110), you use the check box and list of features to determine whether the Telephone—Features page appears and, if so, which features the users in this group can view and change. The list of features contains all the non-key features listed alphabetically by prompt in LD 10 and LD 11. Each feature is assigned a restriction of Hidden, ReadOnly, or ReadWrite. If Hidden, the feature does not appear in the end user Feature drop-down list.

Read/Write capability requires the OTM Premium package.

Figure 110 Telephone access properties dialog box—Features tab



HelpDesk- User Group Properties

Name: HelpDesk
Last Modifed: 12/8/01 3:53:49 PM
Number of Users: 1

Options:

User Sync Options: User can sync changes

☑ Show Trouble Shooting link

☑ Allow user to restore pending changes

☑ Show this page

Set each feature to be hidden, read only or read/write   Show: ReadWrite

Restrictions for telephone features page

Mnemonic	Description	Restrictions
AAA	Automatic Answer Back	ReadWrite
AACD	Meridian Link Associated ACD Agent	Hidden
ABDA	CDR on Abandoned Calls	ReadOnly
ADAY	Alternate Redirection by Day	ReadWrite
ADCP	All-Digital Connection Prefix - Discon...	ReadWrite
ADV	Data Port Verification	ReadWrite
AEFD	Alternate External Flexible Call Forw...	ReadWrite
AEHT	Alternate External Hunt DN	ReadWrite

Telephone Profile data retrieved

To configure the Telephone—Features page:

1 Click the "Show this page" check box to allow this user group to be able to view the Telephone—Features page.

2 Use the drop-down lists in the Restrictions column to configure each feature as ReadWrite, ReadOnly, or Hidden.

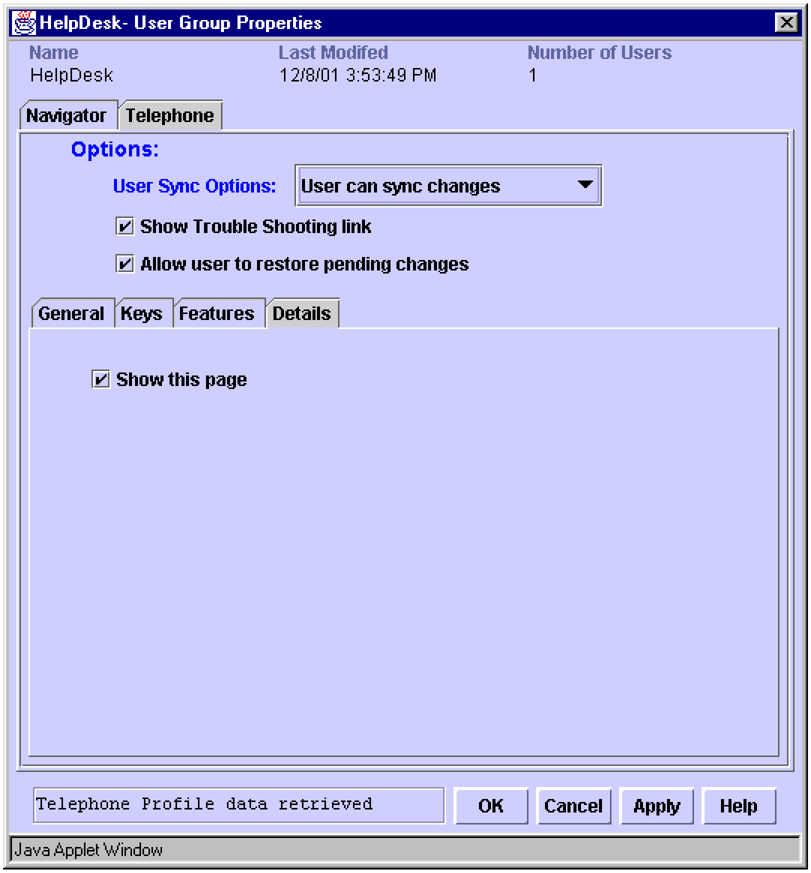
   The Show drop-down list contains All, Hidden, ReadOnly, and ReadWrite. This is used to limit the size of the list.

3 Click Apply to apply your changes.

Details tab

In the Details tab (Figure 111), you use the check box to determine whether the Telephone—Details page appears.

Figure 111 Telephone access properties dialog box—Details tab



HelpDesk- User Group Properties

Name	Last Modifed	Number of Users
HelpDesk	12/8/01 3:53:49 PM	1

Options:

User Sync Options: User can sync changes

☑ Show Trouble Shooting link

☑ Allow user to restore pending changes

☑ Show this page

Telephone Profile data retrieved

Installing and Configuring Desktop Services

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

1 Install OTM. See “Adding OTM Web Navigator users” on page 193.

2 Create Windows NT accounts for Help Desk users and End Users as required.

3 Log in to the Web Navigator as Administrator, and go to the User Groups page.

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.

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

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

5 Enter the Help Desk user's Login Name and Access Profile in the user's OTM Directory entry. See "Enable Web desktop access in the OTM Directory" on page 210.

6 Enter the End User's Login Name and Access Profile in the user's OTM Directory entry. See "Enable Web desktop access in the OTM Directory" next.

7 Select the desired Web Reporting Role in the user's OTM Directory entry.

Enable Web desktop access in the OTM Directory

You can give End Users an account on the OTM server using the same process that is used to allow Administrators and Help Desk users to access the Windows and Web Navigators; however, End Users are typically authenticated through a Windows NT domain account or LDAP. End Users do not normally have accounts on the OTM Server. When the Windows NT domain or LDAP authentication method is used, mapping for the following attributes is performed using the OTM Directory:

- Login Name - required to associate users with their telephones
- User Group - determines what users can see and changes that they can make on their telephones
- Web Reporting Access Rights - controls access to Web TBS billing reports

With LDAP, it is possible to determine the User Group during authentication. For this to occur, the LDAP directory must support the OTMUserGroup attribute, and return the User Group value with the authentication.

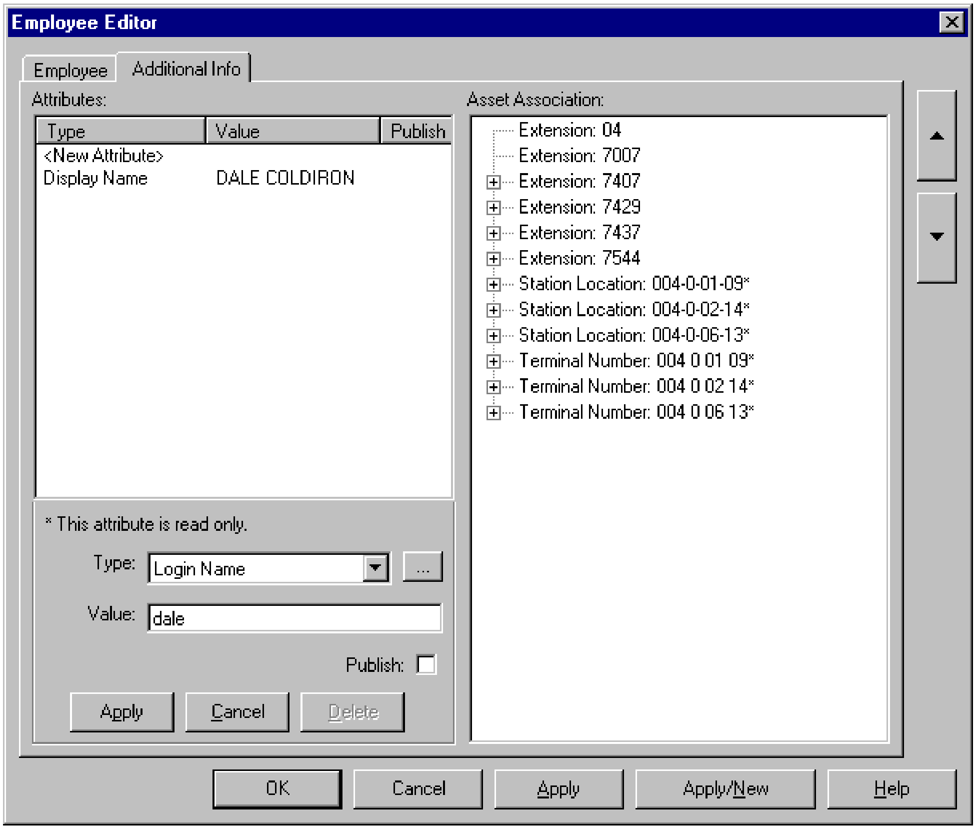
1 From Station Administration, select View > Employee Selector.

2 Double-click an employee's name in the Employee Selector window.

The Employee Editor window for the selected employee appears.

3 Click the Additional Info tab in the Employee Editor window (Figure 112).

Figure 112 Entering Login Name attribute



Type	Value	Publish
<New Attribute>		
Display Name	DALE COLDIRON	

Extension: 04
Extension: 7007
Extension: 7407
Extension: 7429
Extension: 7437
Extension: 7544
Station Location: 004-0-01-09*
Station Location: 004-0-02-14*
Station Location: 004-0-06-13*
Terminal Number: 004 0 01 09*
Terminal Number: 004 0 02 14*
Terminal Number: 004 0 06 13*

* This attribute is read only.

Type: Login Name

Value: dale

Publish: □

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 NT is the authentication method chosen for desktop users).

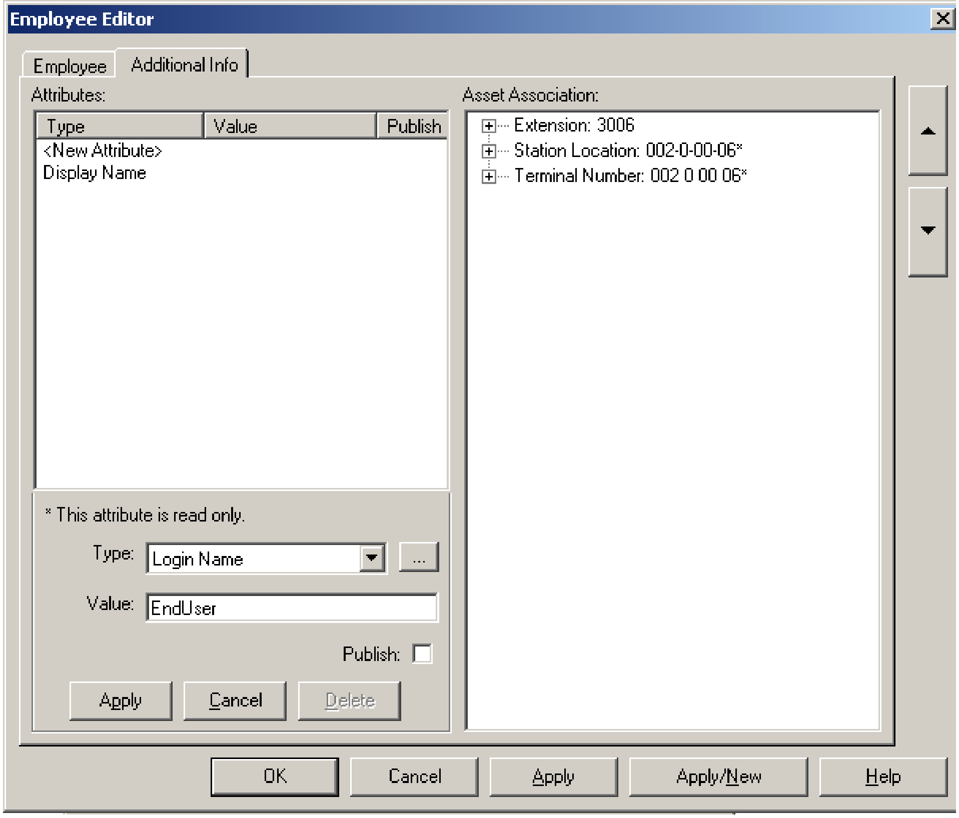
7 Click the “Publish” check box to enable synchronization with an optional LDAP-compliant server.

8 Click Apply in the Attributes pane.

9 Select <New Attribute> in the Attributes pane.

10 Select User Group from the Type drop-down box (Figure 113).

Figure 113 Entering User Group attribute



Type: Login Name

Value: EndUser

Publish: □

11 Select EndUser from the attribute Value drop-down list to enable End User Web desktop user access, both for LDAP and Windows NT access.

Select HelpDesk from the attribute Value drop-down list to enable Help Desk Web desktop user access, both for LDAP and Windows NT access.

12 Click Apply in the Attributes Pane.

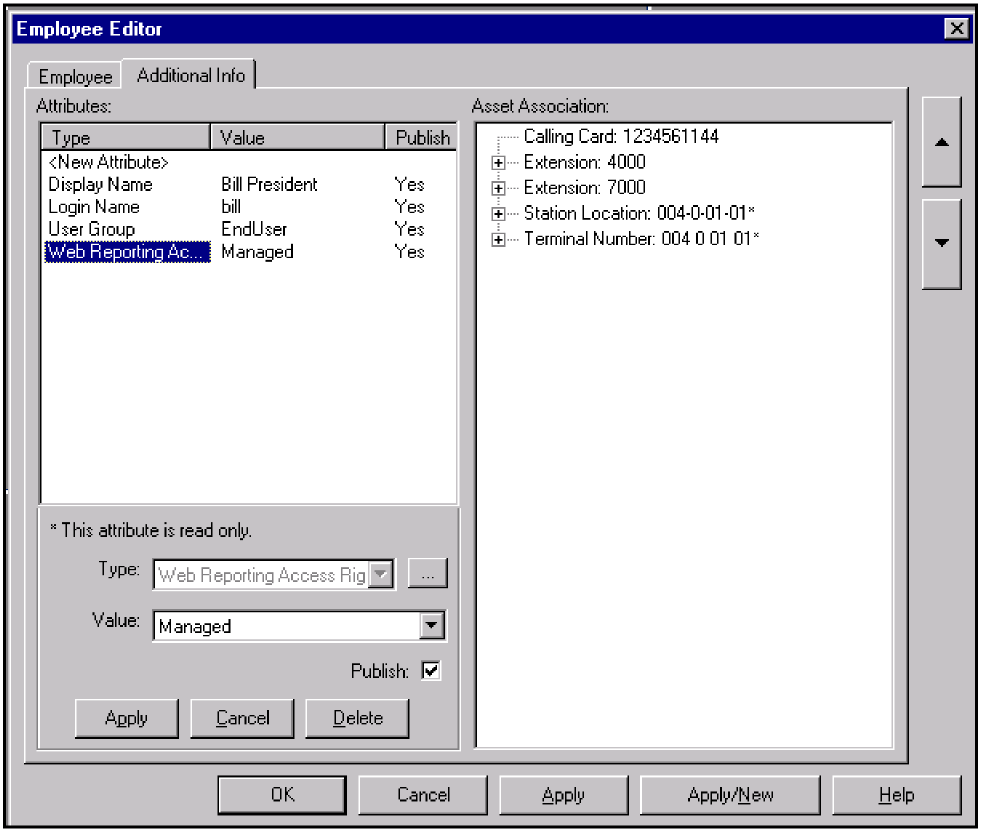
13 Select <New Attribute> in the Attributes pane.

14 Select Web Reporting Access Rights from the Type drop-down box (Figure 114).

15 Select one of the following access levels for the attribute value:

- All - Users assigned this role have the authority to view all the reports for the site/systems to which they are assigned. This is the access level that you typically assign to an Administrator.
- Peer - Users assigned this role have the authority to view the reports for all the entities in the same node in the Organizational Hierarchy and all its sub-nodes. This is the access level that you typically assign to a person who manages several departments.
- Managed - Users assigned this role have the authority to view their own reports and the reports for all of the entities in the sub-nodes below their organization node in the Organizational Hierarchy. This is the access level that you typically assign to a department manager.
- Personal - Users assigned this role have the authority to view their own data. This is the access level that you assign to a non-managerial employee.
- No Access - If no role is assigned for a user, their reporting access rights default to No Access.

Figure 114 Entering Web Reporting Access Rights attribute



Type	Value	Publish
<New Attribute>		
Display Name	Bill President	Yes
Login Name	bill	Yes
User Group	EndUser	Yes
Web Reporting Ac...	Managed	Yes

Calling Card: 1234561144
Extension: 4000
Extension: 7000
Station Location: 004-0-01-01*
Terminal Number: 004 0 01 01*

* This attribute is read only.

Type: Web Reporting Access Rig

Value: Managed

Publish: ☑

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

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

Setting up the Meridian 1 or Succession system

This section contains information on:

- Setting up a system
- Determining IP address
- Enabling system alarms

Setting up a system

Follow this procedure to set up a system.

1. Verify that the Meridian 1 or Succession system has the following system configuration:
   - The appropriate X11 release, configured with the appropriate packages
   - 48 MB 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 attach one cable to each IOP, IOP/CMDU, or IODU/C.
     - — For Option 11C, an NTDK27AA Ethernet cable
2. For Ethernet networks, you 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

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

  - For 10Base2 cabling, an RG58 cable with BNC connectors

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

- For the 10BaseT interface, an Ethernet hub

Caution: If you plan to connect the Meridian 1 or Succession CSE 1000 system to a corporate network, you require an Ethernet gateway or router to separate the system from the corporate network. If you connect the Meridian 1 or Succession CSE 1000 system without a gateway or router, you will adversely affect the system's call handling ability.

3 For PPP communication, you need the following:

- Hayes command compatible modem
- Modem cables
- For Meridian 1 or Succession CSE 1000 SDI ports, user type MTC and SCH set in LD 17

4 For serial communication, you 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
- For Meridian 1 and Succession SDI ports, the appropriate user type set in LD 17 for each OTM application (Table 8)

Table 8 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 system:

User input is shown in **`bold`** following the > prompt (for example, >**`LD 17)`**.

a Install the appropriate release (minimum is Release 22 for Meridian 1, and Release 25.30 for Succession systems) of software.

b Perform an INIT.

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

d Configure LAPW. OTM communicates with the Meridian 1 and Succession systems through LAPW IDs and passwords configured on the Meridian 1 and Succession systems.

e 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 *Features and Services* (553-3001-306).

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

`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
```

f 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
```

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. Alert others of any changes (for example, all technicians with access to the Meridian 1 or Succession 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
```

6 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 Succession 1000M Cabinet and Meridian 1 Option 11C Cabinet 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
```

7 Configure Ethernet and PPP at the Meridian 1 or Succession CSE 1000 system:

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 the 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 the 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 LOCAL_PPP 47.0.0.2
  >CHG PPP LOCAL LOCAL_PPP M1ACTIVEIP

  >LD 117
  >NEW HOST REMOTE_PPP 47.0.0.3
  >CHG PPP REMOTE REMOTE_PPP 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`** (disable Ethernet interface)
  .**`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 must INIT the Meridian 1 or Succession CSE 1000 system.

Determining the OTM PC IP address

To find your PC's IP address using Windows™ 9x:

1. From Start, select Settings > Control Panel. The Control Panel window appears.
2. Open the Network icon to display the tabbed dialog box. Click the Configuration tab. A list of installed network components is presented.
3. Select the TCP/IP network component used by your PC. Based on the number of installed components, you may have to scroll to see the correct component.
4. With the component selected, click Properties. The TCP/IP tabbed window appears.
5. Click the IP Address tab. Note the IP address shown. This is the IP address unique to this PC. You 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 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 appears.

2 Click Ethernet/PPP (Overlay Passthru), and then click OK.

The System Terminal window appears.

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 appears. 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 "Determining the OTM PC IP address" on page 223 for more information.

Caution: If you assign your IP address to a slot currently in use, it disconnects that user from the system preventing the user from receiving alarm information.

7 Enter

```
prt open_alarm
```

The list of slots and IP addresses receiving alarms appears. Verify that your particular slot and IP address are included.

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.

Configuring Succession systems for survivability

This section contains information on:

- Configuring IP line data for Succession 1000M and Succession 3.0
- Transmitting configuration data to the line cards

Configuring IP Line data for a Succession 1000M Cabinet system

When distributing IP Line cards across different Survivable Expansion Cabinets, you can configure the Survivable Expansion Cabinets 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 IP Line cards. For a remote location, the Survival IP address of the IP 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 is configured to a single Survivable Expansion Cabinet SSC IP address.

The information below provides more information on these two options:

Separate nodes for expansion cabinets

Configuring survivable expansion cabinets in separate nodes for IP Line cards is mandatory if survivable expansion cabinets are in a different location from 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 IP Line card fails, IP telephones can register to another IP Line card only if it is contained within the same cabinet.
- Users cannot make IP telephone calls from one Survivable Expansion Cabinet to another.

Same node for IP Line cards

- Trunks and Gateway channels are only available for IP telephones on one Survivable Expansion Cabinet but can be used by all IP Line cards.
- Less administration is required since there is only one node to manage.
- If the IP Line cards fails, IP telephones can register to other IP Line cards in different Survivable Expansion Cabinets.
- Users can make IP telephone calls from one Survivable Expansion Cabinet to another.

Summary of steps to configure IP Line data on OTM

Refer to “Configuration of IP Telephony node using OTM 2.1” *IP Line: Description, Installation, and Operation* (553-3001-365), for a detailed description of these steps.

1 Manually add an IP Line 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 IP Line card properties.

3 Configure the DSP profile data.

4 Configure the Main Cabinet ELAN IP address, Survivable Expansion Cabinet ELAN 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 115).

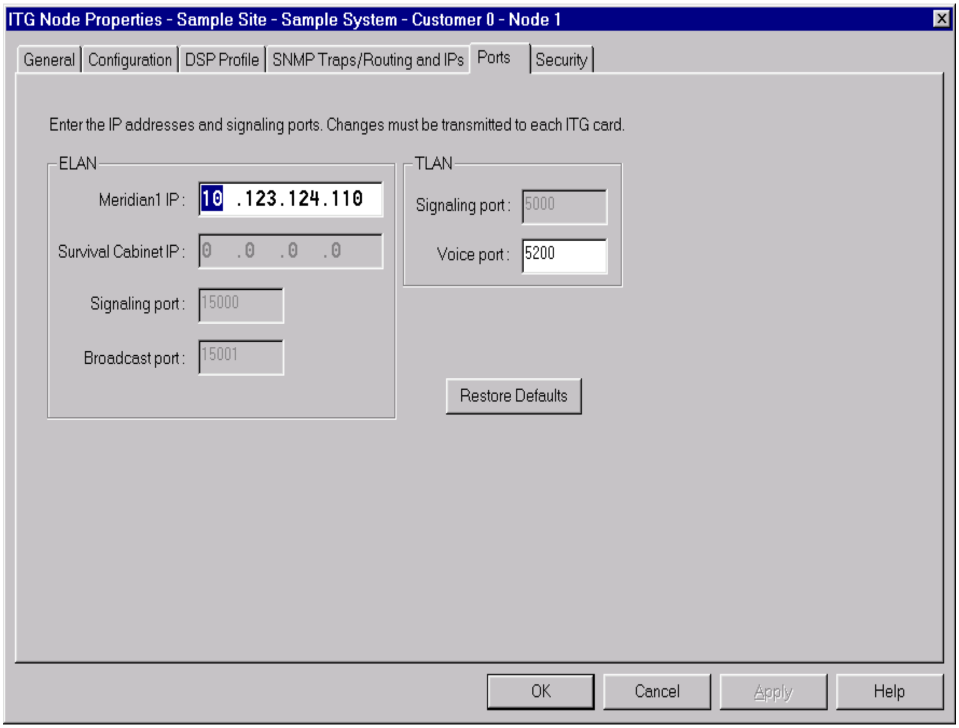
The ELAN IP address of the Survivable Expansion Cabinet must be on the same subnet as the Main Cabinet. If the Expansion Cabinet is on a different subnet, use the VLAN concept to keep both ELAN addresses on the same subnet.

5 Configure SNMP traps and the ELAN GW Routing table.

6 Configure security for SVMP access.

7 Configure the Alarm Notification feature in OTM.

Figure 115 ITG IP Phones - ITG Node Properties dialog box - Ports tab



ITG Node Properties - Sample Site - Sample System - Customer 0 - Node 1

Enter the IP addresses and signaling ports. Changes must be transmitted to each ITG card.

ELAN

Meridian1 IP: 10 .123.124.110

Survival Cabinet IP: 0 .0 .0 .0

Signaling port: 15000

Broadcast port: 15001

TLAN

Signaling port: 5000

Voice port: 5200

Configuring IP Line data for a Succession 3.0 system

When distributing IP Line cards across different Media Gateways, you can configure the Media Gateways 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 IP Line cards. For a remote location, the Survival IP address of the IP 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 IP Line cards is configured to a single Media Gateway SSC IP address.

The information below provides more information on these two options:

Separate nodes for Media Gateways

Configuring Media Gateways in separate nodes for IP Line cards is mandatory if Media Gateways are in a different location from 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 IP Line card fails, IP telephones can register to another IP Line card only if it is contained within the same cabinet.
- Users cannot make IP telephone calls from one Media Gateway to another.

Same node for IP Line cards

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

Summary of steps to configure IP Line data on OTM

Refer to *IP Line: Description, Installation, and Operation* (553-3001-365) for a detailed description of these steps.

Failure to have the correct software release and issue configured in OTM can result in an unsupported node configuration being added to the system.

1. Manually add an IP Line 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 IP 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 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 (Figure 115 on page 229).

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

Transmitting IP Line node configuration data from OTM to the IP Line cards

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

Refer to *IP Line: Description, Installation, and Operation* (553-3001-365) for a detailed description of these steps.

1. Set the Leader 0 IP address using a TTY connected to the local RS-232 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.

Setting up virtual terminal service

This section contains information on configuring virtual ports and communications settings.

Virtual ports

In the Terminal Server application, the Virtual Ports Properties dialog box 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, and then selecting Terminal Server in the Windows Programs list in the Start menu.

Configuring a virtual port

To configure a virtual port, click Systems, 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 box. This allows the user to quickly change the settings for a particular device.

In the Virtual Port Properties dialog box, 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).

VT220 Ethernet/PPP does not support connection to Meridian Mail. Use only the serial connection to access Meridian Mail.

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

Virtual port configuration for Succession BCM is the same as for a Generic System.

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

Enabling virtual port connection for a device

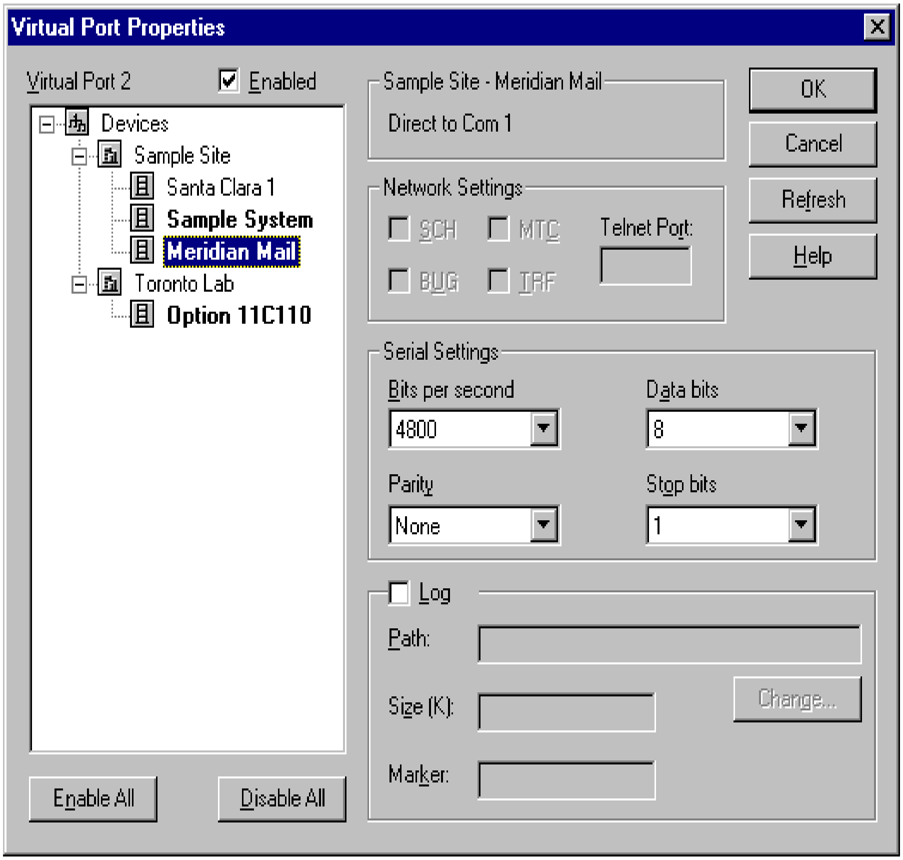
1. Do one of the following:
   - Double-click the disabled item in the tree.
   - Select the item, and check the Enabled check box.
   - Click Enable All to enable all the items listed in the tree with the default configuration.

   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 appears in the Terminal Server's main window.

   For a serial connection, "Direct to Com *x*" appears, where *x* is the Com port number (Figure 116).

Figure 116 Configuring Virtual Ports (serial, logging disabled)



Virtual Port 2 ☑ Enabled

Sample Site - Meridian Mail

Direct to Com 1

Network Settings

☐ SCH ☐ MTC ☐ BUG ☐ TRF

Telnet Port:

Serial Settings

Bits per second: 4800

Data bits: 8

Parity: None

Stop bits: 1

☐ Log

Path:

Size (K):

Marker:

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

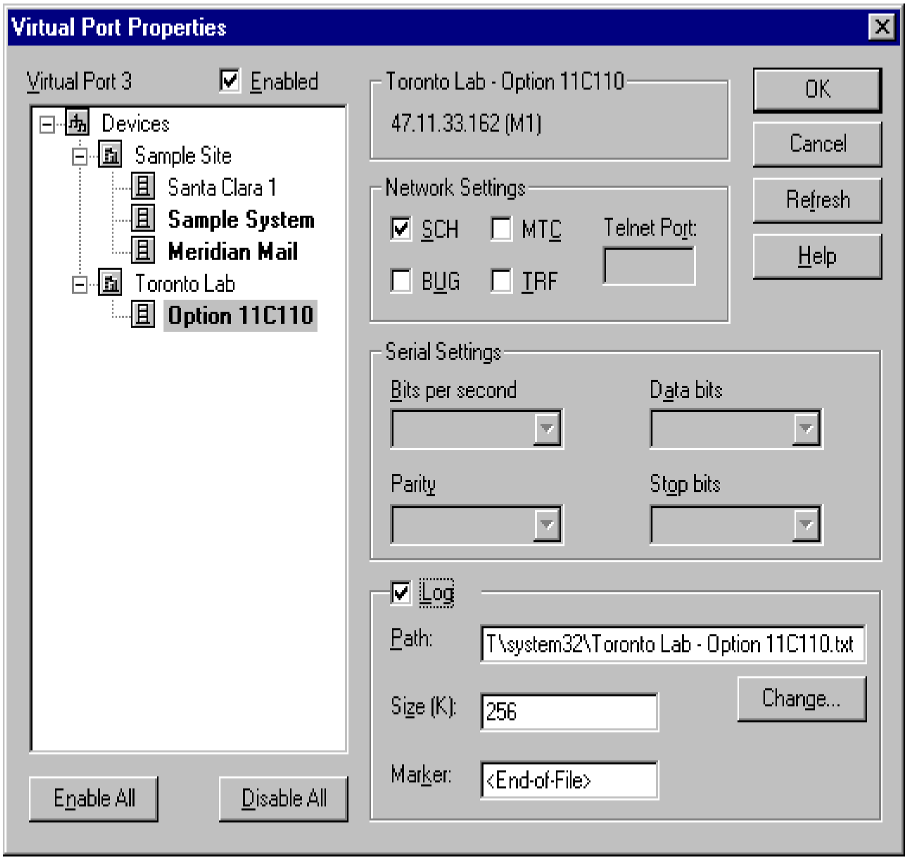
You can change the settings in the dialog box.

For a network connection, the IP address appears. 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 Refresh to update 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 117 appears.

Figure 117 Configuring Virtual Ports (Meridian 1 system, logging enabled)



Virtual Port Properties

Virtual Port 3 ☑ Enabled

- Devices
  - Sample Site
    - Santa Clara 1
    - **Sample System**
    - **Meridian Mail**
  - Toronto Lab
    - **Option 11C110**

Toronto Lab - Option 11C110

47.11.33.162 (M1)

Network Settings

☑ SCH ☐ MTC ☐ BUG ☐ TRF

Telnet Port:

Serial Settings

Bits per second:

Data bits:

Parity:

Stop bits:

☑ Log

Path: T\system32\Toronto Lab - Option 11C110.txt

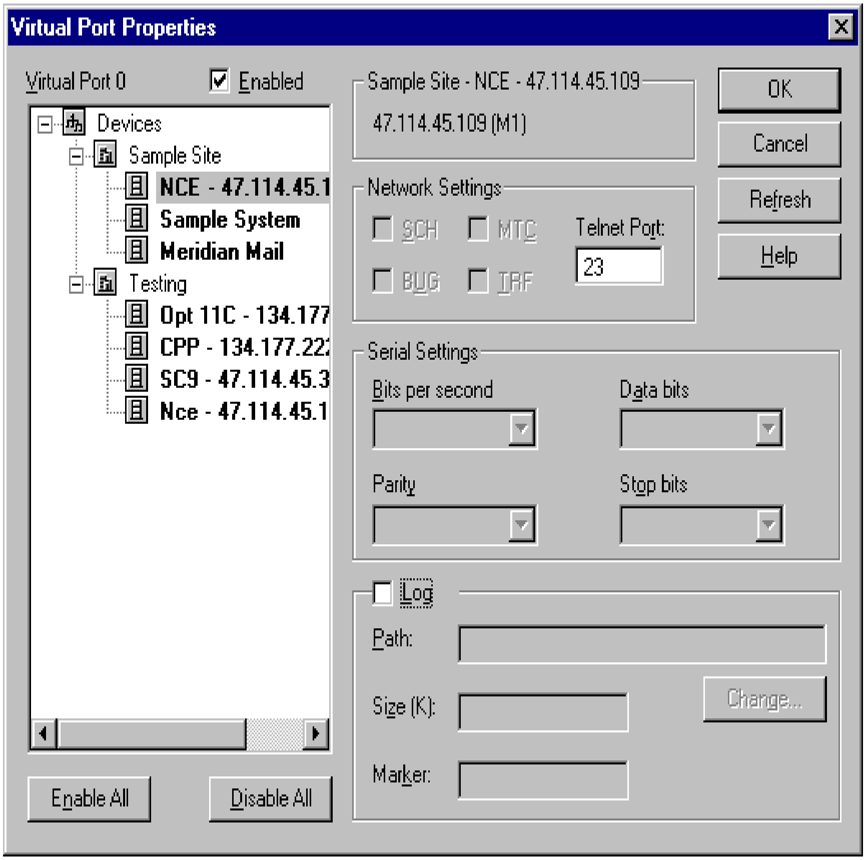
Size (K): 256

Marker: <End-of-File>

- 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 118 appears.

Figure 118 Configuring Virtual Ports (Telnet system, logging enabled)



Virtual Port Properties

Virtual Port 0 ☑ Enabled

- Devices
  - Sample Site
    - NCE - 47.114.45.1
    - Sample System
    - Meridian Mail
  - Testing
    - Opt 11C - 134.177
    - CPP - 134.177.22
    - SC9 - 47.114.45.3
    - Nce - 47.114.45.1

Sample Site - NCE - 47.114.45.109

47.114.45.109 (M1)

Network Settings

□ SCH □ MTC □ BUG □ TRF

Telnet Port: 23

Serial Settings

Bits per second:

Data bits:

Parity:

Stop bits:

□ Log

Path:

Size (K):

Marker:

- 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 tab in the System Properties dialog box.

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. You can change the path and the file name by typing in the edit box or clicking Change.

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

Due to 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 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 click Cancel to discard them.
5. To disable a virtual port connection for a device, do one of the following:
   - Double-click an enabled item in the tree
   - Select the item and uncheck the Enabled check box
   - Click Disable All 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 eight 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, and so on.

Communication Settings

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

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.

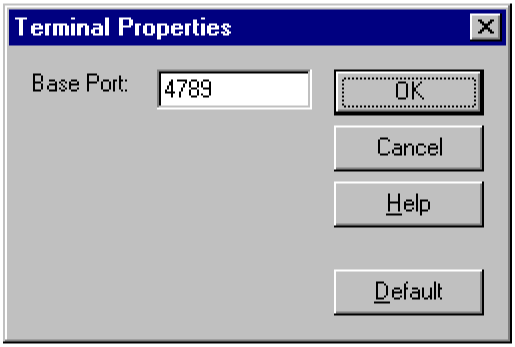
By default, the Terminal Server and Terminal Client communicate through network ports 4789 up to 5045 (4789 to send connection requests, 4790-5045 for up to 256 terminal sessions). Of course, the number of ports actually used depends on the number of virtual ports configured.

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

1 In the Terminal Server application, click Terminals.

The Terminal Properties dialog box appears (Figure 119).

Figure 119 Terminal Properties dialog box



Terminal Properties

Base Port: 4789

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

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

Setting up FTP Server support for CDR Data Collection (Succession DCM)

This section contains information on:

- Two ways to set up FTP support
- Scheduling the CDR application

Set up Succession BCM for FTP support in one of two ways:

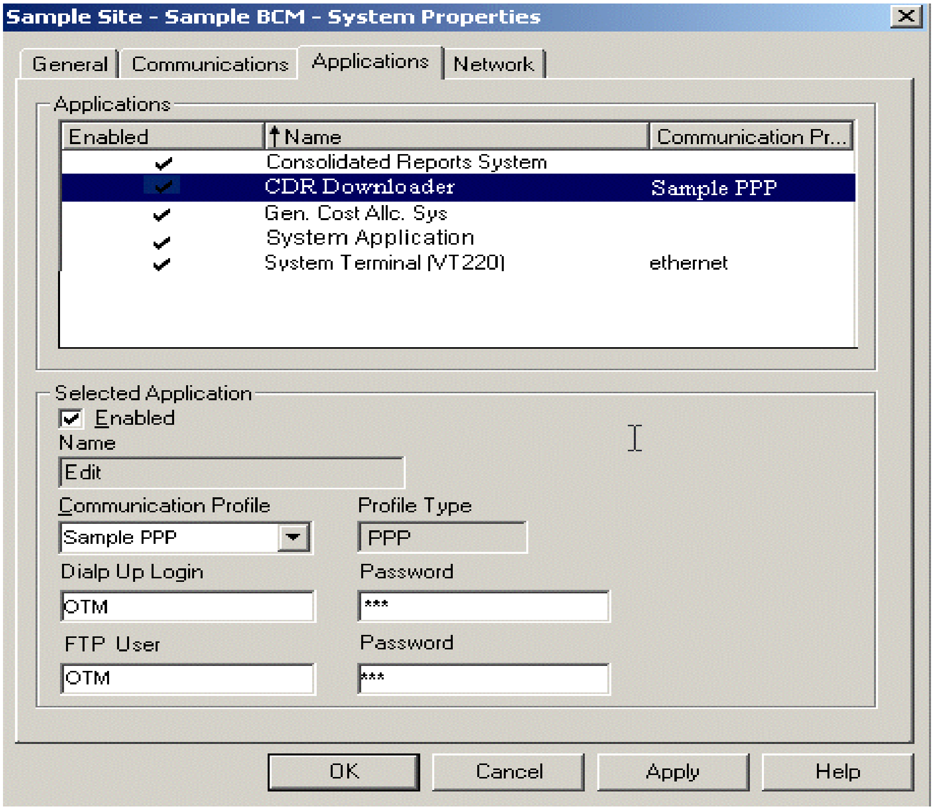
- **CDR Pull Method**: A BCM system is reached through Ethernet or Dialup (PPP)
- **CDR Push Method**: A BCM system that uses SNMP and requires a SMNP MIB entry for FTP status.)

The FTP server for a OTM Server/Standalone uses port number '21'. The FTP client on the BCM switch uses 'CDR Push transfer' method to upload the CDR files to the OTM server, even when OTM is not running. The root directory for BCM FTP client is ‘<otm root>/Common Data'.

BCM FTP client uses the relative path “<site name>/<system name>” to upload CDR data to system folder.

CDR Pull Method

Figure 120 CDR Downloader application



Applications

Enabled	Name	Communication Pr...
✓	Consolidated Reports System	
✓	CDR Downloader	Sample PPP
✓	Gen. Cost Allc. Sys	
✓	System Application	
✓	System Terminal (VT220)	ethernet

Selected Application

☑ Enabled

Name: Edit

Communication Profile: Sample PPP

Profile Type: PPP

Dialp Up Login: OTM

Password: ***

FTP User: OTM

Password: ***

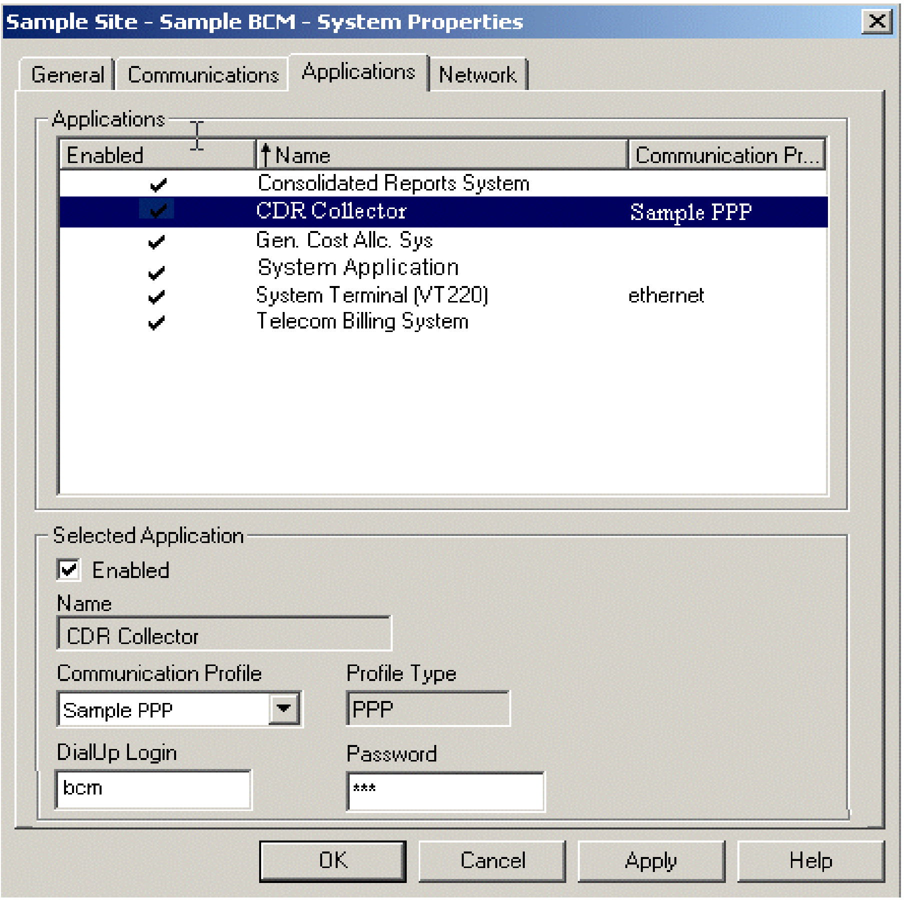
1 From the BCM Systems window, select CDR Downloader.(Figure 120)

2 Enter the Communication Profile (Dialup/Ethernet), Dialup login and Password, FTP User and Password and click Apply.

3 Click OK

CDR Push Method

Figure 121 CDR Collector application



Enabled	Name	Communication Pr...
✓	Consolidated Reports System	
✓	CDR Collector	Sample PPP
✓	Gen. Cost Allc. Sys	
✓	System Application	
✓	System Terminal (VT220)	ethernet
✓	Telecom Billing System	

☑ Enabled

Name: CDR Collector

Communication Profile: Sample PPP

Profile Type: PPP

DialUp Login: bcm

Password: ***

1 From the BCM Systems window, select CDR Collector.(Figure 121)

2 Enter the Communication Profile (Dialup/Ethernet), Dialup login and Password, and click Apply. Click OK.

Scheduling the CDR application

Two methods are available.

Pull Method

1. From the BCM system window, select File>Download CDR Data.
2. Select the FTP Settings download option.
3. Click Schedule.
4. Select the download times and click OK.

Push Method

1. From the BCM system window, File>Collect CDR Data.
2. Select the download times and click OK.

➡ **Supported FTP Commands**:

- User
- Password
- get - for downloading a single file
- put - for uploading a single file
- mget - to download multiple files.
- mput - to upload multiple files.
- Type - mode of transmission i.e 'binary' or 'ASCII'
- cd - to set the relative current working directory
- quit - close the connection

Setting 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 appears.

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.

   Based 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 shows Connected in the window title. For serial connections, the session is 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 *Optivity Telephony Manager: System Administration* (553-3001-330).

Setting up the LDAP server

This section contains information on how 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

Scheduled synchronizations 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 *Optivity Telephony Manager: System Administration* (553-3001-330).

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

Setting 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 *Optivity Telephony Manager: System Administration* (553-3001-330).

Backing up and restoring OTM

This section contains information on:

- Available types of backup and restore
- Performing backups and restores

Read the procedures before you begin, so you can determine which type of backup and restore you should do.

Media Gateway restriction

A Media Gateway System cannot be backed up/restored alone. It must be associated with a Succession 3.0 system.

Performing a backup of your OTM data and applications:

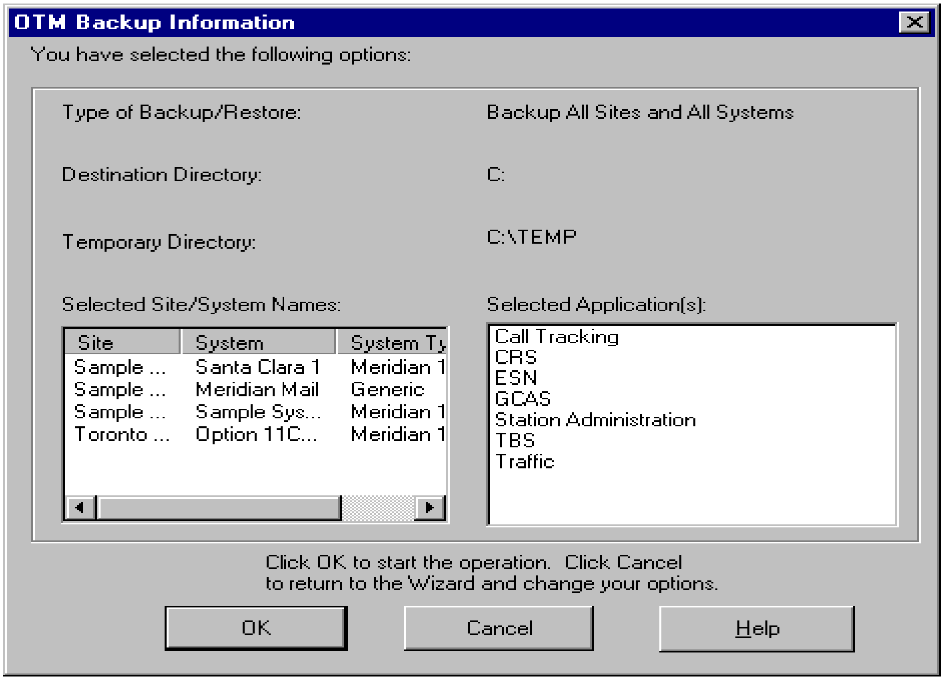
1. In OTM Windows Navigator, select Utilities > Backup.
2. Select one of the following backup types:
   - For *All sites, All systems, A single site*, or *A single system,* press Next and proceed to Step 3.
   - For *OTM Full* press next and proceed to Step 4.
3. Choose one of the following:
   - For *All sites, All systems*, select the OTM application data to be backed up and press next.
   - For *A single site*, select a site and press next.
   - For *A single system*, select a system and press next

Note: Saving Backups can overwrite existing Backup files. Ensure you are choosing the correct Backup file.

4 Select a directory to store the backup file and press OK.

5 The OTM Backup information dialog box displays (Figure 122).

Figure 122 OTM Backup Information dialog box



OTM Backup Information

You have selected the following options:

Type of Backup/Restore: Backup All Sites and All Systems

Destination Directory: C:

Temporary Directory: C:\TEMP

Selected Site/System Names:

Site	System	System Ty
Sample ...	Santa Clara 1	Meridian 1
Sample ...	Meridian Mail	Generic
Sample ...	Sample Sys...	Meridian 1
Toronto ...	Option 11C...	Meridian 1

Selected Application(s):

Call Tracking
CRS
ESN
GCAS
Station Administration
TBS
Traffic

Click OK to start the operation. Click Cancel to return to the Wizard and change your options.

All Media Gateway applications belonging to this Succession system are non-selectable and are automatically backed up.

All Survivable Cabinet and Media Gateway applications belonging to this Succession system are non-selectable and are automatically backed up.

The dialog box summarizes the options selected for the backup:

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

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.

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

Performing a restore of OTM data and applications:

1 In OTM Windows Navigator, select Utilities > Restore.

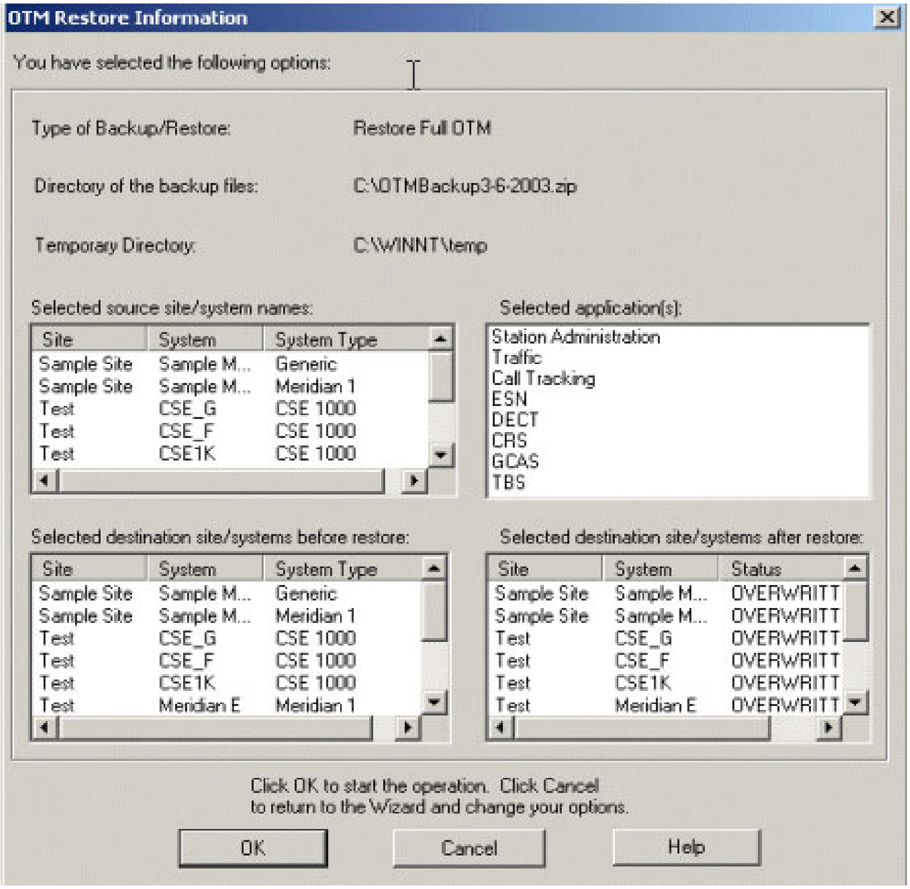
2 Select a Restore Type and press Next.

3 Select the Backup file to be restored.

- For *All sites, All systems*, select the OTM application data to be backed up and press next.
- For *A single site*, select a site and press next.
- For *A single system*, select a system and press next.
- For *OTM Full* press next.

4 The OTM Restore Information dialog box displays. (Figure 123).

Figure 123 OTM Restore Information dialog box



OTM Restore Information

You have selected the following options:

Type of Backup/Restore: Restore Full OTM

Directory of the backup files: C:\OTMBackup3-6-2003.zip

Temporary Directory: C:\WINNT\temp

Selected source site/system names:

Site	System	System Type
Sample Site	Sample M...	Generic
Sample Site	Sample M...	Meridian 1
Test	CSE_G	CSE 1000
Test	CSE_F	CSE 1000
Test	CSE1K	CSE 1000

Selected application(s):

Station Administration
Traffic
Call Tracking
ESN
DECT
CRS
GCAS
TBS

Selected destination site/systems before restore:

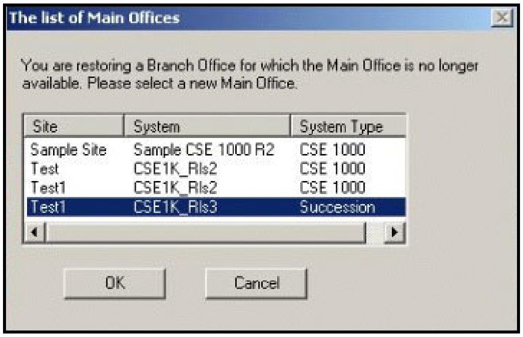
Site	System	System Type
Sample Site	Sample M...	Generic
Sample Site	Sample M...	Meridian 1
Test	CSE_G	CSE 1000
Test	CSE_F	CSE 1000
Test	CSE1K	CSE 1000
Test	Meridian E	Meridian 1

Selected destination site/systems after restore:

Site	System	Status
Sample Site	Sample M...	OVERWRITT
Sample Site	Sample M...	OVERWRITT
Test	CSE_G	OVERWRITT
Test	CSE_F	OVERWRITT
Test	CSE1K	OVERWRITT
Test	Meridian E	OVERWRITT

Click OK to start the operation. Click Cancel
to return to the Wizard and change your options.

Note: During restoring branch office, if its main office is not available, the restore wizard pops up the dialog titled "The list of Main Offices" showing the list of available main offices and prompts the user to select a main office.



The list of Main Offices

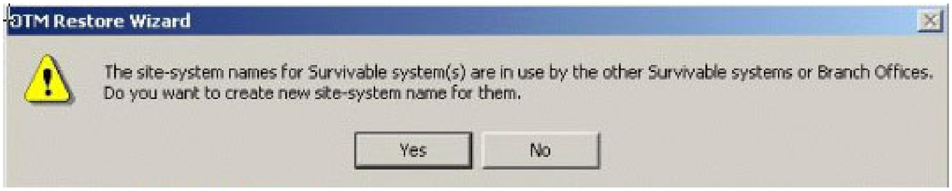
You are restoring a Branch Office for which the Main Office is no longer available. Please select a new Main Office.

Site	System	System Type
Sample Site	Sample CSE 1000 R2	CSE 1000
Test	CSE1K_Rls2	CSE 1000
Test1	CSE1K_Rls2	CSE 1000
Test1	CSE1K_Rls3	Succession

During restoration, step 5, a check is made using the site-system name to determine if the Media Gateway already exists. If the Media Gateway with the same name already exists, please continue to step 6.

5 Click OK to start the restore operation, or click Cancel to go to the restore wizard and change your options.

6 If the Media Gateway with the same name already exists the following dialog box displays. Click Yes.

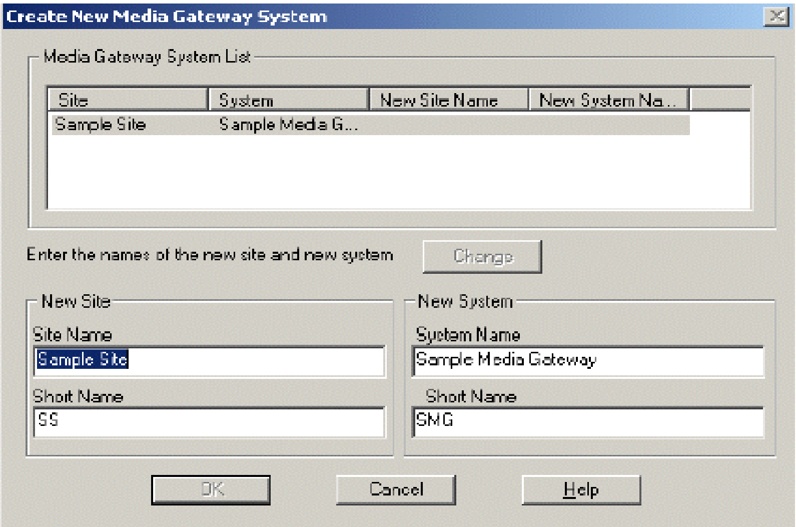


OTM Restore Wizard

The site-system names for Survivable system(s) are in use by the other Survivable systems or Branch Offices. Do you want to create new site-system name for them.

7 A new dialog box displays associated with the type of system selected. Choose one of the following:

Figure 124 Succession 3.0 CSE System


Create New Media Gateway System

Media Gateway System List

Site	System	New Site Name	New System Na...
Sample Site	Sample Media G...		

Enter the names of the new site and new system

New Site

Site Name: Sample Site

Short Name: SS

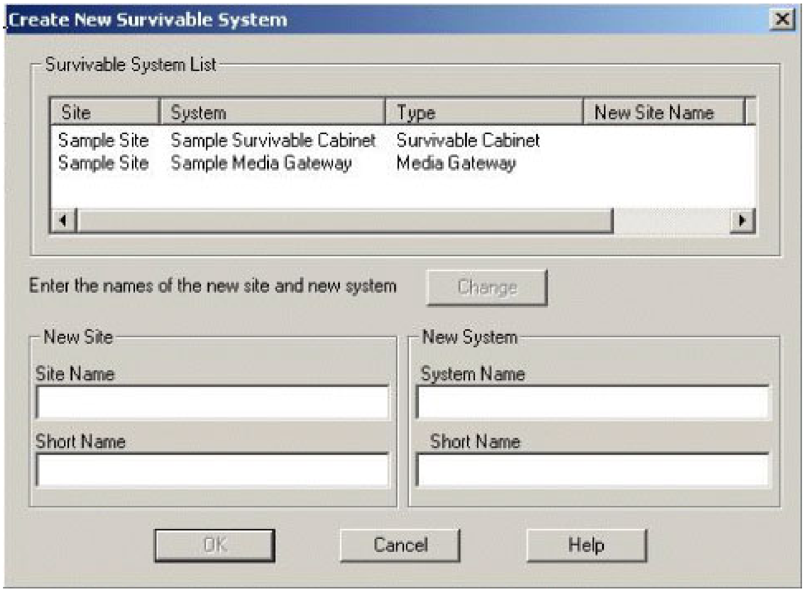
New System

System Name: Sample Media Gateway

Short Name: SMG

Enter new Site, System, and Short name(s) and click OK.

Figure 125 Succession 3.0 Small System


Create New Survivable System

Survivable System List

Site	System	Type	New Site Name
Sample Site	Sample Survivable Cabinet	Survivable Cabinet	
Sample Site	Sample Media Gateway	Media Gateway	

Enter the names of the new site and new system

New Site

Site Name

Short Name

New System

System Name

Short Name

Enter new Site, System, and Short name(s) and click OK.

Installing OTM Web browser client

This section contains information on installing the OTM Web browser client.

Make sure that the PC Client requirements have been met, as described in "OTM hardware requirements" on page 27.

Accessing the OTM Server Web Navigator via the PC Client

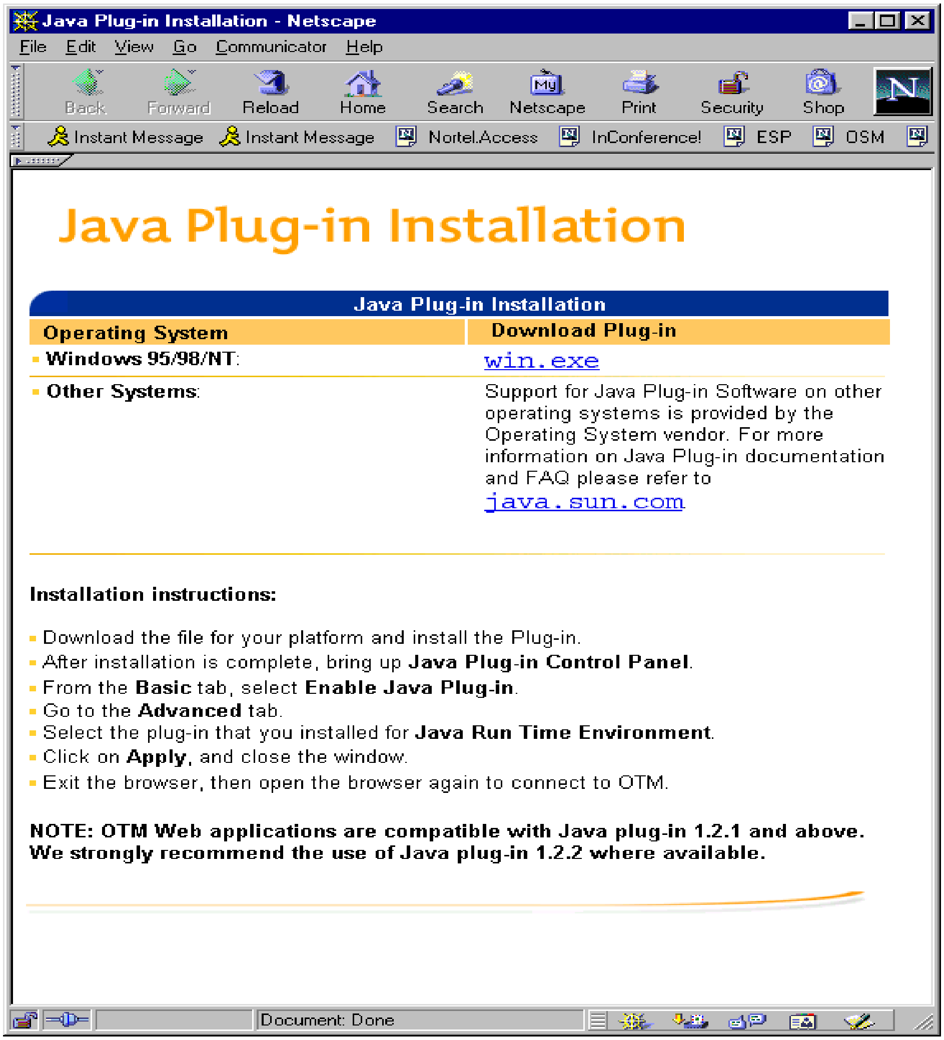
To access the OTM Server Web Navigator:

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

Software plug-in

The first time the OTM Server Web Navigator loads, you are prompted to download a software plug-in (Figure 126). The software you download is a standard Java Runtime Environment (JRE) plug-in of about 7-8 MB size.

Figure 126 JRE Plug-in download prompt



Java Plug-in Installation - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop
Instant Message Instant Message Nortel.Access InConference! ESP OSM
Document: Done

Java Plug-in Installation

Java Plug-in Installation	
Operating System	**Download Plug-in**
Windows 95/98/NT:	win.exe
Other 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 java.sun.com

Installation instructions:

- Download the file for your platform and install the Plug-in.
- After installation is complete, bring up **Java Plug-in Control Panel**.
- From the **Basic** tab, select **Enable Java Plug-in**.
- Go to the **Advanced** tab.
- Select the plug-in that you installed for **Java Run Time Environment**.
- Click on **Apply**, and close the window.
- Exit the browser, then open the browser again to connect to OTM.

NOTE: OTM Web applications are compatible with Java plug-in 1.2.1 and above. We strongly recommend the use of Java plug-in 1.2.2 where available.

Integrating OTM with Optivity NMS

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

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 inter-networking devices. Through Optivity NMS, you can monitor your OTM Servers.

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

By using Optivity NMS InfoCenter, you can manually add OTM Servers into the Telephony Managers Resources folder. Property information that you add about the OTM Servers is added to the Optivity NMS database. For access to the Optivity NMS documentation, in your web browser go to http://www.nortelnetworks.com/documentation. Choose Optivity Network Management System in the Select a Product drop-down list, and click View Documents.

InfoCenter graphically identifies when a device is in an alarm state. By 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 computer from Optivity NMS.
- For more information refer to the OIT support web site at http://support.nortelnetworks.com. See the procedure on page 261 for details.
- OTM integrates with Optivity NMS through OIT on any NMS platform. See "Checklist for installing the Optivity Integration Toolkit" on page 263. Co-residence with Optivity NMS, however, is supported only on Windows NT Server and Windows 2000 Server.
- All software requirements for OTM should be met. Particularly Windows NT Service Pack 6, 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.

There are certain restrictions in OTM application features when installed coresident with Optivity NMS. For more information about these restrictions, refer to the Optivity Telephony Manager (OTM) General Release Bulletin.

- Optivity NMS and OTM use different Web servers: Apache and IIS respectively.

  In the OTM installation, when installing IIS, make sure that the default HTTP port 80 is not used by both the Apache and the IIS web servers.

- 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. If a port clash occurs, the default port on the Apache server must be changed.

The process of OTM–ONMS integration

OTM does not automatically install any OIT files. You must manually install the OIT files. The OIT files can be downloaded from the OIT support web page. To download the OIT files:

1. In your web browser, go to http://support.nortelnetworks.com.
2. Click the View by a Product link.
3. In the drop-down list, select Optivity Network Management System OIT, and click Save,
4. In the drop-down list for software types, select Optivity NMS OIT for Optivity Telephony Manager.
5. Click the link under the Description heading that matches your operating system platform.
6. Click the link to the Readme file to view the installation instructions in your web browser. This file is also included in the zipped archive.
7. Click the link to the zipped archive to download the latest OTM OIT files.

Integration with ONMS versions prior to 10.0

When it detects ONMS, OTM no longer installs OIT files as part of the OTM installation process. You must manually install both the device and application OIT files to complete the integration process. The latest OIT files can be obtained from the OIT support web page.

Integration with ONMS version 10.0

ONMS version 10.0 comes pre-installed with the device OIT files required for releases of OTM prior to OTM 2.0. You must download and install the device OIT file for OTM 2.0 and the application OIT file manually. The application OIT file is common to all releases of OTM. These OIT files can be obtained from the OIT support web page. See the procedure on page 261 for details.

OTM OIT files

OTM 2.0 requires the following OIT files for integration with ONMS:

- NMS_otm_v10-B.oit

  OTM Server device support entries

  OTM Open Alarm II definitions
- NMS_otmApp_v10-B.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."

Checklist for installing the Optivity Integration Toolkit

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 1.4.2). 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.

Checklist for an OTM installation on an existing Optivity NMS server.

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 subdirectories in OITHOME.

All of the subdirectories 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

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.

What you do

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.

For OTM, you must manually add the OTM Server.

What OIT does

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 for 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.

You must be logged in as administrator / root to perform this activity.

Configuring Optivity NMS InfoCenter for OTM

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 127).

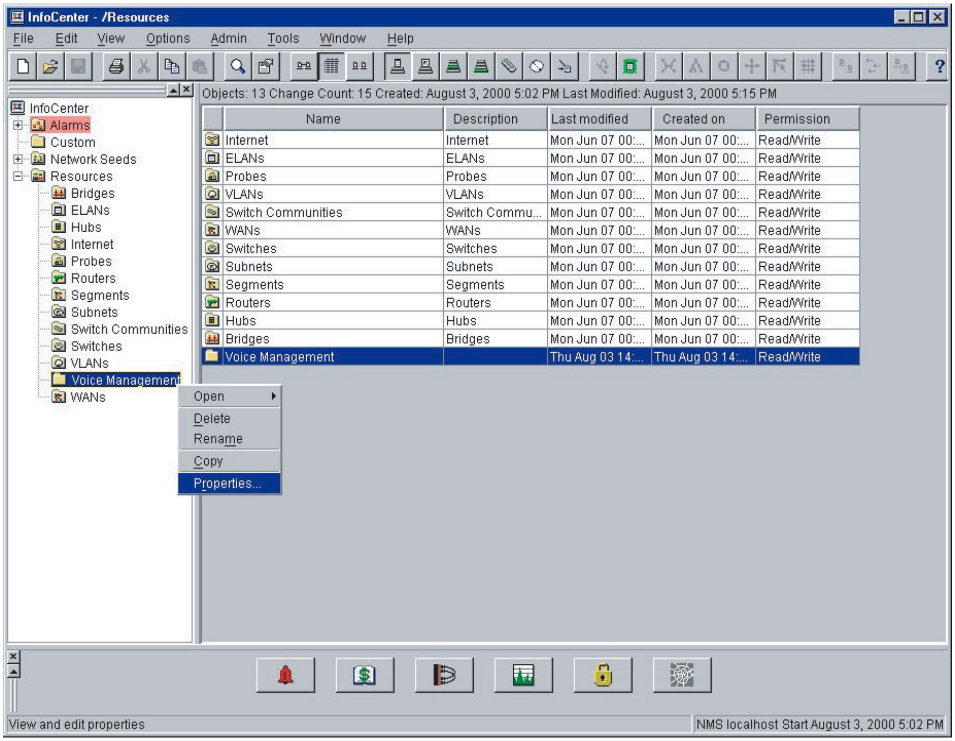
   b Open the ManagementServer folder.

   c Select Optivity Telephony Manager (Figure 128 on page 267).

   d Click Apply.

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

Figure 127 InfoCenter Resources



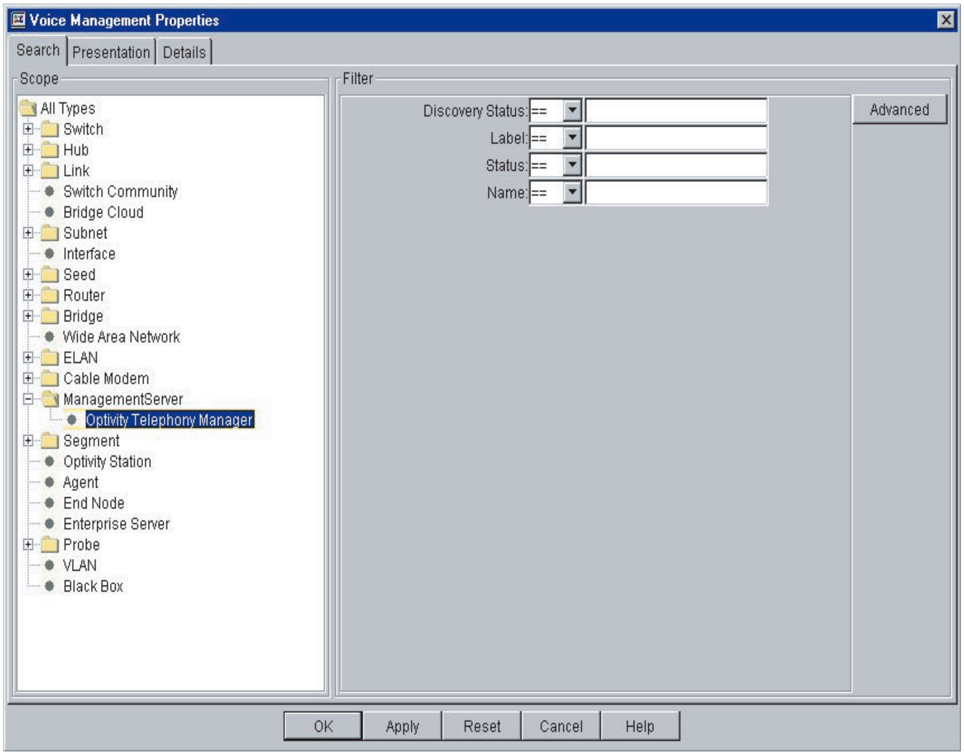
Objects: 13 Change Count: 15 Created: August 3, 2000 5:02 PM Last Modified: August 3, 2000 5:15 PM

Name	Description	Last modified	Created on	Permission
Internet	Internet	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
ELANs	ELANs	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Probes	Probes	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
VLANs	VLANs	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Switch Communities	Switch Commu...	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
WANs	WANs	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Switches	Switches	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Subnets	Subnets	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Segments	Segments	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Routers	Routers	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Hubs	Hubs	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Bridges	Bridges	Mon Jun 07 00:...	Mon Jun 07 00:...	Read/Write
Voice Management		Thu Aug 03 14:...	Thu Aug 03 14:...	Read/Write

View and edit properties

NMS localhost Start August 3, 2000 5:02 PM

Figure 128 InfoCenter Voice Management Properties dialog box



Discovery Status: ==
Label: ==
Status: ==
Name: ==

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 in to InfoCenter.

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

The Optivity NMS InfoCenter login window appears.

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

Optivity NMS InfoCenter appears.

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 cannot 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 appears with the Device tab selected (Figure 129).

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 an Optivity Telephony Manager subtype for the object.

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

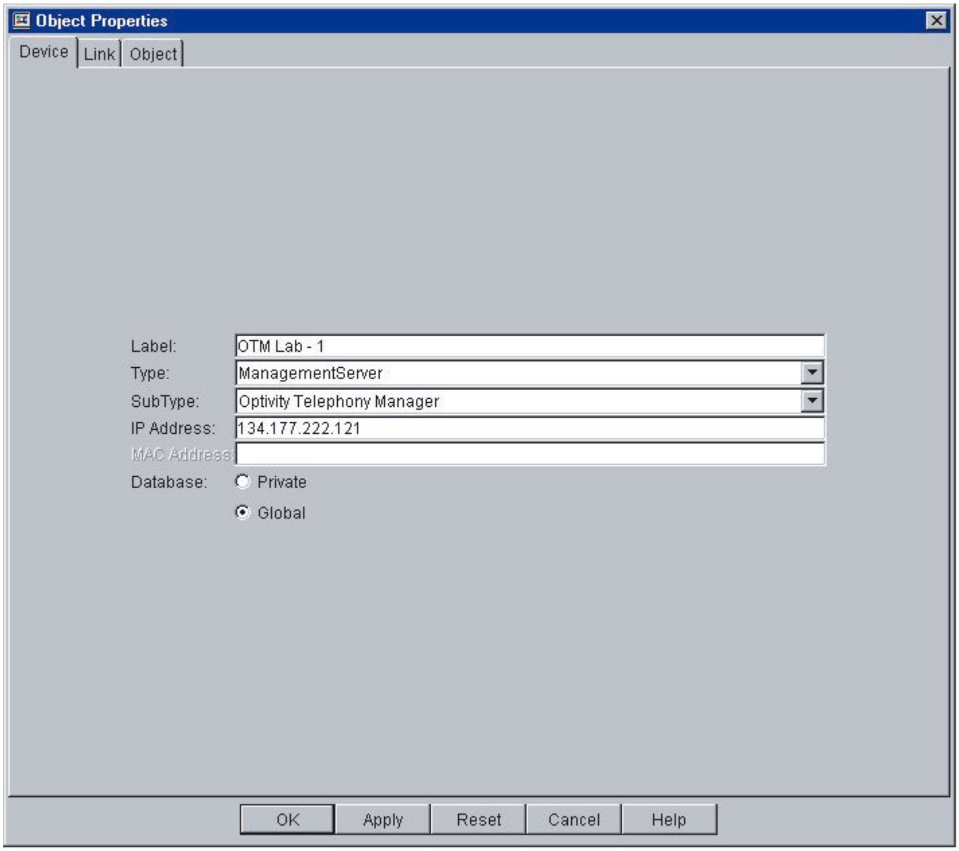
e Click Private or Global.

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 129 InfoCenter Object Properties dialog box



Label: OTM Lab - 1

Type: ManagementServer

SubType: Optivity Telephony Manager

IP Address: 134.177.222.121

MAC Address:

Database: ○ Private ● Global

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 appears, displaying the properties for the selected network object. 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 appears, displaying the properties for the selected network object.
4. Edit the object properties that you want. Click OK.

Starting OTM Web Applications

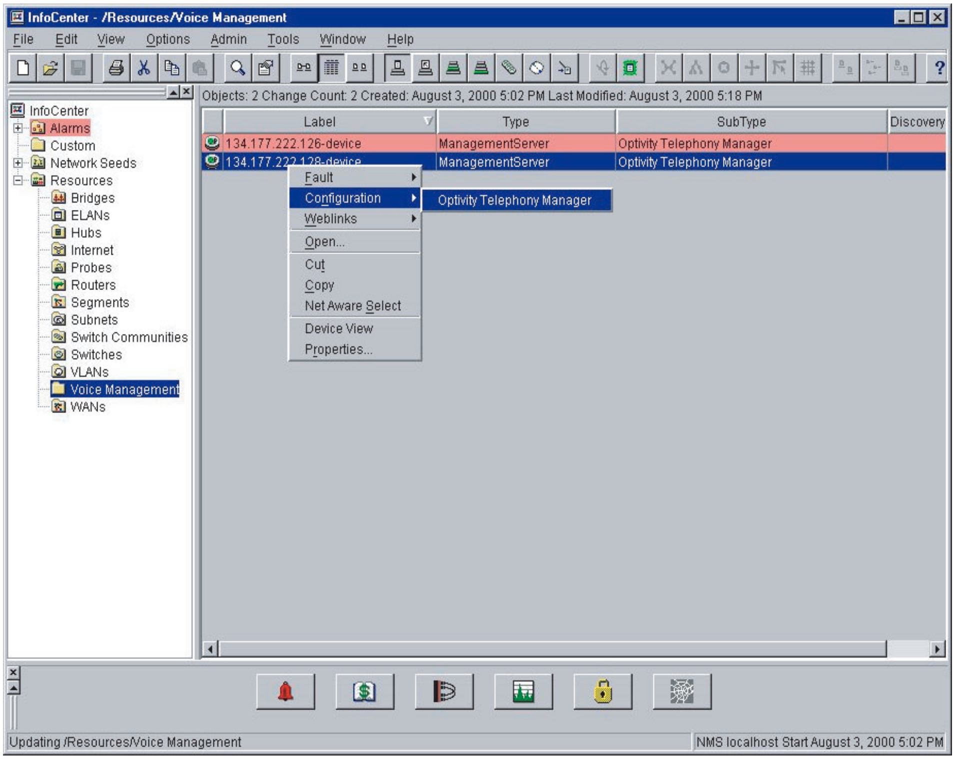
OTM Web Application links are integrated with Optivity NMS when an OTM Server is added.

The OTM system being accessed can be running on the same server as Optivity NMS (for Windows NT), or it can 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 130).

This action launches the default Web browser for your system and connects to the OTM Web Server. See “Java Runtime Environment for OTM and Optivity NMS” on page 271 for details on JRE.

Figure 130 Starting OTM Web Applications



Objects: 2 Change Count: 2 Created: August 3, 2000 5:02 PM Last Modified: August 3, 2000 5:18 PM

Label	Type	SubType	Discovery
134.177.222.126-device	ManagementServer	Optivity Telephony Manager	
134.177.222.128-device	ManagementServer	Optivity Telephony Manager	

Updating /Resources/Voice Management

NMS localhost Start August 3, 2000 5:02 PM

Java Runtime Environment for OTM and Optivity NMS

OTM Web applications require Java Plug-In 1.4.2 on the client browser. Optivity NMS uses JDK 1.1.x, which is older than the version used by OTM.

JRE clash for OTM and Optivity NMS web clients

In both coresident and non-coresident situations, OTM and Optivity NMS applications cannot be launched simultaneously. The successful launch of OTM and Optivity NMS web applications accessing JRE depends on the version of JRE currently loaded in the system.

If a version of JRE that is different than 1.4.2 is loaded in the system and you access OTM web applications, you are prompted to install and load Java Plug-In 1.4.2 the first time that you try to connect to the OTM Server. With the Java Plug-In 1.4.2 loaded, OTM web applications load successfully.

If a version of JRE that is higher than 1.2.2 is loaded on the system, then Optivity NMS web applications that require JRE cannot be launched. This may occur even when the lower version is installed, but not loaded, on the system. To successfully launch Optivity NMS web applications, you must remove the higher version of JRE, and run the JRE 1.2.2 set-up program.

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 FaultSummary

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

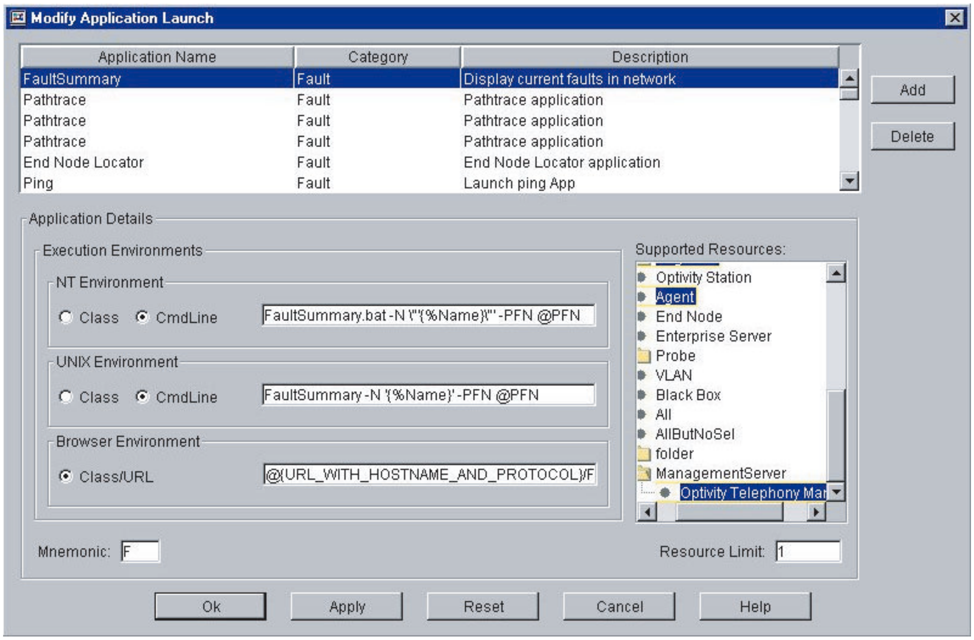
Upon receiving a Meridian 1 or Succession alarm (or other traps that it has been configured to handle), OTM reformats it and forwards it to Optivity NMS. Optivity NMS recognizes the trap (from OIT definitions) and should now be able to reflect the changed status.

Setting up FaultSummary

To set up FaultSummary:

1. Select Application Launch from InfoCenter’s top menu.
2. Select the Fault Summary application (Figure 131).
3. While holding down the Ctrl and Shift keys, select the ManagementServer > Optivity Telephony Manager resource to enable FaultSummary for OTM.
4. Click Apply.

Figure 131 Modify Application Launch dialog box



Modify Application Launch

Application Name	Category	Description
FaultSummary	Fault	Display current faults in network
Pathtrace	Fault	Pathtrace application
Pathtrace	Fault	Pathtrace application
Pathtrace	Fault	Pathtrace application
End Node Locator	Fault	End Node Locator application
Ping	Fault	Launch ping App

Application Details

Execution Environments

NT Environment: ○ Class ● CmdLine FaultSummary.bat -N \"'{%Name}\"' -PFN @PFN

UNIX Environment: ○ Class ● CmdLine FaultSummary -N '{%Name}' -PFN @PFN

Browser Environment: ● Class/URL @{URL_WITH_HOSTNAME_AND_PROTOCOL}/F

Supported Resources:
- Optivity Station
- Agent
- End Node
- Enterprise Server
- Probe
- VLAN
- Black Box
- All
- AllButNoSel
- folder
- ManagementServer
  - Optivity Telephony Mar

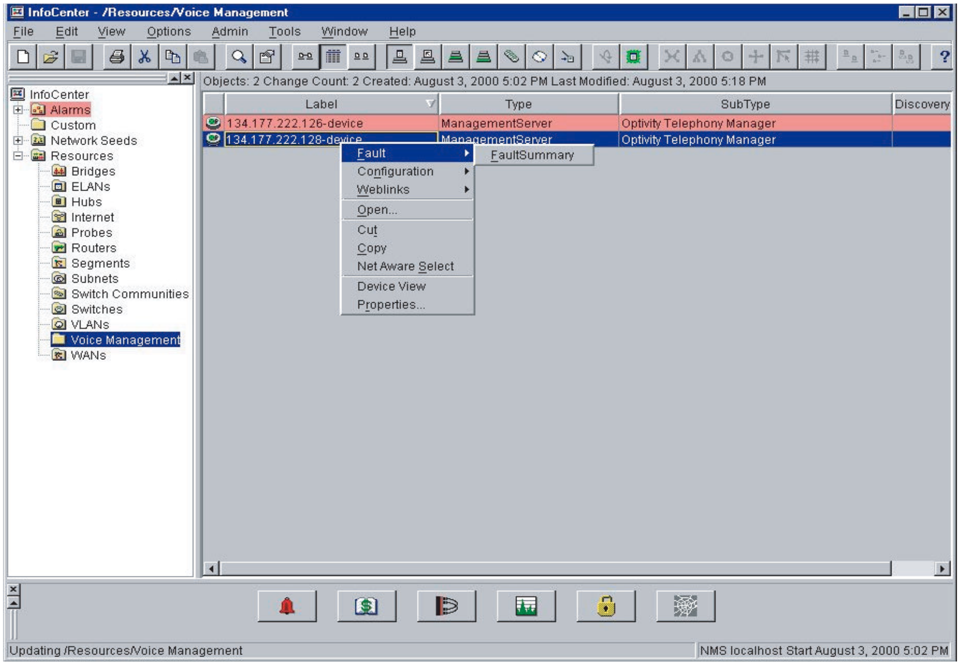
Mnemonic: F

Resource Limit: 1

To launch FaultSummary:

Select the OTM icon and use the right-click menu to launch FaultSummary (Figure 132).

Figure 132 Launch FaultSummary



Objects: 2 Change Count: 2 Created: August 3, 2000 5:02 PM Last Modified: August 3, 2000 5:18 PM

Label	Type	SubType	Discovery
134.177.222.126-device	ManagementServer	Optivity Telephony Manager	
134.177.222.128-device	ManagementServer	Optivity Telephony Manager	

Updating /Resources/Voice Management

NMS localhost Start August 3, 2000 5:02 PM

Configuring OTM

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

The OTM Alarm notification application forwards traps of interest to Optivity NMS.

Sample scripts are provided with the Alarm Notification application, which 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, as so on.

- Modify the sample scripts to forward traps from devices other than Meridian 1, Succession 3.0, and other OTM devices to Optivity NMS.

  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, 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 the 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 and receiving traps.
- 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. FaultSummary should be enabled for ManagementServer > Optivity Telephony Manager.

Integrating OTM with HP OpenView

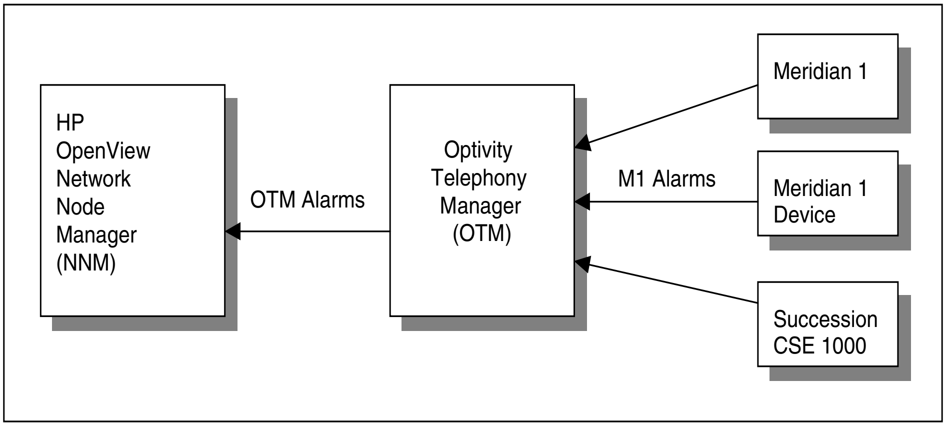
This section provides information on the integration of the HP* OpenView* (HP OV) Network Node Manager (NNM) management platform with Nortel Networks' Optivity Telephony Manager (OTM). It discusses the type of integration supported. The included procedures provide detailed step-by-step instructions on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

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 HP OpenView. It includes the following information:

- "Limitations" on page 278
- "Hardware and software requirements" on page 279
- "System integration" on page 279
- "Installation and configuration" on page 282

Figure 133 OTM alarm integration with HP OpenView Network Node Manager


HP OpenView Network Node Manager (NNM)
OTM Alarms
Optivity Telephony Manager (OTM)
M1 Alarms
Meridian 1
Meridian 1 Device
Succession CSE 1000

As seen in Figure 133, Meridian 1 systems, Succession 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, you can also configure the NNM to allow the network administrator easy access to the OTM server.

Refer to *Optivity Telephony Manager: System Administration* (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.
- Coresidency is not supported for NNM and OTM on the same PC. However, for web clients, if JRE 1.3.1 is loaded in the system and the default web browser in Internet Explorer, both OTM and HP OpenView web applications can be launched simultaneously.
- The OTM Server does 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)

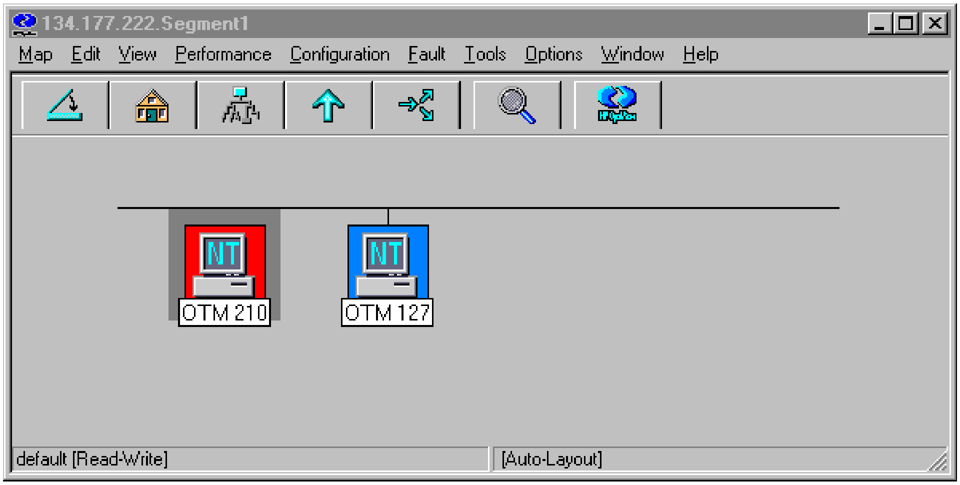
- OTM Release 1.01 or above with:
  - Alarm Notification application
  - Web-based alarm browser

System integration

HP OV NNM Network Map

On the NNM Network Map (Figure 134), an OTM server can be represented as an object. You can configure incoming events 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 134 HP OpenView Network Node Manager Network Map

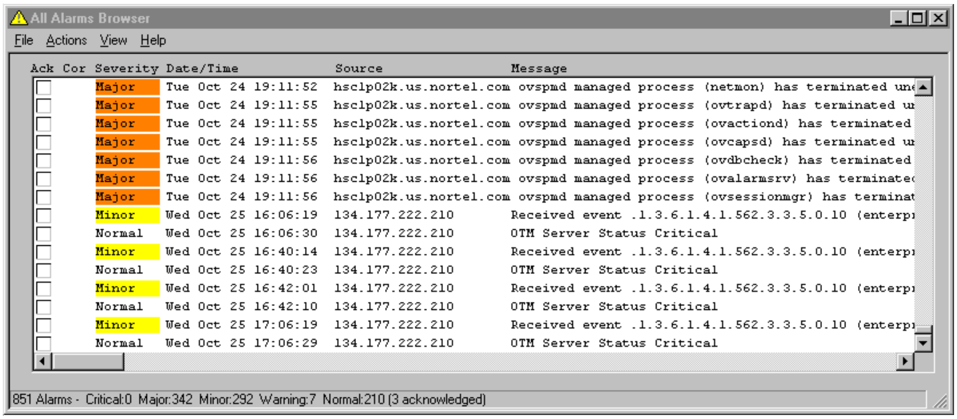

134.177.222.Segment1
Map Edit View Performance Configuration Fault Tools Options Window Help
NT
OTM 210
NT
OTM 127
default [Read-Write]
[Auto-Layout]

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 appears 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 Alarms Browser (Figure 135).

Figure 135 HP OV NNM Alarms Browser

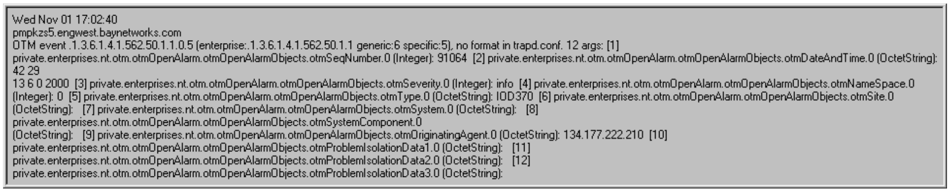


Ack	Cor	Severity	Date/Time	Source	Message
□		Major	Tue Oct 24 19:11:52	hsclp02k.us.nortel.com	ovspmd managed process (netmon) has terminated un
□		Major	Tue Oct 24 19:11:55	hsclp02k.us.nortel.com	ovspmd managed process (ovtrapd) has terminated u
□		Major	Tue Oct 24 19:11:55	hsclp02k.us.nortel.com	ovspmd managed process (ovactiond) has terminated
□		Major	Tue Oct 24 19:11:55	hsclp02k.us.nortel.com	ovspmd managed process (ovcapsd) has terminated u
□		Major	Tue Oct 24 19:11:56	hsclp02k.us.nortel.com	ovspmd managed process (ovdbcheck) has terminated
□		Major	Tue Oct 24 19:11:56	hsclp02k.us.nortel.com	ovspmd managed process (ovalarmsrv) has terminate
□		Major	Tue Oct 24 19:11:56	hsclp02k.us.nortel.com	ovspmd managed process (ovsessionmgr) has terminat
□		Minor	Wed Oct 25 16:06:19	134.177.222.210	Received event .1.3.6.1.4.1.562.3.3.5.0.10 (enterp
□		Normal	Wed Oct 25 16:06:30	134.177.222.210	OTM Server Status Critical
□		Minor	Wed Oct 25 16:40:14	134.177.222.210	Received event .1.3.6.1.4.1.562.3.3.5.0.10 (enterp
□		Normal	Wed Oct 25 16:40:23	134.177.222.210	OTM Server Status Critical
□		Minor	Wed Oct 25 16:42:01	134.177.222.210	Received event .1.3.6.1.4.1.562.3.3.5.0.10 (enterp
□		Normal	Wed Oct 25 16:42:10	134.177.222.210	OTM Server Status Critical
□		Minor	Wed Oct 25 17:06:19	134.177.222.210	Received event .1.3.6.1.4.1.562.3.3.5.0.10 (enterp
□		Normal	Wed Oct 25 17:06:29	134.177.222.210	OTM Server Status Critical

851 Alarms - Critical:0 Major:342 Minor:292 Warning:7 Normal:210 (3 acknowledged)

You can also highlight a specific alarm message on the NNM Alarms Browser, and right-click to display the message content in a separate window (Figure 136). You can then analyze the different variables and their values.

Figure 136 Alarm message content



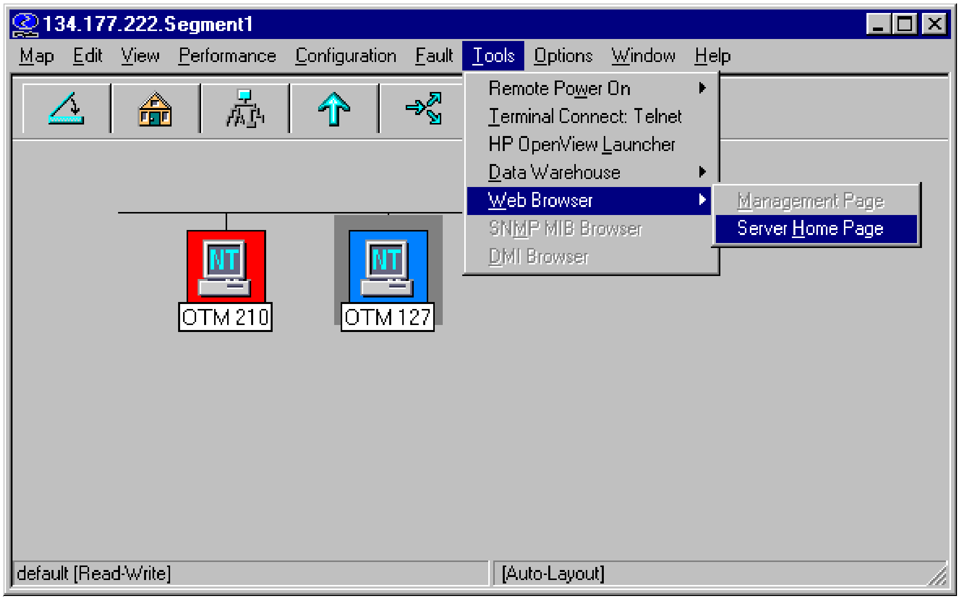
```
Wed Nov 01 17:02:40
pmpkzs5.engwest.baynetworks.com
OTM event .1.3.6.1.4.1.562.50.1.1.0.5 (enterprise:.1.3.6.1.4.1.562.50.1.1 generic:6 specific:5), no format in trapd.conf. 12 args: [1]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSeqNumber.0 (Integer): 91064  [2] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmDateAndTime.0 (OctetString):
42 29
13 6 0 2000  [3] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSeverity.0 (Integer): info  [4] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmNameSpace.0
(Integer): 0  [5] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmType.0 (OctetString): IOD370  [6] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSite.0
(OctetString):   [7] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSystem.0 (OctetString):   [8]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmSystemComponent.0
(OctetString):   [9] private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmOriginatingAgent.0 (OctetString): 134.177.222.210  [10]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmProblemIsolationData1.0 (OctetString):   [11]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmProblemIsolationData2.0 (OctetString):   [12]
private.enterprises.nt.otm.otmOpenAlarm.otmOpenAlarmObjects.otmProblemIsolationData3.0 (OctetString):
```

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 137).

Figure 137 OTM Web Access



Your default Web browser is 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.

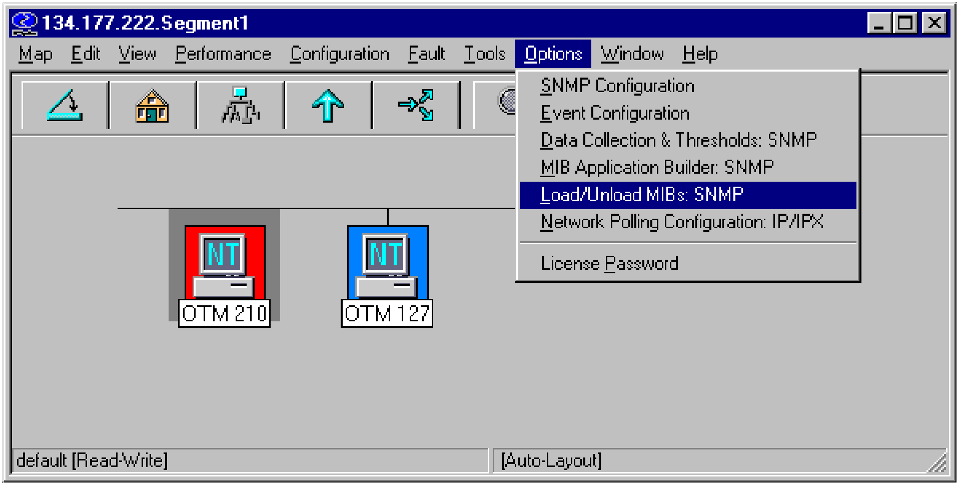
HP OV NNM (HP OV PC)

The following configuration procedures are performed while NNM is running:

OTM Alarm MIB installation

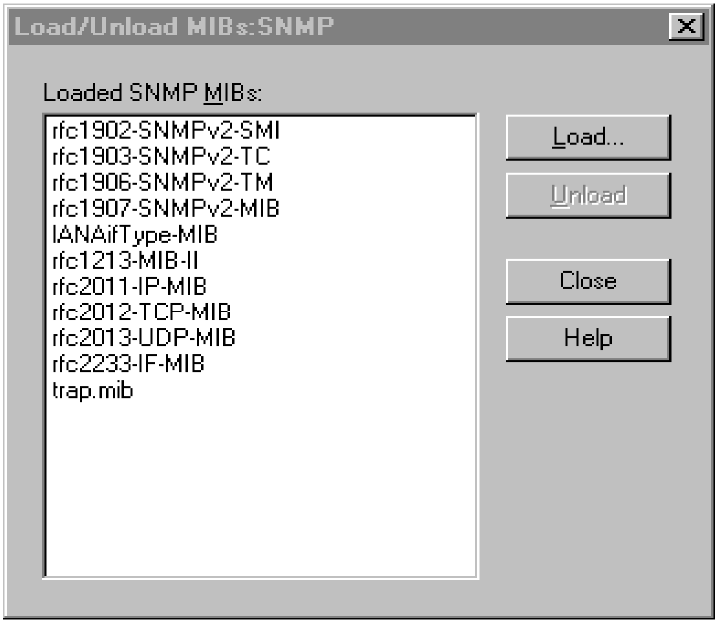
1 Select Options > Load/Unload MIBs:SNMP (Figure 138).

Figure 138 NNM Load/Unload MIBs



2 Click Load in the Load/Unload MIBs dialog box (Figure 139).

Figure 139 Load/Unload MIBs

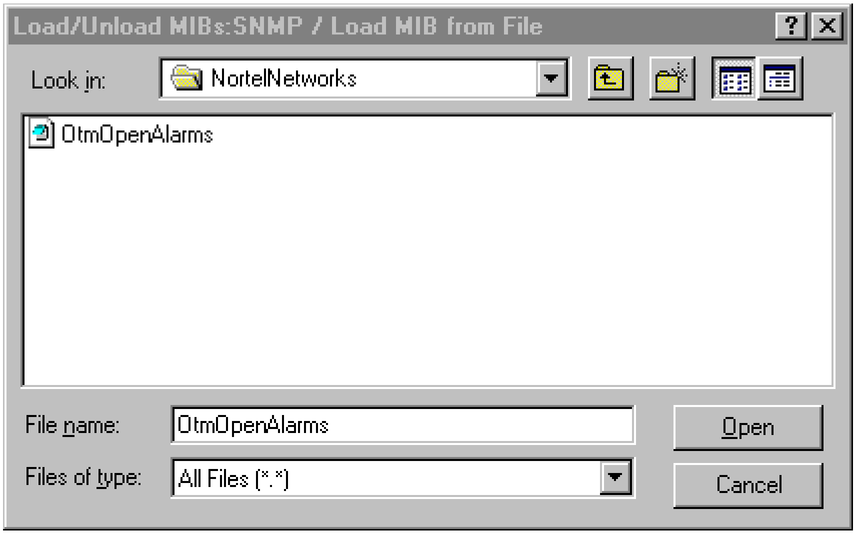


Loaded SNMP MIBs:

rfc1902-SNMPv2-SMI
rfc1903-SNMPv2-TC
rfc1906-SNMPv2-TM
rfc1907-SNMPv2-MIB
IANAifType-MIB
rfc1213-MIB-II
rfc2011-IP-MIB
rfc2012-TCP-MIB
rfc2013-UDP-MIB
rfc2233-IF-MIB
trap.mib

3 Open the OtmOpenAlarms.mib file (Figure 140).

Figure 140 Load MIB



Look in: NortelNetworks

File name: OtmOpenAlarms

Files of type: All Files (*.*)

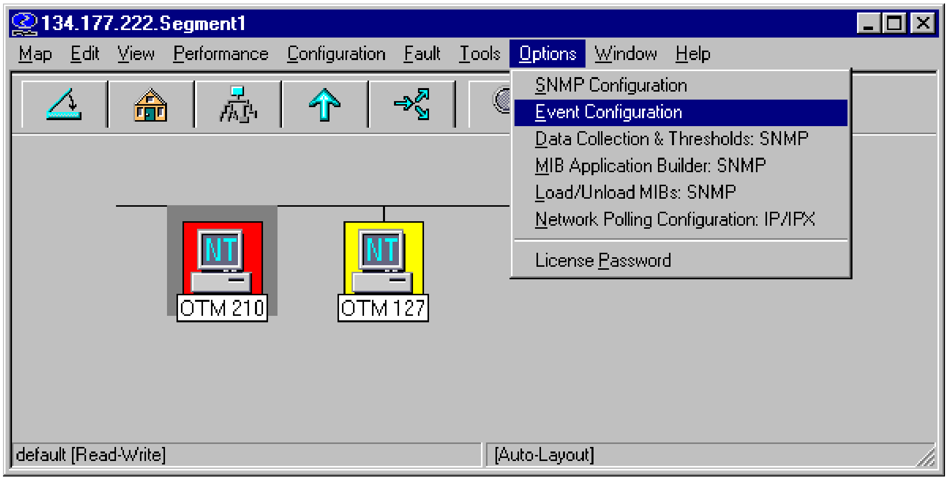
The OTM alarm MIB definitions are now loaded into the NNM's MIB database.

Event Configuration

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

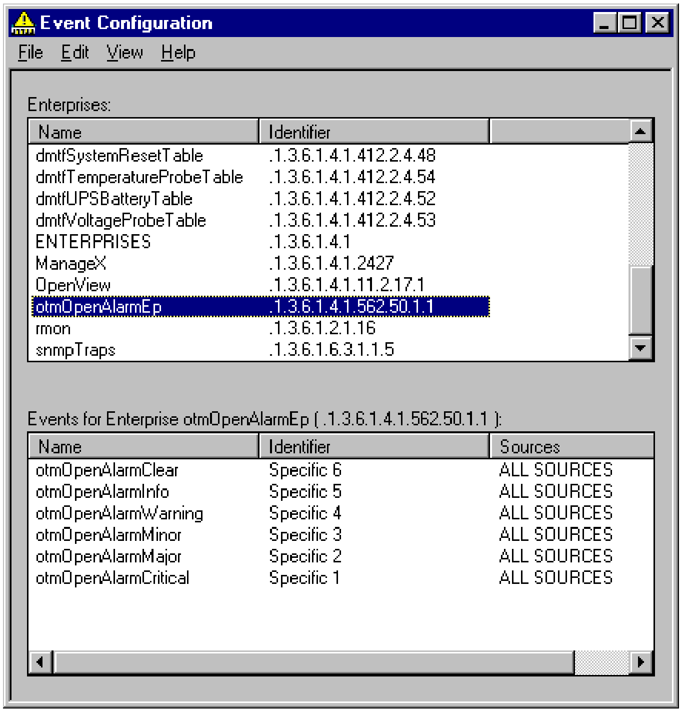
1 Select Options > Event Configuration (Figure 141).

Figure 141 NNM Main Menu - Event Configuration


134.177.222.Segment1
Map Edit View Performance Configuration Fault Tools Options Window Help
SNMP Configuration
Event Configuration
Data Collection & Thresholds: SNMP
MIB Application Builder: SNMP
Load/Unload MIBs: SNMP
Network Polling Configuration: IP/IPX
License Password
NT
OTM 210
NT
OTM 127
default [Read-Write]
[Auto-Layout]

2 Locate and select “otmOpenAlarmEp” from the list of Enterprises (Figure 142).

Figure 142 Event Configuration



Enterprises:

Name	Identifier
dmtfSystemResetTable	.1.3.6.1.4.1.412.2.4.48
dmtfTemperatureProbeTable	.1.3.6.1.4.1.412.2.4.54
dmtfUPSBatteryTable	.1.3.6.1.4.1.412.2.4.52
dmtfVoltageProbeTable	.1.3.6.1.4.1.412.2.4.53
ENTERPRISES	.1.3.6.1.4.1
ManageX	.1.3.6.1.4.1.2427
OpenView	.1.3.6.1.4.1.11.2.17.1
otmOpenAlarmEp	.1.3.6.1.4.1.562.50.1.1
rmon	.1.3.6.1.2.1.16
snmpTraps	.1.3.6.1.6.3.1.1.5

Events for Enterprise otmOpenAlarmEp (.1.3.6.1.4.1.562.50.1.1):

Name	Identifier	Sources
otmOpenAlarmClear	Specific 6	ALL SOURCES
otmOpenAlarmInfo	Specific 5	ALL SOURCES
otmOpenAlarmWarning	Specific 4	ALL SOURCES
otmOpenAlarmMinor	Specific 3	ALL SOURCES
otmOpenAlarmMajor	Specific 2	ALL SOURCES
otmOpenAlarmCritical	Specific 1	ALL SOURCES

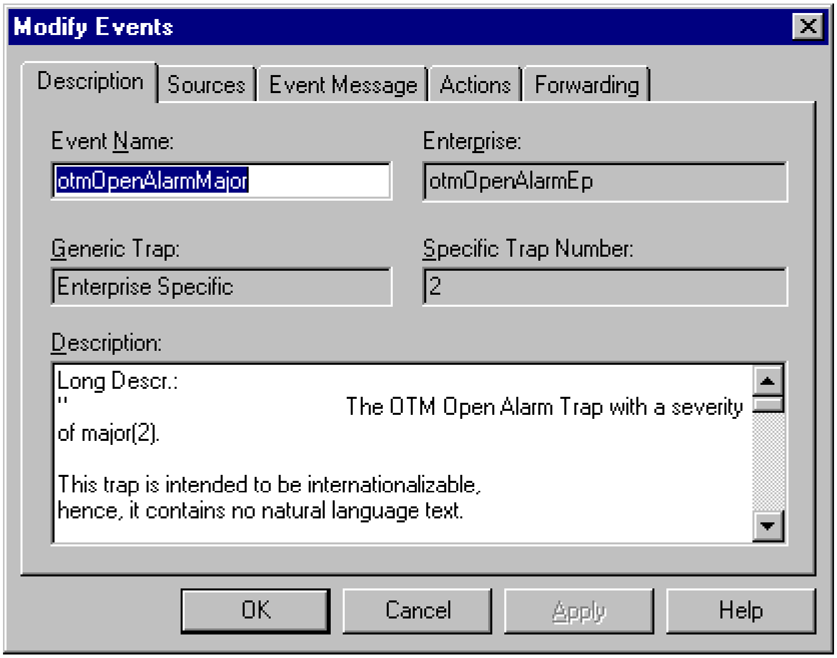
There are six events defined for the otmOpenAlarmEp Enterprise. For each event, you configure the desired actions to be taken if the event occurs.

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

1 Double-click the corresponding entry on the list.

The Modify Events dialog box appears (Figure 143).

Figure 143 Modify Events - Description



Event Name: otmOpenAlarmMajor

Enterprise: otmOpenAlarmEp

Generic Trap: Enterprise Specific

Specific Trap Number: 2

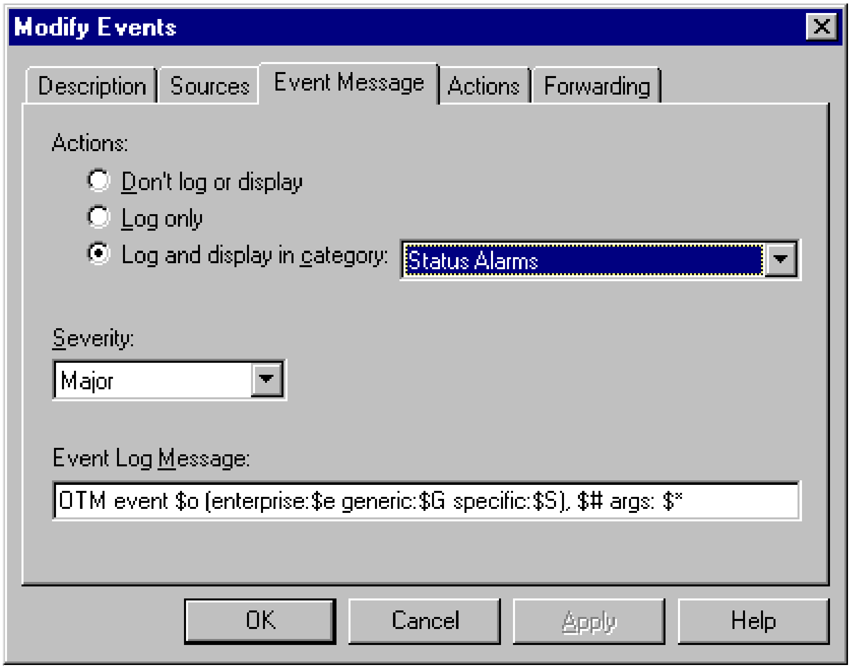
Description:

Long Descr.:
''   The OTM Open Alarm Trap with a severity
of major(2).

This trap is intended to be internationalizable,
hence, it contains no natural language text.

2 Select the Event Message tab (Figure 144).

Figure 144 Modify Events - Event Message



Actions:

○ Don't log or display

○ Log only

● Log and display in category: Status Alarms

Severity: Major

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

3 Configure the following:

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

This enables 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 displayed message shows the contents of the event message.

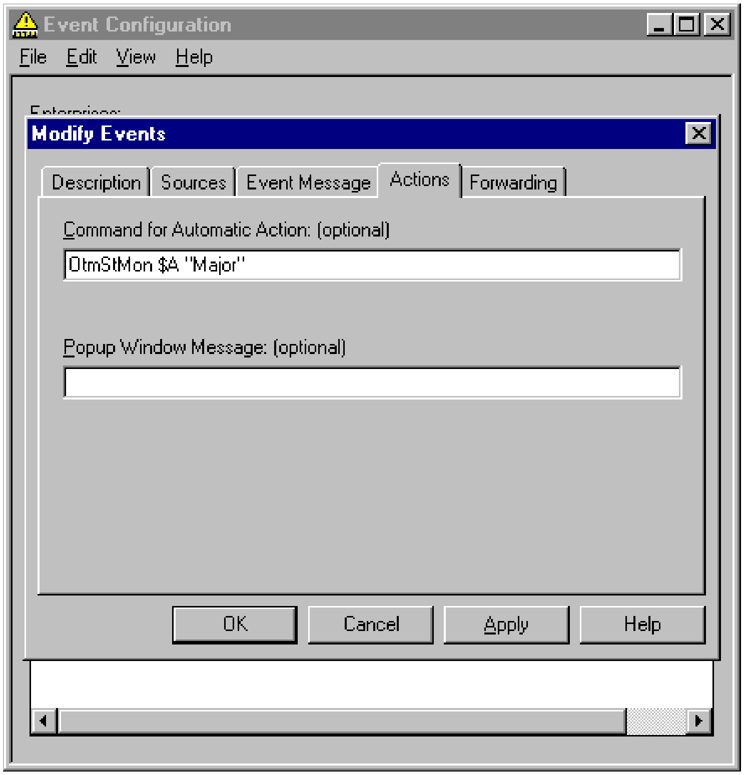
You are allowed to display any message that you choose in the Alarm Browser.

Table 9 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 145).

Figure 145 Modify Events - Actions



Command for Automatic Action: (optional)

OtmStMon $A "Major"

Popup Window Message: (optional)

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 is also 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 two 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 appears. 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*> is HP OV NNM’s unique selection name for an object item on the Network Map

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

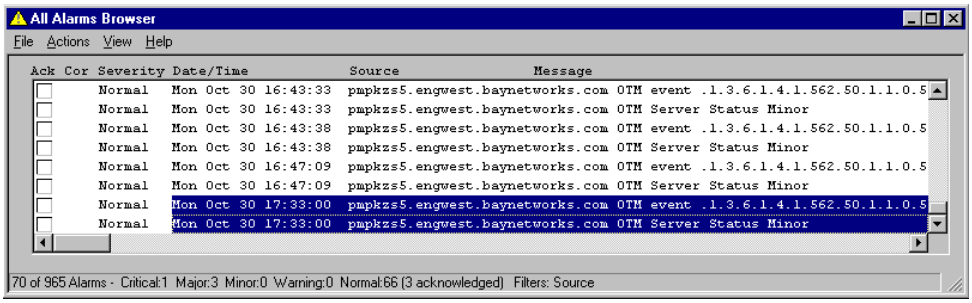
If the OTM Status Monitor is not called, then the color of the object that appears on the Network Map does not change for the incoming event.

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

A call to the OTM Status Monitor results in a message, in addition to the original incoming event message, appearing in the NNM All Alarms Browser (Figure 146). This message is logged whenever the OTM Status Monitor changes the color of an object.

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 may want to configure these events in such a way to simply log the incoming event message and not call OtmStMon.

Figure 146 All Alarms Browser



```
Ack Cor Severity Date/Time           Source                          Message
 ☐      Normal   Mon Oct 30 16:43:33 pmpkzs5.engwest.baynetworks.com OTM event .1.3.6.1.4.1.562.50.1.1.0.5
 ☐      Normal   Mon Oct 30 16:43:33 pmpkzs5.engwest.baynetworks.com OTM Server Status Minor
 ☐      Normal   Mon Oct 30 16:43:38 pmpkzs5.engwest.baynetworks.com OTM event .1.3.6.1.4.1.562.50.1.1.0.5
 ☐      Normal   Mon Oct 30 16:43:38 pmpkzs5.engwest.baynetworks.com OTM Server Status Minor
 ☐      Normal   Mon Oct 30 16:47:09 pmpkzs5.engwest.baynetworks.com OTM event .1.3.6.1.4.1.562.50.1.1.0.5
 ☐      Normal   Mon Oct 30 16:47:09 pmpkzs5.engwest.baynetworks.com OTM Server Status Minor
 ☐      Normal   Mon Oct 30 17:33:00 pmpkzs5.engwest.baynetworks.com OTM event .1.3.6.1.4.1.562.50.1.1.0.5
 ☐      Normal   Mon Oct 30 17:33:00 pmpkzs5.engwest.baynetworks.com OTM Server Status Minor
```

70 of 965 Alarms - Critical:1 Major:3 Minor:0 Warning:0 Normal:66 (3 acknowledged) Filters: Source

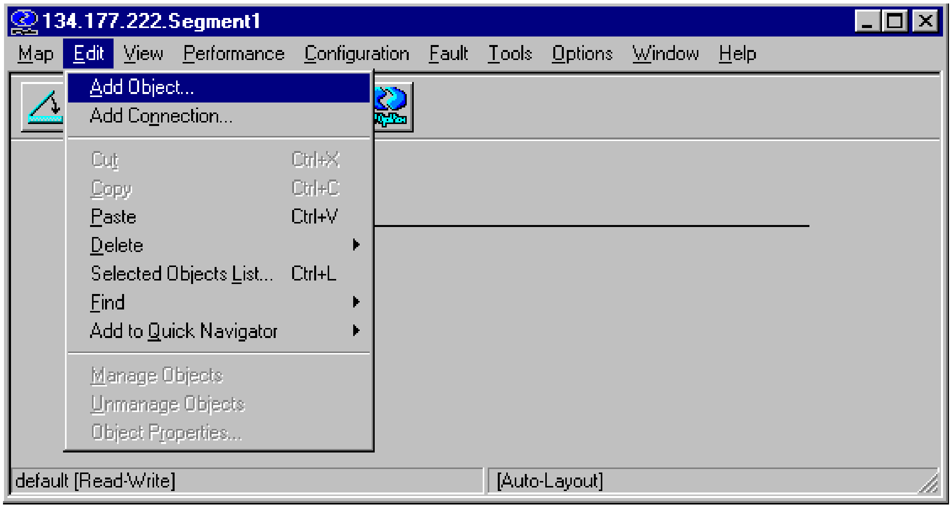
Network Map set up

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

1 Locate the appropriate place in the Network Map for the OTM Server.

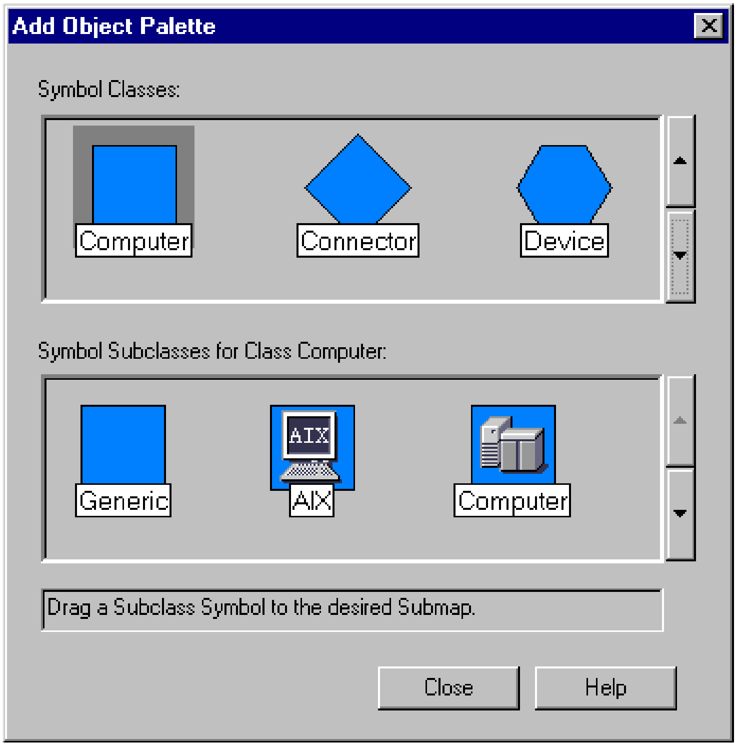
2 Select Edit > Add Object (Figure 147).

Figure 147 NNM Edit - Add Object



3 Select Computer from the Symbol Classes in the Add Object Palette dialog box (Figure 148).

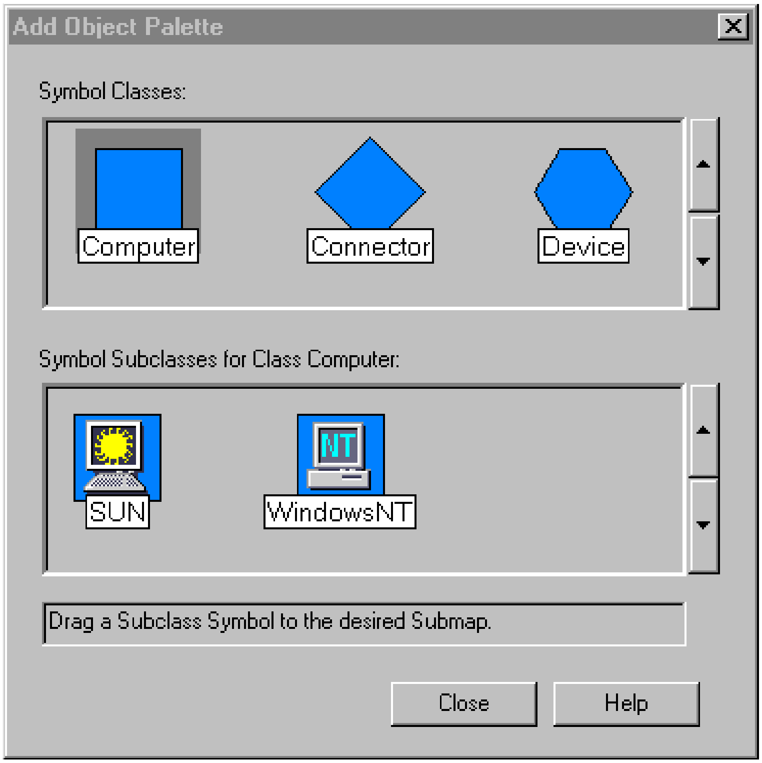
Figure 148 Add Object Palette dialog box



Drag a Subclass Symbol to the desired Submap.

4 Select and drag the standard WindowsNT icon from the Symbol Subclasses (Figure 149) onto the appropriate location on the Network Map.

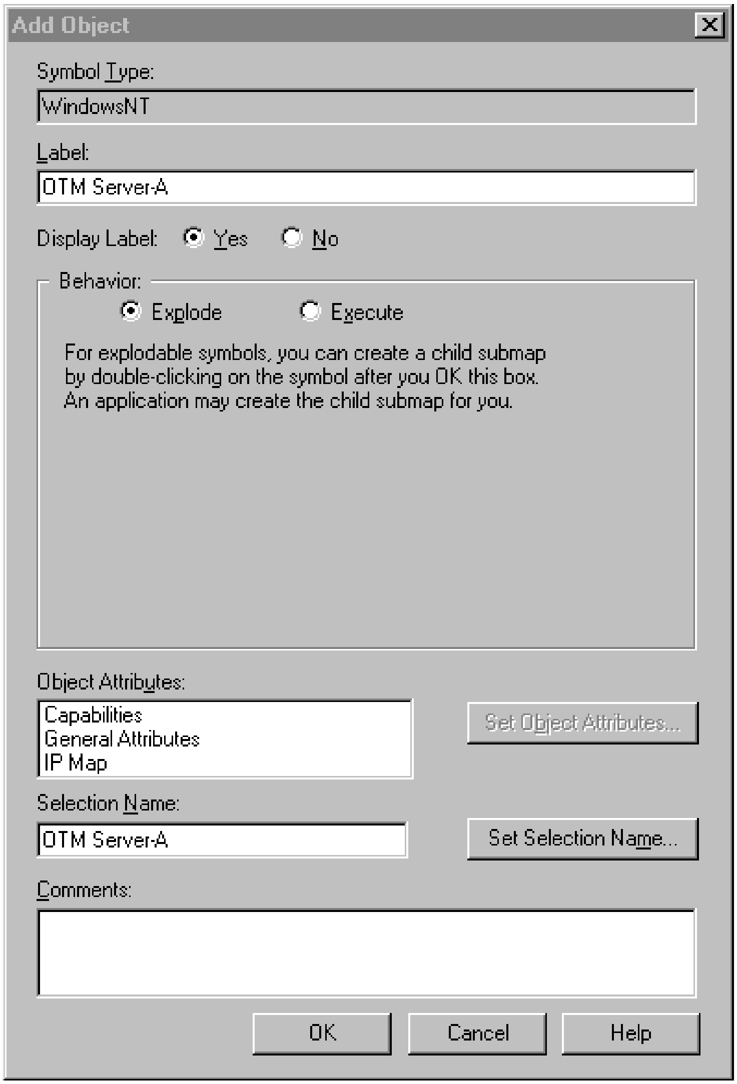
Figure 149 Add Object Palette dialog box II



Drag a Subclass Symbol to the desired Submap.

5 The Add Object dialog box opens. Fill in the Label field (OTM Server-A in this example) (Figure 150).

Figure 150 Add Object dialog box



Add Object

Symbol Type: WindowsNT

Label: OTM Server-A

Display Label: ● Yes ○ No

Behavior: ● Explode ○ Execute

For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

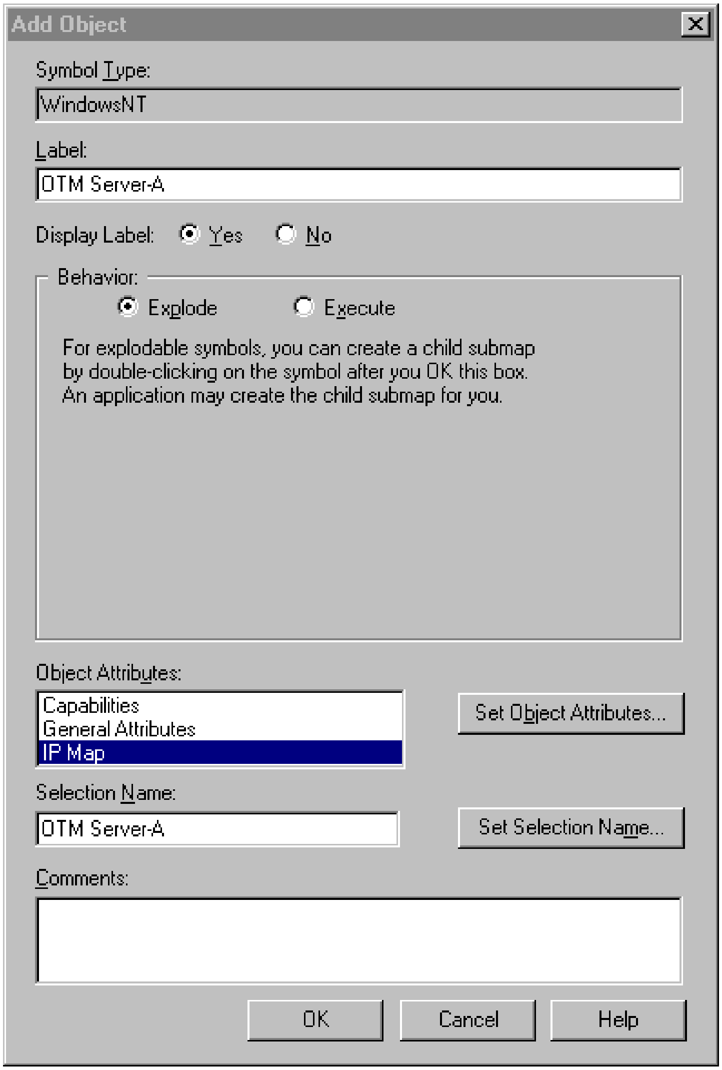
Object Attributes:
Capabilities
General Attributes
IP Map

Selection Name: OTM Server-A

Comments:

6 Select IP Map under Object Attributes, and click Set Object Attributes (Figure 151).

Figure 151 Add Object - IP Map



Add Object

Symbol Type: WindowsNT

Label: OTM Server-A

Display Label: ● Yes ○ No

Behavior: ● Explode ○ Execute

For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

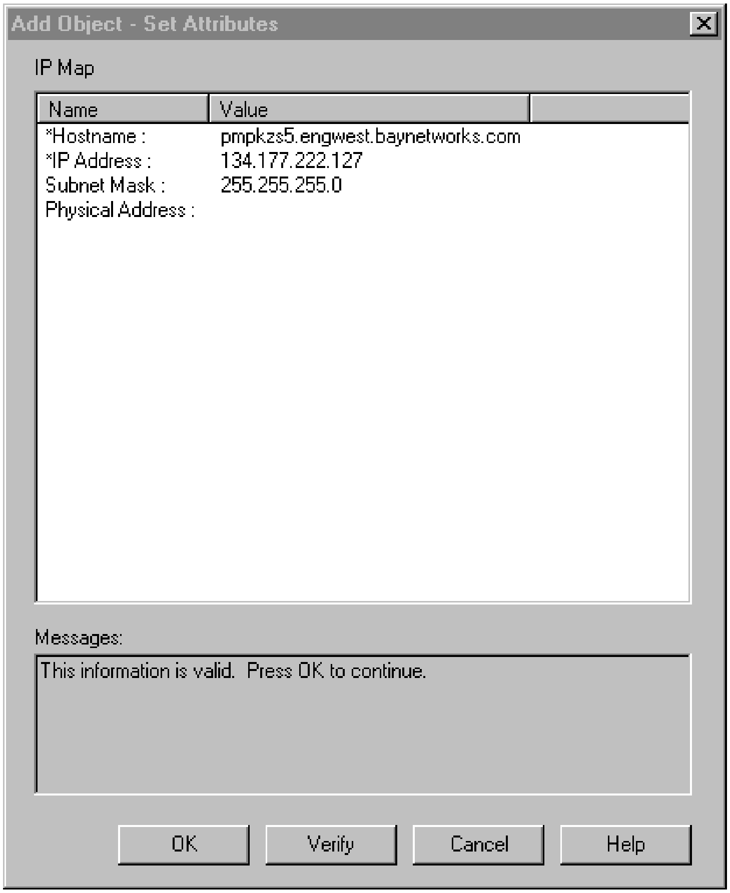
Object Attributes:
Capabilities
General Attributes
IP Map

Selection Name: OTM Server-A

Comments:

7 Select and fill in the entries for Hostname, IP Address, and Subnet Mask (Figure 152).

Figure 152 Add Object - Set Attributes dialog box



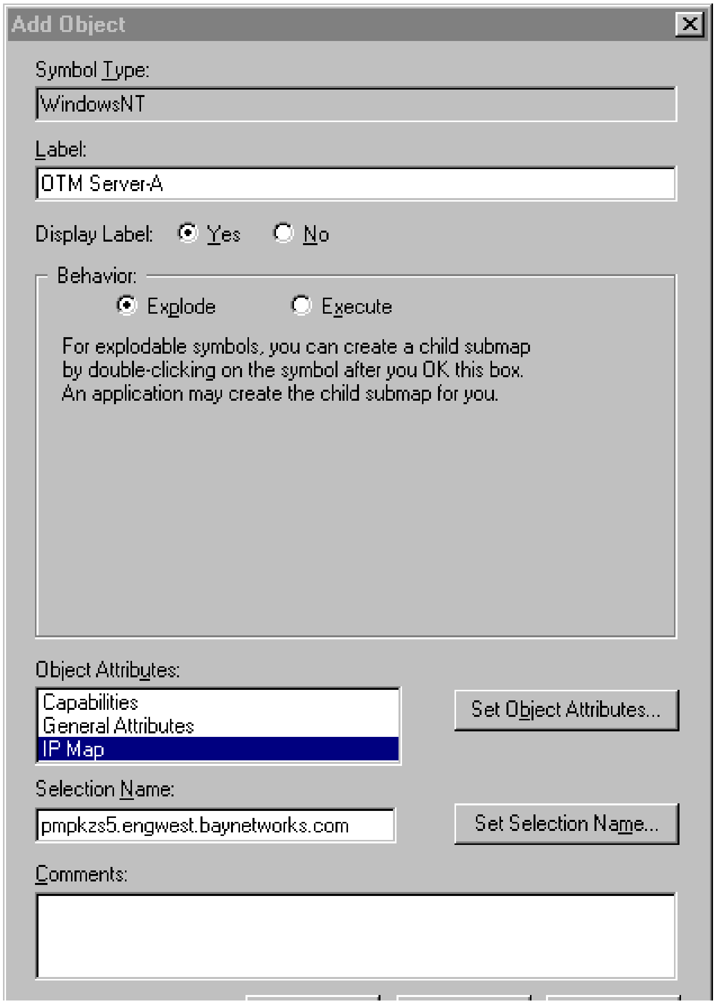
Name	Value
*Hostname :	pmpkzs5.engwest.baynetworks.com
*IP Address :	134.177.222.127
Subnet Mask :	255.255.255.0
Physical Address :	

Messages:

This information is valid. Press OK to continue.

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 153).

Figure 153 Add Object - Selection Name



Add Object

Symbol Type: WindowsNT

Label: OTM Server-A

Display Label: ● Yes ○ No

Behavior: ● Explode ○ Execute

For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

Object Attributes:
Capabilities
General Attributes
IP Map

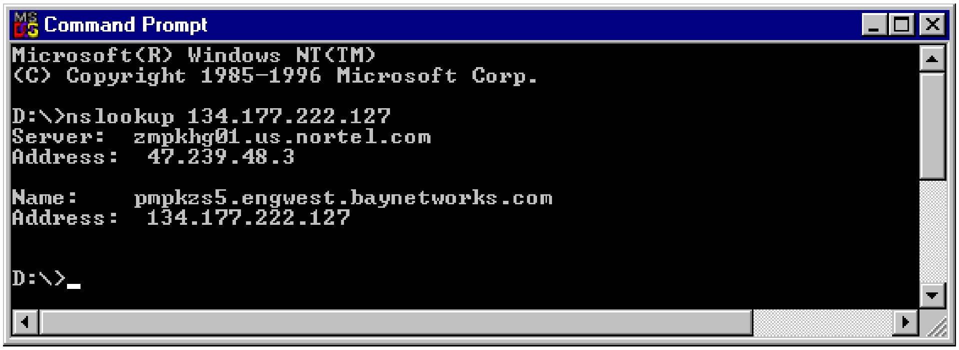
Selection Name: pmpkzs5.engwest.baynetworks.com

Comments:

9 Click OK. 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 154). If the IP address cannot be interpreted locally, then enter the dotted decimal representation.

Figure 154 nslookup command



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

D:\>nslookup 134.177.222.127
Server:  zmpkhg01.us.nortel.com
Address:  47.239.48.3

Name:    pmpkzs5.engwest.baynetworks.com
Address:  134.177.222.127


D:\>_
```

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 155, Figure 156).

Figure 155 NNM Main Menu - Symbol Properties

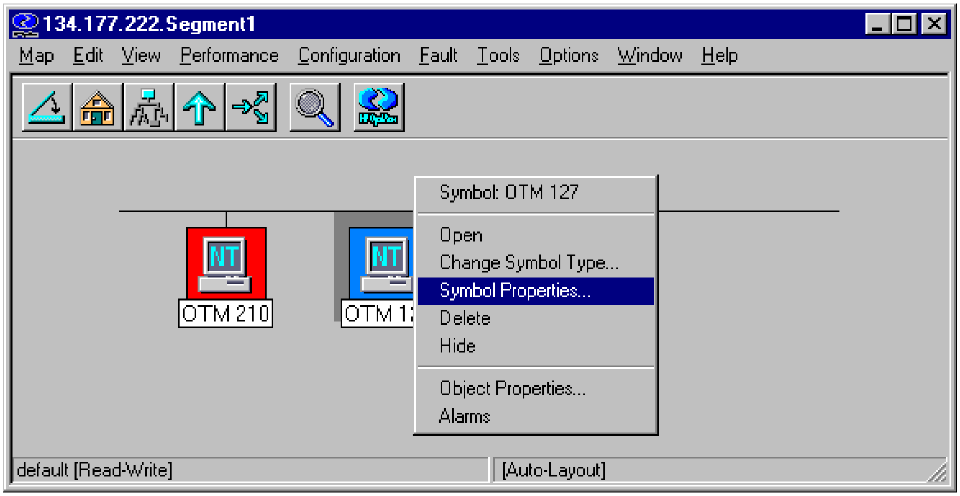
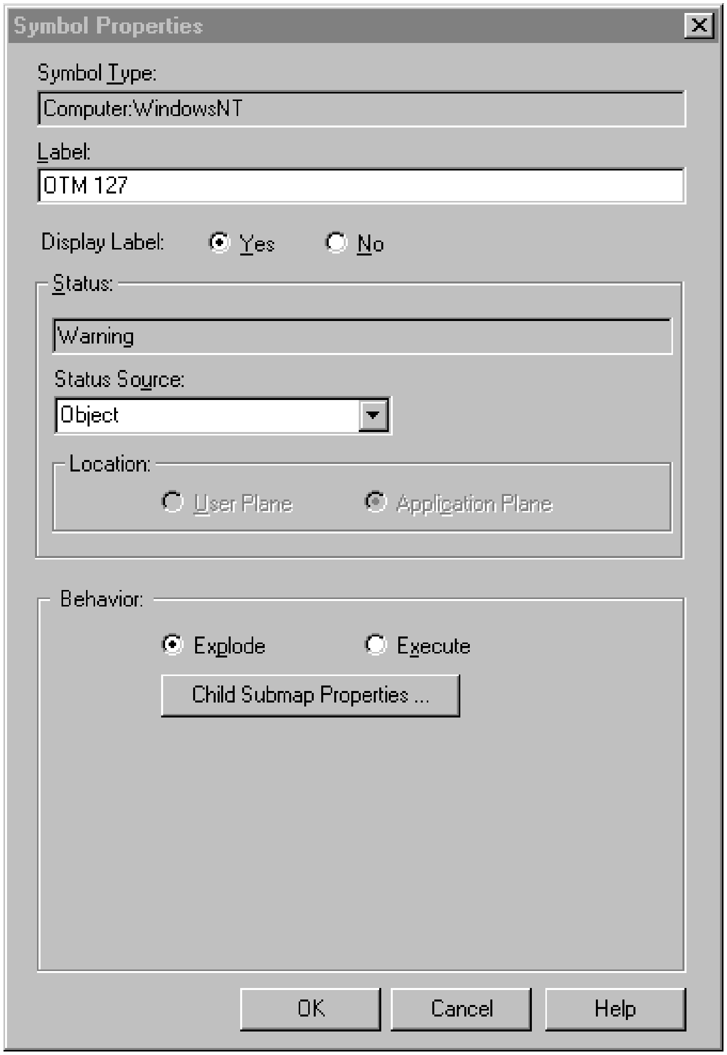


Figure 156 Symbol Properties dialog box



Symbol Properties

Symbol Type: Computer:WindowsNT

Label: OTM 127

Display Label: ● Yes ○ No

Status: Warning

Status Source: Object

Location: ○ User Plane ● Application Plane

Behavior: ● Explode ○ Execute

OTM Web Server Access configuration

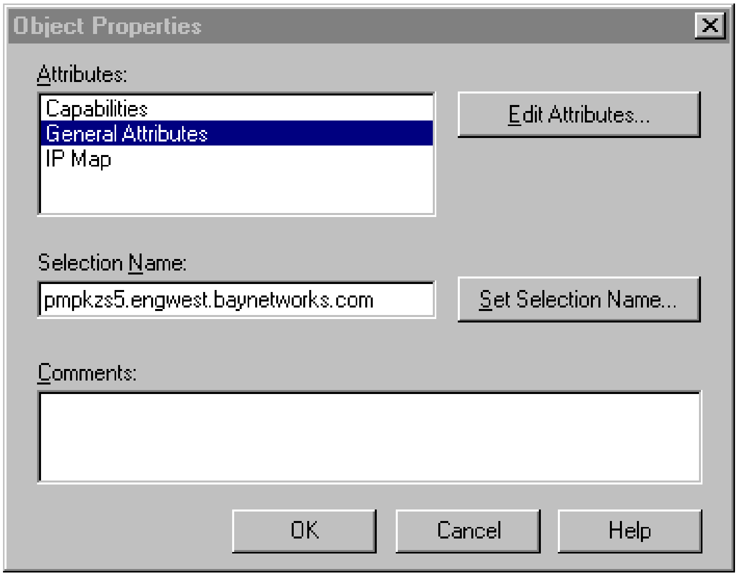
You can also configure the Management URL to access the OTM Server (Figure 157, Figure 158).

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.

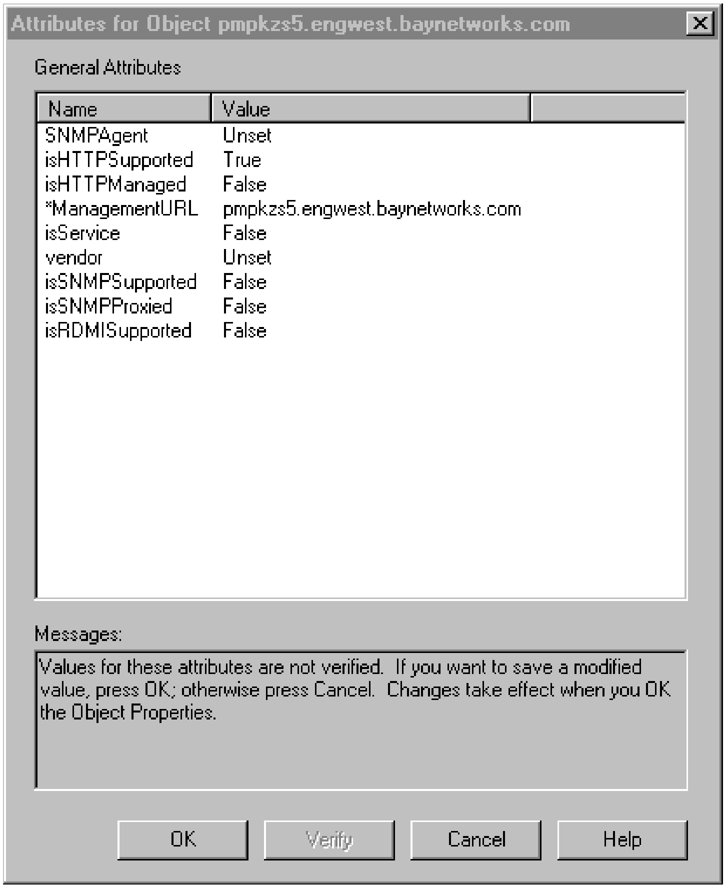
Figure 157 Object Properties dialog box



Selection Name: pmpkzs5.engwest.baynetworks.com

Comments:

Figure 158 Attributes for Object dialog box



Attributes for Object pmpkzs5.engwest.baynetworks.com

General Attributes

Name	Value
SNMPAgent	Unset
isHTTPSupported	True
isHTTPManaged	False
*ManagementURL	pmpkzs5.engwest.baynetworks.com
isService	False
vendor	Unset
isSNMPSupported	False
isSNMPProxied	False
isRDMISupported	False

Messages:

Values for these attributes are not verified. If you want to save a modified value, press OK; otherwise press Cancel. Changes take effect when you OK the Object Properties.

OTM configuration (OTM PC)

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

Windows NT and Windows 2000 reference

This chapter provides reference information related to the Windows NT and Windows 2000 operating systems. The following topics are presented:

- "Installing Windows NT"
- "Installing Windows 2000" on page 314
- "Testing network cards" on page 319

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.

- "Running the Windows NT setup program" on page 304
- "Installing Windows NT components" on page 305
- "Installing Network Adapter software" on page 306
- "Configuring TCP/IP" on page 307
- "Configuring Initial Workgroups" on page 308
- "Configuring system settings" on page 308
- "Creating an Emergency Repair disk" on page 308
- "Completing the Windows NT installation" on page 309
- "Installing Remote Access Service on Windows NT" on page 309

Hardware compatibility check

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

Running the Windows NT setup program

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 computers, 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 dialog box. 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 the 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 set up Windows NT.
10. In the Windows NT Server Setup dialog box, 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 a partition, and type the size of partition you want. The largest boot partition that you can create is 4095 MB. If the system was previously configured as an NT Workstation, select N for new.

14 Select “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 the 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*.

The disk format takes approximately 3 minutes for a 4 G drive and only a few seconds on a drive controlled by a RAID controller.

17 The default Winnt is prompted. You may 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 computer 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 computer 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 dialog box appears, click Next on “Gathering information about your computer.”

2 Enter your Name and Organization Name, and then 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 dialog box (StandAlone Server is highly recommended).

6 Enter the password for the Local Administrator.

7 Create an Emergency Repair Disk.

8 Select Components, and then Click Next.

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

Installing Network Adapter software

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 CLAN card is recommended to install on the top PCI slot and ELAN on the second-from-the-top PCI slot.

1 In Windows NT Setup, verify that the Wired to the network check box is checked, and then click Next.

2 In the Install Microsoft Internet Information Server dialog box, uncheck the box, and then click Next.

3 Click Select from the List in the Network Adapter dialog box.

4 Click Have Disk and insert the floppy disk 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 widow displays your LAN card. Since the server has two LAN cards, click on Select from the list to install the CLAN card driver, and follow the previous step to install the CLAN card.

6 In the Network Protocol dialog box, only select TCP/IP protocol, and then click Next to continue.

7 In the Network Services dialog box, you see the following services:

- RPC configuration
- NetBIOS Interface
- Workstation

- Server

Click to select the desired services.

8 Click Next to install selected components.

9 Click OK for Adapter Properties.

10 If the ELAN card is the same type as the previously installed CLAN card, the following message may appear: “A network card of this type is already installed in the system. Do you want to continue?” Select OK.

11 The Adapter Properties dialog box appears for the second LAN card. Click OK to continue.

Configuring TCP/IP

Configure TCP/IP as follows:

1 The TCP/IP Setup dialog box appears. If you have a DHCP server and want to configure the IP address from the DHCP server, then select Yes. Otherwise, select No and proceed to the next step.

2 In the TCP/IP Configuration dialog box:

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

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

3 In the Show Binding For dialog box:

a Select all Protocols.

b Configure the binding order so that the CLAN adaptor comes first, then the ELAN adaptor, then the Virtual Adapters for RAS.

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

Configuring Initial Workgroups

1. In the Domain / Workgroup Setting dialog box, use the default Workgroup settings and click OK to continue.
2. Click Finish in the Finishing Setup dialog box.
3. In the Internet Information Server Installation dialog box, remove the gopher selection.
4. Install the SQL server driver.
5. In the Microsoft Internet Information Server dialog box, 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 dialog box, select your Time Zone.
2. Select the check box (default is checked) for automatically adjusting for Daylight Saving Time.
3. In the Display Setting dialog box:
   - Select OK to verify that the video adapter was detected.

     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, and then click OK to test the 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 dialog box, 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.

Installing Remote Access Service on Windows NT

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

No specific configuration of RAS is required because OTM uses RAS APIs directly.

- If RAS service is disabled (or not configured), no components are affected by disabling RAS (RAS service is disabled by default).
- If RAS is configured, Nortel Networks recommends that RAS be configured to enable the incoming call to Access the Computer Only. This setting accesses only the RAS server but not the rest of the network.

Procedure

1. Choose Control Panel > Network. Click the Services tab, and then click Add to add Remote Access Service software.
2. Insert the Windows NT server CD, and then click Continue.
3. Select Yes to “invoke the modem installer to enable you to add a modem.”

   A modem does *not* have to be attached to install this software.
4. In the Install New Modem dialog box, 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 dialog box, select COM1, and then click Next.

8. In the Location Information dialog box, enter your Area Code, click Next, and then click Finish.
9. A dialog box 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 dialog box, select This Computer only. Select Use Static Pool, and enter the initial range as 1.0.0.1 to 1.0.0.255. Click OK to return to the Remote Access Setup dialog box and click Continue.
13. In the “Remote Access Service has been successfully installed” dialog box, click OK.
14. In the Network dialog box, click OK. Click Close.

    The system binds all the network protocol software. Remove the Windows NT Server CD, and press Enter to restart your server.

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, Nortel Networks recommends allowing the incoming call to access “The computer only,” which is the RAS Server itself.

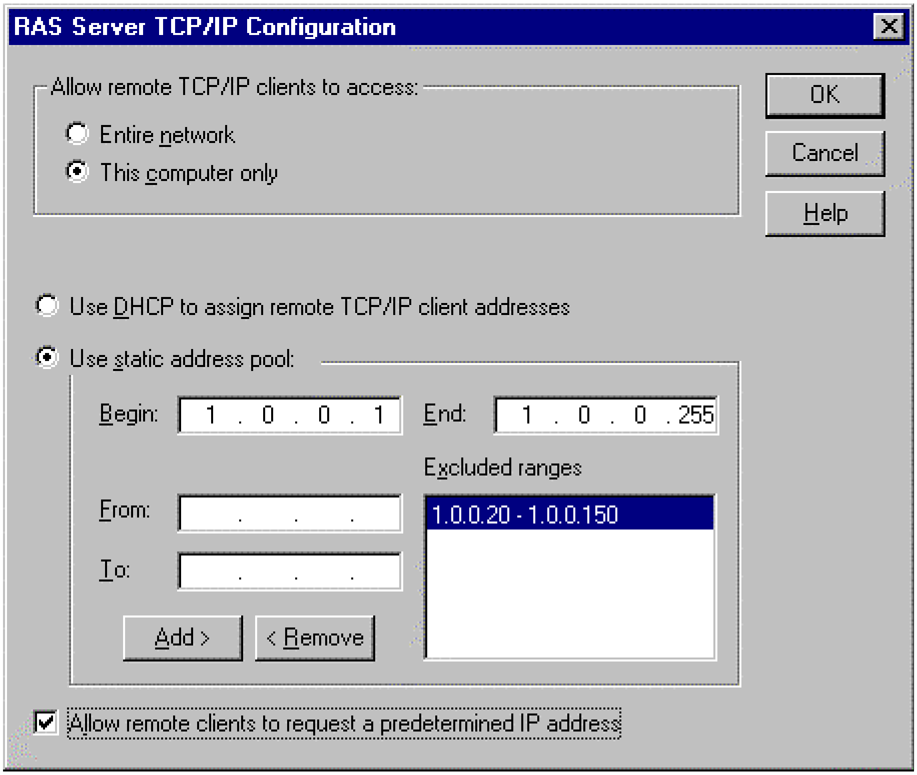
This configuration is only available on Windows NT Server. If you run OTM on a Windows NT Workstation, you do not have this capability.

As shown in Figure 159, 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)
- Configure the IP address to come from a pool of IP addresses maintained on the RAS Server

- Allow the incoming connection to request its own IP address

Figure 159 RAS Server TCP/IP Configuration dialog box



RAS Server TCP/IP Configuration

Allow remote TCP/IP clients to access:

○ Entire network
● This computer only

○ Use DHCP to assign remote TCP/IP client addresses

● Use static address pool:

Begin: 1 . 0 . 0 . 1
End: 1 . 0 . 0 . 255

Excluded ranges

1.0.0.20 - 1.0.0.150

From: . . .
To: . . .

☑ Allow remote clients to request a predetermined IP address

Grant permission

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

Callback

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 160, the default setting for RAS password authentication is to require Microsoft Encrypted Authentication. When you select this option, Nortel Networks assumes you only use Microsoft clients (Windows 98, Windows NT Server or Workstation, Windows 2000 Server or Professional computers) to 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 enables 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 56 Kbps modems with Multilink enabled, your bandwidth can be aggregated to 134.4 Kbps.

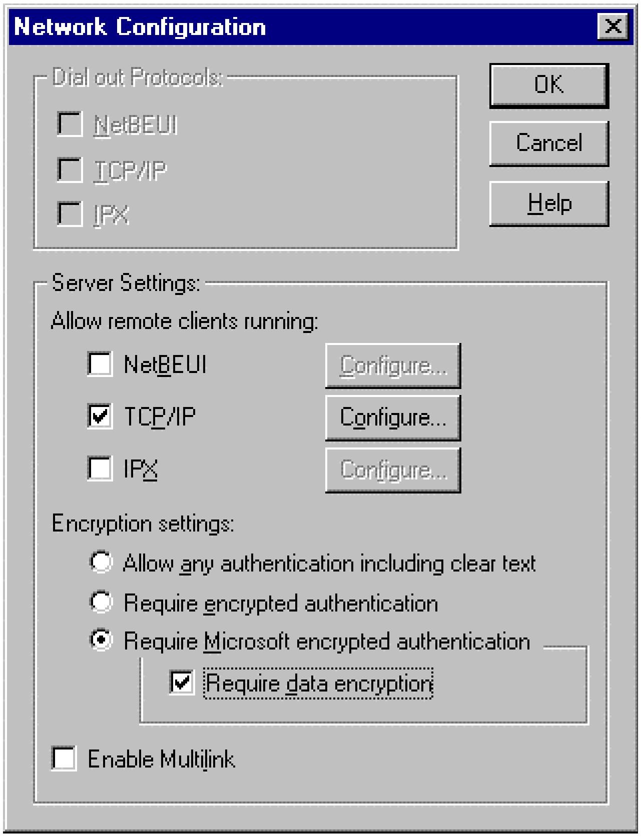
To use Multilink, both the server and client must have Multilink enabled.

For more information, refer to Chapter 6 in the *Windows NT Server Networking Supplement*.

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 160 Network Configuration dialog box



Network Configuration

Dial out Protocols:

□ NetBEUI

□ TCP/IP

□ IPX

Server Settings:

Allow remote clients running:

□ NetBEUI

☑ TCP/IP

□ IPX

Encryption settings:

○ Allow any authentication including clear text

○ Require encrypted authentication

● Require Microsoft encrypted authentication

☑ Require data encryption

□ Enable Multilink

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

Installing Windows 2000

This section describes an example of Windows 2000 installation. Due to hardware and software differences, this example may not match your installation.

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

- "Running the Windows 2000 setup program" on page 314
- "Installing Windows 2000 components" on page 315
- "Configuring TCP/IP" on page 316
- "Installing a modem" on page 318
- "Installing Remote Access Service on Windows 2000" on page 318

Hardware compatibility check

Check all hardware against the documentation available on Microsoft's web site at http://www.microsoft.com/windows2000/support/onlinedocs/default.asp.

Running the Windows 2000 setup program

1. Make sure the first bootup option on CD-ROM in the BIOS is enabled.
2. Insert the Windows 2000 server setup CD-ROM into the CD-ROM drive.
3. Boot the system.
4. In the Windows 2000 Server Setup Welcome dialog box, press Enter to set up the Windows 2000 Server.
5. In the Windows 2000 Licensing Agreement dialog box, press Page Down to go to the bottom of the page, and then choose F8.
6. Press C to create a partition, and then type the size of the partition that you want to create.
7. Use the up and down arrow keys to select the partition created on the first disk in step 6.
8. Press Enter to set up Windows 2000 on the selected item.
9. Use the up and down arrow keys to select Format partition using the NTFS files system, and then press Enter.

10 Wait while the setup program formats the partition. This will take several minutes.

11 Wait while the setup program copies files to the Windows 2000 installation folders. This will take several minutes.

12 Reboot the system.

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

Installing Windows 2000 components

Windows 2000 Server setup continues after the reboot.

13 The Installing Devices dialog box appears. This will take several minutes.

14 The Regional Settings dialog box appears. Select the default values or configure as needed, and then click Next.

15 The Personalize Your Software dialog box appears. Enter your name and the name of your organization, and then click Next.

16 The Your Product Key dialog box appears. Enter the product key, and then click Next.

17 The Licensing Modes dialog box appears. Select the default value, or choose Per Server or Per Seat, as appropriate, and then click Next.

18 The Computer Name and Administrator Password dialog box appears. Enter the computer name and the administrator password, and then click Next.

19 The Windows 2000 Components dialog box appears. Select the default values or select specific components, as appropriate, and then click Next.

20 The Date and Time Settings dialog box appears. Adjust the Date, Time, and Time Zone, as appropriate, and then click Next.

21 Wait for the Network Settings dialog box to appear. This will take several minutes.

22 When the Network Settings dialog box appears, accept the default value, Typical Settings, and then click Next.

23 The Workgroup or Computer Domain dialog box appears. Make the appropriate selection, and then click Next.

24 Wait while the set up program installs components. This will take several minutes.

25 Wait while the set up program performs final tasks. This will take several minutes.

26 The Completing the Windows 2000 Setup Wizard dialog box appears. Click Finish to reboot the system.

Note: In order to allow OTM client access wthout being logged in to the server at all times, the following configuration change for Windows Server 2000 is required:

1 If required, log in to the Windows 2000 server.

2 Go to **Start > Programs > Administrative Tools > Component Services.**

3 From the Component Services window, expand **Computers > My Computer > COM+ Applications**

4 Select **OTM Application**, and open the Properties window.

5 Select the **Identity** tab and click on the **This User** radio button.

6 Enter the local administrator account and password.

7 Click **OK**.

Note: This procedure will work for all applications except DECT.

Configuring TCP/IP

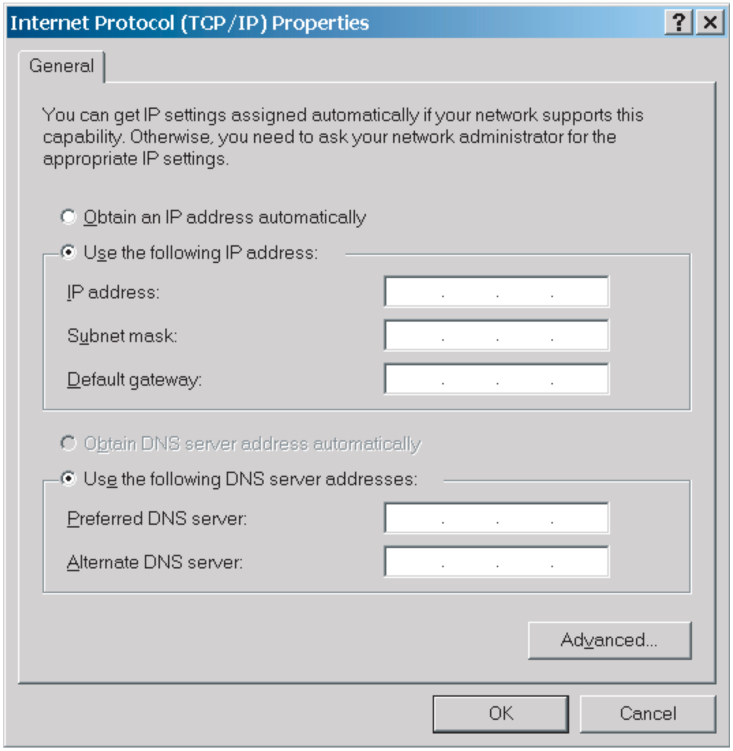
1 Choose Start > Settings > Network and Dialup Connections.

2 In the Network and Dialup Connections dialog box, right-click the Local Area Connection icon, and then select Properties.

3 In the Local Area Connection Properties dialog box, click to select Internet Protocol (TCP/IP), and then click Properties.

The Internet Protocol (TCP/IP) Properties dialog box appears (Figure 161).

Figure 161 Internet Protocol (TCP/IP) Properties dialog box



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

4 If you have a DHCP server and you want to configure the IP address from the DHCP server, click the Obtain an IP address automatically radio button, and go to step ; otherwise, proceed to the next step.

5 Click the Use the following IP address radio button. Enter the IP address, Subnet Mask, Default gateway, and DNS server information.

To enter WINS server information, click Advanced in the Internet Protocol (TCP/IP) Properties dialog box.

Click OK.

6 Reboot the system.

Installing a modem

1. Choose Start > Settings > Control Panel.
2. Double-click the Phone and Modem Options icon.
3. In the Phone and Modem Options dialog box, click the Modems tab.
4. If the modem on the computer is not already installed, click Add.

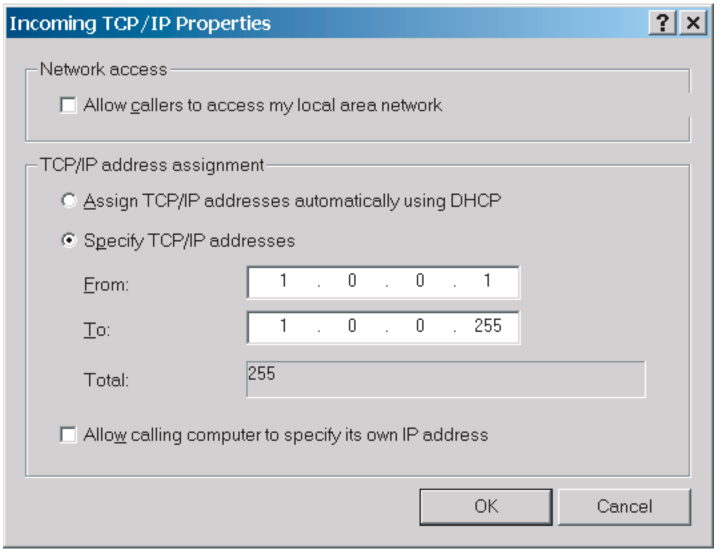
   If it is attached to the computer, Windows 2000 can detect and install a modem automatically.
5. In the Install New Modem dialog box, click Next to continue.
6. If the system is unable to detect the modem, you must insert the modem manufacturer's disk that came with the modem, and then select Have disk to install.
7. If the system does not have a modem attached, select Standard 28800 bps Modem from the list.
8. Click Finish to close the dialog box.

Installing Remote Access Service on Windows 2000

1. Choose Start > Settings > Network and Dialup Connections.
2. Double-click the Make New Connection icon.
3. In the Network Connection Wizard welcome dialog box, click Next.
4. In the Network Connection Type dialog box, select Accept incoming connections, and then click Next.
5. In the Devices for Incoming Connections dialog box, select the appropriate connection device, and then click Next.
6. In the Incoming Virtual Private Connection dialog box, check the Do not allow virtual private connections check box, and then click Next.
7. In the Allowed Users dialog box, select the users that are allowed to connect to the server, and then click Next.
8. In the Networking Components dialog box, click to select Internet Protocol (TCP/IP), and then click Properties.

   The Incoming TCP/IP Properties dialog box appears (Figure 162).

Figure 162 Incoming TCP/IP Properties dialog box



Incoming TCP/IP Properties

Network access

□ Allow callers to access my local area network

TCP/IP address assignment

○ Assign TCP/IP addresses automatically using DHCP

● Specify TCP/IP addresses

From: 1 . 0 . 0 . 1

To: 1 . 0 . 0 . 255

Total: 255

□ Allow calling computer to specify its own IP address

9 In the Incoming TCP/IP Properties dialog box, uncheck the Allow callers to access my local area network check box. Click the Specify TCP/IP address radio button. Enter the initial range as From 1. 0 . 0 . 1 To 1 . 0 . 0 . 255, and then click OK.

10 In the Networking Components dialog box, click Next.

11 In the Completing the Network Connection Wizard dialog box, type the connection name, and then click Finish.

Testing network cards

Test the network cards after you complete the Windows NT or Windows 2000 installation.

Testing the Customer LAN

1 Configure the Captive Client IP address on the same subnet as the Customer LAN (CLAN). The equivalent subnet would be the BINARY AND of the full Captive Client IP address with the CLAN subnet mask (for example, 255.255.240.0). The subnet mask of the Captive Client would be the same as that for the CLAN.

2 Ping the CLAN IP Address from Captive Client (for example, 47.82.38.100).

Testing the Embedded LAN

1 Configure the Captive Client IP address on the same subnet as the Embedded LAN (ELAN). The equivalent subnet would be the BINARY AND of the full Captive Client IP address with the ELAN subnet mask (for example, 255.255.240.0). The subnet mask of the Captive Client is the same as that for the ELAN.

2 Ping the ELAN Address from Captive Client (for example, 47.114.45.3).

Uninstall OTM

This chapter contains information about using Uninstall to remove software that is no longer needed, or that has become damaged or was incorrectly installed.

Procedure

1 Access Uninstall:

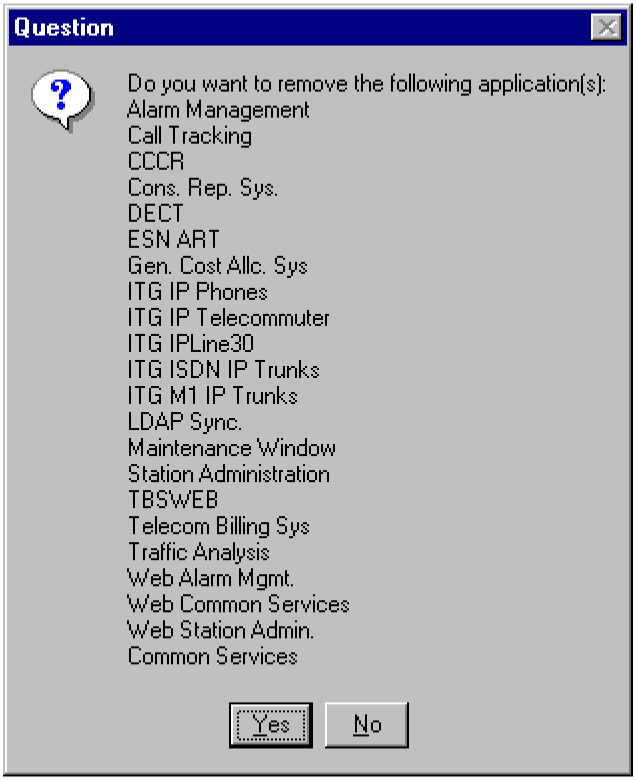
a From the Start menu, select Programs > Optivity Telephony Manager > OTM Uninstaller.

or

b In the Software Installation Wizard, select Uninstall in the Setup Choices dialog box. See Setup choices in the chapter on Installing OTM Server software.

2 The Uninstall Confirmation dialog box (Figure 163) displays a list of the OTM applications that are currently installed, and asks for confirmation that you want to delete them. Click Yes to continue.

Figure 163 Uninstall Confirmation dialog box

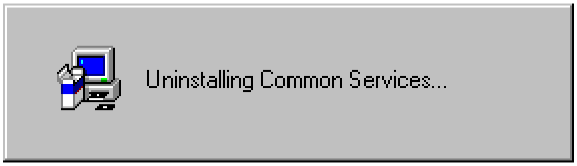


Question

Do you want to remove the following application(s):
Alarm Management
Call Tracking
CCCR
Cons. Rep. Sys.
DECT
ESN ART
Gen. Cost Allc. Sys
ITG IP Phones
ITG IP Telecommuter
ITG IPLine30
ITG ISDN IP Trunks
ITG M1 IP Trunks
LDAP Sync.
Maintenance Window
Station Administration
TBSWEB
Telecom Billing Sys
Traffic Analysis
Web Alarm Mgmt.
Web Common Services
Web Station Admin.
Common Services

3 The status box (Figure 164) provides a visual indicator of the progress of the uninstall process. Common Services is the last application to be uninstalled.

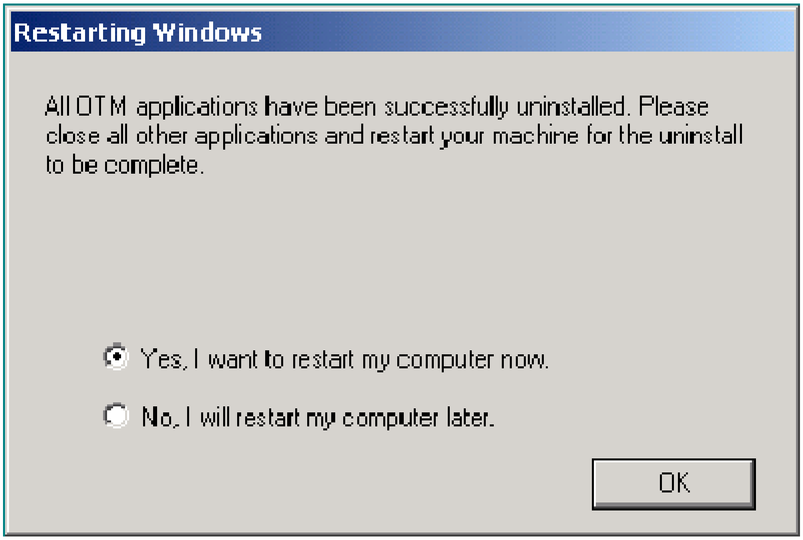
Figure 164 Uninstall status box



Uninstalling Common Services...

4 The Reboot request dialog box appears requesting that you reboot the PC, giving the option of performing the reboot now or later (Figure 165). Select your preference and click OK to continue.

Figure 165 Reboot request dialog box



Restarting Windows

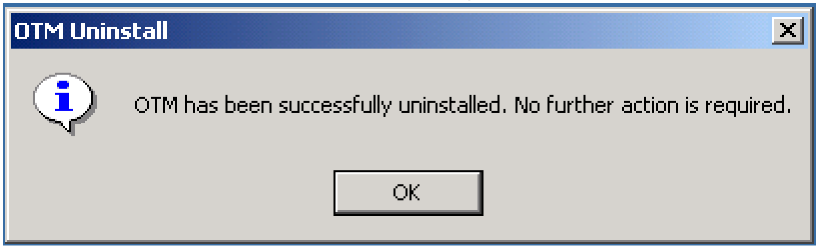
All OTM applications have been successfully uninstalled. Please close all other applications and restart your machine for the uninstall to be complete.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

5 After the PC has been rebooted, the Uninstall complete dialog box appears indicating that OTM has been removed (Figure 166). Click OK to exit.

Figure 166 Uninstall complete dialog box



OTM Uninstall

OTM has been successfully uninstalled. No further action is required.

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 3.0 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
- Web and OTM Clients and their impact on OTM Server resources
- Web-based Station Administration Write capability (that is, performing Station updates over the Web) and its impact on the OTM Server
- Succession 1000 and Meridian 1 and their impact on OTM Server resources

- Communications between the OTM Server and Succession 1000, Meridian 1 systems, OTM/Web Clients, LDAP Server, and so on, and their impact on the network to which they are connected

The Billing applications result in a processor load that 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.

Impact analysis

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

Based upon this analysis, recommendations are made as to:

- The resources required on the OTM Server
- The number of Clients, Succession 1000 and Meridian 1 systems that can be connected to a single OTM Server
- Network bandwidth and routing considerations

Analysis of the results of benchmark testing are presented in Table A-3 on page A-343, Table A-4 on page A-351, and Figure A-1 on page A-354. The tables can be used to calculate the resources and connections possible for various OTM Server usage scenarios.

- Table A-3 highlights PC performance for several OTM applications.
- Table A-4 highlights the peak and average transfer rates for various OTM activities.
- Figure A-1 presents a graphical representation of station response time compared with round trip time (RTT).

To aid in this process, this appendix analyzes four typical OTM Server configurations. Use these configurations as examples and the raw table data to extrapolate configurations specific to a given customer/distributor setup.

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

Running in stand-alone mode, OTM provides access to Meridian Administration Tools (MAT)-equivalent features only. As a result, the engineering rules for this setup mimic those required for MAT.

Hardware and Software Comparisons

Sr. No.	Hardware with X21 Release 3 software	System Type	Machine Type
1.	CSE	CSE 1000	CSE 1000

Table 10 Hardware Machine Type for Meridian 1 hardware with Succession 3.0

		When 'Signaling Server' checkbox in 'Network' page is un-checked		**When 'Signaling Server' checkbox in 'Network' page is checked**	
Sr. No.	**Hardware with Succession 3.0**	**System Type**	**Machine Type**	**System Type**	**Machine Type**
1.	11C/Mini	Meridian1	11C / 11C Mini	Succession	Succession 1000M Small
2.	51C 060	Meridian1	51C 060	Succession	Succession 1000M Half Group 060
3.	51C 060E	Meridian1	51C 060E	Succession	Succession 1000M Half Group 060E
4.	61C 060	Meridian1	61C 060	Succession	Succession 1000M Single Group 060
5.	61C 060E	Meridian1	61C 060E	Succession	Succession 1000M Single Group 060E
6.	61C PII	Meridian1	61C PII	Succession	Succession 1000M Single Group PII
7.	81, 81C 060	Meridian1	81, 81C 060	Succession	Succession 1000M Multi Group 060
8.	81, 81C 060E	Meridian1	81, 81C 060E	Succession	Succession 1000M Multi Group 060E
9.	81C PII	Meridian1	81C PII	Succession	Succession 1000M Multi Group PII

Software limits

Co-residency support

Following is the current list of available co-residency support for OTM.

.

Table 11 Co-residency support (Part 1 of 6)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
HPUX 11.0	Netscape 4.79 English	N/A	N/A	ONMS 10.1/ONMS “livewire”
Solaris 2.8	Netscape 4.79 English	N/A	N/A	ONMS 10.1/ONMS “livewire”
XP Pro	IE 6 English	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in English	2.1 English client or standalone	• PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8 • McAffee VirusScan 7
2000 Pro	IE 6 English	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in English	2.1 English client or standalone	• ONMS 10.1/ONMS “livewire” client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (English) • SECC 4.2 SMI Workbench (English) Symposium Web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0, • PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8 • McAffee VirusScan 7

Table 11 Co-residency support (Part 2 of 6)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 Server	IE 6 English	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in English	2.1 English server installation	• PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8
NT 4.0 Server	IE 6 English	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in English	2.1 English server installation	• PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8
2000 Pro in French	IE 6 French	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in French	2.1 French client or standalone	• ONMS 10.1/ONMS “livewire” client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (French) • SECC 4.2 SMI Workbench (French) • Symposium Web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0 • PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8 • McAffee VirusScan 7

Table 11 Co-residency support (Part 3 of 6)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 Pro in German	IE 6 German,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in German	2.1 German client or standalone	• ONMS 10.1/ONMS “livewire” client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (German) • SECC 4.2 SMI Workbench (German) • Symposium Web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0 • PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8 • McAffee VirusScan 7
2000 Pro in Japanese	IE 6 Japanese,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Japanese	2.1 English client or standalone	• ONMS 10.1/ONMS “livewire” client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (Japanese) • SECC 4.2 SMI Workbench (English) • Symposium Web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0 • PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8 • McAffee VirusScan 7

Table 11 Co-residency support (Part 4 of 6)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 Pro in Chinese Simplified	IE 6 Chinese Simplified,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Simplified Chinese	2.1 English client or standalone	• ONMS 10.1/ONMS “livewire” client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (Simplified Chinese) • SECC 4.2 SMI Workbench (English) • Symposium Web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • NetVision Administrator 4.0 • PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8 • McAffee VirusScan 7
2000 Pro in Spanish	IE 6 Spanish,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Spanish	2.1 English client or standalone	• ONMS 10.1/ONMS “livewire” client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (Spanish) • SECC 4.2 SMI Workbench (English) • Symposium Web Center Portal Administrator client 4. • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8 • McAffee VirusScan 7

Table 11 Co-residency support (Part 5 of 6)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
2000 Pro in Brazilian	IE 6 Brazilian,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Brazilian	2.1 English client or standalone	• ONMS 10.1/ONMS “livewire” client • CallPilot 2.5/3.0 Application Builder • SCCS 4.2/5.0 System Management Interface (SMI) Workbench (English) • SECC 4.2 SMI Workbench (English) • Symposium Web Center Portal Administrator client 4.0 • Symposium Agent 2.3 • Remote Office 1.3.5/1.4 Configuration Manager • PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8 • McAffee VirusScan 7
2000 Server in Japanese	IE 6 Japanese,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Japanese	2.1 English server installation	• PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8
NT 4.0 Server in Japanese	IE 6 Japanese,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Japanese	2.1 English server installation	• PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8
2000 Server in Simplified Chinese	IE 6 Simplified Chinese,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Simplified Chinese	2.1 English server installation	• PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8

Table 11 Co-residency support (Part 6 of 6)

Operating System	Browser	Office Components	OTM Installed	Other Coresident Applications
NT 4.0 Server in Simplified Chinese	IE 6 Simplified Chinese,	• Excel 2000/ 2002 • Word 2000/ 2002 (from Office XP) in Simplified Chinese	2.1 English server installation	• PC Anywhere 10.5 • Norton AntiVirus Corporate Edition 8
Web Clients:				
Any PC OS listed in above table which supports IE 6	IE 6	N/A	OTM 2.1 Web Client (Administrator UI)	• Call Pilot 2.5/3.0 Web Clients (Administrator Call Pilot Web Client) on IE 6 • SCCS 4.2/5.0 Web Admin Client 4.5/5.0 on IE 6 • Symposium Agent (Administration Workstation) on IE 6 • Symposium Agent Greeting 2.0 on IE 6 • BCM 3.5 Web Management Interface on IE 6 • MIVS version 1.17 web browser management tool on IE 6.
Any PC OS listed in above table which supports IE 6	IE 6	N/A	OTM 2.1 Web Client (Desktop UI)	• Call Pilot 2.5/3.0 Web Clients (My CallPilot) on IE 6 • SCCS 4.2/5.0 Web Client 4.5/5.0 (Agent UIs) on IE 6 • Symposium Agent Greeting on IE 6 • MIVS version 1.17 web browser management tool on IE 6.

Hard-coded limits

The following section lists the hard-coded limits in the OTM software.

Table A-1 outlines the maximum value for many of the parameters associated with the various components of OTM.

Table A-1 OTM capacity parameters

Parameter	Maximum Value
Windows Common Services	
Maximum number of Sites that can be created on an OTM server	3000
Maximum number of Branch Office systems can be created under a specific site	256
Maximum number of M1 synchronization / Update tasks (number of Log Windows) that can be executed at the same time	5
Number of Customers of M1 System	100
Range of DN	0-9999999
Maximum number of Survivable Expansion Cabinet	4
Maximum number of modem scripts that can be created	3000
Windows Common Services	
Maximum number of application jobs that can be scheduled in the Scheduler application	2000
Max String Length for:	
Site name	31
System name	31
Address	44
City	24
State/Province	24
Country	24
Zip/Postal Code	16
Comments	255
IP Address	15
Display (CPP profile)	1000
Timeout (CPP)	60
Phone Number (CPP)	50

Table A-1 OTM capacity parameters (Continued)

Parameter	Maximum Value
Access ID (CPP)	50
Modem Password (CPP)	50
Modem Installation String (CPP)	50
Issue	99
System ID	16
Maximum Speed Call Lists	8191
Maximum ACD Agents	1200
PDT password	16
Customer Name	31
Directory Numbers	24
Customer Password	16
HLOC	9999
Dial Intercom Group	2045
User ID	2045
LDAP	
Maximum number of LDAP Sync Log files that can be created separately	2000
Number of LDAP entries that can be synchronized at the same time	10,000
Number of entries that can be added from LDAP Server to OTM Directory	15,000
Corporate Directory	
Maximum number of customized reports that can be created	2000
Number of data fields that can be defined into a corporate report	111
Maximum number of reports that can be generated at the same time	1
Maximum string length of all parameters	255 characters
Data Buffering and Access (DBA)	
Maximum number of Action records that can be defined in a DBA session	1000
Maximum number of Rule records that can be defined in a DBA session	1000
Maximum number of CDRs that can be collected	5,000,000
List Manager	
Maximum number of speed call lists that can be created	8190
Maximum number of group call lists that can be created	63

Table A-1 OTM capacity parameters (Continued)

Parameter	Maximum Value
Maximum number of group hunt lists that can be created.	8190
Maximum String length for:	
Speed Call List	
List Name	50
Entry Name	50
Dialed Digits	31
Speed Call List	
Entry Number	999
PLDN	31
Group Call list:	
List Name	50
Entry Name	50
Entry Number	19
Group Hunt List:	
List Name	50
Maximum String length for:	
Group Hunt List:	
PLDN	50
Dialed Digits	31
Entry Name	50
Entry Number	95
Station Administration	
Maximum number of External Parties that can be created	5000
Maximum number of Role/Projects that can be created	5000
Maximum number of employees that can be created	16,000
Maximum string length of all parameters	128 characters
OTM DECT	
Maximum number of DECT Systems	500
Maximum String length for:	
DECT system name	255
Password	Unlimited

Table A-1 OTM capacity parameters (Continued)

Parameter	Maximum Value
IP Address	15
OTM server IP Interface	15
Phone Number	64
PARI (Access Right Identification tab)	8
SARI (Access Right Identification tab)	8
Upstream Manager IP address (Access Right Identification tab)	15
Maintenance Windows	
Maximum number of maintenance commands that can be run at the same time	10
Maximum number of maintenance commands that can be executed at the same time in Web Maintenance	10
OTM Web	
Maximum number of clients that can log on to the Administration page of the same OTM server at the same time	5
OTM Web	
Maximum number of clients that can log on to the web EndUser page of the same OTM server at the same time	20
Maximum number of sessions that can be controlled by OTM web server	1000
Maximum number of telephones that can be assigned to an end user	200
Data Buffering and Access (DBA)	
Maximum number of Meridian 1 or Succession CSE 1000 systems	256
Corporate database	
Maximum number of organizational levels	20
Virtual Terminals	
Maximum number of Virtual Terminals that can be enabled at one time	256
Call Detail Recording (CDR)	
Maximum number of call records per costing configuration in TBS	2,500,000
Maximum number of call records for CCCR	5,000,000
Alarm Management	
Maximum number of traps in the circular queue	1360 (see Note)

Rate of alarm production

A single system 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 system without losing alarm information.

Starting with Release 25 of Meridian 1 system software and in all releases of Succession software, there is the capability of filtering traps, on the PBX, based upon their categorization (for example, minor, major, critical, and so on). This can greatly reduce the alarm rate by permitting only major and critical alarms to be sent to OTM.

Filtering increases the number of systems that can be connected. However, when a single system begins having a problem, it begins 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

OTM Web interface

Usage of 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 places 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.

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 percent causing a performance degradation to other applications.

Web Station

Web Station Write capability requires more OTM Server resources than earlier versions of OTM without this capability. For example, a station change performed through the Web interface takes 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 only 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.

Performance of 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 percent, Add/Move/Change activity through the Web interface consumes up to 36.0 percent of CPU usage compared to only 23.8 percent if performed using the Windows interface.

Web Desktop Services for end users

When you configure the write capability for end users in Web Desktop Services, you place a 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 percent (approximately 27 telephones), enabling the write capability for end users in Web Desktop Services increases CPU usage for Add/Move/Change activity from 23.8 percent to 29.8 percent.

Note that the ability for end users to make changes may decrease the need for the network administrator to make changes; therefore, the impact of configuring the write capability for end users in Web Desktop Services may not be significant in certain configurations.

Web support on Server and Workstation platforms

Table A-2 outlines the differences observed in Web support when OTM is running on server grade platforms and workstation platforms.

Table A-2 Web support on servers and workstations

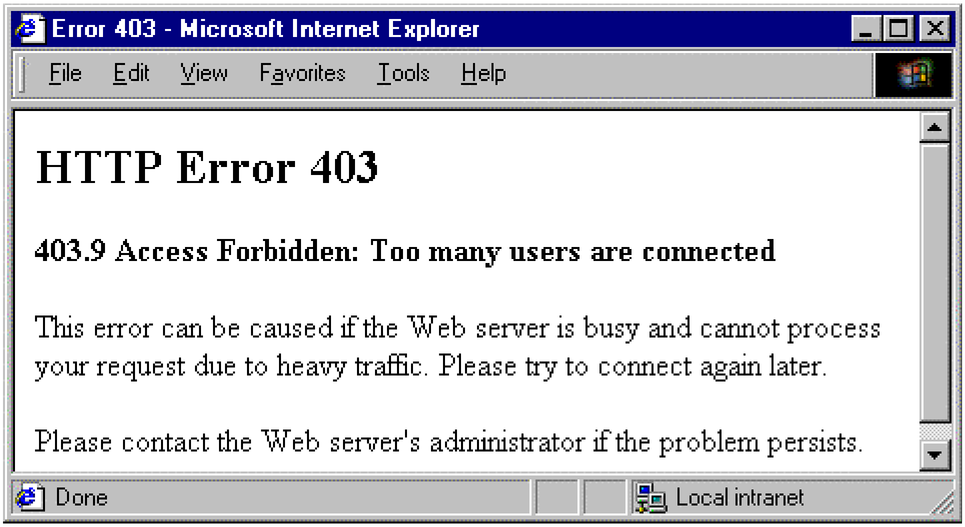
	IIS on Windows NT Server or Windows 2000 Server	**PWS on Windows NT Workstation or Windows 2000 Professional**
Concurrent Internet Explorer sessions	Only limited by OTM capacity	5
Concurrent Netscape Navigator sessions	Only limited by OTM capacity	2
Restricted Access by IP address and domain name	Yes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

Personal Web Server (PWS) is only intended to provide low-volume Web publishing capability. Performance degrades with increased traffic and complex Web pages or Java applications.

The number of sessions supported by PWS is 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, an error message appears (Figure A-1).

Figure A-1 Too-many-users-are-connected error message



HTTP Error 403

403.9 Access Forbidden: Too many users are connected

This error can be caused if the Web server is busy and cannot process your request due to heavy traffic. Please try to connect again later.

Please contact the Web server's administrator if the problem persists.

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 with 256 MB of memory and ATAPI hard disk interface
- A Meridian 1 Option 61C CP PII \Meridian 1 Option 81C CP PII, assumes that 1% of a total of 1000 lines are changed on a daily basis by the network administrator

  For an Meridian 1 Option 11C Cabinet or Succession 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-3 lists those OTM applications that have a significant impact on the performance of the OTM Server PC. The table lists CPU utilization and elapsed time statistics, as appropriate, when connected to a single system.

Table A-3 PC performance by application

	Real Time (CPU)		
Application	**Peak**	**Average**	**Elapsed Time**
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 capability 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. This server's resources are impacted by 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.

PC hardware

This section describes the PC hardware requirements necessary to run OTM optimally. Use the guidelines provided in the sections "Physical memory" on page A-344, "Hard disk" on page A-345, and "Processor speed" on page A-346:

See Chapter , "Preparing for installation for "OTM hardware requirements" on page 27

- 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 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 or SCSI interface, or both
  - Using a faster CPU
- Scale your PC for future growth, and utilize a PC that:
  - Has a reserve PCI Card slot for a SCSI Interface Card (See "Hard disk" on page A-345 for details.)
  - Has a spare storage bay and power for adding an internal hard disk
  - Can accommodate increasing the memory capacity to 1GB or greater (Most PCs have 2 to 4 memory card slots that can accommodate DIMMS of various capacity.)

Response-time testing is based upon the recommended configuration, not the minimum configuration. Response-time performance is only supported on the recommended configuration.

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.
- Accessing the disk while memory swapping steals disk resources away from applications that need to read and write to the hard disk.

The OTM Server software and the Windows NT Server software require ~150 MB without active features. The minimum server memory is 256 MB.

The amount of memory does not grow significantly as features are running and windows are opened.

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

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 significant 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 Update of Station Data

  Station Update from a single system is not affected by disk performance, as the speed of transmission from the system is slower than the PC accessing its disk.
- Web/OTM Client Station Access

“Physical memory” (page A-344) recommends a hard disk using the ATAPI interface. It also recommends a single hard disk.

To improve performance you can:

- Use the fastest Ultra-Wide SCSI Interface (15K RPM).

Disk Performance increases 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 percent or better.

SCSI disk drives come in various speeds.

- Add 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.

Disk size

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

You must 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 creates a 700 MB file.

Station~ =500 kb per 100 telephones. From the example in Tables A-7 and A-6: Disk space = 500 kb/100 telephones*10,000 lines = 50 MB of disk space.

Directory~= 80 kb per 100 records. From the example in Tables A-7 and A-6: Disk space = 80 KB/100 telephones * 10,000 lines = 8 MB of disk space.

Processor speed

The 600 MHZ CPU recommended is sufficient for the maximum configurations presented here.

An increase in 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 percent increase in OTM capacity.

Replacement of the motherboard, not just the CPU chip, can further increase CPU performance, since the newer motherboard is designed to take advantage of the high processor speeds (for example, faster CPU bus, faster memory, and so on). The PC is still heavily bound to disk access and network speeds.

Network bandwidth

Typical configurations

Figure 167 shows how OTM connects to Meridian Mail and to older 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 15.24 meters (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 user can connect to OTM using a remote access software package (for example, pcANYWHERE*).

Figure 167 Connecting OTM to legacy Meridian 1 systems (pre-Ethernet)

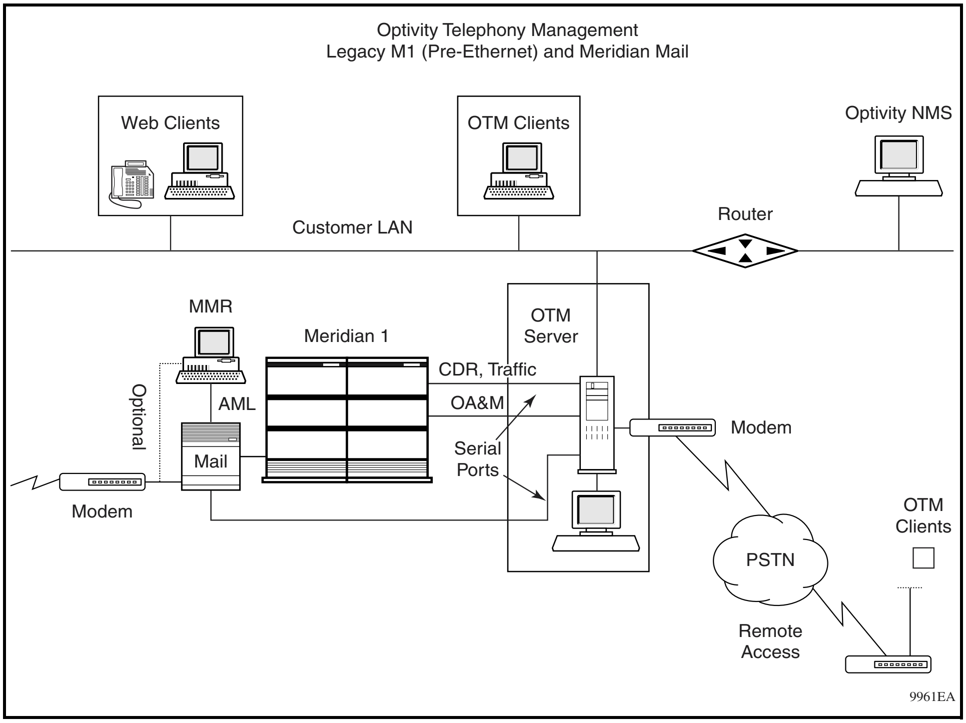
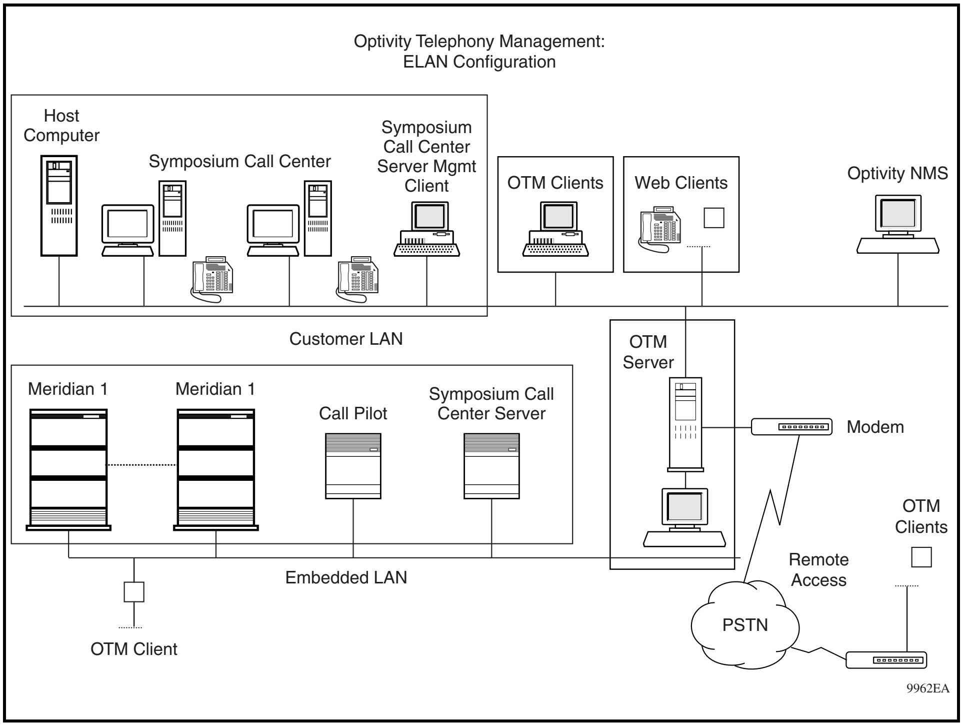


Figure A-1 represents how OTM connects to Meridian Applications and to systems that are packaged with Ethernet. In this picture, OTM is connected to these systems via Ethernet using the Meridian 1 or Succession CSE 1000 system's embedded LAN (ELAN). Meridian 1 and Succession CSE 1000 systems require that the ELAN be protected from the customer's LAN. Therefore, if OTM is to be connected to the customer's LAN (CLAN), 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-1 Connecting OTM to ELAN connected Meridian 1 and Succession CSE 1000 Systems

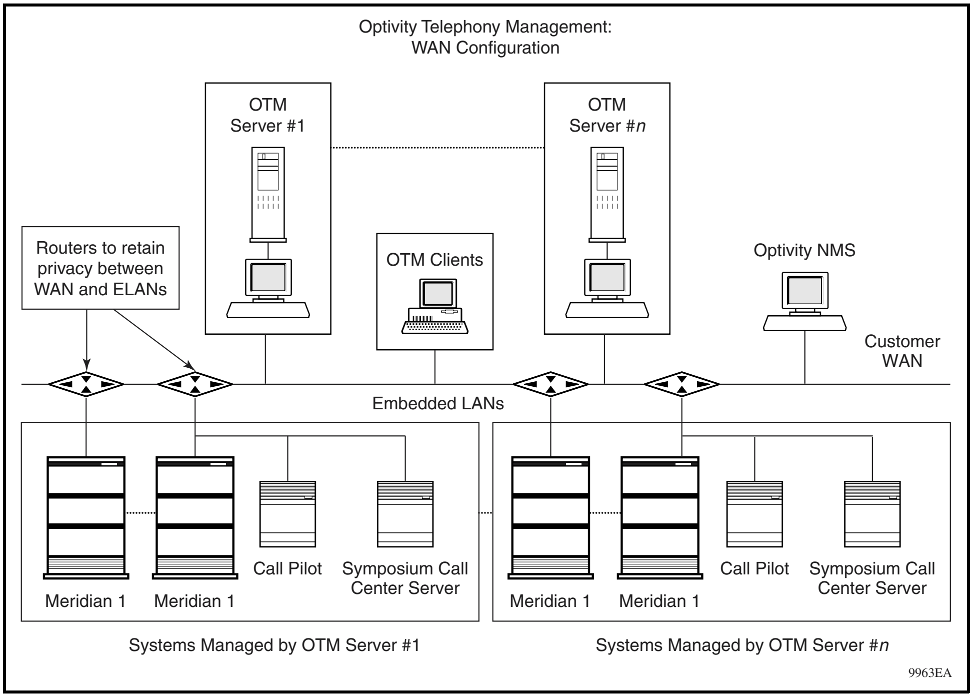


This configuration provides optimum performance, as all communications between OTM and the Meridian 1 or Succession CSE 1000 systems are private. In this case, there is no impact to this communication due to Customer LAN traffic. It also meets the requirement of protecting the ELAN from the CLAN as required for Meridian 1 and Succession CSE 1000 systems by having OTM act as a router.

Physical limitations on 10 Mbps Ethernet connections limit the ELAN distance to 500 meters (1640 feet) using a maximum of four hubs/repeaters. The maximum distance from end-device to hub and hub-to-hub is 100 meters (328 feet). Creation of a separate embedded WAN (EWAN), which connects ELAN segments utilizing switches or routers, or both, 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 or buildings, or both), can make the EWAN option less practical.

Figure A-2 pictures OTM connected directly to the customer WAN (CWAN). Connection of 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 (for example, 100 Mbps, 1 Gbps, and so on). The disadvantage is that available bandwidth must be shared with Customer traffic.

Figure A-2 Connecting OTM to CWAN connected Meridian systems


Optivity Telephony Management:
WAN Configuration
OTM
Server #1
OTM
Server #*n*
Routers to retain privacy between WAN and ELANs
OTM Clients
Optivity NMS
Customer WAN
Embedded LANs
Meridian 1
Meridian 1
Call Pilot
Symposium Call Center Server
Meridian 1
Meridian 1
Call Pilot
Symposium Call Center Server
Systems Managed by OTM Server #1
Systems Managed by OTM Server #*n*
9963EA

Bandwidth utilization

The trade-off is the cost of OTM versus the cost of increased network bandwidth or network subnets. Once OTM Servers are attached to the WAN, the customer’s network may be impacted, but there is a saving on the number of OTMs needed.

Never expect to fully utilize Ethernet bandwidth. Performance degrades quickly as the utilization exceeds a certain threshold (approximately 35 percent). Consult the network administrator for details on network bandwidth utilization.

Table A-4 lists the average and peak traffic for the ELAN and CLAN. This is based upon traffic analysis of a system running on a CP4 CPU. For an Succession 1000M Cabinet and Meridian 1 Option 11C Cabinet system, divide the ELAN numbers by 2, except for alarms. For the CPP CPU, multiply the ELAN numbers by 4, except for alarms.

Table A-4 Network bandwidth usage per Meridian 1 system

	Transfer rate (bits/second)	
OTM Activity	**Average**	**Peak**
Station Add/Chg/Del, ELAN	32 kb	32 kb
Station Sync with M1, ELAN	NA	48 kb
CDR, ELAN	35 kb	70 kb
Traffic, ELAN	24 kb	48 kb
Alarm, ELAN	1 kb	3 kb
Sync with LDAP Server, CLAN	NA	720 kb
Total, ELAN	~92 kb	~201 kb
Total, CLAN		~720 kb

Alarm Processing

There are OTM alarms and ITG/Switch alarms.

OTM alarm details

The OTM Trap Server can handle 25–50 incoming SNMP traps per second. However, this limitation varies considerably with network load, PC processing power, and CPU availability.

Traps are stored in a circular queue of 1360 traps. You can view the queue using the Web Alarm Browser. If the rate of trap arrival is heavy, some traps are not entered into the queue even though they are received by the Trap Server and Alarm Notification application. The circular queue can handle an incoming rate of 50 traps in 10 seconds without any loss of information.

An SNMP trap has an average size of approximately 400 bytes. You can use this information to approximate the bandwidth requirements for trap processing. For example, 1000 devices, each producing one trap every 10 seconds, would require a bandwidth of 320 Kbps:

400 bytes/trap * 8 bits/byte * 1000 devices * 0.1 trap/sec/device = 320 Kbps

ITG/Switch alarm details

Under normal conditions, a Meridian 1 system generates one trap approximately every ten seconds. Beginning with X11 Release 25, you can use filtering on the Meridian 1 to reduce the output of traps. However, there is no filtering capability on ITG. ITG does not generate traps under normal operating conditions. In an abnormal situation, ITG could be expected to generate an alarm every 5 seconds.

ITG may generate a large number of alarms when Quality of Service (QoS) monitoring is enabled. When QoS monitoring is enabled, an alarm is raised or cleared for every QoS threshold crossing (excellent, good, or fair) per codec. A network with varying QoS will have many threshold crossings resulting in a large number of alarms.

Recommended usage

For bandwidth and processing reasons, alarm traffic should be minimized. If alarms from the switch are sent to OTM, use filtering to limit the traffic to only important alarms. Since it is unlikely that multiple ITG cards will simultaneously exhibit problems, the alarms generated by ITG cards should not create traffic problems. To limit alarm traffic, Nortel Networks recommends that you not enable Network QoS Monitoring. Changes to ITG to allow filtering will help this situation. The incoming rate of alarms must match the handling capabilities of the OTM configuration.

The alarm circular queue can be quickly exhausted if there is significant alarm traffic.

ITG operational measurement processing

ITG cards collect operational measurement (OM) information on an hourly basis. This data is stored on the cards until it is retrieved by OTM using an FTP operation. The data can be retrieved on demand, however, the FTP operation is normally scheduled to occur on a daily basis. The data file generated by an ITG card in a 24-hour period is approximately 5 KB.

When retrieval occurs, the information is collected from all cards on all nodes. There is no capability to retrieve the information on an individual node basis.

The retrieved information is parsed and written to comma separated values (CSV) files on the OTM Server. The number of files created is dependent upon the number of records retrieved.

If there are many cards in the system, the retrieval operation should be scheduled to occur during off-hours.

OTM System Performance

Network impact on OTM Windows Client/Server

Network performance has a significant impact on OTM Windows Client/Server applications.

Figure A-1 shows the relationship between Station Administration response time and RTT (Round Trip Time) in a lab environment. Customers may experience different response times depending on their network performance.

Figure A-1
Station Administration Response Time versus Round Trip Time

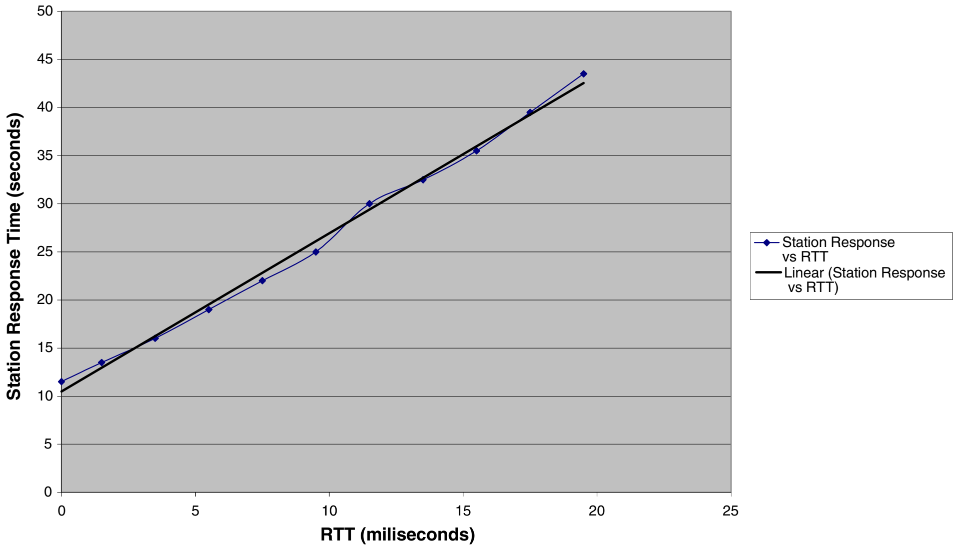
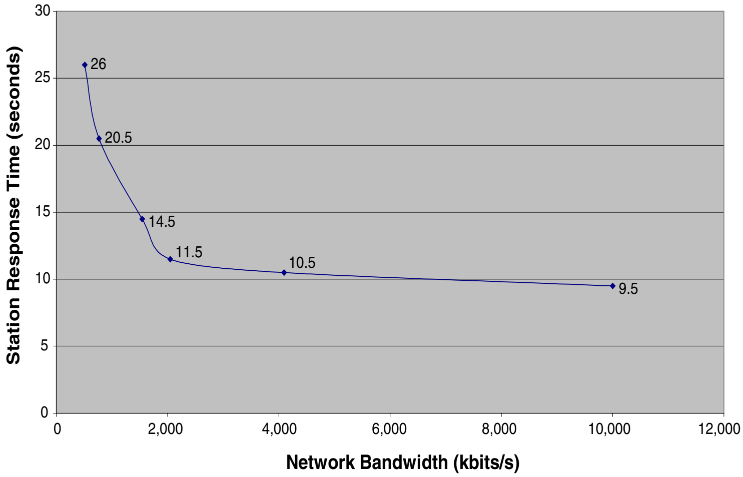


Figure A-2 shows the relationship between Station Administration response time and Bandwidth in a lab environment. Customers may experience different response times depending on their network performance. Note the negative exponential impact of using bandwidth that is less than 2 Mbps.

Figure A-2
Station Administration Response Time versus Network Bandwidth



Hostname resolution

LMHOSTS file

When Microsoft TCP/IP is used on a local network with any combination of computers running Windows 98, Windows NT, Windows 2000, and so on, server names are automatically matched to their corresponding IP addresses. However, to match server names across remote networks connected by routers (or gateways), the LMHOSTS file can be used if WINS servers are not available on the network. Figure A-3 and Figure A-4 show an example of an LMHOSTS file.

The LMHOSTS file is commonly used to locate remote computers for Microsoft networking file, printer, and remote access services, and for domain services such as logon, browsing, replication, and so on.

Microsoft TCP/IP loads the LMHOSTS file into memory when the computer is started. The LMHOSTS file is a text file in the Windows directory that lists the IP addresses and computer names of remote Windows networking servers that you want to communicate with. The LMHOSTS file should list all the names and IP addresses of the servers you regularly access.

For example, the LMHOSTS table file entry for a computer with an address of 192.53.63.2 and a NetBIOS computer name of Building1 would be:

192.53.63.2 Building1

To create an LMHOSTS file:

1 Use a text editor to create a file named LMHOSTS.

Or

Edit the default file named LMHOSTS.SAM.

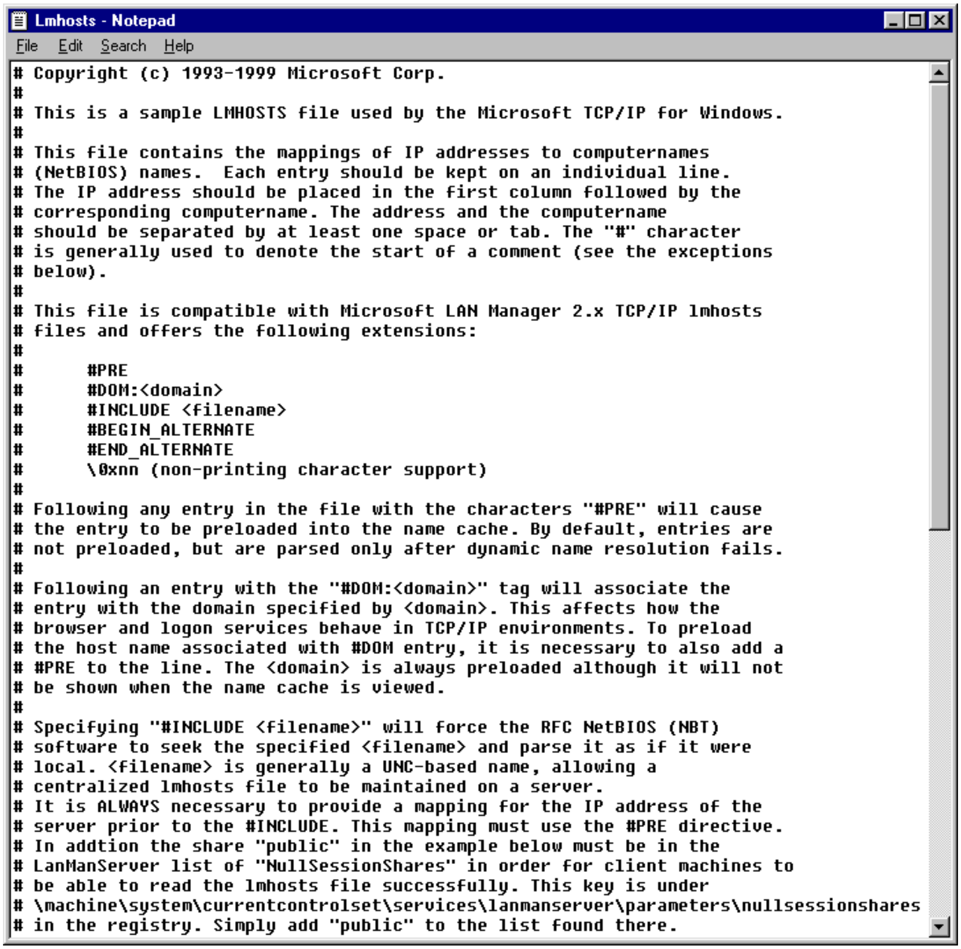
> This file is located in the ***<system root>***\system 32\drivers\etc directory for Windows NT and Windows 2000 systems and in the C:\Windows directory for Windows 98 systems.

2 In the LMHOSTS file, type the IP address and the host name of each computer that you want to communicate with.

For example, on each OTM Client machine add the OTM Server name and its IP address. Separate the items with at least one space.

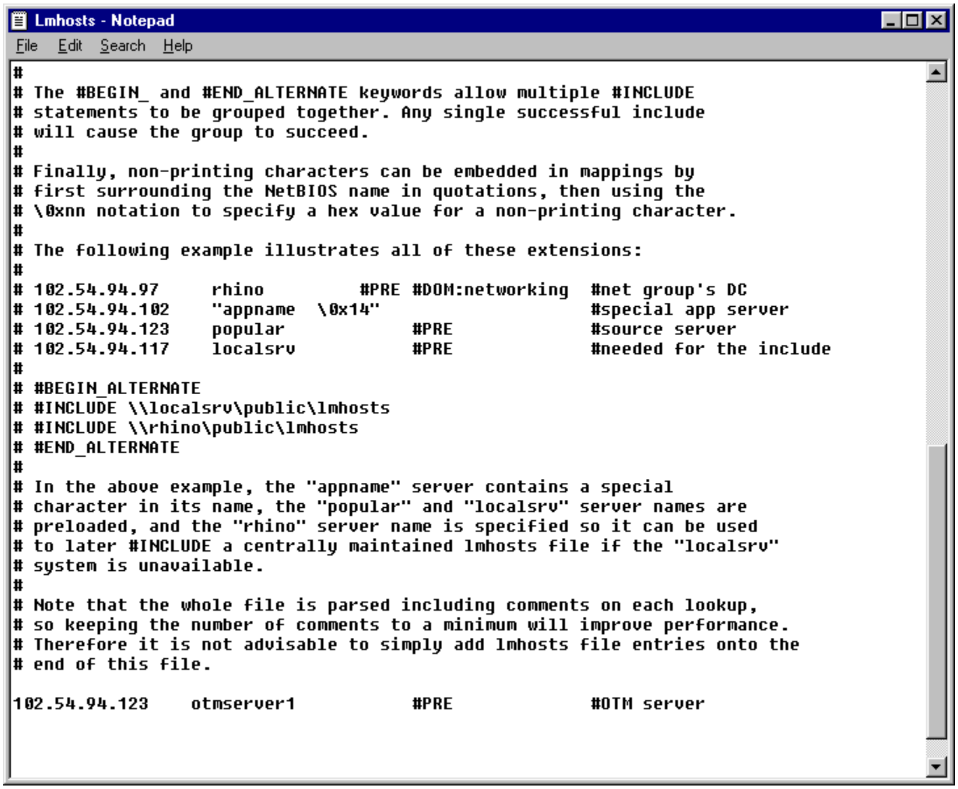
Note that entries in the LMHOSTS file are not case-sensitive.

Figure A-3
Example of LMHOSTS file (part 1)



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to computernames
# (NetBIOS) names.  Each entry should be kept on an individual line.
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
#      #PRE
#      #DOM:<domain>
#      #INCLUDE <filename>
#      #BEGIN_ALTERNATE
#      #END_ALTERNATE
#      \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
# In addtion the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
# \machine\system\currentcontrolset\services\lanmanserver\parameters\nullsessionshares
# in the registry. Simply add "public" to the list found there.
```

Figure A-4
Example of LMHOSTS file (part2)



```
#
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE
# statements to be grouped together. Any single successful include
# will cause the group to succeed.
#
# Finally, non-printing characters can be embedded in mappings by
# first surrounding the NetBIOS name in quotations, then using the
# \0xnn notation to specify a hex value for a non-printing character.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97     rhino         #PRE #DOM:networking  #net group's DC
# 102.54.94.102    "appname  \0x14"                    #special app server
# 102.54.94.123    popular            #PRE             #source server
# 102.54.94.117    localsrv           #PRE             #needed for the include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
# character in its name, the "popular" and "localsrv" server names are
# preloaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
# end of this file.

102.54.94.123    otmserver1           #PRE             #OTM server
```

3 Save the file as LMHOSTS.

Note that the filename is LMHOSTS with no extension.

LMHOSTS is normally used for smaller networks, or to find hosts on remote networks that are not part of the WINS database (because name query requests are not broadcast beyond the local subnetwork). If WINS servers are in place on an internetwork, users do not have to rely on broadcast queries for name resolution, because WINS is the preferred method for name resolution. Therefore, with WINS servers in place, LMHOSTS may not be necessary.

The LMHOSTS file is read when WINS or broadcast name resolution fails. Resolved entries are stored in a system cache for later access. When the computer uses the replicator service, and does not use WINS, LMHOSTS entries are required on import and export servers for any computers on different subnetworks participating in the replication.

To configure TCP/IP to use LMHOSTS on a Windows 2000 PC:

1. Open Network and Dial-up Connections.
2. Right click the network connection you want to configure, and then click Properties**.**
3. On the General tab (for local area connection) or the Networking tab (all other connection), click Internet Protocol (TCP/IP), and then click Properties. Click Advanced, click the WINS tab. Select the Enable LMHOSTS lookup check box. This option is enabled default.
4. To specify the location of the file that you want to import into the LMHOSTS file, click Import LMHOSTS, and then select the file in the Open dialog box.
5. To complete the configuration, either:

   a. Reboot the computer

      Or

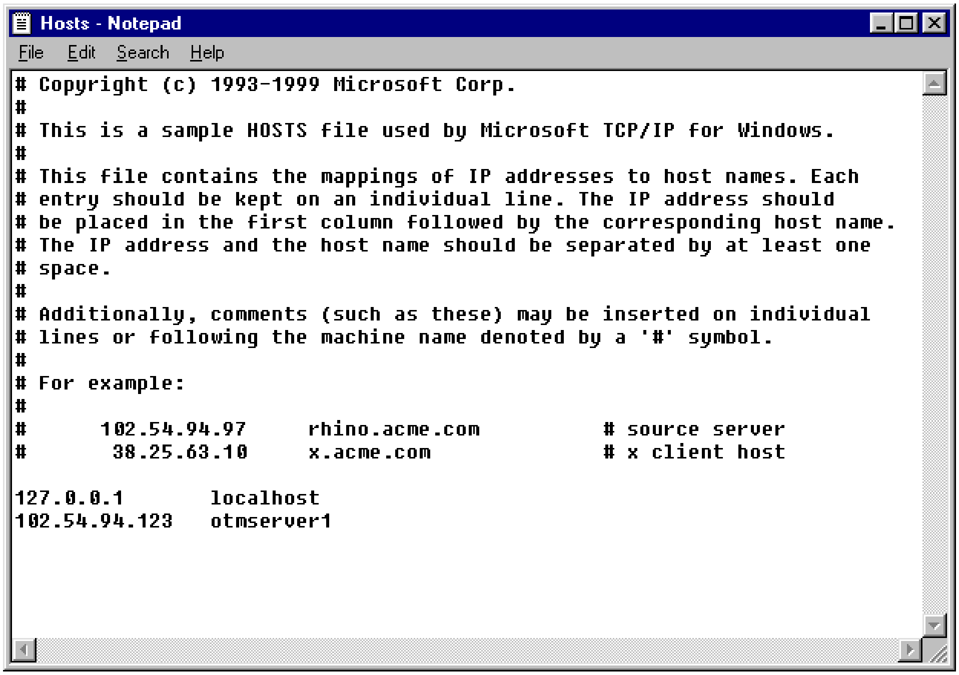
   b. Go to the command prompt, and enter the following text:

      ```
      nbstat -R
      nbstat -c
      ```

HOSTS file

The HOSTS file contains a list of host name to IP address mappings. It is a regular text file. The HOSTS file is located in the ***<system root>***\system 32\drivers\etc directory for Windows NT and Windows 2000 systems. For Windows 98 systems, the HOSTS file is located in the C:\Windows directory.

Figure A-5
Sample HOSTS file



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
102.54.94.123   otmserver1
```

Use a text editor to edit the HOSTS file. In the HOSTS file, type the IP address and the host name of each computer that you want to communicate with, for example, on each OTM client computer add the OTM Server IP address followed by its name. Separate the items with at least one space. Entries in the HOSTS file are not case-sensitive. Note that the HOSTS filename has no extension.

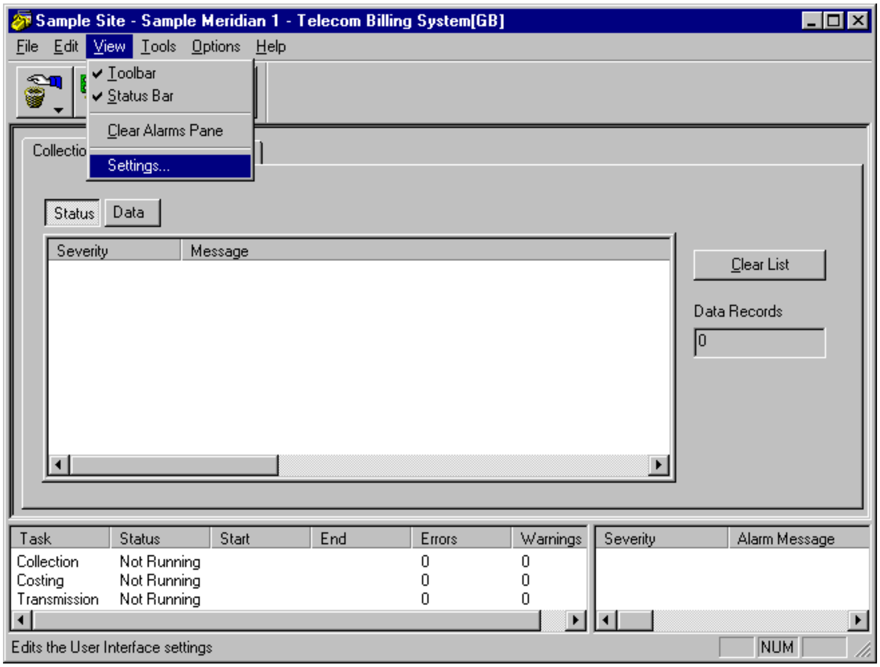
Telecom Billing System Display option

The Telecom Billing System (TBS) Display option for collecting, costing, and transmitting call records negatively impacts system performance by consuming system resources.

To improve system performance, disable the Display option:

1 In the Telecom Billing System application, select View > Settings (Figure A-6).

Figure A-6
Telecom Billing System

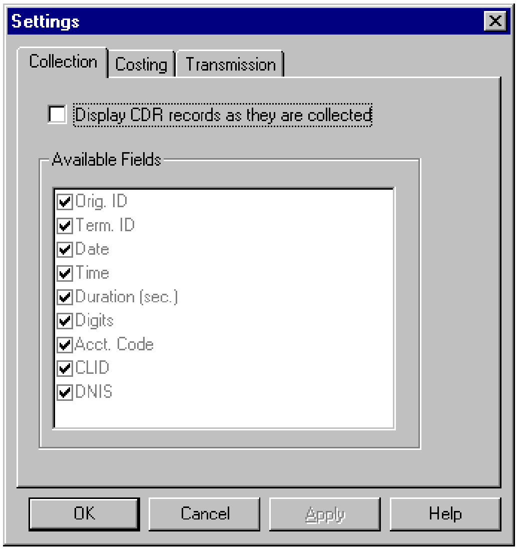


Task	Status	Start	End	Errors	Warnings
Collection	Not Running			0	0
Costing	Not Running			0	0
Transmission	Not Running			0	0

Edits the User Interface settings

The Settings dialog box opens with the Collection tab selected (Figure A-7).

Figure A-7
Settings dialog box—Collection tab



□ Display CDR records as they are collected

Available Fields

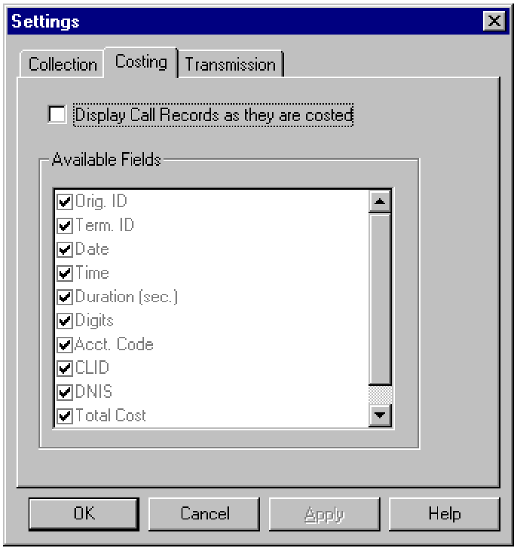
☑ Orig. ID
☑ Term. ID
☑ Date
☑ Time
☑ Duration (sec.)
☑ Digits
☑ Acct. Code
☑ CLID
☑ DNIS

2 Ensure that the Display CDR records as they are collected check box is unchecked.

3 Click the Costing tab.

The Settings dialog box—Costing tab appears (Figure A-8).

Figure A-8
Settings dialog box—Costing tab



□ Display Call Records as they are costed

Available Fields

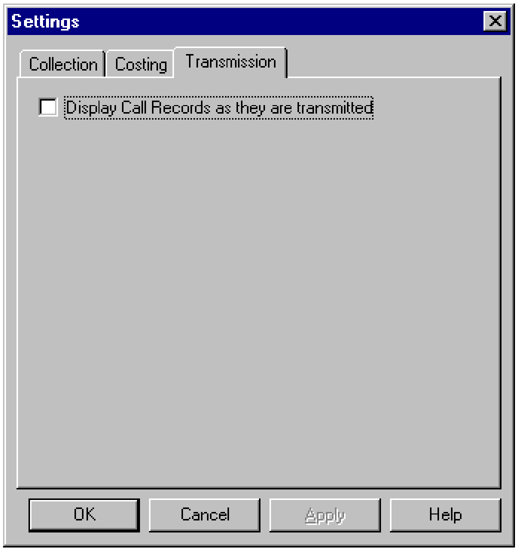
☑ Orig. ID
☑ Term. ID
☑ Date
☑ Time
☑ Duration (sec.)
☑ Digits
☑ Acct. Code
☑ CLID
☑ DNIS
☑ Total Cost

4 Ensure that the Display Call Records as they are costed check box is unchecked.

5 Click the Transmission tab.

The Settings dialog box—Transmission tab appears (Figure A-9).

Figure A-9
Settings dialog box—Transmission tab



□ Display Call Records as they are transmitted

6 Ensure that the Display Call Records as they are transmitted check box is unchecked.

7 Click OK.

OTM port usage

When using OTM to monitor and maintain systems, various ports and protocols are used to communicate between OTM and the desired client, server, or application. Table A-5 lists typical port usage based on the flow of information between OTM and these system components.

Table A-5 OTM port usage

OTM Sending To:	**Port**	**Type**	**Protocol**	**Component**
Meridian 1 or Succession CSE 1000 system	513	TCP	Rlogin	Session Connect, System Terminal, Station Admin, CPND, List manager, ESN
Meridian 1 or Succession CSE 1000 system	161	UDP	SNMP	Alarm Management, Maintenance Window
Meridian 1 or Succession CSE 1000 system	21	TCP	FTP	Corporate Directory Upload
Meridian 1 or Succession CSE 1000 system	20	TCP	FTP	Corporate Directory Upload
Meridian 1 or Succession CSE 1000 system	1929	UDP		DBA **Note:** DBA uses 1 port per session, starting with port 1929.
SMTP server	25	TCP	SMTP	Alarm Notification
ITG	21	TCP	FTP	OTM ITG
WinClient	139	TCP	NetBEUI	Windows Client File Sharing
LDAP Server	389	TCP	LDAP	LDAP Synchronization
LDAP Server over SSL	636	TCP		LDAP Synchronization
OTM Receiving From:	**Port**	**Type**	**Protocol**	**Component**
Web Client	80	TCP	HTTP	Web CS, Desktop Services, Web Telecom Billing System
Web Client	4789–5045	TCP		Virtual System Terminal **Note:** VT uses 1 port per session, starting with port 4789.
Win Client	139	TCP	NetBEUI	Windows Client File Sharing
Win Client	3351	TCP	Btrieve	Station Administration **Note:** Station Administration uses 1 port per session, starting with port 3351.
Meridian 1 or Succession CSE 1000 Sending To:	**Port**	**Type**	**Protocol**	**Component**
OTM	162	UDP	SNMP	Alarm Traps (LD 117), Maintenance Window

Table A-5 OTM port usage

OTM Sending To:	Port	Type	Protocol	Component
OTM	1929	UDP		DBA **Note:** DBA uses 1 port per session, starting with port 1929.
DECT	5099	TCP	RMI	OTMDECT
Station	1583	TCP	Btrieve	Station Administration

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 system 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, Alarm Management, MDECT configuration, and other applications

Example 2

Configuration and Alarm Management with Web/OTM Client Access and LDAP Service and Web Station Write configured for end users (full OTM system)

Example 3

Alarm 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 system configurations used for this example:

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

  Refer to Figure A-1 on page A-349.
- 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 operations. For example, Maintenance windows and ITG configuration.
  Routine operations as defined in Table A-3 on page A-343 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 a.m. to 5:00 p.m. every day). The default value is the peak six hours of the day (9:00 a.m. to 12:00 p.m. and 1:00 p.m. to 4:00 p.m.). Daily activities are based on the following assumptions:
  - — Percentage of lines changed by the network administrator per day is 1 percent. For example, a system with 2000 lines has 20 lines changes by the network administrator during a normal work day.
  - — Number of lines changed by end users through Web Desktop Services is 0.25 percent. For example, a system with 2000 lines has approximately 5 lines changed by end users during a normal work day provided that the Web Desktop Services Write feature is configured.
- Off-hours operations can use 100 percent of the CPU, and are limited as follows (from Table A-3):
  - — Station retrieve/reconcile is performed once a week, or twice a month, on the weekend. The maximum period of time reserved for this activity is theoretically 48 hours. For these examples, reserve the time from 9:00 p.m. on Sunday to 6:00 a.m. on Monday, or 9 hours.
  - — Station transmit will be scheduled and performed during the peak 6 hours (for example, from 9:00 a.m. to 12:00 p.m. and 1:00 p.m. to 4:00 p.m.).
  - — Assume, for a Succession 1000M Cabinet and Meridian 1 Option 11C Cabinet, that OTM can run Station update for two devices simultaneously (based upon processor speed and CPU usage figures).
  - — CDR Reports are performed once a day. For these examples, off-hours are from 12:00 a.m. (midnight) to 6:00 a.m., or 6 hours.
  - — LDAP Sync is performed once a week, on the weekend.
    For these examples, reserve the time from 9:00 p.m. Sunday to 6:00 a.m. on Monday, or 9 hours.

Table A-6 and Table A-7 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-6 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	

Table A-7 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.

Configuration calculations

Example: 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% CPU utilization
  - — If administration is done primarily through the OTM Web interface:

    Adds/Moves/Changes = approximately 36% CPU utilization
- 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 = 80 kb/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

Example: 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% CPU utilization
  - If administration is done primarily through the OTM Web interface:

    Adds/Moves/Changes = approximately 36% CPU utilization
- 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

The average alarms and MDECT usage are so small that their impact on routine, off-hour, and network bandwidth is negligible.

Example: 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% CPU utilization

    If Web Desktop Services Write for End Users is configured, then Adds/Moves/Changes = approximately 17.88% CPU utilization
  - 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% CPU utilization

    If Web Desktop Services Write for End Users is configured, then Adds/Moves/Changes = approximately 25.2% CPU utilization
  - 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 = 80 kb/second
  - LDAP Sync operation = 720 kb/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

Example: Succession 1000M Cabinet and Meridian 1 Option 11C Cabinet = 26 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% CPU utilization

    If Web Desktop Services Write for End Users is configured, then Adds/Moves/Changes = approximately 29.8% CPU utilization
  - 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% CPU utilization

    If Web Desktop Services Write for End Users is configured, then Adds/Moves/Changes = approximately 42.0% CPU utilization
  - 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 systems
- Network bandwidth:
  - Station (peak) operations = 40 kb/second
  - LDAP Sync operation = 720 kb/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: 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% CPU utilization
  - If administration is done primarily through the OTM Web interface:

    Adds/Moves/Changes = approximately 14.67% CPU utilization
- 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
  - 21,600 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 = 118 kb/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

Example: 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% CPU utilization
  - If administration is done primarily through the OTM Web interface:

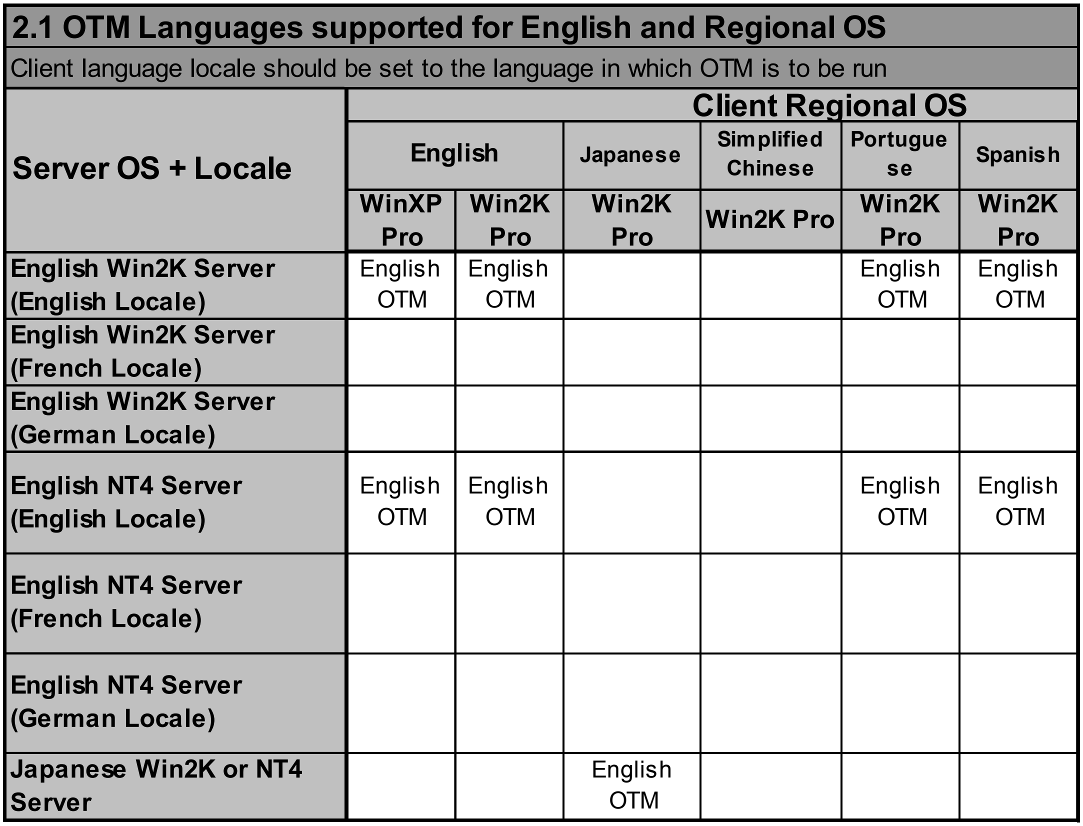
    Adds/Moves/Changes = approximately 8.67% CPU utilization
- Off-hours operation:

- 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

OTM Language Support

OTM supports the following language configurations:



2.1 OTM Languages supported for English and Regional OS

Client language locale should be set to the language in which OTM is to be run

Server OS + Locale	Client Regional OS					
	English		Japanese	Simplified Chinese	Portuguese	Spanish
	WinXP Pro	Win2K Pro	Win2K Pro	Win2K Pro	Win2K Pro	Win2K Pro
English Win2K Server (English Locale)	English OTM	English OTM			English OTM	English OTM
English Win2K Server (French Locale)						
English Win2K Server (German Locale)						
English NT4 Server (English Locale)	English OTM	English OTM			English OTM	English OTM
English NT4 Server (French Locale)						
English NT4 Server (German Locale)						
Japanese Win2K or NT4 Server			English OTM			

Appendix B: 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

Ethernet connections:

[ ] X11 Release 22 or later

[ ] Release 24B or later 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

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

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

Stand-alone mode consists of a single web-based Client and no Windows Clients.

[ ] Intel Pentium III Processor 400 MHz (600 MHz for XP)

[ ] 2 GB (1 GB plus customer data storage)

[ ] 256 MB of RAM minimum; 512 MB of RAM recommended

[ ] Ethernet Network Interface Card

[ ] Windows XP Professional (Service Pack 1), Windows 2000 Server (Service Pack 3), Windows 2000 Professional (Service Pack 3) or Windows NT Server

[ ] OTM dongle/USB dongle

[ ] Printer port (LPT)/USB Port required for dongle

[ ] OTM CD and keycode

[ ] Remote Access Service (RAS)

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

If multiple web Clients are connected to the stand-alone system, the requirements are equivalent to the OTM Server requirements.

OTM Server installation

[ ] Intel Pentium III Processor 600 MHz

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

[ ] 256 MB of RAM minimum; 512 MB of RAM recommended

[ ] Two Ethernet Network Interface Cards

[ ] PC COM port with 16550 UART

[ ] Hayes compatible modem (optional)

[ ] Windows NT Server 4.0 (Service Pack 6a); or Windows 2000 Server (Service Pack 3)

[ ] Windows NT Option Pack 4

[ ] Remote Access Service (RAS)

[ ] OTM dongle/USB dongle

[ ] OTM CD and Keycode

[ ] Configure and test network interfaces

[ ] Enable IP routing (if applicable)

OTM Client installation

[ ] **Windows Client** - 233 MHz Intel Pentium II Processor or equivalent (300 MHz Pentium II required for Telecom Billing System application) minimum; Pentium III 400 MHz (600 MHz for XP) recommended
Web Client - 160 MHz Intel Pentium Processor or equivalent

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

[ ] **Windows Client** - 128 MB of RAM minimum (256 MB of RAM recommended for improved performance and for the Billing Enhanced level applications)
Web Client - 32 MB of RAM

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

[ ] Ethernet Network Interface Card

[ ] Windows XP Professional (Service Pack 1), Windows 2000 (Service Pack 3), or Windows NT Server

[ ] **Windows Client** - Remote Access Service (RAS)

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

[ ] **Web Client** - Java Runtime Environment (JRE) 1.4.2, and Microsoft Internet 6.0 SP 1or Netscape Navigator 4.7

Index