COMPAQ

. . . .

Integrating Compaq Insight Manager with ManageWise

Compaq TechNote

Includes information on:

- Innovative server management solutions for ManageWise

- Preinstallation considerations

- Detailing the integration process

- Performance recommendations

- Using Compaq Insight Management Agent MIBs

. . . .

NOTICE

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication contains information protected by copyright. No part of this publication may be photocopied or reproduced in any form without prior written consent from Compaq Computer Corporation.

The software described in this guide is furnished under a license agreement or non disclosure agreement. The software may be used or copied only in accordance with the terms of the agreement.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state, or local requirements. Compaq does not warrant products other than its own strictly as stated in Compaq product warranties.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Integrating Compaq Insight Manager with ManageWise

Contents

Chapter 3
Compaq Management Technologies

Chapter 4
Preinstallation Considerations

Chapter 5
Integrating Compaq Insight Manager with ManageWise

Figures

Tables

Tables *continued*

Chapter 1
About This TechNote

This TechNote provides Compaq server management integration guidelines for ManageWise. The network and hardware configurations that Compaq selected to test might not be the same as your configuration.

This TechNote also provides:

■ Overview of network management terms, standards, and methods.

■ Discussion of Compaq Insight Manager technologies and how they easily integrate with other management platforms.

■ Summary of the ManageWise architecture and components to help you understand the complete management platform and where each component resides on your network.

■ Discussion of preinstallation considerations providing informational tips along with some prerequisites you need to know about before you start the installation process.

■ Recommendations on performance that can assist you in deciding how to deploy Compaq Insight Manager and ManageWise as well as enhance their performance.

■ Discussion on using Compaq Management Information Bases (MIBs) and how they can be helpful to you.

■ Procedures on installing and integrating Compaq Insight Manager with ManageWise in addition to the technological differences between ManageWise and NetWare Management System (NMS).

■ Detailed examples of innovative server management solutions.

This TechNote is for system integrators and network administrators with a knowledge of Compaq Server products, Compaq Insight Manager, and ManageWise. It is a supplement to the *Compaq Insight Manager User Guide, Compaq Insight Management Agents for NetWare User Guide, Compaq Hardware Reference* documentation, and the *ManageWise 1.0* documentation set available from Novell.

Chapter Organization

This chapter is intended to help you use this TechNote; therefore, each chapter is summarized as follows:

■ *Chapter 1* -- Introduces the TechNote with a brief summary of each chapter, general information about conventions used, and additional resources you can use to find more information on network management and the test environment used.

■ *Chapter 2* -- Provides a network management overview that includes terminology, standards, a discussion of the complexity of network management, methods of managing network resources, and server and desktop management as a subset of network management.

■ *Chapter 3* -- Describes the Compaq management technologies that include Compaq server management technologies, Compaq Desktop PC management technologies, Compaq Insight Manager software, integration with operating system management, and network management interoperability.

■ *Chapter 4* -- Discusses preinstallation considerations such as the minimum hardware and software requirements necessary to properly install ManageWise and Compaq Insight Manager.

■ *Chapter 5* -- Discusses integrating and using Compaq Insight Manager with ManageWise as well as defining the differences between ManageWise and NetWare Management System (NMS).

■ *Chapter 6* -- Provides performance recommendations on performance tuning issues such as implementing configuration modifications to specific files and architectural implementation of management agents.

■ *Chapter 7* -- Provides innovative server management solutions for using Compaq Insight Manager with ManageWise.

■ *Appendix A* -- Provides the organization and key information on Compaq MIBs needed to help you diagnose and solve Compaq server-related problem scenarios.

■ *Appendix B* -- Provides a brief overview on traps generated by Compaq Insight Management Agents to assist you in translating trap variables.

■ *Appendix C* -- Provides information on how to order printed Compaq TechNotes, including pricing information, 1 (800) telephone numbers, and a list of the latest TechNotes available. This information also includes the TechNotes available on the Internet.

■ *Glossary* -- Defines management technologies and other related networking terms.

Notational Conventions

Table 1-1 defines the text conventions used within this TechNote.

<div align="center">

Table 1-1
Notational Conventions

</div>

Convention	Use
Enter	When instructed to enter information, type the information in using your keyboard.
FILENAMES	Names of files appear in uppercase italic in the DOS and other environments.
items of importance	Presents important or specific points of information. These items appear in italics in all chapters of this TechNote.
Key + **Key**	When you see a plus sign between two keys, hold down the first key while you simultaneously press the second key. For example, "Press the **Ctrl** + **Z** keys" means to press the **Ctrl** key while you simultaneously press and release the **Z** key.
Keys	Keys on your keyboard appear in boldface.

continued

Notational Conventions *continued*

Convention	Use
"new terms" and "prompts"	The first occurrence of a technical term, prompts, or references to a word other than a command appears in quotes.
PROGRAMS, COMMANDS, UTILITIES, DIRECTORY NAMES, and DRIVE NAMES	These items appear in uppercase in the DOS and other environments.
Select *item* → *item*	Items separated by arrows indicate items you select in a sequence.
Set, Get	Screen button labels appear in bold initial caps.
screen selections and *variables*	These items appear in italics in all chapters of this TechNote.
user input and screen display	Information you type exactly as it appears on the screen.
USER INPUT	Information you type exactly as it appears is shown in uppercase.
CAUTION	Indicates that failure to follow directions could result in damage to equipment or loss of information.
! IMPORTANT	Presents clarifying or specific points of information.
NOTE:	Presents commentary, sidelines, or interesting points of information.

Additional Resources to Use

Use the following list of resources, which are used throughout this TechNote, for more information on Compaq Insight Manager, ManageWise, or network management technology:

■ Compaq TechNote, *Integrating Compaq Insight Manager with Enterprise Management Platforms*, P/N 145806-003

This TechNote provides Compaq server management integration guidelines for managing Compaq servers with SunNet Manager, HP OpenView, and IBM NetView for AIX.

■ *Compaq Insight Manager User Guide,* P/N 133394-008

This document explains how to install, configure, and use Compaq Insight Manager. There is also a discussion on Compaq Insight Asynchronous Management guidelines, server discovery process, and alarms.

■ *Compaq Insight Management Agents for NetWare User Guide*, P/N 145890-005

This document explains how to install, use, and troubleshoot Compaq Insight Management Agents for NetWare. There is also a discussion on Compaq Insight Asynchronous Management guidelines.

■ *Compaq Hardware Reference* documentation

This documentation can help isolate a problem to a certain computer component or cable segment. Some network problems occur because of malfunctioning hardware; check the documentation that came with the hardware involved.

■ *ManageWise 1.0 NetWare Management System Software: Getting Started,* P/N 100-002434-001

This guide introduces the NetWare Management System (NMS) platform software which provides discussions on operating environment, user interface, database management system, and alarm management system.

■ *ManageWise 1.0 NetWare Management System Software: Managing NetWare Servers*, P/N 100-002436-001

This guide discusses the NetWare server management functions of NMS software that monitor and manage NetWare servers on networks running Internet Packet Exchange (IPX) and Internet Protocol (IP).

■ *ManageWise 1.0 NetWare Management System Software: Analyzing Your Network*, P/N 100-002435-001

This guide describes how to use NMS to manage your network on a segment-by-segment basis.

■ *ManageWise 1.0 NetWare Management System Software: LANDesk Manager Tools,* P/N 100-002421-001

This manual discusses the LANDesk Manager Tools that are included with ManageWise such as Inventory Manager and LANDesk Virus Protect.

■ *ManageWise 1.0: Setup Guide,* P/N 100-002420-001

This manual contains all of the information necessary for installing ManageWise.

■ *ManageWise 1.0 NetExplorer Discovery System,* P/N 100-001927-001

This document describes the components of the NetExplorer system, provides a brief theory of operation, gives some tips for planning a NetExplorer Discovery session, and describes the system requirements for each of the components and their impact on network performance.

■ *The Simple Book - An Introduction to Internet Management.* Marshall T. Rose. Englewood Cliffs, NJ: Prentice-Hall, 1994.

This book explains the technology used to manage large internets, which includes wide and local area networks. It also discusses managing of internets using Simple Network Management Protocol (SNMP) and SNMPv2.

■ *The Basic Reference Model of Open Systems Interconnection (OSI),* ISO 7498 - Part 4.

This document provides a description of the activities necessary for systems to interwork using communication media. Additionally it provides supplemental information on the framework and structure of OSI Management.

■ Internet

This service is available to interact with other users and support engineers or to get product information.

❏ To access the Compaq home page on the Internet: *http:// www.compaq.com*

❏ To access the Novell home page on the Internet: *http://www.novell.com*

❏ To access the Intel home page on the Internet: *http://www.intel.com*

Integration Environment

Compaq tested the ManageWise integration using the following hardware and software configuration:

- Console

    - Compaq Deskpro XL 4/50 with 16 megabytes of memory, 500 megabyte hard disk drive, CD-ROM drive, SVGA monitor, and a mouse

    - Microsoft Windows 3.1

    - Compaq Insight Manager 2.5

    - ManageWise 1.0

- Server

    - Compaq ProLiant 1000 5/60 with 32 megabytes of memory and 1.05 gigabytes of hard disk space

    - NetWare 3.12

    - Compaq Insight Management Agents for NetWare 2.5

    - ManageWise 1.0

Chapter 2
Network Management

This TechNote is intended for network administrators who need to know the critical success factors for integrating the management technologies and tools of Compaq servers and client desktop PCs into a broader network management environment. Compaq servers support Compaq developed, SNMP-based management agents running under network operating systems such as NetWare, Microsoft Windows NT, SCO UNIX, UnixWare, and IBM OS/2 to provide management of the hardware. The new Compaq Deskpro Family supports "Intelligent Manageability." Intelligent Manageability moves many Compaq server management technologies to the desktop. Compaq Desktop Management Solution Partners access these Intelligent Manageability features.

The typical network configuration can include devices such as routers, bridges, gateways, and other SNMP-host computers. Figure 2-1 is an example of such a network.
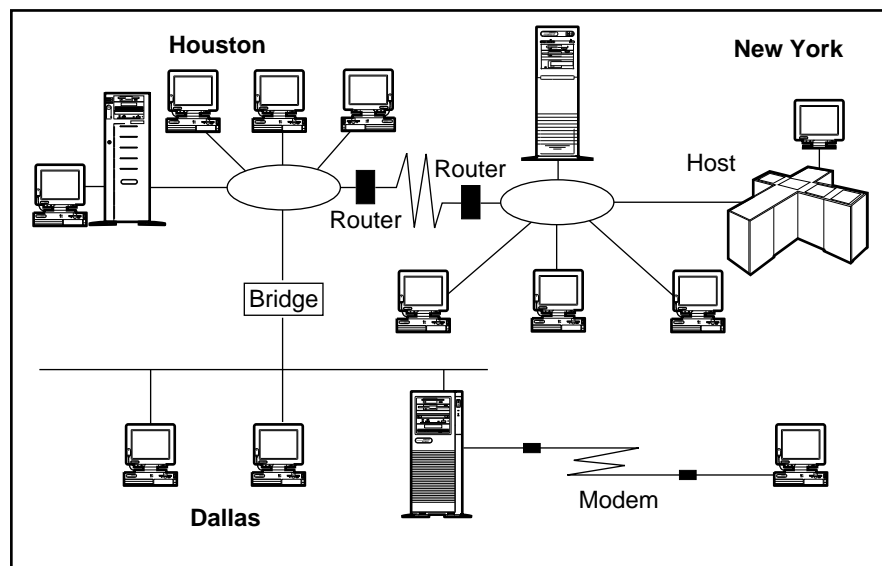
Figure 2-1. Typical network configuration

Managing a multivendor, multioperating system environment, similar to the typical network configuration illustrated in Figure 2-1, is a complex process. However, such networks are not uncommon in many organizations and might resemble your own.

Compaq provides you with tools for managing Compaq servers and desktops. These tools build upon the functionality and features engineered into the servers and desktops. The tools, used in combination with tools specific to your network operating system, can provide you with cost-effective methods to manage your network.

Compaq server management technologies, desktop Intelligent Manageability, and tools adhere to popular network management standards such as:

■   Simple Network Management Protocol (SNMP)

■   Point-to-Point Protocol (PPP)

■   Transmission Control Protocol and Internet Protocol (TCP/IP)

■   Internet Packet Exchange (IPX)

■   Telnet

■   Windows Internet Name Service (WINS)

■   Dynamic Host Configuration Protocol (DHCP)

■   American Network Standards Institute (ANSI) terminal emulation

The Compaq commitment to standards assures you the flexibility and cost-effectiveness of an open, industry-standard solution.

Network Management Terms

Table 2-1 contains a list of network management terms and definitions associated with computing devices, infrastructure devices, and network protocols. In this TechNote, the *first reference* of the network management term is used to introduce a term and the *second reference* is used for the remainder of the document.

Table 2-1
Network Management Terminology

First Reference	Second Reference	Definition of Term
Attribute	Attribute	Characteristics of the object provided to a network administrator (for example fault, performance, and configuration information).
Element Manager	Element Manager	Application that manages a device or a subsystem.
Managed Device	Device	Computing and infrastructure devices that are manageable (for example, servers and routers that run management agents and therefore are manageable).
Managed Object	Object	Component of a device that is manageable (for example, network interface, storage subsystem, operating system, active applications, or hardware configuration).
Management Agent	Agent	Software or firmware installed and running in a managed device that provides attribute information to an element manager.
SNMPv1	SNMP	Industry-standard protocol for the exchange of management data between management applications and management agents.
Subsystem	Subsystem	Major components of a device (for example, disk subsystem, storage subsystem, memory subsystem, and processor subsystem).

Figure 2-2 illustrates the relationship between the network management terminology described in Table 2-1.
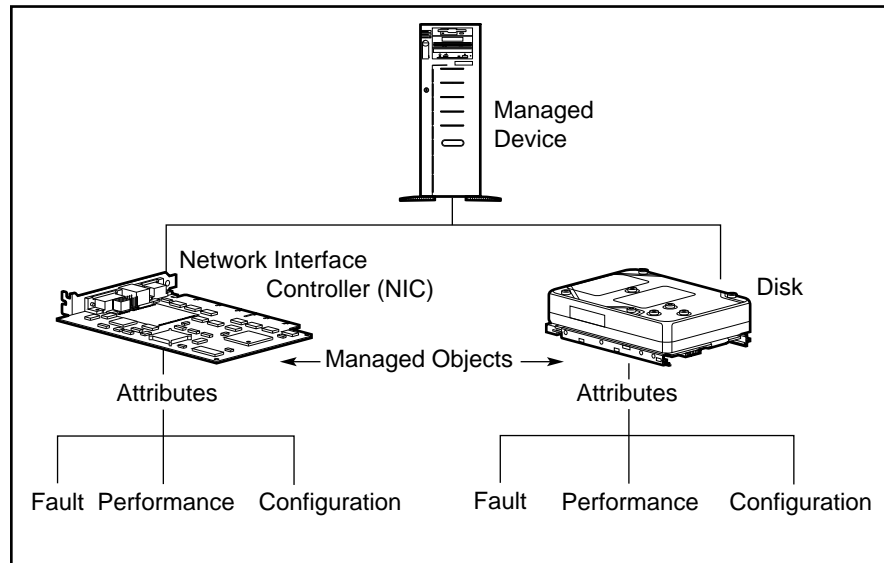
Figure 2-2. Relationship of network management terms

In summary, every managed device:

■ Possesses a set of managed objects that correspond to hardware subsystems and software components.

■ Possesses a number of attributes that describe the objects. The attributes of the managed device are *readable* and might be *writable* by a management application.

■ Sends notification of changes in operating status and information about a failure condition to a management application.

Discussion of Network Management

Network management enables the monitoring, analysis, and control of computing and infrastructure devices, as well as the network protocols.

Managed devices include the following devices:

■   Computing devices -- servers, desktops, workstations, hosts, and mainframes

■   Infrastructure devices -- bridges, routers, gateways, and hubs

Today, management applications allow you to monitor the status of attributes, analyze their condition, and perform a resulting action on a managed device. For example, you might choose to reset a port on a hub when the device attached to that port generates an excessive number of network errors.

A benefit of network management is that it allows you to provide acceptable service levels to your users in the most cost-effective manner. This service, in turn, depends on several issues such as:

■   How critical is uptime to your network?

■   How much do you want to restrict access to the network?

■   What level of performance do you expect to achieve?

■   What does it cost to manage your network effectively?

Network management often requires you to balance several objectives that could be contradictory. For example, two of your requirements might be to reduce costs and reduce downtime. However, the cost of 100-percent uptime is often prohibitive.

The following is a sample of the factors that contribute to the complexity of network management:

■ Networks containing a variety of devices.

■ Varying requirements from one user organization to another; each organization perceives its needs to be unique.

■ Users have a sharply different perception and expectation than network administrators and MIS management within an organization. This problem becomes more complicated because of the growing influence of new technology and the need for businesses to rightsize their computing environments.

■ Lack of easy to use, broad-based solutions.

■ The focus of many management solutions today is to manage a single-network element such as a bridge, a router, or a server. For PC-based networks, some solutions specialize in certain areas of network management such as configuration or performance monitoring. Management solutions that can manage several network devices and support multiple functional areas of network management typically require additional systems integration.

Standards-Based Network Management Model

The International Standards Organization (ISO) has formulated a network management framework because the scope of network management is so broad. This management framework is a document that provides a reference for coordinating development of management standards. *The Basic Reference Model of Open Systems Interconnection (OSI), ISO 7498 — Part 4* describes the functional areas of network management. This reference document supplements the ISO Open Systems Interconnection (OSI) model. The OSI model describes the seven protocol layers (that is, physical through application layer) and the activities necessary, at each layer, for systems to interconnect over communications media such as a telephone line, a serial cable, or a coaxial cable.

The ISO network management model identifies five functional areas of management. They are:

■   Fault Management

■   Performance Management

■   Configuration Management

■   Security Management

■   Accounting Management

There are several publications, as well as the ISO standard itself, that can provide you with complete details on each of these management areas. The following is just a brief overview of the typical requirements in each area.

Fault Management

Detecting faults and notifying administrators of a fault occurrence is an intrinsic function of network management. This function becomes critical in a distributed networking environment, particularly in an economic climate where shrinking budgets force MIS departments to automate remote fault detection and resolution. Compaq recognizes the importance of this category by providing devices that provide a wide array of fault tolerant features, and monitorable error indicator attributes, and "fault prediction" attributes. With fault prediction attributes, you can proactively manage the devices to predict faults and provide maximum server uptime.

Performance Management

Performance management allows you to monitor, analyze, and tune devices and network operation. This function is important in a distributed networking environment where the application or network uptime is mission critical. With performance data available, you can do capacity planning to enable the cost-effective growth of your ever-changing network.

Configuration Management

New devices such as servers, workstations, printers, routers, and specialized high-speed links are constantly added to networks as the prices of computing resources drop. The term *network* takes on new meaning when you consider devices such as laptops, that at times are not connected to the network. With configuration management you can effectively monitor the existence and configuration of the computing assets deployed on your network.

Security Management

There are two facets to security management. They are:

■   Allowing legitimate users access to information relevant to their job function

■   Restricting unauthorized users

Under no circumstances should all users automatically get rights to access all information. Access rights must be set up in a consistent manner, so you can quickly track access violations.

As your organization grows, it might become necessary to separate your network into smaller workgroups, each part of a logical domain such as Sales, Marketing, Engineering, and so on. You need to control intra-domain access in a way that makes it easy for your users to share information, while preventing abuse. Similar, though more restrictive, access applies to exchanging information with external sources such as your suppliers, customers, consultants, and so on. Another concern is physical security (access to the hardware), as well as operating system security and network security (access to data).

Accounting Management

Today, networks can offer a variety of services from video conferences, to
e-mail, to file sharing. It is often necessary to monitor the usage of these services so
you can distribute the costs equitably and charge back to individual cost centers.
Knowledge of usage patterns can also assist you in capacity planning and in
redeploying network resources to serve changing needs.

Network Management Standards

As discussed earlier, managing a network is complex. Management
becomes even more complicated without standards. When an organization purchases
multiple management tools, each with a different method of managing a particular
hardware or software product, it must then maintain
and train administrators in different tools. This is expensive and inefficient.
Consequently, standards committees have developed protocols for
network management.

SNMP Standard

The Internet Engineering Task Force (IETF), the standards rating body for the
world-wide Internetwork, has defined a management protocol. The Simple Network
Management Protocol (SNMP) has garnered a major share of the market and has the
support of over 20,000 different products. SNMP has its roots in the Internet
community — the complexity of large international TCP/IP networks provided the
necessary impetus to develop a standard method of managing devices on the
network.

Within the SNMP framework, manageable network devices (routers, bridges,
servers, and so on) contain a software component called a management agent. The
agent monitors the various subsystems of the network element and stores this
information in a management information base (MIB). Conceptually, the MIB is a
database, readable and writable by a management application using the SNMP
standard.

There are two types of MIBs:

■ Internet Management MIBs -- These MIBs include MIB-II, RMON, and others. These MIBs, standardized by the Internet community, represent the core objects that are common across the widest range of network devices implementing the Internet protocols. Examples of these objects include network protocols such as TCP/IP and network devices such as Ethernet network interfaces.

■ Vendor MIBs -- These MIBs represent objects that are unique to an individual vendor's product or product line. Over 500 vendors and organizations have created their own vendor MIBs. Compaq was the first personal computer company to develop a MIB that enabled SNMP management of server hardware.

The majority of vendors of internetworking devices have embraced the SNMP standard, including:

■ Bay Networks Incorporated

■ Cisco Systems Incorporated

■ Cabletron

■ 3Com Corporation

SNMP has also gained acceptance among vendors who have developed compliant management platforms, including:

■ ManageWise (Novell and Intel)

■ HP OpenView (Hewlett-Packard Company)

■ NetView for AIX (IBM)

■ SunNet Manager (SunConnect -- a Sun Microsystems, Inc. Business)

Among server vendors, Compaq offers SNMP-compliant management agents that provide specific Compaq device information. These include:

■ Compaq Insight Management Agents for NetWare

■ Compaq Insight Management Agents for Microsoft Windows NT

■ Compaq Insight Management Agents for UnixWare

■ Compaq Insight Management Agents for SCO UNIX

■ Compaq Insight Management Agents for IBM OS/2

SNMP often uses the network for sending and receiving management information. This is called "in-band" management, however, SNMP is not limited to in-band management. In-band management is discussed in more detail later in this chapter.

SNMP supports both read and write operations (GET and SET) commands on attributes. Some vendors do not support the SET command because of the potential to allow an unauthorized person to alter critical parameters on a network element. Insight Agents support the SNMP community string and a command line argument to control SET operation behavior of non-critical parameters. For more detailed information, refer to the appropriate *Compaq Insight Management Agents User Guide*.

NOTE: Some users of SNMP have expressed concern over the low level of security mechanisms employed. In response to that concern, the Internet community has recently specified SNMPv2. SNMPv2 is the next version of the Simple Network Management Protocol that includes improvements to SNMP in the areas of performance, security, confidentiality, and manager-to-manager communications. At this time, SNMPv2 has not been implemented by vendors of network devices.

SNMP is associated with TCP/IP and monitoring devices on Ethernet networks because of its long association with the Internet. However, you can use SNMP over other protocols such as IPX and AppleTalk. For example, the Compaq Insight Manager application supports SNMP over IPX and IP.

NOTE: For an in-depth discussion of SNMP, refer to *The Simple Book - An Introduction to Internet Management* by Marshall T. Rose (Prentice-Hall).

SNMP specifies four operations that a management application can use to manage information *known* to the agent. These are the GET, GET-NEXT, SET, and TRAP operations, all briefly described as follows:

■   GET and GET-NEXT

The management application uses the GET and GET-NEXT (read) commands to acquire the data, the MIB variables, that provide the mechanism for monitoring. The Compaq Insight MIBs, included with the Compaq Insight Agents, describe the MIB variables.

■   SET

The SET (write) operation allows the management application to set or change a variable value that is known to the agent.

■   TRAP

The management agents can send asynchronous trap messages or unsolicited information when they determine that a significant fault or performance event has occurred. All traps generated by Insight Agents are Compaq enterprise traps.

Methods of Managing
Network Resources

There are two different methods to access your network resources. Your
management PC can access the managed device(s) "in-band" using the network or
"out-of-band" through a point-to-point connection such as a modem link. The
operational status of your network device(s) influences the actions that you perform
at the management PC. The element is either "online," providing its network services
(such as routing packets or sharing files), or "offline," *not* providing network
services due to routine maintenance or catastrophic failure.

In-Band Device Access

Regardless of the operational status of the device, in-band access requires an
operational network link between the device and management PC. In-band
management is useful for local access or even remote access when you are confident
of your LAN and WAN infrastructure.

Out-of-Band Device Access

In contrast to in-band device access, out-of-band access does not require an
operational network. You can remotely access a device using out-of-band
management when access does not exist to a LAN or WAN, either by design or due
to the failure of a network link. Typically, you would establish an
out-of-band device access to provide a point-to-point connection between a
management console and the managed device. For example, you might use
out-of-band management when the remote office is not on the network.

Online Management

Online management refers to the management of an operational network device. The following sections discuss online in-band and online out-of-band management.

Online In-Band Management

This is the most common management model, since most network administrators are confident of their LAN and WAN infrastructure. The management actions between the management application and the managed device occur within the network. These actions include reading and writing attributes. The network carries regular data as well as management data. This model is very cost-effective because management data typically uses only a small percentage of overall network bandwidth, and you do not need an alternate network to carry the data. However, overloading the network with management data can cause network performance degradation.

Online Out-of-Band Management

This management model is less common, but can be useful for branch office environments. In contrast to in-band management, the management actions between the application and the managed device occur outside a network, usually via an asynchronous or modem connection. Otherwise, all capabilities are the same as online in-band management.

You can use two standard transport protocols to perform out-of-band SNMP management:

■   Serial Line Internet Protocol (SLIP)

■   Point-to-Point Protocol (PPP)

In addition to SLIP and PPP, many vendors use proprietary protocols to perform out-of-band management.

Offline Management

When you need to perform an operation such as recovery of a failed network device, one that no longer provides services to the network, the operation is usually considered maintenance. In general, offline maintenance tasks require the use of recovery tools, as well as the replacement of failed components. Typically, this management style requires a remote login to the failed device to perform recovery operations such as diagnostics, configuration, or firmware update.

Offline In-Band Management

Applications to perform offline in-band management include:

■   NetWare Virtual Terminal (NVT) over IPX

■   Telnet over IP

Offline Out-Of-Band Management

Local terminals (or via modem) with ANSI and VT100 terminal emulation capabilities perform offline out-of-band management.

In addition to Telnet, ANSI, and VT100, many vendors use proprietary protocols and applications to perform offline management.

Server Management as a Subset of Network Management

LANs are strategic resources for the development and deployment of critical applications. Businesses are increasingly deploying LANs to rightsize their operations and capitalize on improved economic results. Consequently, the cost associated with hiring, training, and keeping skilled network administrative personnel to support a growing and complex LAN environment continues to increase. LAN management tools help control the rising costs of LAN administration while increasing the dependability of network environments.

Network administrators have sophisticated management tools for network resources such as bridges, routers, and concentrators, as well as network protocols. However, to manage servers, a key network resource, administrators have typically used simple tools. The comprehensive manageability of servers and sophisticated server management tools are essential requirements for PC networks. As shown in Figure 2-3, these server management requirements include in-depth monitoring, analysis, and control of the performance, fault, and configuration aspects of the server operation.
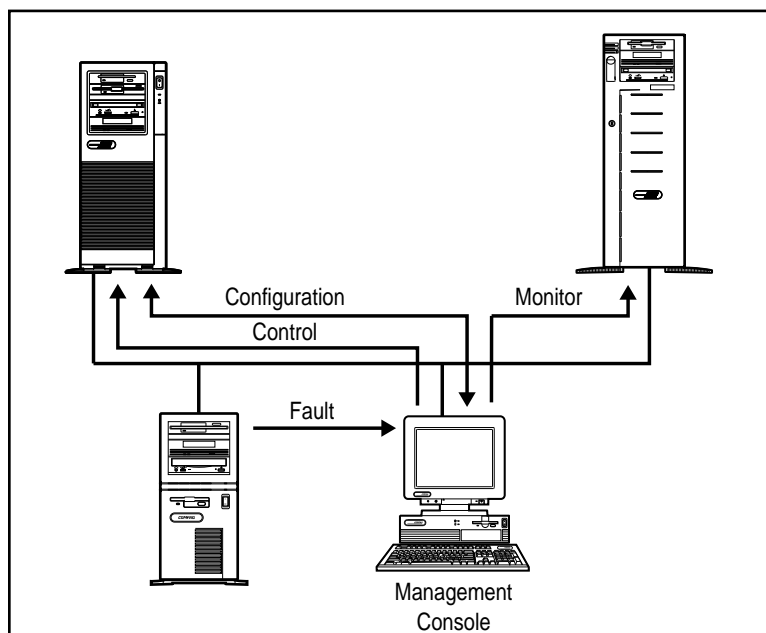
Figure 2-3. Server management data flow

Effective server management requires:

■   Built-in capabilities to the server and options

■   Strict adherence to popular network management standards for communication protocols and data interchange

■   Tools that operate within the customer's preferred environment

The combination of these capabilities allows you to manage the server to ensure that it is one of the most reliable resources in the network.

Desktop Management as a Subset of Network Management

The increasing emphasis on PC LANs has made manageability of PC networks a key customer need. Many businesses are increasing their dependence on PC networks. Large businesses are installing increasingly larger and more complex PC networks; therefore, customers are now demanding significant network dependability.

To meet these customer needs, Compaq has forged close alliances with leading vendors of PC LAN management applications. In conjunction with this effort, Compaq has also implemented desktop PC management capabilities called Intelligent Manageability.

These comprehensive management capabilities make network PCs easier to manage and less expensive to maintain. Figure 2-4 illustrates an example of today's typical data flow when managing a PC network.
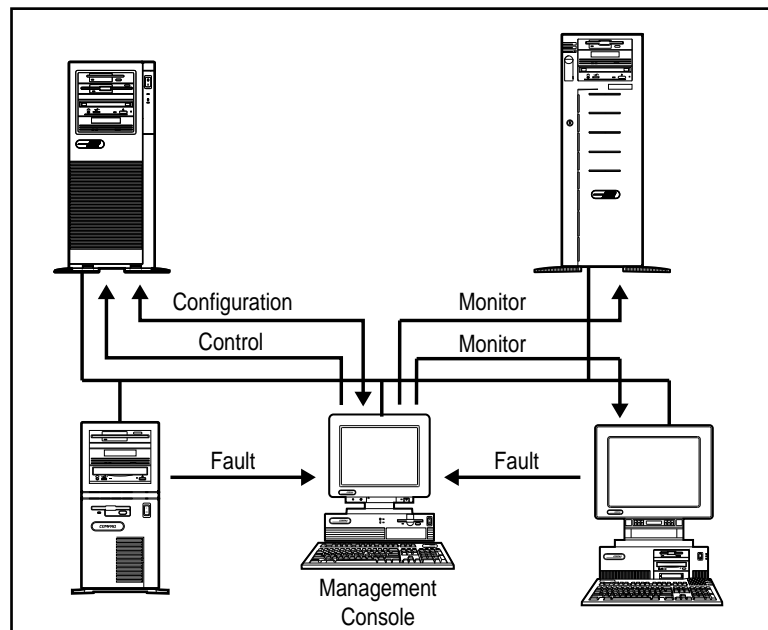
Figure 2-4. Desktop and server management data flow

Effective desktop management requires:

■ Enhanced desktop hardware features that provide a rich set of management capabilities, including Asset and Fault Management

■ Close integration of hardware, operating systems, and management software

■ Support for a wide range of network management standards

■ Fault management of client PCs through standard management products

All of these Intelligent Manageability features are designed to provide manageable PCs that work in any customer's strategic environment. No matter what scale of management a customer uses, the Compaq Deskpro Family has features that add value in the realm of managing networks.

Chapter 3
Compaq Management Technologies

Compaq integrates hardware management features and complementary management tools to provide a complete server and desktop PC management solution for the network administrator.
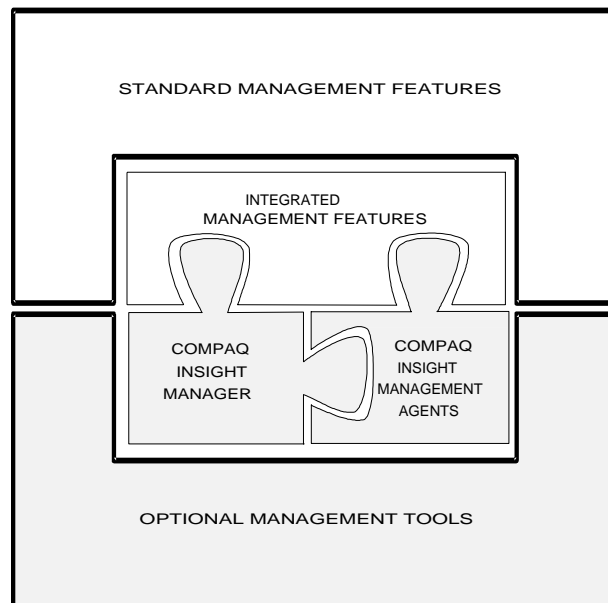
Figure 3-1. Compaq server management framework

The technology framework focuses on hardware management and Compaq Insight Management software that ensures dependable, easy-to-manage computers. The following sections provide a detailed overview of the components of the framework:

■ Compaq Server Management Technologies

■ Compaq Desktop PC Management Technologies

■ Compaq Insight Manager Software

■ Integration with Operating System Management

■ Network Management Interoperability

Compaq Server Management Technologies

The ability to manage server fault conditions, using advanced technologies, is a significant aspect in any server operation. Every hardware subsystem (such as the hard drive, system memory, and system processor) in Compaq servers has a robust set of management capabilities, designed-in, that address one or more of the fault, performance, and configuration management aspects of a server operation.

Network dependability is enhanced by delivering timely information on the operational status of critical server subsystems. Using this information to manage faults is the focus of a comprehensive design approach to server and network uptime. Compaq refers to this design as "Full-Spectrum Fault Management." These fault management technologies provide you with the ability to prevent faults before they happen, keep the system up and running in case of an unlikely failure, or deliver rapid recovery to normal operation after a fault condition.

Full-Spectrum Fault Management is built into Compaq servers. Figure 3-2 illustrates the fault management process.

Fault Prevention → **Fault Tolerance** → **Rapid Recovery**

- **Predicts and avoids failures**
- **Keeps server running in event of component failure**
- **Quickly and automatically recovers from critical failures**
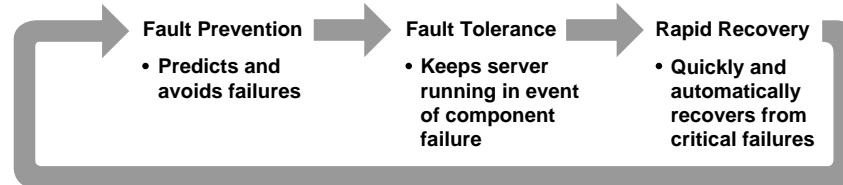
Figure 3-2.   Compaq full-spectrum fault management process

Fault Prevention

Server Parameter Tracking forms the foundation of Compaq server management. Server Parameter Tracking combines hardware, firmware, and industry-standard management software. It provides timely fault, performance, and configuration information for the critical processor, memory, and I/O (storage and network interface) server subsystems and server environment.

Server Parameter Tracking immediately notifies you of impending component failures, enabling preventive maintenance that avoids server failures and maximizes network uptime. For example, predictive storage subsystem tracking warns you of impending failure, allowing you to replace the hard drive or disk controller prior to failure.

Fault Tolerance

Compaq servers also provide a set of fault-tolerant features designed to keep the server up and running if a failure occurs. Compaq ProLiant servers come standard with the "Hot-Pluggable Drive" capability. This feature allows you to replace hard drives without interrupting server operation, thereby maximizing server availability.

Compaq ProLiant servers also can include an "Off-Line Backup Processor." The Offline Backup Processor automatically reboots to a second processor if the first processor fails.

These features complement additional capabilities such as Advanced Error Checking and Correcting (ECC) Memory and the Compaq SMART SCSI Array Controller to maintain a high level of server availability and ensure data integrity.

Rapid Recovery

Compaq servers offer another important built-in capability to manage faults. If a critical server failure occurs, the server can automatically recover. The "Compaq Rapid Recovery Engine" is engineered into Compaq ProLiant servers to diagnose and rapidly return the server to full operation. You can use the Rapid Recovery Engine independently of other server management products or you can use it with Compaq server management tools.

The Rapid Recovery Engine performs several functions that can intelligently and automatically restart the server without user intervention, including:

■ Server Health Logging

■ Capturing snapshots of the subsystem parameters that indicate failure and placing them into nonvolatile health logs and history tables.

■ Automatic Server Recovery-2 (ASR-2)

❑ Restarting the server and resetting all option boards.

❑ Using the nonvolatile logs to recover, reconfigure, and automatically correct failures to the processor and cache, memory failures, and software errors.

Figure 3-3 illustrates how the Rapid Recovery Engine process detects and
resolves critical errors in your Compaq server.
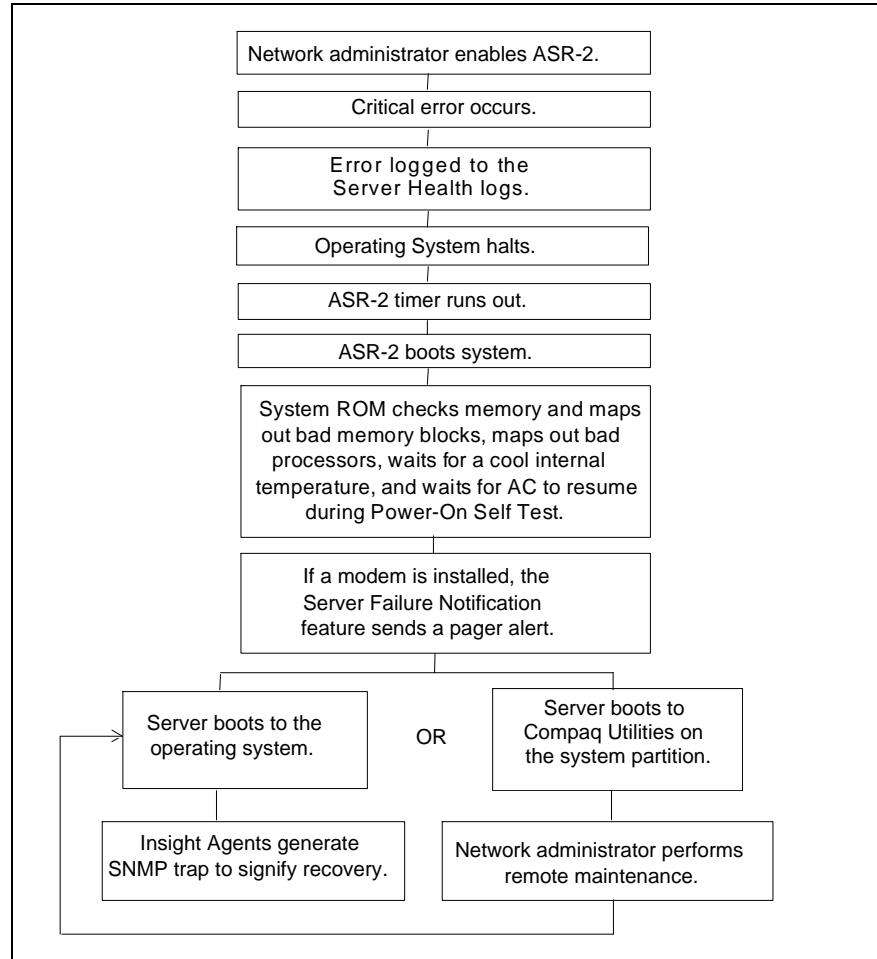
Figure 3-3. Rapid Recovery Engine flowchart

3-6 Compaq Management Technologies

Server Health Logs

Server Health Logs store error information in nonvolatile memory so that Compaq Utilities and network administrators can retrieve and analyze the data later. You can view the Server Health Log contents using the Compaq Inspect Utility or Compaq Insight Manager. By analyzing the data from the Server Health Logs, you can increase your efficiency in resolving current server problems as well as prevent future server errors. The Compaq Diagnostics software also uses the data from the Server Health Logs to streamline its testing and quickly pinpoint problems.

The Server Health Logs include:

■ Critical Error Log -- records catastrophic errors, such as noncorrectable memory, expansion board, and expansion bus arbitration errors. After a critical error occurs, the system ROM indicates on bootup that an error has occurred and prompts you to run Compaq Utilities. The Critical Error Log contains the time, date, and frequency of errors logged. When a critical error is logged, the server can notify you when it reboots.

■ Corrected Error Log -- contains the date, time, frequency, and unique information about errors that the various subsystems have automatically corrected, such as ECC Memory errors.

■ Power-On Error Log -- records any errors that occur during Power-On Self-Test (POST).

■ Revision History Table -- stores board revision information in nonvolatile memory. It logs the system board revision first and then logs other boards that support the Revision History Table, such as the Compaq SMART SCSI Array Controller, Compaq NetFlex-3 Controller, Compaq Fast-Wide SCSI-2 Controller, and Compaq IDA-2 Controller. When you upgrade your server or when you add new expansion boards, the Revision History Table logs this information. As you troubleshoot server problems, you can use this information to determine if a change to the server configuration has caused the server problem.

Refer to the appropriate Compaq server user guide for a more detailed description of the Server Health Logs.

Automatic Server Recovery-2

Automatic Server Recovery-2 (ASR-2) intelligently restarts the server, analyzes the server health logs, and automatically corrects many errors such as processor, memory, server environment failures, and software errors. ASR-2 also informs network administrators by accessing a telephone pager to notify them that a failure has occurred and that it has been corrected.

Table 3-1 describes the critical errors detected by ASR-2.

Table 3-1
ASR-2 Critical Errors

Type	Description
Software Errors	Catastrophic software errors that cause the server to cease operation, such as operating system abnormal termination or "hung" application software.
Memory Errors	Memory errors that cannot be corrected and cause the server operating system to cease operation.
Server Environment Errors	Internal server temperature that exceeds the factory preset threshold.
	AC power failure (requires Compaq UPS).
Processor Board Errors	Catastrophic failure of the system processor board.

Remote Maintenance

The remote maintenance feature allows you to diagnose errors and configure the server from any location, either on the network or via modem. This option is necessary only if the ASR-2 process cannot perform an automatic recovery. During the initial system configuration process, these utilities are copied to a special system utility partition on the hard drive.

Using remote maintenance requires:

■ An operating system with ASR-2 support.

■ Compaq System Configuration Utility 2.22 or greater and Diagnostics utilities installed locally on the system partition of the hard drive.

■ ASR-2 configured to load the Compaq Utilities after the server restarts.

Using a Modem Connection

If you choose to perform remote maintenance using a modem, you must have:

■ A Hayes-compatible modem with the auto-answer feature installed in the server. Compaq ProLiant servers have a management modem slot that allows you to perform remote maintenance over the phone without using an EISA slot.

■ A local terminal with VT100 or ANSI terminal capabilities or management PC configured with Compaq Insight Manager 2.0 or greater.

This arrangement provides the following capabilities:

■ Your server can send notification to your pager.

■ You can dial-in to your server to perform remote control of Compaq Utilities running at the server.

Using a Network Connection

If you choose to perform remote maintenance over a network, you must have:

■ An NVT over IPX or Telnet over IP connection between the server and the management PC.

■ The NVT over IPX or Telnet over IP feature configured and enabled on the server's system utility partition.

■ Compaq Insight Manager 2.20 or greater, or an NVT over IPX or Telnet over IP terminal emulator running on the network.

■ Your network connection enables you to perform remote control of Compaq Utilities running on the server.

Compaq Desktop PC Management Technologies

Compaq has forged close alliances with leading vendors of PC LAN management applications and has leveraged server management technology developed in the Compaq Systems Division. These relationships and expertise have enabled Compaq to create hardware designs and management tools to manage the new Compaq Deskpro Family of PCs installed on networks.

Intelligent Manageability

Intelligent Manageability is the Compaq industry-leading desktop management strategy that makes networked PCs easier to manage today and tomorrow. Compaq is making enhancements to the basic PC hardware to ensure that the PC is easier to inventory, to troubleshoot, and to protect.

These hardware enhancements are then complemented by a wide range of PC LAN management software. Because this software is integrated and compatible with Intelligent Manageability, it ensures that customers can easily manage Compaq PCs over the network using the customer's preferred PC LAN management products.

Inventory and Configuration Management

Computing devices (PCs, servers, printers) and internetworking devices (routers and bridges) are routinely added to the network to satisfy changing business needs. The dynamic nature of these computing environments requires customers to maintain an accurate inventory of the network and to configure the devices rapidly for optimal operation.

Inventory Management

Inventory management is a set of capabilities that provide comprehensive hardware and software component identification and configuration reporting to enable inventory and accounting procedures. This component identification (inventory data) is also a prerequisite to distributing data files and software, troubleshooting remote systems, and managing geographically dispersed assets.

The new Deskpro Family has integrated AssetControl features which allow administrators to maintain an accurate, up-to-date and centralized inventory of desktop PCs and their components. These features enable businesses to maintain control of their PC assets and allow for effective and accurate distribution of software. The features also help streamline service calls because the administrator can provide the service person fast access to the PC's configuration and history.

Asset Information

The new Deskpro Family features used in conjunction with a Compaq Desktop Management Solutions Partner application make a wealth of useful asset information available to the user and the network administrator. The available information includes:

■ The manufacturer, model, and serial number of the PC system, monitor, and hard drive.

■ An Asset Tag, and the revision levels of the system board and system ROM.

Fault Management

Fault management is a set of capabilities that provide an early warning of impending component or subsystem failure. This enables the user to perform preventive maintenance before the failure.

The current Compaq Fault Management implementation includes provisions for IntelliSafe hard drives, environmental fault prevention tracking, and network performance monitoring.

IntelliSafe Hard Drive

An IntelliSafe Hard Drive is the next generation IDE/ATA drive that was co-designed by Compaq and Conner, Quantum, and Seagate (leading drive manufacturers). IntelliSafe Hard Drives contain enhanced firmware that predicts an impending drive failure. System software, working in conjunction with the IntelliSafe hard drive, can notify users and LAN administrators of the impending drive failure. When a failure is predicted, the hard drive can be backed up automatically, either locally or over the network with Windows 95.

Environmental Fault Prevention Tracking

This is a hardware and software feature which tracks the internal temperature of the PC and alerts the user and/or network administrator of excessively high internal temperature. This alert enables the user to take action before damage occurs to data or internal components. Detection of system-damaging internal temperatures automatically shuts off the power to the PC when the temperature climbs far past the point when the initial warning occurred.

NOTE: Environmental Fault Prevention Tracking is only available in a Microsoft Windows 95 operating environment.

Network Performance Monitoring

By using Compaq Insight Manager, a network administrator can monitor and detect performance degredation of the integrated Network Interface Controller (NIC).

NOTE: Network performance monitoring is only available in a Microsoft Windows 95 operating environment.

Rapid Recovery

Rapid recovery is a set of capabilities that provide notification, rapid identification of faults, and automated restart of failed systems or subsystems so that unplanned downtime is minimized. The current Compaq Fault Management implementation includes provisions for proactive tape backup, flashing of ROM BIOS, and availability of accurate contact information.

Proactive Tape Backup

This feature provides added data protection from hard drive failure by automatically backing up the PC hard drive contents to a server tape drive when an impending failure is detected.

NOTE: Proactive tape backup is only available in a Windows 95 operating environment.

Flash ROM BIOS

This allows quick updating of the system ROM without removing the PC cover. If a system error requires an update of the system ROM, the flash ROM capability of the new Deskpro Family provides for a fast recovery by allowing the ROM to be quickly updated via a diskette utility.

Accurate Contact Information

Accurate desktop PC information provided by AssetControl features allows the network administrator to coordinate service responses for maximum efficiency. When a hardware failure occurs, the AssetControl features enable the network administrator to provide the service person with key information such as:

■   The location of the PC

■   The contact person

■   The model and revision level of the PC and components

■   The specific problem, in some cases.

Security Management

Networked PC computing has increased the quantity of easily accessible information that a corporation maintains. Ensuring that this information is accessed only by authorized personnel and that the integrity of the information and PC is maintained is critical in the information age. Security management is concerned with these issues and is comprised of capabilities to safeguard and protect business-critical data and the PC.

Table 3-2 describes the comprehensive security features to protect critical and confidential data and computing resources.

Table 3-2
Deskpro Family Security Features

Feature	Function
Power-on Password	Prevents unauthorized person from booting up the PC.
Setup Password	Prevents unauthorized change of system configuration.
QuickLock/QuickBlank	Allows user to lock keyboard and/or blank screen.
Keyboard Password	Allows PC to boot up but prevents data input until the password is entered.
Network Server Mode	Allows hard drive or network restart while keyboard is disabled.
Diskette Boot Control	Prevents PC from being booted from a floppy diskette.
Diskette Write Control	Prevents unauthorized writing of data to floppy diskette.
Flash ROM Lock	Uses the Setup Password to prevent unauthorized changes to the system ROM.
Parallel Interface Control	Prevents transfer of data through the parallel interface connector.
Serial Interface Control	Prevents transfer of data through the serial interface connector.
Diskette Drive Control	Allows disabling of the diskette drive.
Fixed Disk Drive Control	Allows disabling of the hard drive.
U-bolt/Cable Lock Provision	Allows user to secure PC hardware and protect against theft.

NOTE: All security management features will be maintained under Windows 95.

PC LAN Management Software Support

Compaq is taking a proactive initiative to ensure the compatibility and integration of PC hardware enhancements for manageability with the leading vendors of PC LAN management products. This initiative is called the Compaq Desktop Management Solutions Partners Program. The Solution Partners' products deliver features demanded by network administrators such as server and client monitoring, network protocol analysis, software distribution, and software and hardware inventory.

Compaq Desktop Management Solutions Partners Program

Compaq has worked closely with leading management software vendors to provide remote access to the Intelligent Manageability capabilities of the new Deskpro Family. The broad vendor support ensures that Compaq customers can easily manage Compaq PCs using their choice of tools.

Vendors currently participating in the Compaq Desktop Management Solutions Partners Program include:

■ Cheyenne Software Inc.

■ Frye Computer Systems Inc.

■ Intel Corp.

■ McAfee Associates Inc.

■ Microsoft Corp.

■ Network Computing Inc.

■ Novell Inc.,

■ Saber Software Corp.

■ Symantec Corp.

■ Tally Systems Corp.

Solutions Partners Operating System Support

The Solutions Partners' products provide remote AssetControl support across a wide range of operating environments. This increases the probability that one of the Solutions Partners will have a solution to meet the customer's needs.

Support is available for client PCs using Windows 3.1, OS/2, Windows NT, and (in the future) Windows 95. These clients are supported across a wide range of network operating systems, including NetWare, Windows NT, LAN Manager, LAN Server, and Banyan VINES. Customers must contact specific Solutions Partners to determine the range of support in their particular environment.

**Compaq Insight Manager and the Desktop
Management Solutions Partners Program**

When used with the new Deskpro Family, Compaq Insight Manager and the Solutions Partners products are complementary. Compaq Insight Manager functions primarily as the remote hardware and fault management tool. The Solutions Partners' products handle remote inventory management, software distribution, and so on.

Although Insight Manager does provide access to all of the new Deskpro Family AssetControl information, Insight Manager is primarily a fault management tool providing both IntelliSafe hard drive and thermal monitoring and alerting. Insight Manager will initially be the only product capable of remote alerting for IntelliSafe hard drive or thermal failures. Insight Manager is designed to monitor Compaq hardware only.

The Solutions Partners' products are primarily asset management tools which can provide asset management reports for a range of hardware. The products also might include features such as software distribution, software license metering, and remote workstation control. Although the Solutions Partners' products are designed to manage almost any PC hardware, only the new Deskpro Family provides detailed asset information such as serial numbers and monitor information.

NOTE: Customers must contact specific vendors to gain an up-to-date status on individual product capabilities.

Compaq Insight Manager Software

The Compaq Insight Manager Software architecture is typical of other SNMP-management software and comprises the Compaq Insight Management Agents, and the manager software, Compaq Insight Manager.

Agent software executes on a manageable device such as a server that monitors the fault and performance aspects of the device. These monitored statistics, along with device configuration information, provide data to a management application using the SNMP protocol.

Manager software, such as Insight Manager, provides the user interface to the management features in Compaq servers. You can integrate the Insight Management Agents with SNMP-based management platforms to manage Compaq servers.

Compaq Insight Manager

Compaq developed Insight Manager to make the overwhelming task of server monitoring and server management easy. Insight Manager delivers intelligent monitoring and alerting, remote maintenance, and visual control of the servers in *your* network environment. In the unlikely event of server failures, Insight Manager provides a full spectrum of remote maintenance and control facilities such as system rebooting, system configuration, and system diagnostics.

Insight Manager provides timely server status and the means for remotely controlling servers through the following key features:

■ Server Task List

A list providing easy access to management tasks.

■ Viewing Server Data

Compaq Insight Manager allows you to take an in-depth look at and monitor the health of the system hardware. You can view data such as drive subsystem, recovery options, system configuration, system board, option boards, and NICs, and system utilization.

■ Remote Maintenance

You can perform remote maintenance operations across networks and modem links with this feature; therefore, giving yourself active control of your network servers.

❏ Set - Allows you to update server parameters while the server is online

❏ Remote Server Restart - Allows you to bring down the server, then reboot it to the operating system or Compaq Utilities

❏ Remote Console - Provides a virtual server console under Insight Manager

■ Asynchronous Management

When the network is down, you still have the ability to communicate with a server to perform management functions by establishing a Point-to-Point Protocol (PPP) dial-up connection using the Asynchronous Management feature.

■ Version Control

This feature queries your server(s) for the software version levels, then it compares the findings with a database of Compaq software version information. Version Control is provided on the Compaq SmartStart CD, the Compaq Support Software CD, or SoftPaq SP0965 located on the Web server.

■ Paging

If a server goes down, the paging feature within Compaq Insight Manager notifies you immediately via a pager that an event has taken place. This built-in feature allows you to focus on other aspects of managing a network instead of being tied to your console monitoring the network.

■ Drive Array

This allows the user to take an in-depth look at Compaq Drive Arrays. You can view the physical location of each drive and see the volume in which it belongs. You can also verify the RAID level of each drive array (for example, no fault tolerance, drive mirroring, data guarding, or distributed data guarding).

Additional Compaq Insight Manager features include:

■ Ability to configure the primary UPS server with the network address of secondary servers so if an impending power outage occurs all server gracefully shutdown.

■ Support for tape drive management on NetWare 3.12 and 4.x as well as Microsoft Windows NT 3.5 and 3.51.

■ Ability to recover information from a primary server in the event of a server failure. This feature is known as Standby Recovery Server.

■ Support for Windows Internet Naming Service (WINS) and Dynamic Host Configuration Protocol (DHCP).

Insight Manager adheres to the following standards:

■ Management Protocol -- SNMPv1 running over IPX, IP, or PPP

■ Compaq Insight Management MIB -- all possible manageable objects specific to Compaq hardware

■ Standard Internet MIBs -- support information from MIB-II, Token Ring MIB, and Ethernet MIB

Additionally, Insight Manager stores gathered object information in a Btrieve database. You can retrieve this information using Insight Manager or one of several commercially available applications that can access Btrieve data.

Compaq Insight Management Agents

Insight Agents consist of server and desktop software that integrates Compaq manageability into SNMP-based management environments. Insight Agents perform in-depth monitoring of the fault and performance aspects of the key server subsystems: storage, memory, system processor, network interface, and the environment. Insight Agents provide this information, along with server configuration, to SNMP-compliant management applications such as Insight Manager. In addition, Insight Agents can generate traps to notify the administrator of significant changes in the fault or performance aspects of the computer operation. With these traps, you can proactively manage the computer, minimize unplanned downtime, and maximize performance.

Insight Agents support NetWare, Microsoft Windows NT, SCO UNIX, UnixWare, and IBM OS/2. Insight Agents include the Compaq Insight Management MIBs, ready for compilation in your SNMP management platform. For more information about the Insight Agents for a particular operating system, refer to the appropriate *Compaq Insight Management Agents User Guide.*

Compaq Management Information Base

A management information base (MIB) is a description of a set of manageable objects. A manageable device can implement one or more MIBs, depending on its function. A Simple Network Management Protocol (SNMP) MIB, which Compaq fully supports, is very similar to a database schema in that it describes both the structure and format of a set of data. The Internet-assigned Compaq enterprise ID is 232.

Figure 3-4 shows the location of the Compaq enterprise ID in context within the Internet Naming Tree.
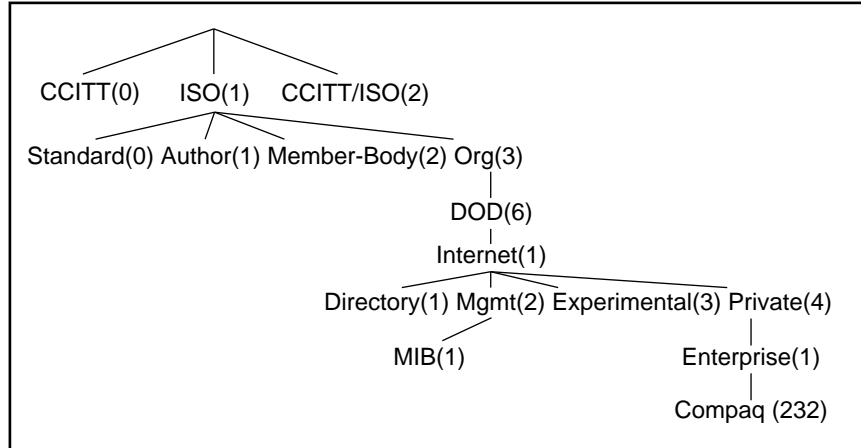
Figure 3-4.   Internet naming tree with Compaq Enterprise ID (232)

The Compaq enterprise ID (232) specifies the location of the Insight MIBs within the Internet Naming Tree. The Insight MIBs are modular, with each subbranch from the Compaq enterprise ID representing a distinct function or subsystem supported by the Insight Agents.

Due to the constant changing, updating, or adding of Insight MIBs, Table 3-3 lists the most recent MIBs:

Table 3-3
Most Recent MIBs

MIB	Describes . . .
Standard PC Equipment Configuration	Information that can be configured on an PCI ISA or EISA system
System Information	Specific Compaq features such as security, asset management, and so on
Intelligent Drive Arrays	Compaq Drive Array Controllers

Most Recent MIBs *continued*

MIB	Describes . . .
SCSI Devices	Compaq SCSI interface products
Server Health	The features that monitor server health, such as thermal sensing
Drive Storage Systems	Compaq ProLiant Storage System
Management Engine	Software components to track statistics, generate alarms, and more
Host OS Information	Generic host OS information, for example, system processor utility, file system information, and so on
Uninterruptible Power Supply Information	Compaq Uninterruptible Power Supply

Although the Insight MIBs are organized according to subsystem, your management application can organize the display of the data from the managed devices to convey the most usable presentation. Refer to Appendix A, "Using Compaq Insight MIB Information," of this TechNote, for more detailed information about Insight MIBs.

Integration with Operating System Management

A complete, SNMP-based, server management solution necessitates developing capabilities that provide server hardware and software management for operating systems and applications. Insight Agents take advantage of the extensible SNMP agents provided by Novell, Microsoft, the Santa Cruz Operation (SCO), and IBM. Developing agents according to the extensible agent specification ensures that Compaq hardware management technologies integrate with the server and desktop software management.

Network Management Interoperability

Delivering hardware management technologies that *integrate* with your SNMP-management environment is as important as building the management technologies themselves. Compaq servers can satisfy your management interoperability requirements.

Compaq servers and Compaq Insight Management Software integrate within your preferred management environment. Compaq adheres to network management standards.

Compaq servers provide an extensive MIB which can be used in a full range of environments from a one-server LAN to a globally dispersed enterprise. Because the information is available through SNMP, it is available to point solutions on the LAN for small installations all the way up to complex WAN/LAN enterprises. As your single network LANs grow into larger routed LANs and then into internetworked WANs, you can be sure that Compaq information will grow with you and support your management needs.

Chapter 4
Preinstallation Considerations

Installing a network management platform is no small task; therefore, this chapter provides you with the minimum hardware and software requirements necessary to properly install Compaq Insight Manager into ManageWise. Before discussing all of the preinstallation considerations, let's discuss ManageWise and its architecture.

What is ManageWise?

Effective system management requires the interaction of intelligent hardware and firmware with powerful management applications. Compaq servers and desktops are designed with self-diagnostic capabilities that continuously monitor and record the operational status of all key subsystems and components. This information can then be accessed by Compaq Insight Manager or other management tools, such as ManageWise, to provide you with a detailed, integrated view of the operational status of your business-critical network resources.

ManageWise is the network management platform that provides you with an end-to-end management solution for large and small networks. ManageWise provides a global view of an entire network, enabling you to monitor and manage both hardware and software devices on a network. ManageWise discovers and inventories all network devices and constantly monitors for alarms which can pinpoint network problems as well as protect the network from software viruses.

ManageWise supports the Simple Network Management Protocol (SNMP) which allows easy integration with management applications, such as Compaq Insight Manager.

ManageWise components include:

■ NetWare Management System (NMS) 2.0

■ NetWare Management Agent (NMA) 1.0

■ NetWare LANalyzer Agent 1.0

■ LANDesk Manager 1.51

■ LANDesk Virus Protect 2.1

For detailed descriptions of each ManageWise component, refer to the ManageWise documentation you received when you purchased the product.

Understanding the ManageWise Architecture

Novell provides their customers with a network and systems management strategy that offers a set of management services collectively known as NetWare Distributed Management Services (NDMS). These services provide scaleable and flexible management capabilities for your entire NetWare environment. When Novell and Intel combined their efforts to integrate their tools and services available for managing networks, the integrated management solution developed became ManageWise.

ManageWise integrates easily into the NDMS architecture because it is comprised of multiple components that reside on different parts of the network. For example, as shown in Table 4-1, the device discovery engine and its database reside on the NetExplorer Server, while the Network Management Map and its database reside on the console. This is an example of how the distributed components of ManageWise align with the NDMS architecture.

Table 4-1 lists the ManageWise components, abbreviations, functions and locations on your network. This table should assist you in a better understanding where each distributed component of ManageWise resides.

Table 4-1
ManageWise Components

Component	Abbreviations	Location	Component Function
NetExplorer	NXP	Server	Discovers all devices within an entire network.
NetWare LANalyzer Agent	LANZ	Server	Gathers information for analyzing the network traffic.
NetWare Management Agents	NMA	Server	Allows the server to be monitored and managed remotely.
NetExplorer Plus	NXPPLUS	Server	Provides additional information on network devices.
LANDesk Inventory	LDINV	Server	Maintains the inventory database and the client inventory scanning components.
LANDesk Virus Protect	LDVP	Server	Prevents viruses from being introduced into servers and desktop PCs.
NetExplorer Manager	N/A	Console	Controls the timing and duration of updates from the NetExplorer components.
LANDesk Inventory Manager	N/A	Console	Displays, queries, and modifies hardware and software inventory information.
LANDesk Desktop Manager	N/A	Console	Provides a comprehensive set of desktop management tools.

Figure 4-2 illustrates how ManageWise integrates into the NDMS architecture and displays the component locations in a typical multiserver network configuration.
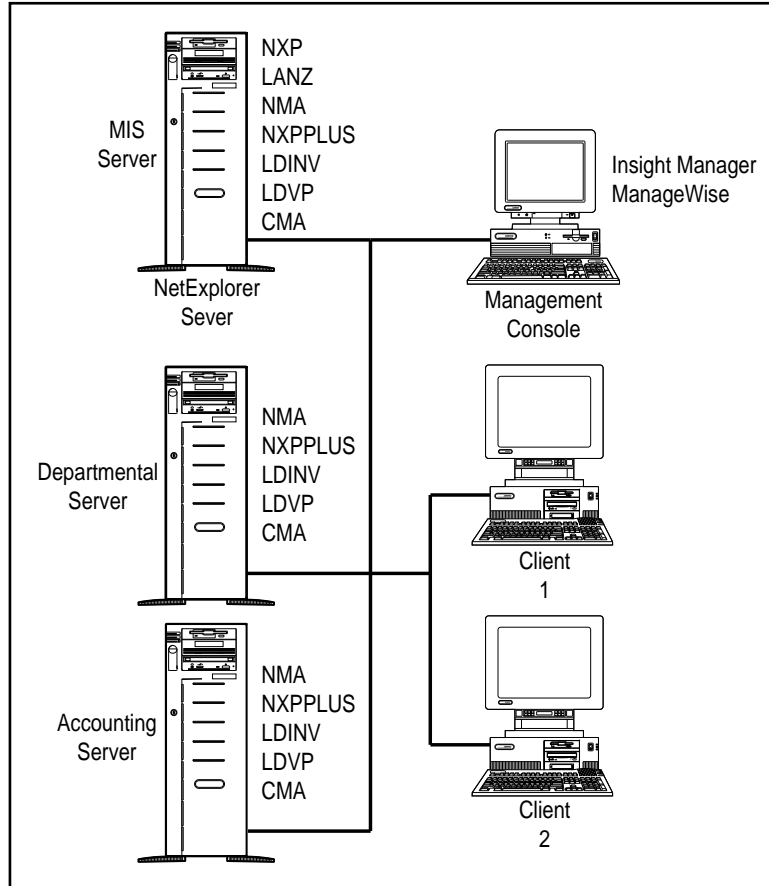

Figure 4-1. ManageWise configuration on a typical multiserver network

NOTE: Not every server on the network needs to have all of the ManageWise components installed (for example, NXP). However, Compaq Insight Management Agents (CMA) are installed on all servers on the network. Additionally, the LANalyzer Agent is installed (by default) but can be disabled.

Preinstallation Considerations

This section provides you with the information to ensure the ManageWise installation process is smooth and seamless. The topics covered in this section are:

■ Hardware and software requirements

■ Product installation sequence

■ ManageWise considerations

■ Compaq Insight Manager considerations

Hardware and Software Requirements

Each management platform has hardware and software requirements. This section discusses those requirements for the ManageWise server, ManageWise console, Compaq Insight Management Agents, and Compaq Insight Manager.

ManageWise Server Requirements

The installation program for ManageWise has several requirements for the server. These minimum requirements can vary based on which ManageWise components you install. The baseline for resource requirements is established on a server configured with all of the ManageWise components.

■ Compaq server 386/33 MHz

■ 10 megabytes of additional RAM
  (2 megabytes without NetExplorer installed)

■ 23 megabytes of disk space

■ Network Interface Controller

■ NetWare 3.1x, 4.02, or 4.1

■ User account with SUPERVISOR rights

■ Btrieve 6.10c (available on ManageWise CD-ROM)

ManageWise Console Requirements

The installation program for ManageWise has several requirements for the console as well. It is important to have a stable console to ensure the reliability of your system. If the console is unstable before installing ManageWise, the reliability of your management console decreases and could be jeopardized. The ManageWise console must meet the following minimum requirements to ensure stability:

■   Compaq desktop 486/33 MHz

■   VGA monitor

■   16 megabytes of RAM

■   512 kilobytes conventional memory

■   Accessible CD-ROM drive

■   50+ megabytes of disk space

■   MS-DOS 6.22 or Novell DOS 7 software

■   A network connection

■   Microsoft Windows 3.1x

■   NetWare Client 1.2 (included on the ManageWise CD-ROM)

NOTE: When you install NetWare Client 1.2, *SHARE.EXE* must not be loaded. However, you must load *SHARE.EXE* to install ManageWise properly.

Compaq Insight Management Agents for NetWare Requirements

Insight Management Agents for NetWare require the following minimum requirements:

■ Compaq server

■ 1 megabyte of reserved disk space

■ NetWare 3.1x, 4.02, or 4.1

> **NOTE:** Agents running on NetWare 3.11 need the *AFTER311.NLM* file loaded to operate.

Compaq Insight Manager Requirements

The following requirements are necessary to install Compaq Insight Manager on a management PC running Windows 3.1:

■ 8 megabytes of RAM (minimum)

■ 27 megabytes of reserved disk space
(8 megabytes for programs, 19 megabytes for databases)

■ VGA graphics or better

■ Network Interface Controller - Compatible with NetWare Open Datalink Interface (ODI)

■ Microsoft Windows 3.1 running in enhanced mode

Product Installation Sequence

The process for installing the complete management platform (ManageWise wtih Compaq Insight Manager) is quite simple. However, it is important to install each product in the proper sequence, because each product requires the previous one for a proper installation. Table 4-2 lists the correct product installation sequence.

Table 4-2
Product Installation Sequence

Sequence	Product
1	DOS/Windows 3.x
2	NetWare Client for DOS and Windows v1.2
3	ManageWise Server Setup
4	ManageWise Console Setup
5	Compaq Insight Management Agents
6	Compaq Insight Manager

NOTE: Be sure to designate your first ManageWise server as the NetExplorer Server. The NetExplorer Manager must connect to the NetExplorer Server in order to download the topological information ManageWise requires to build the Network Management Map.

ManageWise Considerations

Once you have decided to use ManageWise on your network there are some informational tips as well as prerequisites you need to consider before you start the installation process. These considerations include topics such as:

■ Accessing a CD-ROM locally or across the network

■ Loading the *SHARE.EXE* file

■   Using the ManageWise License Diskette

■   Connecting to the NetExplorer server

■   Discovery mechanisms

Accessing a CD-ROM Locally or Across the Network

To install ManageWise, you need access to a CD-ROM drive either locally or across the network. To access the ManageWise CD locally, place the ManageWise CD into the CD-ROM drive. To access the ManageWise CD across the network, follow these steps:

1. Place the ManageWise CD into the CD-ROM drive on the targeted File Server.

2. Mount the CD-ROM as a volume from the File Server Console.

3. Map a drive connection to that volume, then start the installation program.

Loading the *SHARE.EXE* File

When you install the NetWare Client, do not load the *SHARE.EXE* file into memory. However, when you are ready to install ManageWise, load *SHARE.EXE* into memory before launching Windows. After completing this task, you can start the ManageWise and Insight Manager installation process.

NOTE: ManageWise and Insight Manager require you to load the *SHARE.EXE* file, so they can properly access their databases.

Using the ManageWise License Diskette

During the server setup portion of the ManageWise installation, the program prompts you for the ManageWise License Diskette. You need this diskette to continue the installation. The installation program requires this diskette to serialize all of the ManageWise components on the server.

Connecting to the NetExplorer Server

During the ManageWise Console installation process, the program requires a ManageWise server to be up and running. At this time, the installation program prompts you for the name of the ManageWise NetExplorer Server responsible for providing topological information to the console. The installation program uses this information to:

■ Verify the NetExplorer Server exists.

■ Confirm the installation of ManageWise on the NetExplorer Server.

NOTE: If the installation program cannot confirm this information, you cannot continue with the console installation.

Discovery Mechanisms

ManageWise uses a combination of discovery mechanisms to identify all devices on the network. This combination is made up of the NetWare protocol, called the Service Advertising Protocol (SAP), and a transient rule.

SAP is a NetWare protocol used to identify the services and addresses of servers attached to the network. The responses are used to update a table in the router known as the Server Information Table.

The transient rule determines which application, such as Insight Manager or NetWare Management Agents, will be the default action when double clicking on that node. The transient rule for Insight Manager is that it first launches to the NetWare Management Agents, then you can access Insight Manager.

Compaq Insight Management Agents and NetWare Management Agents SAP identifications are:

■ Compaq SAP ID - 372 (0x174)

■ Novell SAP ID - 563 (0x233)

Compaq Insight Manager Considerations

The following section discusses the recommendation of installing ManageWise before you install Insight Manager.

Installing ManageWise Before Insight Manager

Install ManageWise before you install Insight Manager; otherwise, Insight Manager installs as a standalone application and does not integrate with ManageWise.

If you have installed Insight Manager before ManageWise, the option for installing ManageWise or NMS support (shown below) does not appear during the Insight Manager Installation. To correct this, abort the Compaq Insight Manager installation and verify that ManageWise is installed and running on your machine. Once you have done this, proceed with the Insight Manager installation.

❑ Install Compaq Insight Manager 2.50
❑ Install ManageWise or NMS Support
❑ Install Asynchronous Management

Why Use the Compaq Management Information Base?

The Compaq Insight Management Agents Management Information Bases (MIBs) provide the base structure for managing Compaq hardware. Compaq provides a set of MIBs that can be compiled into any SNMP compliant management platform, such as ManageWise. With these MIBs, ManageWise can understand Compaq SNMP traps and add valuable messages to the ManageWise alarm monitor log.

Compaq MIB items show up as SNMP events for configuration of the alarm dispositions. This means you can configure how ManageWise processes and logs the SNMP trap and you can also launch an application.

Chapter 5
Integrating Compaq Insight Manager with ManageWise

This chapter discusses installing ManageWise on your server and on your console, then integrating Compaq Insight Manager to work in conjunction with ManageWise.

Installing ManageWise on Your Server

To install ManageWise on your server, follow these steps:

1. Place the ManageWise CD into the CD-ROM drive.

2. Start Windows, then select *File* → *Run* from the Program Manager menu.

3. Type [CD drive]:\SETUP, then select *OK* and after a few seconds the ManageWise Setup Screen appears.

4. Select *Set Up Server* to configure a NetExplorer server on the network. A NetExplorer server must be set up on your network before you can proceed to set up the ManageWise console.

> **!** **IMPORTANT:** During the planning stage of your ManageWise installation, you must designate at least one server on the network as the NetExplorer Server. This allows ManageWise to automatically discover each device on the network.

5. Insert the ManageWise License diskette into the diskette drive and select *OK*.

   NOTE: If you are going to install ManageWise on more than one server, you need an additional ManageWise License diskette for each additional server.

6. Select a drive on the ManageWise Server Target Information Screen that is mapped to the SYS Volume on the server on which you want to install ManageWise. When you have done this, select the *Install* button to proceed with the installation.

    NOTE: If you currently do not have a drive mapped to this SYS volume, select the *Network* button to create a mapping to that drive. Also, if you choose an incorrect volume, you will receive an incorrect volume error message. To correct the error, select the proper drive.

7. Select *Install NetExplorer on this server* only if you want this server to be the NetExplorer server. Select *Continue* to proceed.

8. Enter a password for the new NETMAN account you are about to create, confirm the password, and select *Continue*.

    NOTE: ManageWise uses the NETMAN account information to verify access rights during any management sessions.

    Now that you have created a new NETMAN account, the ManageWise installation process is next. ManageWise installs the following management tools during installation:

    ❏ NetWare Management System 2.0

    ❏ NMS 2.0c patch

    ❏ NetWare Management Agent 1.0

    ❏ NetWare LANalyzer Agent 1.0

    ❏ LANDesk Manager 1.51

    ❏ LANDesk Virus Protect 2.1

    NOTE: During the ManageWise installation if you have any outdated files, ManageWise prompts you to update them.

9. Select the *Accept* button so ManageWise can modify the System Login Script
    and the *AUTOEXEC.NCF* files for LANDesk Manager.

10. Complete the *Server To Do List*. This list must be completed to enable all of the
    components just installed on your server. Once you have completed this list,
    select *Done*.

> **!** **IMPORTANT:** Do not reboot the server to run NetExplorer until you install
> the Compaq Insight Management Agents on each server you want to
> manage. This allows the NetExplorer to recognize these servers as Compaq
> manageable devices.

Installing ManageWise on Your Console

To continue the ManageWise installation, you must next set up the console. Because
you have already set up your server, the installation program returns you to the
ManageWise Setup menu. Use the following steps to set up your ManageWise
console:

1. Select *Set Up Console*, then place the ManageWise License diskette into the
    diskette drive and select *OK*.

    The installation program prompts you for this diskette to verify your licensed
    user count (the amount of users you are licensed for) and serial number so
    that it can serialize the software.

2. Select the drive mapped to the root of the SYS Volume on which you
    installed ManageWise, then select *Install*.

3. Select the size of your network (the approximate number of nodes in your
    network), then choose *OK*. The average size for a medium network is
    approximately 100 to 1000 nodes.

4. Enter your name and Company, then select *Continue*. The console installation program prompts you to verify this information.

5. Enter the name of the NetExplorer Server, then select *OK*.

   NOTE: The default server name for your network might not be the designated NetExplorer Server. If the server name is not the NetExplorer Server, change it now.

   Just before the NMS console is installed, the installation program prompts you to choose options such as, *Installing the NMS tutorials* and *Installing TCP/IP software*.

6. Select *Installing TCP/IP software* if you use TCP/IP on your network, then select *OK*.

   NOTE: The installation program might modify some of your configuration files such as the *AUTOEXEC.BAT, CONFIG.SYS, SYSTEM.INI, WIN.INI,* and the *NET.CFG* files. The system saves the old filename with the extension *.NMS*.

7. Accept or Deny changes to your *AUTOEXEC.BAT* and *SYSTEM.INI* files. The console installation program prompts you for this information. If you accept *all* changes, the console installation begins.

   > **!** **IMPORTANT:** If you do not accept *all* of the changes, the ManageWise console will not run properly.

8. Select a time zone.

9. Select *OK* and the LANDesk Virus Protect Installation program launches.

10. Complete the *Console To Do List*. This list must be completed to enable all of the components just installed on your server. Once you have completed this list, select *Done*.

You have successfully completed your ManageWise installation.

To fully comprehend the integration process that occurs when Insight Manager integrates into ManageWise, you need to understand the differences between ManageWise and the NetWare Management System (NMS).

ManageWise and NetWare Management System Differences

The technological differences between the base platform of ManageWise and NetWare Management System (NMS) are minimal. ManageWise uses NMS 2.0c as its base platform. Novell combined NMS 2.0c with additional features added from other software packages to provide a complete management solution all in one box. The software packages integrated with NMS to create ManageWise include:

■   NetWare Management Agent 1.0

■   NetWare LANalyzer Agent 1.0

■   Intel LANDesk Manager 1.51

■   Intel LANDesk Virus Protect 2.1

Even though ManageWise is a combination of these software packages and NMS, each program still exists under its original directory structure. For example, if you install ManageWise, each product directory appears the same as if you installed each product individually. There is only one slight modification. The ManageWise directory appears as the main directory instead of NMS or LANDesk Manager.

This is how the integration process of all these packages work together. To make all of these products appear as one, the console directory structure has been modified. Rather than having two separate subdirectories, one for NMS and one for LANDesk Manager, there is only one main directory for ManageWise. Located under the ManageWise main directory are the subdirectories for NMS and LANDesk Manager. Refer to Figure 5-1 for an overall view of the ManageWise directory structure and Table 5-1 for descriptions for each abbreviation.
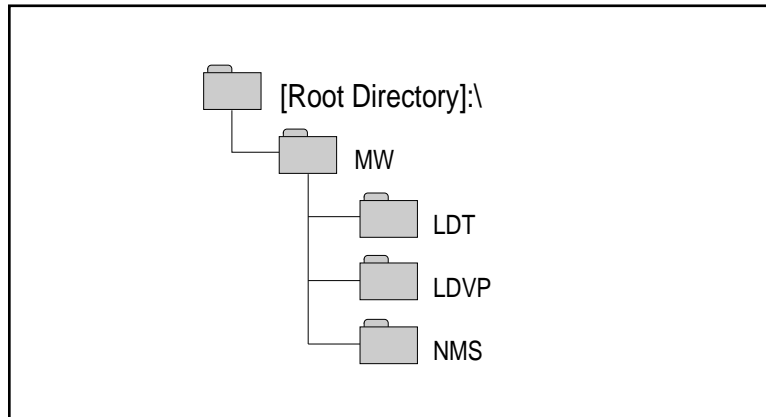
Figure 5-1. The ManageWise directory structure

Table 5-1
ManageWise Directory Abbreviations

Abbreviations	Descriptions
MW	ManageWise
LDT	LANDesk Manager
LDVP	LANDesk Virus Protect
NMS	NetWare Management System

By having LANDesk Manager and LANDesk Virus Protect integrated into NMS
2.0c to create ManageWise, you now have all of the basic tools
necessary to manage any NetWare LAN from end-to-end.

Installing Compaq Insight Management Agents

This section describes the installation procedure for installing the Compaq Insight Management Agents for NetWare. Read the installation instructions completely before trying to install the software.

NOTE: If you have already installed the Compaq Insight Management Agents by using SmartStart, skip to "Setting up the SNMP System Description and Trap Destinations."

The *Compaq Insight Management Agents for NetWare* diskette provides the installation file, *CPQFPYIN.NCF*, and the installation utility, *CPQAGIN.NLM*, to install and configure the Insight Management Agents for NetWare on a NetWare Server. From a NetWare server console, follow these steps:

1. Insert the *Compaq Insight Management Agents for NetWare* diskette into diskette drive. At the Command Console, type:

    A:\COMPAQ\CPQFPYIN

2. Select *Install NetWare Agents from Diskette* to install or upgrade Insight Management Agents. The installation program lists the agents to be loaded on to your NetWare Partition.

    NOTE: Online help is available throughout the installation by pressing **F1**.

3. Highlight the agent you want loaded, then select *Yes* or *No*. You can then move the cursor to select additional agents or save the information and continue.

    NOTE: You must install CPQBSSA for Insight Manager to recognize that the server is manageable.

4. Select the parameters you want to configure the agents. They include:

    ❏ SNMP Monitor and Control support (community and monitor strings)
    ❏ SNMP Set support
    ❏ Insight Manager Remote Server Reboot
    ❏ Polling Interval

NOTE: If you have INETCFG on your system, you must use INETCFG to change the SNMP Community and Monitor strings.

The screens that follow depend on the individual agents installed:

■ CPQBSSA can be configured to issue or not issue NetWare SAP packets, and monitor or not monitor Ethernet and Token Ring information.

■ CPQTHRSA can be configured for the maximum number of threshold entries to support.

NOTE: If you are installing Insight Management Agents on a NetWare 3.11 server, you must manually install the correct versions of *SNMP.NLM*, *AFTER311.NLM*, and *TCPIP.NLM*. These files are included on the *Compaq Insight Management Agents for NetWare* diskette.

Table 5-2 lists the Insight Management Agents (NLMs) delivered with the v2.50 software release.

Table 5-2
Integrating Compaq Insight Manager with ManageWise
Insight Management Agents, Drivers, and Installation Utilities

File Name (NLM)	Description
CPQBSSA.NLM	Base system agent
CPQDSKSA.NLM	Storage system agent
CPQHTHSA.NLM	Server Health agent
CPQSMBSA.NLM	Server Manager/R agent
CPQUPSSA.NLM	UPS agent
CPQTHRSA.NLM	Alert threshold support agent
CPQSYSMN.NLM	Server Manager/R device driver
CPQCPAT.NLM	Patch for *CLIB.NLM* versions before 11/11/92
CPQAGIN.NLM	Compaq Insight Agent Installation & Configuration
CPQDSPAT.NLM	Compaq ASPI stub for CPQDSKSA

Setting Up the SNMP System Description and Trap Destinations

The final step to installing the Insight Management Agents is to update the *SNMP.CFG* and *TRAPTARG.CFG* files to match your server and network management configuration.

Sample configuration files, *SNMP.CFG* and *TRAPTARG.CFG*, are in the \NOVELL\ETC directory of the *Compaq Insight Management Agents for NetWare* diskette. If your server does not have these files in the SYS:ETC directory, copy the sample files from the NetWare diskette to your server.

Editing the *SNMP.CFG* File

The *SNMP.CFG* is an ASCII text file that provides the *SNMP.NLM* with server name, hardware, location, and contact information. The *SNMP.CFG* is a sample and should be edited to reflect the correct information about your installation.

NOTE: The *SNMP.NLM* allows configuration of some MIB-II system identification information with the *SNMP.CFG* file. You must have the *SNMP.CFG* file in the SYS:ETC directory when the *SNMP.NLM* is loaded for proper configuration of the identification information.

Editing the *TRAPTARG.CFG* File

The sample *TRAPTARG.CFG* file provides the *SNMP.NLM* with information about where to send alarm information.

The *TRAPTARG.CFG* is an ASCII text file that lists the addresses of management console that should be alerted when the SNMP Insight Management Agents detect an important event. The *TRAPTARG.CFG* in SYS:ETC is a sample. Edit the file to reflect the correct information. Follow the instructions provided in the sample *TRAPTARG.CFG* file to update this file to match your environment configuration. Be sure to place the alarm destination address under the appropriate protocol section and to indent each address with at least one space.

To help you determine the network address of your management PC when using IPX, you can execute the USERLIST program. At the DOS prompt, type:

USERLIST /A

For NetWare 4, type:

NLIST USER /A

A list of PCs logged into the server and their addresses is displayed. The entry with an asterisk preceding the user name is the PC you are using. Both the network address and the node address given by USERLIST are needed by the *TRAPTARG.CFG* file.

NOTE: If you are using Insight Manager, verify that the network address of the management PC where Insight Manager runs is included in *TRAPTARG.CFG* file.

One method for ensuring that you have the proper address configured is to use Compaq Insight Management Agents for NetWare installation program to generate a test trap. To do this, use the option *Initiate Test Trap* located on the main Agent Options window of the installation program. This option generates and sends a test trap to any address(es) specified in the *TRAPTARG.CFG* file.

Updating SNMP Support for NetWare 3.11

Servers with NetWare 3.11 installed might require you to update the SNMP support files located in the system directory of the server. Table 5-3 lists the minimum versions of SNMP support files required by the Insight Management Agents.

Table 5-3
SNMP Support Files

NLM File	Version	Date
SNMP.NLM	2.08 or later	4/06/93
AFTER311.NLM	2.00a or later	1/26/93
TCPIP.NLM	2.02l or later	2/20/93

NOTE: The NLM dates and versions mentioned in Table 5-3 are the minimum required for NetWare 3.11. They are not meant to specify the latest versions of these NLMs.

To update the NetWare 3.11 SNMP support files, follow these steps:

1. Rename the existing SNMP support files listed in Table 5-3 in the SYS:SYSTEM directory of the NetWare server. Do this so the files will not be written over or deleted. For example:

    RENAME SNMP.NLM SNMPOLD.NLM

> △ **CAUTION:**   Do not copy the files on the *Compaq Insight Management Agents for NetWare* diskette directly over the SNMP support files already installed on your system.

2. Copy the files in the \NOVELL\NW311\SYSTEM directory of the *Compaq Insight Management Agents for NetWare* diskette into the \SYSTEM directory of the NetWare server. For example:

    COPY A:\NOVELL\NW311\SYSTEM*.* F:\SYSTEM*.*

3. Create a SYS:ETC directory on the server if one does not already exist.

4. If your server does not already have the *SNMP.CFG* and *TRAPTARG.CFG* files installed and updated for your particular configuration, copy the sample files in the \NOVELL\ETC directory of the *Compaq Insight Management Agents for NetWare* diskette to the SYS:ETC directory of the NetWare server. For example:

    COPY A:\NOVELL\ETC*.* F:\ETC*.*

Now you are finished updating of the NetWare 3.11 SNMP support files.

SNMP Monitor and Control
Community Strings

SNMP defines a community as a relationship between an SNMP agent and one or more SNMP managers. When SNMP messages are exchanged, they contain two parts:

■ A community name and information to validate the sending SNMP entity as a member of an identified community

■ Data

The community name defines the authentication mechanism.

The *SNMP.NLM* allows you to specify two different user communities on the command line: the monitor community and the control community. The monitor community provides access to all SNMP attributes with read-only access. The control community provides read-write access or SET privileges.

To enable Insight Manager to perform SET operations on server parameters on a NetWare server, you must load the *SNMP.NLM* with a community string specified for the control community. If the *SNMP.NLM* is loaded without specifying either community, it uses *public* as a default monitor community and disables the control community. This default condition means that no read-write access is allowed; therefore, no SNMP SET commands will function.

NOTE: This is the same default as Compaq Insight Manager. If you enter a different community string, you must also enter it on the management PC that is responsible for the server. To change the community string in Insight Manager, select the *Server Setup* button from the Task List Window. This opens the Server Setup Window, where the community string can be set. For more information on community strings, refer to the *Compaq Insight Manager User Guide*.

The community string usage is described below:

■   Monitor Community

This community string has a 32-character maximum which is to be used for read-only access to the SNMP attributes. If you do not specify the MONITOR COMMUNITY parameter, the *SNMP.NLM* uses *public* as the default community string. Since there will always be a MONITOR COMMUNITY string, there will always be read-only access. Community names are case-sensitive.

■   Control Community

This community string has a 32-character maximum which is to be used for read/write access to the SNMP attributes. If the CONTROL COMMUNITY parameter is not specified, the *SNMP.NLM* disables all read-write access. Community names are case-sensitive.

Table 5-4 provides some examples on providing access to the following communities:

Table 5-4
NetWare SNMP Community Access Configuration Examples

Access Rights	Community String
Read-only	Monitor = HELPDESK Control = \<Blank>
Read-only and Read/Write	Monitor = HELPDESK Control = ADMIN
Read/Write	Monitor = \<Any string> Control = ADMIN

NOTE: For configuring SNMP access for other operating systems, refer to the *Compaq Insight Management Agents User Guide* for each operating system.

> **CAUTION:** *SNMP.NLM* must be loaded before the *TCPIP.NLM* in the *AUTOEXEC.NCF* file to enable set commands or to change the default community string parameters. If you do not load *SNMP.NLM* before *TCPIP.NLM*, the *TCPIP.NLM* file automatically loads the *SNMP.NLM* with default command line parameters and a subsequent LOAD command for the *SNMP.NLM* fails.

For information on installing and configuring the Compaq Insight Management Agents for Microsoft Windows NT, SCO UNIX, UnixWare, and IBM OS/2, refer to the *Compaq Insight Management Agents User Guide* for each operating system.

> **IMPORTANT:** To activate the Compaq Insight Management Agents and the NetExplorer, you must bring down and reboot the server.

Installing Compaq Insight Manager

To configure ManageWise for use with Insight Manager, follow these steps:

1. Start Windows.

    > **IMPORTANT:** If you are currently running ManageWise and you continue with the Insight Manager installation, the installation program will shut down all ManageWise components.

2. Place the SmartStart CD into the CD-ROM drive or the Insight Manager Diskette #1 into the diskette drive.

3. Select *File → Run* from the Program Manager menu.

4. Type [cd drive]:\CIM\INSTALL\SETUP or [diskette drive]:\SETUP, then select *OK*. After a few seconds, the installation program displays a registration window.

5. Fill in the registration information and select the *Continue* button.

6. Select *OK* on the confirmation window to confirm the registration information or select *Retry* to change the registration information.

> **❗ IMPORTANT:**   If you have a previous version of Insight Manager installed, the installation program notifies you that an old version exists and will be unusable if you continue with the installation.

7. Select *OK* to continue with the installation and upgrade your previous version or *Cancel* to quit the installation. If you choose to Cancel, the installation program will abort and preserve your previous version of Insight Manager.

8. Select the checkbox, *Install Compaq Insight Manager 2.5* and *Install ManageWise or NMS Support*, then select *OK* to continue. Do not select the option to install Asynchronous Management.

> ❏ Install Compaq Insight Manager 2.5
> ❏ Install ManageWise or NMS Support
> ❏ Install Asynchronous Management

> **❗ IMPORTANT:**   Asynchronous Management is not supported when Insight Manager is installed under ManageWise.

9. Enter the directory path where you want to install Compaq Insight Manager 2.5. Fill in the information and select *OK* to continue.

10. Enter the location of your *TCPIP.EXE* and *VTCPIP.386* files. Provide the correct path to these files and select *OK*. Select *Cancel* if you do not use the TCPIP stack.

11. Confirm your installation selections, then select *OK* to continue, *Go Back* to change the installation settings, or *Exit Setup* to abort the installation.

12. Upgrade your databases and forms, if necessary, by selecting the appropriate boxes, then select *OK* to continue or *Cancel* if you do not want to update your databases.

   NOTE: The installation program prompts you to update your databases and forms only if you are upgrading an older version of Insight Manager. Also, Insight Manager backs up the currently installed database.

13. Enter the location where you want to install the Compaq Insight Manager program group and select *OK*.

14. Verify all of the installation options you have chosen during the Insight Manager Setup, then select *OK* to proceed with the installation.

The Insight Manager installation is now complete. Follow these steps to complete the integration process.

1. Use the ManageWise Database Administration Tool (or the Database Reset Tool) to reset your database.

2. Edit your *AUTOEXEC.BAT* file if you had a previous version of Insight Manager installed. To do this, open the file and remove any references to the previous Insight Manager path. Also Setup automatically adds the *SHARE.EXE* file and the location of the current version of Insight Manager to the end of the PATH statement.

   NOTE: In MS-DOS, the PATH statement cannot exceed 128 characters. If your PATH statement exceeds this length, you must remove some items to allow room for the Insight Manager directory.

3. Restart the management PC before running Insight Manager. Once you have done this, your installation of Compaq Insight Manager under ManageWise is complete.

   ! IMPORTANT: Be sure to run the NetExplorer Manager so that the console database is updated with the NMS Discovery information from the NetExplorer server. This database contains information on the newly configured Compaq servers. Make sure the Insight Management Agents are running properly before you run the NetExplorer Manager.

Installing and Compiling the Compaq MIBs into ManageWise

This section assumes that you have the ManageWise management PC running successfully. If this is a new installation, your ManageWise management PC needs to complete the automatic discovery process for your network. Depending on your network, this process can take up to several hours.

Integrating the Compaq Insight MIB Files

Insight MIBs can integrate with a ManageWise management PC, allowing you to browse the Insight MIB on any server running the Insight Management Agents. ManageWise can also interpret Insight MIB traps that are sent by the servers running Insight Management Agents.

To integrate Insight MIB files with a ManageWise management PC, follow these steps:

1. Insert the Insight MIBs diskette into the diskette drive of the ManageWise management PC.

2. Change to the MW\NMS\SNMPMIBS\CURRENT directory on the drive where ManageWise is installed. For example:

   C:> CD\MW\NMS\SNMPMIBS\CURRENT

3. Copy all MIB files from the diskette drive to the current directory. For example:

   COPY A:\CPQ_MIB*.MIB

4. Start Windows and open the ManageWise console.

5. Select the SNMP MIB Compiler option from the Tools menu.

6. Select *Compile* to compile all the MIB files in the CURRENT directory of the ManageWise database.

7. Select *Exit* to exit the SNMP MIB Compiler. Do this at the end of the compile process.

This ends the MIB integration procedure for ManageWise.

Configuring ManageWise Alarm Dispositions

You can view Compaq alarms by selecting the *Fault* option, followed by *Alarm Disposition* on the menu bar and change the Alarm Family list box to *SNMP*. These alarms, or traps, have been preconfigured with Severity (critical, major, minor, warning, or unknown) and Object State (operational, degraded, or non-operational). Figure 5-2 illustrates an example of alarm dispositions.
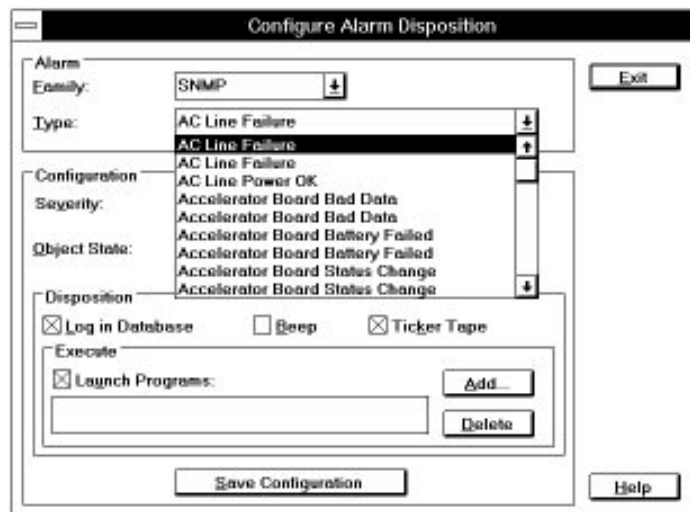
Figure 5-2.   Configuring alarm dispositions

You have the option of launching a program for each trap or alarm. For example, when the ManageWise management PC receives a CPQ SCSI
Logical Drive Status Change alarm, it indicates a status change to the logical drive configuration. If the logical drive configuration includes fault tolerance (RAID 2, RAID 4, or RAID 5), it can still operate, but a problem exists that requires your attention. By default, an alarm disposition appears:

■ On the network management map.

■ In the Alarm Monitor view.

■ Printed and viewed in the Alarm Report.

In addition to logging the alarm, you can have the management PC:

■ Beep.

■ Display a message.

■ Launch an application when the alarm occurs.

If you want to launch an application when an alarm occurs, select the *Launch Programs* box and type the command line for the application. The command line can contain batch or executable files.

The following are customized alarm configurations that you can specify:

■ If you receive the CPQ SCSI Logical Drive Status Change alarm, you can run a batch file that contains the NetWare SEND command that sends a specific message to the ADMIN group.

■ If you have a problem with a specific server, you can launch a communications application with a script to call a beeper number and leave a numerical message that indicates the problem.

You can configure each alarm differently to meet your specific needs. Refer to the *ManageWise 1.0 NetWare Management System Software: Getting Started* document for more information on alarm management.

When you customize alarms for your configuration, ManageWise can interpret the alarms sent by Compaq servers. You can also use the SNMP MIB Browser to build profiles to query Insight MIB objects on Compaq servers.

Compaq Insight Manager Version Differences

Compaq maintains its commitment to network management by continually enhancing its integration with ManageWise. One of the enhancements in Compaq Insight Manager 2.5 is having the knowledge of the ManageWise 1.0 platform. ManageWise 1.0 introduces integration issues that were not present in previous versions of NMS. Two of these issues are:

■ TCP/IP version required by Insight Manager for Remote Control

■ Btrieve patch required by Insight Manager

TCP/IP Version for Remote Control

The version of TCP/IP required by Insight Manager for its Remote Control feature is newer than the version shipped with ManageWise. Compaq Insight Manager can now verify the version of TCP/IP that is currently being used. Insight Manager will then perform the upgrade if necessary.

Configuring Btrieve for Earlier Versions of Insight Manager

Insight Manager and the ManageWise Inventory Manager use two different versions of Btrieve. Insight Manager uses version 5.10 and ManageWise uses version 6.10. These two versions of Btrieve use the same naming convention for their DLL files, but one is for local databases (client-based) and the other is for remote databases (client/server). Having the same name for each DLL file causes incompatibility between the two applications. The Compaq Insight Manager 2.5 installation program applies a Btrieve patch allowing the local version of Btrieve on Insight Manager to run concurrently with other applications that use the remote version of Btrieve.

> **!**   **IMPORTANT:**   Compaq Insight Manager 2.5 or later automatically configures Btrieve to properly run with ManageWise.

If you do not have at least Compaq Insight Manager 2.5, perform the following procedures to allow compatibility between the two applications.

1. Obtain this Windows utility from CompuServe by downloading the self-extracting ZIP file, *BT515.EXE*, from the Current Upgrades Library located in the Btrieve Technologies Forum.

    NOTE: *BT515.EXE* contains the self-extracting ZIP file *BTRREQ.EXE*.

2. Extract *WNDBCNVT.EXE* from *BTRREQ.EXE*.

3. Start Windows after making sure Insight Manager is not running.

4. Select *Run* from Program Manager's File menu, then type *WNDBCNVT.EXE* and select *OK*.

5. Select *Convert* from the Convert menu item and enter the path where Insight Manager is installed, then select *OK*.

    This conversion program saves the *WBTRCALL.DLL* file as *WBTRCALL.SAV*, then the program creates the *WBTRLOCL.DLL* file in the Insight Manager directory.

    After this conversion process is complete, Btrieve will run in both local and remote modes.

6. Exit Windows.

7. Copy (from the DOS prompt) the newly created *WBTRLOCL.DLL* file from the Insight Manager directory to the LANDesk Manager directory. For example:

    COPY C:\INSIGHT\WBTRLOCL.DLL C:\MW\LDT

8. Copy the Client/Server Btrieve files, *WBTRCALL.DLL* and *BTRVRES.DLL*, from the LANDesk Manager directory to the Insight Manager directory as follows:

    COPY C:\MW\LDT\WBTRCALL.DLL C:\INSIGHT

    COPY C:\MW\LDT\WBTRVRES.DLL C:\INSIGHT

9. Enable access to the local Btrieve files. By default, the Windows Requester is not configured for accessing files locally. From the Windows directory, open the *NOVDB.INI* file by typing:

EDIT NOVDB.INI

> **NOTE:** The *NOVDB.INI* file might be called *BTI.INI*.

10. Set the local profile string in the [brequestDPMI] section to *Yes*. For example:

[brequestDPMI]

local=Yes ; allow access to Client-Only Btrieve DLL

11. Press **Alt** + **F** to open the File menu, save changes, and exit the *NOVDB.INI* or *BTI.INI* file.

Upon completion of this procedure, both applications should run properly.

Using Compaq Insight Manager with ManageWise

This section describes how to launch Compaq Insight Manager when running it under ManageWise. This section also describes the differences between the snap-in version and the standalone version of Insight Manager.

Launching Insight Manager from ManageWise

Once you integrate Insight Manager with ManageWise, you can launch Insight Manager by using the Compaq server icon, NetWare server icon, or the Insight Manager option located under the Tools menu.

Launching Insight Manager Using the Compaq Server Icon

To launch Insight Manager from ManageWise using the Compaq server icon, follow these steps:

1. Select a Compaq managed server icon from the ManageWise network management map as shown in Figure 5-3.
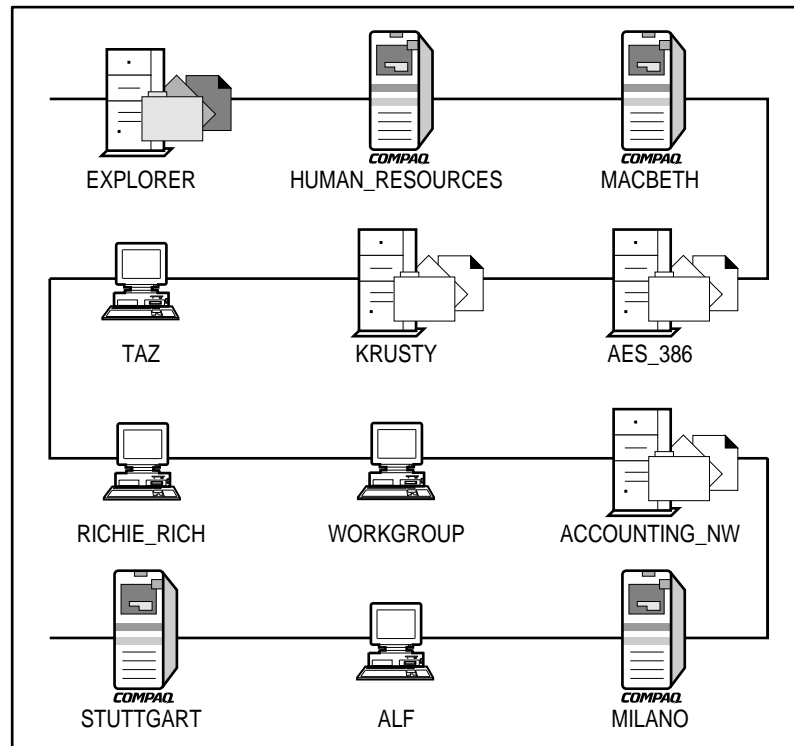
Figure 5-3. Network management map after integration

2. Click again to launch Insight Manager to the designated Compaq server.

Launching Insight Manager Using the NetWare Server Icon

To launch Insight Manager from ManageWise using the NetWare server icon, follow these steps:

1. Select the NetWare server icon located on the network management map shown in Figure 5-3.

   This opens the NetWare Server Configuration window. This is only for servers managed by both Insight Manager and ManageWise.

2. Select the Compaq server icon at the bottom of the NetWare Server Configuration window to launch Insight Manager.

Launching Insight Manager Using the Tools Menu

To launch Insight Manager from ManageWise using the Tools menu, follow these steps:

1. Select the designated server located on the network management map shown in Figure 5-3.

2. Select the Insight Manager option from the Tools menu. This launches Insight Manager.

Differences Between Insight Manager Snap-In Application and Standalone

The standalone version of Insight Manager and Insight Manager under ManageWise are configured differently. Once you integrate Insight Manager with ManageWise, you no longer use the standalone version of Insight Manager. The snap-in application that is used under ManageWise does not contain the following items:

■ The Server List is not available.

   Since Insight Manager is launched from ManageWise or NMS, the server list and the discovery process are provided by the platform.

■ The Server Inaccessible menu item from the Alarms menu is not available.

   The polling process that detects inaccessible servers is not available under the platform, so the alarms will not be generated.

■ The Insight Manager program icon is not installed in the Insight Manager program group.

■ The Server and Task List configuration options are not available.

■ Insight Asynchronous Management is not supported because the platform does not support PPP.

Installing Insight Manager with the Server List

Once the integration process of Insight Manager and ManageWise takes place, the Insight Manager icon does not appear in the Compaq Insight Manager program group, as shown in Figure 5-4. However, the Compaq Insight Manager program group for the standalone application contains the Insight Manager program icon.

Figure 5-4. The Compaq Insight Manager program group
after integration

After integrating the two products, ManageWise launches Insight Manager when you
select a server from the network management map. You cannot view the Insight
Manager Server List once integration occurs. Nevertheless, you can maintain the
integration of Insight Manager into ManageWise and also have the Insight Manager
Server List. However, installing the Server List causes additional network polling by
Insight Manager.

To install Insight Manager with the Server List, follow these steps.

1. Install Insight Manager again.

2. Select only the *Install Compaq Insight Manager 2.5* option. Choose the same
    directory used in the previous install of Insight Manager.

    Also do not choose *Install ManageWise or NMS Support* or the option *Install
    Asynchronous Management*.

> ❏ Install Compaq Insight Manager 2.5
> ❏ Install ManageWise or NMS Support
> ❏ Install Asynchronous Management

Now when Insight Manager is launched from ManageWise, Insight Manager
launches to the correct server, but also displays the list of servers on
the network.

Modifying the Task List Window Setup

When Insight Manager is integrated into ManageWise, the menu item to modify the task list window setup is not available; therefore, the task list window remains the top window by default. This might not be your preference. You can change this setting by modifying the *CIM20.INI* file.

To modify the task list window setup, follow these steps:

1. Exit Insight Manager.

2. Open the *CIM20.INI* file found in the default Windows directory.

3. Modify the parameter ServerTListOnTop in the [Task Manager] section of the INI file to look like the following:

   ServerTListOnTop=0

4. Save, then exit the *CIM20.INI* file.

5. Start Insight Manager again.

Chapter 6
Performance Recommendations

This chapter discusses several performance recommendations that help maximize the performance of Insight Manager and ManageWise while minimizing the load put on the network by the platform. These Compaq recommendations consist of discussions on performance tuning issues such as implementing configuration modifications to specific files and architectural implementation of management agents.

The ManageWise Server

There are several configuration modifications you can make to enhance the performance of the ManageWise server. Some of these modifications require editing files while others require decisions on which programs to load and how to configure them. The following sections discuss the most prevalent configuration modifications to enhance the performance of your ManageWise server.

Designating Only One NetExplorer Server

To help maximize the performance of ManageWise and Insight Manager, designate only one NetExplorer server per network. The NetExplorer server can discover entire networks, including LANs and WANs. The NetExplorer engine requires approximately 8 megabytes of RAM. By not installing the NetExplorer on every ManageWise server, you can allocate this memory for cache buffers. The NetExplorer engine also can cause slow performance due to the polling cycles for discovering the network.

> **!** **IMPORTANT:** Because the NetExplorer server can discover all devices within the entire network and it requires a large amount of resources, Compaq recommends not installing it on every server on which you are going to run ManageWise. However, if you manage a regional area WAN, designate one NetExplorer server for each region on your network.

Limiting NetExplorer Server Discovery

Because the NetExplorer's function is to discover all devices within an entire network, you need to specify or limit these discovery areas to only those networks you want to monitor. By limiting the NetExplorer's scope, you can:

■ Reduce traffic on the network.

■ Limit the view of the network.

■ Discover the desired IP and IPX network segments

IPX scoping allows you to selectively choose which IPX network(s) the autodiscovery process discovers. By default, the IPX discovery finds all IPX networks in your IPX internetwork. Thus, IPX scoping reduces the number of IPX networks discovered and displayed in the ManageWise Internet Logical Map. Setting up IPX scoping does not completely eliminate the NetExplorer IPX traffic outside the specified networks. IPX discovery periodically tries to see whether there are any new IPX addresses that match one of the specified networks.

IP scoping allows you to expand the discovery of your IP networks. The IP discovery default mode is to discover an entire IP network where the NetExplorer is directly attached, as defined by the class of the IP network. IP scoping extends the discovery of additional IP networks by adding IP network addresses to the *NXPIP.INI* file. You must manually create and place the *NXPIP.INI* file in the following directory:

SYS:\NMDISK

If your IP network is connected to the Internet, use caution with the IP scoping feauture because you might unintentionally start discovering the Internet.

For more information on limiting the NetExplorer server scope, refer to the *ManageWise 1.0 Setup Guide* document available from Novell, or refer to the sample *NXPIP.INI* and *NXPIPX.INI* files listed in the next two sections of this chapter.

For more information on the discovery process of the NetExplorer server, refer to the *ManageWise 1.0 NetExplorer Discovery System* document available from Novell.

Sample *NXPIPX.INI* File

The following sample *NXPIPX.INI* file illustrates how to limit the NetExplorer's discovery to one set of servers on one network. The first reference to *IPXQNET=00000002* limits the discovery to network 2. This is valuable information if there are several segments on the network.

The second reference to *IPXQNET=107?????* limits the discovery only to the servers that have internal IPX network numbers matching the pattern 107xxxxx. The discovery limit defined here would discover servers with internal network numbers such as 10705007, 10731001, and 1073500A, but not discover servers with an internal network number of 1275583F.

```
REM
REM gStandAloneTest = 0
REM gPlayback = 0
REM gFixTimeOut = 0
REM
REM gTestData = 0-0-0-0-0-0-0-0-0-0-0-0-0-0
REM gTestServerName =
REM

REM *** ADDED TO LIMIT THE SCOPE OF THE NETWORK
REM *** DISCOVERY TO THE MAIN CORPORATE SEGMENT

IPXQNET=00000002

REM *** LIMIT SCOPE TO DISCOVER ADDITIONAL SERVERS IN THE
REM *** ENGINEERING GROUP (BY INTERNAL IPX NETWORK NUMBER).


IPXQNET=107?????
```

Sample *NXPIP.INI* File

The following sample *NXPIP.INI* file illustrates how to limit the discovery of IP networks and machines. In the sample *NXPIP.INI* file there are entries that reference specific machines (.003) and entries with wild cards (???). These wild card entries allow the discovery of other IP network segments.

```
131.168.190.???
131.168.190.50
172.25.67.003
192.7.1.???
```

Tuning the LANalyzer Agent for Optimum Network Monitoring Efficiency

ManageWise, by default, installs the LANalyzer Agent on every ManageWise server; however, not every server needs to monitor network traffic. This default requires you to deactivate the LANalyzer Agent monitoring for all servers you do not want monitoring a network segment. To deactivate the LANalyzer Agent, change the line located in the *AUTOEXEC.NCF* that executes the *LANZ.NCF* to the following:

```
REM LANZ.NCF
```

To fully diagnose network problems, ManageWise requires only one server per network segment to load the LANalyzer Agent for monitoring network traffic.

Sample *LANZ.NCF* File

The following sample *LANZ.NCF* file illustrates how to configure the NetWare LANalyzer Agent to allocate additional resources. By modifying the *LANZ.NCF* file, you can:

■ Capture a larger set of packets for network traffic diagnostics.

■ Connect to the LANAlyzer agent with multiple consoles.

The following sample illustrates a *LANZ.NCF* file:

```
#                 NetWare LANalyzer Agent
#                     Version 1.0
# LANZ.NCF: NetWare LANalyzer Agent Load File

# This NCF file is created by the NetWare LANalyzer Agent install program. It is used to
# load the NetWare Loadable Module files that make up NetWare LANalyzer Agent.

# WARNING:  You should not modify this file unless you need to change one of the
# configuration parameters documented below. Other changes to this file are not
# recommended.
#------------------------------------------------------------------------------
LOAD LANZSU.NLM
LOAD LANZMEM.NLM bound=10000
LOAD LANZLIB.NLM
LOAD LANZDI.NLM
LOAD LANZAEL.NLM
LOAD LANZHIS.NLM
LOAD LANZFCB.NLM
LOAD LANZSM.NLM topn=10
LOAD LANZTR.NLM
LOAD LANZCTL.NLM trapreg=1
```

To modify *LANZ.NCF* file, follow these steps:

1. Open the *LANZ.NCF* file, then add the parameter, bound=10000, to the LOAD LANZMEM.NLM line so that it looks similar to the following:

   LOAD LANZMEM.NLM bound=10000

   NOTE: This parameter allows the agent to dynamically allocate more memory.

2. Add the parameter, TOPN=10, to the LOAD LANZSM.NLM line so that it looks similar to the following:

   LOAD LANZSM.NLM topn=10

   NOTE: This parameter allocates additional resources to handle the load required when multiple consoles connect to the agents.

3. Save and exit the *LANZ.NCF* file.

4. Unload all of the LANalyzer agents by typing in the following command at the file server console:

   ULANZ

5. Reload all of the LANalyzer agents by typing in the following command at the file server console:

   LANZ

For more information on the LANalyzer Agent, refer to the *ManageWise 1.0 NetWare Management System Software: Analyzing Your Network* document available from Novell.

Configuring LANDesk Virus Protect

LANDesk Virus Protect is an NetWare Loadable Module that prevents viruses from being introduced onto NetWare servers, personal computers, or any other devices on your network. You can configure this application to scan (continuously or on-demand) all of the file servers and personal computers on your network. When and how often LANDesk Virus Protect scans the server remains at your discretion. However, you can affect the performance of the server if you choose a scanning time during peak periods of network traffic.

You can configure Virus Protect to scan network volumes using the following parameters:

■ Scan only the files being written to the server

■ Scan only the files being read from the server

■ Scan all files at all times

Obviously, the more often you scan files the greater the impact on server performance. If you choose to install Virus Protect, Compaq recommends a combination of the performance and protection parameters. You can achieve this balance by scanning only the files being written to the server. By choosing the combination of performance and protection, you accomplish several things:

■ Prevent the server from scanning all network applications

■ Ensure Virus Protect scans all new files introduced to the server

NOTE: To manually scan for viruses on your server, use the LANDesk Virus Protect option located on the NetWare Management Map Menu.

For more information on LANDesk Virus Protect, refer to the *ManageWise 1.0 LANDesk Manager Tools* document.

The ManageWise Console

You can make several configuration modifications to enhance the performance of the management console. Some of these modifications require editing files while others are informational tips on using the console applications.

Memory Tuning

To enhance memory resources, ensure that at least 512 kilobytes of memory is available on your system before launching Windows. By doing this, you allow the Windows resources to allocate the maximum amount of memory available for ManageWise and Compaq Insight Manager.

You need 75 percent of the Windows resources available so ManageWise and Insight Manager can open the maximum number of windows possible. The less memory you have on your system, the fewer number of windows can be opened. This constraint could hinder the effectiveness of ManageWise and Insight Manager on your network. For example, if you do not have enough available resources, you cannot open the number of windows that might be required to diagnose the problem.

To ensure that at least 512 kilobytes of memory is available on your system, follow these steps:

1. Add the NOEMS parameter to the *EMM386.EXE* command line within your *CONFIG.SYS* file. For example:

   DEVICE=C:\DOS\EMM386.EXE NOEMS

   NOTE: The NOEMS parameter provides access to extended memory but prevents access to expanded memory; therefore, makes more upper memory available for TSRs (Terminate and Stay Resident).

2. Load as many drivers and TSRs as possible into high memory.

   NOTE: If you are running MS-DOS 6.22 or above, run *MEMMAKER.EXE*, found in the C:\DOS directory, to configure the loading of your drivers into upper memory optimally.

3. Remove any unnecessary drivers not needed for ManageWise such as your CD-ROM drivers.

4. Use the multiple boot configuration option in MS-DOS 6.22 to help load only the necessary drivers.

For more information on configuring MS-DOS memory and multibooting using MS-DOS 6.22, refer to the documentation provided with the MS-DOS Manuals, or refer to the sample *CONFIG.SYS* and *AUTOEXEC.BAT* files.

Sample *CONFIG.SYS* File

The following sample file illustrates how to edit the *CONFIG.SYS* file to configure the boot process and memory of your console optimally.

Multiple boot configurations allow you to load into memory only the drivers necessary to boot the console. For example, under the [DOS] configuration section the *CONFIG.SYS* file loads drivers to support a CD-ROM drive. Under the [MANAGEWISE] configuration section there is no support for a CD-ROM drive. By using this configuration, you can:

■ Maximize the amount of memory available when running ManageWise.

■ Access the CD-ROM.

The *CONFIG.SYS* file also contains several settings for memory and performance tuning. To maximize the amount of MS-DOS base memory before entering Windows, load all device drivers (or as many as possible) into high memory by using the DEVICEHIGH command. Your command lines should look similar to the following:

    DEVICEHIGH=FS2_ASPI.SYS/1

    DEVICEHIGH=FS2_CD.SYS /D:CDROM1

Finally, the *CONFIG.SYS* file also contains bracketed options such as [menu]. These options are *tokens* (or key words) to MS-DOS. Items that follow the [menu] option define the multiboot configuration selection menu. For example, the command line that is responsible for the ManageWise Configuration option is as follows:

    menuitem=MANAGEWISE,ManageWise Configuration

NOTE: Each configuration option defined in the [menu] section has a corresponding section in the *CONFIG.SYS* and *AUTOEXEC.BAT* files.

The following sample illustrates a *CONFIG.SYS* file:

```
[menu]
menuitem=DOS,DOS Configuration with CD-ROM
menuitem=MANAGEWISE,ManageWise Configuration
menudefault=MANAGEWISE,10

[DOS]
SHELL=C:\DOS\COMMAND.COM /P /E:1536
STACKS=9,256
DEVICE=C:\WINDOWS\HIMEM.SYS
DEVICE=C:\WINDOWS\EMM386.EXE NOEMS x=F000-F5FF
DOS=UMB
DOS=HIGH
BUFFERS= 40
FILES= 100


LASTDRIVE=Z

[MANAGEWISE]
SHELL=C:\DOS\COMMAND.COM /P /E:1536
STACKS=9,256
DEVICE=C:\WINDOWS\HIMEM.SYS
DEVICE=C:\WINDOWS\EMM386.EXE NOEMS x=F000-F5FF
DOS=UMB
DOS=HIGH
BUFFERS= 40
FILES= 100
LASTDRIVE=Z
```

Sample *AUTOEXEC.BAT* File

The *AUTOEXEC.BAT* file also contains several settings for memory and
performance tuning just like the *CONFIG.SYS* file. To maximize the amount of
MS-DOS base memory before entering Windows, load all TSRs (or as many as
possible) into high memory by using the LOADHIGH command. Your command
lines should look similar to the following:

    LH DOSKEY /INSERT /KEY_BUFFER=128

    LH SHARE

    LH brequest /r:26

NOTE: Load your network drivers into high memory as well.

Secondly, the *AUTOEXEC.BAT* file uses the MS-DOS *SMARTDRV.EXE* file.
SMARTDrive is a disk-caching executable file that comes with MS-DOS. The
SMARTDrive file loads two parameters that help boost performance. They are:

    C+   1024

The first parameter (C+) tells SMARTDrive to use delayed writes when writing to
the C: drive. This helps boost the performance of disk-intensive applications, such
as ManageWise. The second parameter (1024) tells SMARTDrive how much
memory to use for disk-caching.

> **CAUTION:**   Using delayed writes might cause data corruption if a General
> Protection Fault error occurs or the system loses power. For more
> information on disk-caching, refer to the MS-DOS documentation.

NOTE: The number used in the second parameter depends on the amount of memory
on your system. The more memory you have installed on your system, the more memory
you can use for disk-caching.

Finally, the *AUTOEXEC.BAT* file also contains *tokens* (or key words) to MS-DOS. However, *tokens* in the *AUTOEXEC.BAT* file are preceded by a colon rather than being enclosed with brackets like in the *CONFIG.SYS* file.
For example,

:MANAGEWISE

NOTE: Remember the items that follow a token consist of the multiboot configuration selection menu.

The following sample illustrates an *AUTOEXEC.BAT* file:

```
@ECHO OFF
goto %config%
:DOS
SET PROMPT=$P$G
SET TEMP=C:\TEMP
PATH=C:\WINDOWS;C:\CPQDOS;C:\;C:\DOS;
SET PATH=%PATH%C:\NWCLIENT\;C:\INSIGHT

LH MSCDEX.EXE /D:CDROM1
C:\WINDOWS\SMARTDRV.EXE C+ 1024
LH SHARE
GOTO END

:MANAGEWISE
SET PROMPT=$P$G
SET TEMP=C:\TEMP
SET TZ=EST5EDT
SET HELPFILES=C:\MW\NMS\help\*.HLP
PATH=C:\WINDOWS;C:\CPQDOS;C:\;C:\DOS;
SET PATH=%PATH%C:\MW\NMS\BIN;C:\NWCLIENT\;C:\INSIGHT

C:\WINDOWS\SMARTDRV.EXE C+ 1024
@CALL C:\NWCLIENT\STARTNET
LH SHARE
REM *** BEGIN Intel LANDesk Manager Section ***
REM The following line loads the Btrieve TSR (39kbytes)
REM required by Inventory Manager.
LH brequest /r:26
REM ***   END Intel LANDesk Manager Section ***
GOTO END
:END
```

Launching Compaq Insight Manager

Another recommendation that could help enhance performance is to leave Compaq
Insight Manager running after you launch it for the first time and minimize the
program to an icon. This allows Insight Manager to receive traps. Also by leaving
Insight Manager running in the background, you do not have to wait for the
program to load into memory the next time you need to look at
a server.

NetExplorer Manager

The final recommendation is to run NetExplorer Manager only when necessary. If
your network is reasonably static, there is no need to run NetExplorer Manager
continually. Only execute the NetExplorer Manager when you initially launch
ManageWise or when you make any changes to the network. By doing this, you can
remove some of the input/output and processor load off your system.

However, if you decide not to run NetExplorer Manager continuously,
consult the *ManageWise 1.0 NetWare Management System Software:
Getting Started* document.

NOTE: The default configuration for NetExplorer Manager is to run continuously.

Chapter 7
Server Management Solutions

This chapter provides innovative server management solutions using Compaq Insight Manager with ManageWise. We have discussed in previous chapters how to integrate Insight Manager with ManageWise and the preinstallation considerations and recommendations involved with each product. This chapter presents scenarios you might encounter in your environment and our recommendations for solutions to these network management scenarios, which include:

■   Determining why the network is running slow

■   Planning for capacity needs

■   Controlling servers on the network without using RCONSOLE

■   Polling groups of devices on the network

■   Managing clients

Compaq has integrated Insight Manager with ManageWise to provide your network with the most comprehensive hardware fault management available on the market. By using Compaq Insight Manager with ManageWise, users have the ability not only to prevent hardware problems, but also diagnose operating system issues. Compaq provides end-to-end, tested, and proven management solutions through the integration of Insight Manager and ManageWise.

Table 7-1 lists the most prevalent ManageWise icons used in the procedures located in this chapter. Table 7-1 provides the ManageWise icon and icon name. If you are unfamiliar with ManageWise, use this table to familiarize yourself with the icons; otherwise, proceed to the first solution "Determining Why the Network is Running Slow."

Table 7-1
ManageWise Icons

Icon Name	Icon
Performance Statistics for a Selected Segment	
Create a New Packet Capture Buffer	
Performance Statistics for Stations	
Start the Connectivity Test	
Control Workstation	
Save	

Determining Why the Network is Running Slow

When the network is not performing optimally, your company is less productive and therefore potentially can lose money. The ability of Insight Manager to monitor Compaq hardware coupled with the ability of ManageWise to monitor the network infrastructure provides a proactive approach to determining network problems. The method used for diagnosing network problems with Insight Manager and ManageWise is as follows:

■ Receive notification of a potential network problem

■ Verify the problem on the network

■ Determine cause of the problem

■ Analyze the cause(s) of the problem

Using Insight Manager to Determine Network Problems

The ability to monitor hardware at a low level allows you to pinpoint where and when you have a network problem. Insight Manager provides this information by giving you the ability to set user-defined thresholds on various Ethernet and Token Ring NIC statistics.

To manage your network proactively, you must determine which NIC statistic listed in Table 7-2 or 7-3 is best suited to monitor. However, to accomplish this task you must first determine:

■ Your network configuration

■ A baseline for your network traffic

Tables 7-2 and 7-3 provide a brief description of receive and transmit statistics that can occur within a NIC. Use these tables to determine which statistic type best describes potential problems you might have on your network, then follow the procedures immediately following the tables to set the appropriate threshold for that statistic type.

Table 7-2
Ethernet Receive Statistics

Error Type	Description
Total Packets	The number of unicast, non-unicast, discarded, error, and unknown protocol packets received for this interface. This value is for total packets received on the interface. Since you may have multiple interfaces on one NIC, this value might not represent the total number of packets received by the NIC.

continued

Ethernet Receive Statistics *continued*

Error Type	Description
Alignment Errors	The number of alignment errors that have occurred for this interface after the network interface supporting software was loaded. The alignment of a frame is checked by the receiver after the packet has failed the Cyclical Redundancy Check (CRC). Misaligned packets do not end on an 8-bit boundary. All packets contain a set number of bytes and must end after a defined number of bytes. Packets that do not end on a byte boundary fail the alignment check.
Frame Check Sequence (FCS) Errors	The number of FCS errors that have occurred for this interface after the network interface supporting software was loaded. The FCS field contains a 4-byte Cyclic Redundancy Check (CRC) value. The transmitting station calculates the CRC while sending the packet. The CRC value is placed in the FCS field. The receiving station calculates the CRC while receiving the packet, and matches the resulting value against the contents of the FCS field. If the numbers do not match, an FCS error has occurred.

Track and resolve these errors. The two primary causes of FCS errors are cabling and component problems.

If you receive FCS Errors, check to see whether you have Alignment errors or Late Collision errors. Cabling problems, such as shorts or noise caused by electromagnetic interference, are most likely to blame for CRC/Alignment errors. Improper cabling (not following cable specifications) is the most likely cause for late collisions. If a network is experiencing an increasing number of late collisions, or CRC/alignment errors, check for potential cabling problems. |
| Frame Too Long Errors | The number of times a receiving station found an oversized frame for this interface after the network interface supporting software was loaded. To avoid processing corrupt packets, the receiving station checks several packet characteristics, including the frame size. If a frame is larger than 1518 bytes (including the FCS field), it is considered oversized. |

continued

Ethnernet Receive Statistics *continued*

Error Type	Description
MAC Received Errors	This item increments each time an error occurs for this interface that does not fall into any of the other error categories shown on the screen. For example, this item increments if a frame that is too short is detected. If you see an excessive number of these errors, use a network analyzer to check for short frame errors. The NIC might need to be replaced.

NOTE: For additional information on the causes and resolutions to these NIC statistics, refer to the Compaq Insight Manager Online Help.

Table 7-3
Ethernet Transmit Statistics

Error Type	Description
Total Packets	The number of unicast, non-unicast, discarded, error, and unknown protocol packets received for this interface. This value is for total packets received on the interface. Since you may have multiple interfaces on one NIC, this value might not represent the total number of packets received by the NIC.
Carrier Sense Errors	The number of frames transmitted with carrier sense errors for this interface after the network interface supporting software was loaded. The carrier sense signal is an ongoing activity of a data station to detect whether or not another station is transmitting. Carrier sense errors are detected when a station transmits a frame and does not detect its own signal on the wire.
Late Collisions	The number of late collisions that have occurred for this interface after the network interface supporting software was loaded. Late collisions might be a symptom of cabling problems. A late collision is one that occurred 64 bytes or more into the packet.

continued

Ethernet Transmit Statistics *continued*

Error Type	Description
Excessive Collisions	The number of Excessive Collisions that have occurred for this interface after the network interface supporting software was loaded. A station might attempt to transmit up to 16 times before it must abort the attempt. Once the abort occurs, this counter increments. If you see an increase in deferred transmissions as well as excessive collisions, your network is extremely busy and this segment of the LAN is overcrowded. Reduce the traffic by reorganizing your LAN or adding a NIC to the server. For example, if you have 100 stations on one Ethernet bus, you may want to break it into two Ethernet buses by adding a NIC to your server. In this way you can balance the load by putting 50 stations on one bus and 50 on the other. If there are a few isolated stations creating the traffic, you may want to put them on a separate bus.
MAC Transmit Errors	This item increments each time an error occurs for this interface that does not fall into any of the other error categories shown on the screen. For example, this item increments if a frame that is too short is detected. If you see an excessive number of these errors, use a network analyzer to check for short frame errors. The NIC may need to be replaced.
Multiple Collisions Frames	This item shows the number of multiple collisions that have occurred for this interface after the network interface supporting software was loaded. Multiple collisions are frames involved in more than one collision before being successfully transmitted. These errors mean that the network is experiencing moderate to heavy traffic. If multiple collisions become more frequent, the count for excessive collisions escalates.
Single Collision Frames	This item shows the number of single collisions that have occurred for this interface after the network interface supporting software was loaded. Single collisions are frames that are involved in a single collision and then are transmitted successfully. These errors show that the network has light to moderate traffic. If single collisions become more frequent, the count for multiple collisions escalates.

Ethernet Transmit Statistics   *continued*

Error Type	Description
Deferred Transmits	This item shows the number of frames that were deferred before transmission because the medium was busy. These are deferred transmissions for this interface after the network interface supporting software was loaded. Frames involved in collisions are not counted. Frames that wait before transmission are counted.

Deferred transmissions occur when the network is extremely busy, so busy that the NIC did not try to transmit. High counts of multiple collisions and excessive collisions also occur. |

NOTE: For additional information on the causes and resolutions to these NIC statistics, refer to the Compaq Insight Manager Online Help.

To set the threshold for the statistic type found in Table 7-2 or 7-3, follow these steps:

1. Launch Insight Manager.

2. Select *View Server Data* from the Insight Manager Task List window. The title of this window reflects the selected server name.

3. Select the *NIC* push button from the Server View window.

4. Select the appropriate NIC by slot number from the NIC Overview window.

5. Select the *View Interface* push button located at the bottom of the Slot *x* NIC window.

    NOTE: The *x* within the NIC window represents the slot number for that NIC.

6. Select the *Advanced* push button from the Statistics window.

7. Select the statistic for which you want to set a threshold. For example, select *Transmit Error: Carrier Sense*.

    You can find all of the NIC statistics in the Ethernet Statistics window.

8. Click the right mouse button to bring up the Options menu for the Transmit Error: Carrier Sense statistic.

9. Click the left mouse button to select *Set Threshold*.

10. Select the *New* push button from the Thresholds window.

11. Enter the new threshold parameters for options such as:

    Value or Delta
    Top and Bottom Thresholds

12. Select the *Set* push button from the Set Thresholds window.

You have now set the threshold so that when this threshold is exceeded the Insight Management Agents send an alert to the console.

Using ManageWise to Determine Network Problems

ManageWise has the ability to monitor the traffic on a particular segment of the network by using the LANalyzer Agent. This allows you to determine which node is causing traffic on a particular segment as well as the contents of that traffic.

For information on installing and configuring the NetWare LANalyzer Agent, refer to the *ManageWise 1.0 NetWare Management System Software: Analyzing Your Network* document.

To use ManageWise to diagnosis network problems, follow these steps:

1. Select the *View* option on the ManageWise menu bar.

2. Select *All* from the View drop down menu.

3. Select *Network Segments* off the View menu.

    This action displays all of the network segments that are currently being monitored.

4. Highlight the segment that you want to monitor.

5. Select the *Performance Statistics for a Selected Segment* icon (shown in
    Table 7-1) from the network segments window.

    This displays the network dashboard along with the top 20 busiest
    stations on the network.

Next, you must determine which server (or stations) is generating the
most traffic. If one of the stations displayed on the dashboard is generating
50 percent or more of network traffic, you need to analyze this server. To do
this, you need to either view the conversations the stations are having with the
server or capture the packets associated with that server to determine the
contents of the traffic.

Viewing Performance Statistics

Viewing the performance statistics and conversations that are occurring
with a particular server, you can determine who is generating the traffic: the
server or the user(s) of the server. To view these performance statistics,
follow these steps:

1. Select the *Performance Statistics for Stations* icon (shown in Table 7-1)
    from the Network Segments window.

    This action brings up the Top 20 Stations Statistics window.

2. Select the server that contains the station conversations you want
    to view.

You are now viewing the performance statistics for stations connected to the
selected server. To further diagnose network traffic, proceed to the "Capturing
Packets" section.

Capturing Packets

Packet capture allows you to view the data that is being transmitted, thus allowing you to further diagnose the root cause of the traffic. To capture packets, follow these steps:

1. Select the *Create a New Packet Capture Buffer* icon (shown in Table 7-1) from the Network Segments window.

   This action brings up the Packet Capture Setup window.

2. Configure the packets you want to capture.

By viewing the actual data being generated (for the entire segment or between two nodes on the segment), you can determine which application is generating the traffic.

NOTE: For more information on configuring the packet capture, refer to the *ManageWise 1.0 NetWare Management System Software: Analyzing Your Network* document.

Now that you have configured each server on your network to alert you when a problem occurs, you can easily analyze, tune, correct and protect your network from excessive traffic.

Planning for Capacity Needs

Not knowing what the expansion possibilities and running out of resources on your server make managing your network difficult. However, Insight Manager and ManageWise can help minimize downtime in order to perform the necessary server upgrades.

After being alerted that the server resources are running low, Insight Manager can view the expansion and upgrade options inside the server. With this upgrade information, you can order the necessary components and schedule server downtime to perform the upgrade. Insight Manager can also determine how quickly this resource is being used up by using the Automatic Data Collection (ADC) feature to trend the server resource utilization.

Determining When Resources are Low

If your NetWare server runs out of cache moveable memory or cache buffers, your server resources are low. When this condition takes place the Compaq Insight Management Agents for NetWare automatically alert the ManageWise console, then you can take corrective action.

You can apply this same methodology to monitoring disk space utilization. You can set a threshold on the drive volume space utilization by using Insight Manager.

To set a threshold for drive space utilization, follow these steps:

1. Launch Insight Manager.

2. Select *View Server Data* from the Insight Manager Task List window. The title of this window will reflect the selected server name.

3. Select the *Mass Storage* push button from the Server View window.

4. Select the volume for which you would like to set a threshold.

    For example, select the SYS volume. All of the file system volumes are located on the Mass Storage Overview window.

5. Click the right mouse button to display the Options menu for drive space utilization.

6. Click the left mouse button to select *Set Threshold*.

7. Select the *New* push button from the Thresholds window.

8. Enter the new threshold parameters for options such as:

    > Value or Delta
    > Top and Bottom Thresholds

    A good example for entering new threshold parameters would be to set the Value threshold to 75. By doing this, you receive an alert when more than 75 percent of the total available space on the file system is utilized.

9. Select the *Set* push button from the Set Thresholds window.

You have now set the threshold for drive space utilization on the network.

Determining the Hardware Upgrade Options

Now that you have set your server thresholds, you are ready to take corrective action when you receive an alert. When an alert occurs, launch Insight Manager to view the current hardware configuration. By viewing your hardware configuration, you can determine the upgrade options available such as a hard drive or memory upgrade.

Determining Hard Drive Upgrade Options

To determine the hard drive configuration upgrade options, follow these steps:

1. Launch Insight Manager.

2. Select *View Server Data* from Insight Manager Task List window. The title of this window reflects the selected server name.

3. Select the *Mass Storage* push button from the Server View window.

4. Select the drive controller associated with the alert generated, such as the system board SCSI controller.

    NOTE: The view of the drive subsystem might vary depending on your server and the controller configuration of your system.

5. View any drive slots and SCSI IDs available on the selected controller.

Viewing the hard drive configuration information allows you to determine your upgrade options. Another key resource you might want to view is the server memory. To do this, proceed to the "Determining Memory Upgrade Options" section.

Determining Memory Upgrade Options

To view the memory configuration of your server, follow these steps:

1. Launch Insight Manager.

2. Select *View Server Data* from the Insight Manager Task List window. The title of this window reflects the selected server name.

3. Select the *Configuration* push button from the Server View window.

4. Scroll down the list box window until you reach the section *Memory Board Identified*.

   This displays each memory board that is in the system including the system board, each SIMM socket, and the size of the SIMM in each socket. If there is no SIMM in the socket, Insight Manager displays the SIMM as *Not Installed*.

Now that you have determined what physical resources are available on each server, you can trend the server utilization to determine how quickly the resources are being used.

Trending Resource Utilization

Insight Manager allows you to determine how quickly the volume space utilization is increasing by using the ADC feature. This Insight Manager feature can gather the volume space utilization data, then provide you with a graph so you can view the latest trend for your network.

Gathering the Data

To use Automatic Data Collection, follow these steps:

1. Launch Insight Manager.

2. Select *Server Setup* from the Insight Manager Task List window. The title of this window reflects the selected server name.

3. Select *Automatic Data Collection* in the upper left hand corner of the Server Setup window.

4. Select *OK*.

!   **IMPORTANT:**   You must allow the ADC feature time to gather the
necessary data in order to trend the volume space utilization information. In
addition, you can perform ADC on a maximum of ten servers simultaneously.

Once you have gathered data, you can view the trend of this information by
following the procedures in the "Viewing the Trend" section.

Viewing the Trend

To view the trend of the volume space utilization data, follow these steps:

1. Launch Insight Manager.

2. Select *View Server Data* from the Insight Manager Task List window.
    The title of this window reflects the selected server name.

3. Select the *Mass Storage* push button from the Server View window.

4. Select the volume for which you would like to display a graph.

    For example, select the SYS volume. All of the file system volumes are
    located on the Mass Storage Overview window.

5. Click the right mouse button to display the Options menu for the volume
    space utilization data.

6. Click the left mouse button to select *Graph*.

    This action displays a graph allowing you to analyze volume space
    utilization.

NOTE: For more information on ADC and Graphing, refer to the *Compaq Insight
Manager User Guide* documentation.

You now have the ability to determine the availability of physical resources and
resource utilization. With this information you can decide when a resource is
running low and rectify the problem before it occurs.

Controlling Servers on the Network Without Using RCONSOLE

Insight Manager can establish a TCP/IP-based Telnet connection to any machine on the network that supports Telnet connections and has Compaq Insight Management Agents installed. This TCP/IP based Telnet connection allows you to run a command line prompt session on any server on your network; therefore, allowing you to perform some configuration and diagnostics on the remote machine.

NOTE: If you have Insight Manager installed with the server list and you have TCP/IP loaded on the workstation, you can remotely control and manage Microsoft Windows NT or any other operating system supported by Compaq that has an active Telnet Daemon.

You can also remotely control a Compaq server without running the network operating system. This enables you to control the server while it is running the Compaq System Configuration program or Compaq Diagnostics. For more information about using the Insight Manager Remote Control feature, refer to the *Compaq Insight Manager User Guide* document.

To control a server remotely using Insight Manager, follow these steps:

1. Launch Insight Manager to the desired server.

2. Select *Remote Control* from the task list window.

    This action displays a Telnet window.

    NOTE: If the desired server has both IPX/SPX and TCP/IP, configure the Server Setup to utilize TCP/IP rather than IPX. If the server is configured with IPX, Insight Manager tries to establish an NVT connection to the selected server. For information on configuring the communications protocol for remotely connecting with a selected server, refer to the *Compaq Insight Manager User Guide* document.

3. Login to the server and activate a Telnet session, then perform the tasks to diagnose or configure the machine.

Without using RCONSOLE to control network servers, Insight Manager allows you to perform the necessary functions to manage network servers properly.

Polling Groups of Devices on the Network

To ensure connectivity, you can selectively group devices on the network and then poll all of these devices. This is extremely effective if you want to monitor a select group of routers to regional offices. Monitoring specific routers and servers eliminates excessive alert messages such as *server inaccessible* due to a router to the region went down instead of the server(s).

To create a group and set up polling intervals for that group, follow these steps:

1. Launch ManageWise.

2. Select *Fault* from the ManageWise menu bar.

3. Select *Test Connectivity*, then *Periodically* from the drop down menu.

    This activates the *Add Target* window.

4. Enter the name, IPX address, or IP address of the machine you want to monitor.

5. Enter the interim time for polling the devices. This is know as the polling interval. The default is 5 seconds.

6. Enter the *Number of Retries*.

    This figure determines how many times the connectivity test can fail before it notifies you that the node is unreachable.

7. Select *Add* to add this new node to the group you are creating.

8. Repeat steps 4 through 7 until all the nodes in the group are added.

9. Click on *Exit*.

10. Click on the *Save* icon (shown in Table 7-1) located on the *Connectivity Test* title bar. This displays the *Save Profile* window.

11. Enter a descriptive file name for this group of devices. For example, *NAROUT1.PRF* (North American Regional Routers 1).

12. Select *OK*.

13. Click on the *Start the Connectivity Test* Icon (shown in Table 7-1) on the *Connectivity Test* window title bar.

    The Connectivity Test runs continuously until you turn it off by closing the *Connectivity Test* window.

This completes creating a group and set up polling intervals for that group.

NOTE: For more information on the Connectivity Test, refer to the *ManageWise 1.0 NetWare Management System Software: Getting Started* document.

Managing Clients

Managing clients on a network is an important task for today's network administrator. ManageWise provides the ability to inventory, control, and diagnose clients on your network; therefore, allowing you to resolve user problems and manage your network more effectively.

NOTE: Compaq Insight Manager will have the ability to provide pre-failure alerting for hard drive failures, thermal warnings, and asset information for Compaq Desktop clients that support Intelligent Manageability with the release of Windows 95.

Client Inventory

To access the ManageWise Client Inventory Control features, follow these steps:

1. Launch ManageWise.

2. Select the desired client from the Network Management Map.

3. Select *Tools* from the ManageWise menu bar.

4. Select *Intel LANDesk Tools*, then *Inventory Manager* from the Tools
    drop down menu. This launches the Inventory Manager program which
    displays the current inventory information for the selected node.

    Additionally, Inventory Manager allows you to view client asset
    information for all nodes connected to the server.

You have now viewed inventory information for the selected machine or node
on the network.

NOTE: Intel provides an upgrade for the LANDesk 1.51 portions of ManageWise to
LANDesk Management Suite 2.0 which supports Compaq Desktop Intelligent
Manageability features.

Client Remote Control

To access the ManageWise Client Remote Control features, follow these steps:

1. Launch ManageWise.

2. Select the desired client from the Network Management Map.

3. Select *Tools* from the ManageWise menu bar.

4. Select *Intel LANDesk Tools*, then *Desktop Access* from the Tools drop
    down menu. This launches the Desktop Access program.

    NOTE: All of the LANDesk Tools are available from the ManageWise
    Tools Menu.

5. Select the *Control Workstation* icon (shown in Table 7-1) from the
    Desktop Access tool bar.

You are now remotely controlling a selected node on the network.

Client Diagnostics

To access the ManageWise Client Diagnostics features, follow these steps:

1. Launch ManageWise.

2. Select the desired client from the Network Management Map.

3. Select *Tools* from the ManageWise menu bar.

4. Select *Intel LANDesk Tools*, then *Desktop Access* from the Tools drop down menu. This launches the Desktop Access program.

   NOTE: All of the LANDesk Tools are available from the ManageWise Tools Menu.

5. Select any of the diagnostics tools built into the Desktop Access application from the Desktop Access tool bar such as:

   ❏ Viewing Workstation Information

   ❏ Displaying CMOS Information

   ❏ Displaying Network Diagnostic Information

NOTE: For more information on managing clients with ManageWise, refer to the *ManageWise 1.0 LANDesk Manager Tools* document.

Inventory management, client diagnostics, and remote control of the client workstations are key components when managing any LAN. These features help you keep the machine running and maintain current records on your network resources.

Accomplishing crucial network management tasks within your business-critical environment is possible when you use Insight Manager with ManageWise. Equipped with these tools you can proactively diagnose network traffic in great detail, plan for future network server resource needs, remotely control servers on the network, periodically determine the connectivity to key nodes on the network, and manage clients. The ability to perform all of these critical tasks from the same platform greatly enhances your ability to easily manage your network and lowers the downtime and cost of ownership.

Appendix A
Using the Compaq
MIB Information

This appendix provides you with information that will help you use Insight
MIBs in your SNMP environment. It includes an overview of the Insight MIBs
organization and identifies and describes categories of information contained
within the MIBs. This appendix also discusses common types of information
that you might want to know about the servers in your network.

Organization of Compaq
Insight MIBs

As stated in Chapter 3 of this TechNote, "Compaq Management Technologies,"
Compaq fully supports the SNMP standard. The assigned enterprise ID for
Compaq is 232. Therefore, all MIB variables maintained by Compaq begin
with the ASN.1 syntax 1.3.6.1.4.1.232.

Compaq has defined several MIBs in the Compaq enterprise. The MIBs are
classified, where appropriate, according to the subsystem of a Compaq server.

Table A-1 lists all the current Insight MIBs and a description of each.

Table A-1
Compaq Insight Management MIBs

MIB Name:	Standard Equipment
Object ID:	1.3.6.1.4.1.232.1
MIB File Name:	*CPQSTDEQ.MIB*

Purpose: Contains information that is available on any ISA or EISA system, including system processor, memory, ISA CMOS, EISA NVRAM, serial port, parallel port, ROM, diskette drives, and IDE-compatible hard drive information.

MIB Name:	System Information
Object ID:	1.3.6.1.4.1.232.2
MIB File Name:	*CPQSINFO.MIB*

Purpose: Contains information about Compaq specific features, including Compaq security features, memory module information, board revision information, asset management information, and other system board specific information.

MIB Name:	Intelligent Drive Array
Object ID:	1.3.6.1.4.1.232.3
MIB File Name:	*CPQIDA.MIB*

Purpose: Contains information about the Compaq Drive Array Controllers and drives connected to these controllers, including the SMART Controller, IDA-2 Controller, IDA Expansion Controller, and IDA Controller.

MIB Name:	Server Manager
Object ID:	1.3.6.1.4.1.232.4
MIB File Name:	*CPQSRVMN.MIB*

Purpose: Contains information about the Compaq Server Manager/R board.

MIB Name:	SCSI Device System
Object ID:	1.3.6.1.4.1.232.5
MIB File Name:	*CPQSCSI.MIB*

Purpose: Contains information about the Compaq SCSI interface products, including SCSI drives and generic SCSI device and controller information. This MIB also includes SCSI tape and CD-ROM information. It does *not* include SMART controller information, which is incorporated into the Intelligent Drive Array MIB.

continued

Compaq Insight Management MIBs *continued*

MIB Name:	Health
Object ID:	1.3.6.1.4.1.232.6
MIB File Name:	*CPQHLTH.MIB*

Purpose: Contains information about system health features, including Critical Error Log, Correctable Error Log, ASR feature, Thermal (temperature and fan) sensing features, POST Message tracking, System lifetime, and EISA bus utilization.

MIB Name:	SCSI Storage System
Object ID:	1.3.6.1.4.1.232.8
MIB File Name:	*CPQSTSYS.MIB*

Purpose: Contains information about the Compaq ProLiant Storage System.

MIB Name:	Threshold Management
Object ID:	1.3.6.1.4.1.232.10
MIB File Name:	*CPQTHRSH.MIB*

Purpose: Contains information about the Insight software components that can generate alarms based on user defined thresholds and can track statistics on attributes based on user input.

MIB Name:	Host Operating System
Object ID:	1.3.6.1.4.1.232.11
MIB File Name:	*CPQHOST.MIB*

Purpose: Contains information about host operating system information. This information includes host OS identification information, CPU utilization information, file system information, NIC interface to hardware mapping information, and loaded modules information.

MIB Name:	UPS
Object ID:	1.3.6.1.4.1.232.12
MIB File Name:	*CPQUPS.MIB*

Purpose: Contains information about the Compaq UPS product.

MIB Name:	Recovery
Object ID:	1.3.6.1.4.1.232.13
MIB File Name:	*CPQRECOV.MIB*

Purpose: Contains information about the Compaq Recovery Server option.

NOTE: Object IDs 232.7 and 232.9 are not currently in use.

Key MIB Information

The Insight MIBs contain many attributes that provide you with a comprehensive picture of the configuration, operating statistics, and general status aspects of the operation of your Compaq servers. However, since there are several hundred MIB attributes, the following discussion focuses on several categories which contain key items on major subsystems within your servers. Once you identify a potential problem area, you can retrieve additional information to assist you with a specific problem resolution.

To simplify the key MIB information, it has been grouped into the following general categories:

■ Configuration

■ Operating Statistics

■ Condition Attributes

The following sections describe each general category and provide detailed subsets within each main category. Detailed information about each attribute is found in the referenced MIB file for each attribute. The MIB files are on the Compaq Insight Management MIBs diskette.

With this information you to construct queries that will provide specific details in monitoring your systems. Compaq has included files on the Compaq Insight Management MIBs diskette for HP OpenView and IBM NetView for AIX, which implement queries based upon these items. See the Compaq TechNote, *Integrating Compaq Insight Manager with Enterprise Management Platforms*, for more detailed information.

Configuration

The MIB attributes in the following configuration categories describe information that is determined at system configuration or operating system load time. The attributes typically do not change as a result of ongoing operation of the hardware or software. MIB attributes in these categories provide you with information about the static configuration of the hardware and software of your system.

General System Description

The attributes in this category describe several items which come from the standard SNMP MIB-II (RFC1213) that are of interest in generally identifying the system. Consult the referenced MIB file, which is included with your management console software, for more information on these attributes.

Table A-2
General System Description Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
System Name	sysName	1.5	*RFC1213*
System Description	sysDesc	1.1	*RFC1213*
System Contact	sysContact	1.4	*RFC1213*
System Location	sysLocation	1.6	*RFC1213*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.2.1. to construct the full ASN.1 number for the item.

Hardware Asset Descriptions

The attributes in this category describe items of a general hardware
inventory nature. Consult the referenced MIB file(s) for more information
on these attributes.

Table A-3
Hardware Asset Descriptions Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Total System Memory	cpqSeTotalMem	1.2.3.2	*CPQSTDEQ.MIB*
Keyboard Description	cpqSeKeyboardDesc	1.2.7.1	*CPQSTDEQ.MIB*
Video System Description	cpqSeVideoDesc	1.2.8.1	*CPQSTDEQ.MIB*
Product Name	cpqSiProductName	2.2.4.2	*CPQSINFO.MIB*
System Serial Number	cpqSiSysSerialNum	2.2.2.1	*CPQSINFO.MIB*
CPU Index	cpqSeCpqUnitIndex	1.2.2.1.1.1	*CPQSTDEQ.MIB*
CPU Name	cpqSeCpuName	1.2.2.1.1.3	*CPQSTDEQ.MIB*
CPU Speed	cpqSeCpuSpeed	1.2.2.1.1.4	*CPQSTDEQ.MIB*
Floppy Disk Type	cpqSeFloppyDiskType	1.2.11.1.1.2	*CPQSTDEQ.MIB*
IDE/ESDI Disk Size(s)	cpqSeFixedDiskCapacity	1.2.12.1.1.6	*CPQSTDEQ.MIB*
SCSI Disk Size(s)	cpqScsiPhyDrvSize	5.2.4.1.1.7	*CPQSCSI.MIB*
Drive Array Disk Size(s)	cpqDaPhyDrvSize	3.2.5.1.1.45	*CPQIDA.MIB*
SCSI Tape Type(s)	cpqTapePhyDriveType	5.4.1.1.1.4	*CPQSCSI.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232. to construct
the full ASN.1 number for the item.

Compaq Software Inventory

The attributes in this category provide information about the Compaq device drivers, Insight agents, and system utilities installed on your system. Consult the referenced MIB file for more information on these attributes.

**Table A-4
Compaq Software Inventory Attributes**

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Software Type	cpqHoSwVerType	2.7.2.1.3	*CPQHOST.MIB*
Software Name	cpqHoSwVerName	2.7.2.1.4	*CPQHOST.MIB*
Software Version	cpqHoSwVerVersion	2.7.2.1.8	*CPQHOST.MIB*
Software Description	cpqHoSwVerDescription	2.7.2.1.5	*CPQHOST.MIB*
Software Location	cpqHoSwVerLocation	2.7.2.1.7	*CPQHOST.MIB*
Software Status	cpqHoSwVerStatus	2.7.2.1.2	*CPQHOST.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232.11. to construct the full ASN.1 number for the item.

Operating System

The attributes in this category provide general information about the operating system (OS) running on your system. Consult the referenced MIB file for more information on these attributes.

Table A-5
Operating System Configuration Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
OS Name	cpqHoName	2.2.1	*CPQHOST.MIB*
OS Version	cpqHoVersion	2.2.2	*CPQHOST.MIB*
OS Description	cpqHoDesc	2.2.3	*CPQHOST.MIB*
File System Description	cpqHoFileSysDesc	2.4.1.1.2	*CPQHOST.MIB*
Total File Space	cpqHoFileSysSpaceTotal	2.4.1.1.3	*CPQHOST.MIB*
Total File Names	cpqHoFileSysAllocUnitsTotal	2.4.1.1.6	*CPQHOST.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232.11. to construct the full ASN.1 number for the item.

Detailed Hardware Configuration

The attributes in this category provide detailed information about the hardware configuration of your system. Consult the referenced MIB file(s) for more information on these attributes.

Table A-6
Hardware Configuration Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Total System Memory	cpqSeTotalMem	1.2.3.2	*CPQSTDEQ.MIB*
System ROM Version	cpqSeSysRomVer	1.2.6.1	*CPQSTDEQ.MIB*
CPU Name	cpqSeCpuName	1.2.2.1.1.3	*CPQSTDEQ.MIB*
CPU Speed	cpqSeCpuSpeed	1.2.2.1.1.4	*CPQSTDEQ.MIB*
Floating Point Co-processor Name	cpqSeFpuName	1.2.2.2.1.4	*CPQSTDEQ.MIB*
Floating Point Co-processor Speed	cpqSeFpuSpeed	1.2.2.2.1.5	*CPQSTDEQ.MIB*
CPU Cache Index	cpqSeCacheLevelIndex	1.2.2.3.1.2	*CPQSTDEQ.MIB*
CPU Cache Size	cpqSeCpuCacheSize	1.2.2.3.1.3	*CPQSTDEQ.MIB*
CPU Cache Speed	cpqSeCpuCacheSpeed	1.2.2.3.1.4	*CPQSTDEQ.MIB*
CPU Cache Status	cpqSeCpuCacheStatus	1.2.2.3.1.5	*CPQSTDEQ.MIB*
Serial Port Address	cpqSeSerialPortAddr	1.2.9.1.1.2	*CPQSTDEQ.MIB*
Serial Port Description	cpqSeSerialPortDesc	1.2.9.1.1.3	*CPQSTDEQ.MIB*
Parallel Port Address	cpqSeParallelPortAddr	1.2.10.1.1.2	*CPQSTDEQ.MIB*
Parallel Port Description	cpqSeParallelPortDesc	1.2.10.1.1.3	*CPQSTDEQ.MIB*
Floppy Disk Type	cpqSeFloppyDiskType	1.2.11.1.1.2	*CPQSTDEQ.MIB*

continued

Hardware Configuration Attributes *continued*

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
IDE/ESDI Disk Size	cpqSeFixedDiskCapacity	1.2.12.1.1.6	*CPQSTDEQ.MIB*
SCSI Disk Model	cpqScsiPhyDriveModel	5.2.4.1.1.4	*CPQSCSI.MIB*
SCSI Disk Firmware Revision	cpqScsiPhyDrvFWRev	5.2.4.1.1.5	*CPQSCSI.MIB*
SCSI Disk ID	cpqScsiPhyDrvScsiID	5.2.4.1.1.8	*CPQSCSI.MIB*
SCSI Disk Size	cpqScsiPhyDrvSize	5.2.4.1.1.7	*CPQSCSI.MIB*
SCSI Tape Model	cpqTapePhyDrvType	5.4.1.1.1.5	*CPQSCSI.MIB*
SCSI Tape Magazine Size	cpqTapePhyDrvMagSize	5.4.1.1.1.7	*CPQSCSI.MIB*
Drive Array Disk Model	cpqDaPhyDrvModel	3.2.5.1.1.3	*CPQIDA.MIB*
Drive Array Disk Firmware Revision	cpqDaPhyDrvFWRev	3.2.5.1.1.4	*CPQIDA.MIB*
Drive Array Disk Size	cpqDaPhyDrvSIze	3.2.5.1.1.45	*CPQIDA.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232. to construct the full ASN.1 number for the item.

Operating Statistics

The MIB attributes in the following operating statistics categories describe the ongoing operation of your system hardware and software.

Hard Drive Read/Write/Seek

The attributes in this category provide information about the number of read, write, and seek operations that are occurring on your system. This information is available for SCSI, IDA, IDA-2, and SMART devices. Over time, this information can be used to determine rates of hard drive usage. Consult the referenced MIB file(s) for more information on these attributes.

Table A-7
Hard Drive Read/Write/Seek Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Drive Array Drive Index	cpqDaPhyDrvIndex	3.2.5.1.1.2	*CPQIDA.MIB*
Drive Array Sectors Read (high)	cpqDaPhyDrvHReads	3.2.5.1.1.10	*CPQIDA.MIB*
Drive Array Sectors Read (low)	cpqDaPhyDrvReads	3.2.5.1.1.11	*CPQIDA.MIB*
Drive Array Sectors Written (high)	cpqDaPhyDrvHWrites	3.2.5.1.1.12	*CPQIDA.MIB*
Drive Array Sectors Written (low)	cpqDaPhyDrvWrites	3.2.5.1.1.13	*CPQIDA.MIB*
Drive Array Seeks (high)	cpqDaPhyDrvHSeeks	3.2.5.1.1.14	*CPQIDA.MIB*
Drive Array Seeks (low)	cpqDaPhyDrvSeeks	3.2.5.1.1.15	*CPQIDA.MIB*
SCSI Drive Index	cpqScsiPhyDrvIndex	5.2.4.1.1.3	*CPQSCSI.MIB*
SCSI Drive Sectors Read (high)	cpqScsiPhyDrvHighRead Sectors	5.2.4.1.1.11	*CPQSCSI.MIB*
SCSI Drive Sectors Read (low)	cpqScsiPhyDrvLowRead Sectors	5.2.4.1.1.12	*CPQSCSI.MIB*
SCSI Drive Sectors Written (high)	cpqScsiPhyDrvHighWrite Sectors	5.2.4.1.1.13	*CPQSCSI.MIB*
SCSI Drive Sectors Written (low)	cpqScsiPhyDrvLow WriteSectors	5.2.4.1.1.14	*CPQSCSI.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232. to construct the full ASN.1 number for the item.

Hard Drive Errors

The attributes in this category provide information about a variety of errors that can occur in the SCSI, IDA, IDA-2, or SMART disk subsystems. This information can be used to pinpoint errors that might occur in the ongoing operation of your system. Consult the referenced MIB file(s) for more information on these attributes.

Table A-8
Hard Drive Error Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Drive Array Drive Index	cpqDaPhyDrvIndex	3.2.5.1.1.2	*CPQIDA.MIB*
Drive Array Hard Read Errors	cpqDaPhyDrvHardReadErrs	3.2.5.1.1.16	*CPQIDA.MIB*
Drive Array Recovered Read Errors	cpqDaPhyDrvRecvReadErrs	3.2.5.1.1.17	*CPQIDA.MIB*
Drive Array Recovered Write Errors	cpqDaPhyDrvRecvWriteErrs	3.2.5.1.1.19	*CPQIDA.MIB*
Drive Array Seek Errors (high)	cpqDaPhyDrvHSeekErrs	3.2.5.1.1.20	*CPQIDA.MIB*
Drive Array Seek Errors (low)	cpqDaPhyDrvSeekErrs	3.2.5.1.1.21	*CPQIDA.MIB*
Drive Array Data Request Timeout	cpqDaPhyDrvDrqTimeouts	3.2.5.1.1.26	*CPQIDA.MIB*
Drive Array Other Timeouts	cpqDaPhyDrvOtherTimeouts	3.2.5.1.1.27	*CPQIDA.MIB*
Drive Array Format Errors	cpqDaPhyDrvFormatErrs	3.2.5.1.1.31	*CPQIDA.MIB*
Drive Array POST Errors	cpqDaPhyDrvPostErrs	3.2.5.1.1.32	*CPQIDA.MIB*
Drive Array Not Ready Errors	cpqDaPhyDrvNotReadyErrs	3.2.5.1.1.33	*CPQIDA.MIB*
Drive Array Spin Up Errors	cpqDaPhyDrvSpinUpErrs	3.2.5.1.1.42	*CPQIDA.MIB*

Hard Drive Error Attributes *continued*

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Drive Array Bus Faults	cpqDaPhyDrvBusFaults	3.2.5.1.1.46	*CPQIDA.MIB*
Drive Array Accelerator Index	cpqDaAccelCntlrIndex	3.2.2.2.1.1	*CPQIDA.MIB*
Drive Array Accelerator Read Errors	cpqDaAccelReadErrs	3.2.2.2.1.7	*CPQIDA.MIB*
Drive Array Accelerator Write Errors	cpqDaAccelWriteErrs	3.2.2.2.1.8	*CPQIDA.MIB*
SCSI Drive Index	cpqScsiPhyDrvIndex	5.2.4.1.1.3	*CPQSCSI.MIB*
SCSI Drive Hard Read Errors	cpqScsiPhyDrvHardReadErrs	5.2.4.1.1.15	*CPQSCSI.MIB*
SCSI Drive Hard Write Errors	cpqScsiPhyDrvHardWriteErrs	5.2.4.1.1.16	*CPQSCSI.MIB*
SCSI Drive Seek Errors	cpqScsiPhyDrvSeekErrs	5.2.4.1.1.20	*CPQSCSI.MIB*
SCSI Drive Timeouts	cpqScsiPhyDrvTimeouts	5.2.4.1.1.23	*CPQSCSI.MIB*
SCSI Drive POST Errors	cpqScsiPhyDrvPostErrs	5.2.4.1.1.24	*CPQSCSI.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232. to construct the full ASN.1 number for the item.

Tape Drive Read/Write Items

The attributes in this category provide information about the number of bytes that have been read or written to the tape device(s) on your system. Consult the referenced MIB file for more information on these attributes.

Table A-9
Tape Drive Read/Write Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
SCSI Tape Index	cpqTapeCountersScsiIdIndex	5.4.2.1.1.3	*CPQSCSI.MIB*
SCSI Tape Read/Write Bytes	cpqTapeCountersTotalBytes	5.4.2.1.1.9	*CPQSCSI.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232. to construct the full ASN.1 number for the item.

SCSI Tape Drive Errors

The attributes in Table A-10 provide information about a variety of errors that can occur in the SCSI tape subsystems. This information can be used to pinpoint errors that might occur in the ongoing operation of your system. Consult the referenced MIB file for more information on these attributes.

Table A-10
SCSI Tape Drive Error Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
SCSI Tape Index	cpqTapeCountersScsiIdIndex	5.4.2.1.1.3	*CPQSCSI.MIB*
SCSI Tape Re-Writes	cpqTapeCountersReWrites	5.4.2.1.1.5	*CPQSCSI.MIB*
SCSI Tape Re-Reads	cpqTapeCountersReReads	5.4.2.1.1.6	*CPQSCSI.MIB*
SCSI Tape Total Errors	cpqTapeCountersTotalErrors	5.4.2.1.1.7	*CPQSCSI.MIB*
SCSI Tape Uncorrectable Errors	cpqTapeCountersTotalUncorrectable	5.4.2.1.1.8	*CPQSCSI.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232. to construct the full ASN.1 number for the item.

Network Interface Controller

The attributes in this category provide information about the operation of the network interface controllers (NICs) in your system. Over time, these can be used to determine rates of use and to identify potential network problems. The items in this category are from the standard MIB RFC1213 (MIB-II), which is included with your management console software. Consult this MIB for further information on these attributes.

Table A-11
NIC Information Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Interface Index	ifIndex	2.2.1.1	*RFC1213*
Bytes Received	ifInOctets	2.2.1.10	*RFC1213*
Bytes Transmitted	ifOutOctets	2.2.1.16	*RFC1213*
Broadcast Packets Received	ifInNUcastPkts	2.2.1.12	*RFC1213*
Broadcast Packets Transmitted	ifOutNUcastPkts	2.2.1.18	*RFC1213*
Packets Received with Errors	ifInErrors	2.2.1.14	*RFC1213*
Packets Transmitted with Errors	ifOutErrors	2.2.1.20	*RFC1213*
Received Packets Discarded	ifInDiscards	2.2.1.13	*RFC1213*
Transmitted Packets Discarded	ifOutDiscards	2.2.1.19	*RFC1213*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.2.1. to construct the full ASN.1 number for the item.

Operating System Resource Utilization

The attributes in this category provide information about operating system resource usage of several key system components. Consult the referenced MIB file for more information on these attributes.

Table A-12
Operating System Resource Usage Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
CPU Index	cpqHoCpuUtilUnitIndex	2.3.1.1.1	*CPQHOST.MIB*
CPU Utilization - One Minute	cpqHoCpuUtilMin	2.3.1.1.2	*CPQHOST.MIB*
CPU Utilization - Five Minute	cpqHoCpuUtilFiveMin	2.3.1.1.3	*CPQHOST.MIB*
CPU Utilization - Thirty Minute	cpqHoCpuUtilThirtyMin	2.3.1.1.4	*CPQHOST.MIB*
CPU Utilization - One Hour	cpqHoCpuUtilOneHour	2.3.1.1.5	*CPQHOST.MIB*
File System Description	cpqHoFileSysDesc	2.4.1.1.2	*CPQHOST.MIB*
File System Size	cpqHoFileSysSpaceTotal	2.4.1.1.3	*CPQHOST.MIB*
File System Space Used (MB)	cpqHoFileSysSpaceUsed	2.4.1.1.4	*CPQHOST.MIB*
File System Space Used (%)	cpqHoFileSysPercentSpaceUsed	2.4.1.1.5	*CPQHOST.MIB*
Total Files Allowed	cpqHoFileSysAllocUnitsTotal	2.4.1.1.6	*CPQHOST.MIB*
Total Number of Files	cpqHoFileSysAllocUnitsUsed	2.4.1.1.7	*CPQHOST.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232.11. to construct the full ASN.1 number for the item.

Hardware Utilization

The items in this category provide information about the utilization of the system hardware resources. Consult the referenced MIB file for more information on these items.

Table A-13
Hardware Utilization Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
System Lifetime Power On Time	cpqHeSysUtilLifetime	2.8.1	*CPQHLTH.MIB*
EISA Bus Utilization - One Minute	cpqHeSysUtilEISABusMin	2.8.2	*CPQHLTH.MIB*
EISA Bus Utilization - Five Minute	cpqHeSysUtilEISABusFiveMin	2.8.3	*CPQHLTH.MIB*
EISA Bus Utilization - Thirty Minute	cpqHeSysUtilEISABusThirtyMin	2.8.4	*CPQHLTH.MIB*
EISA Bus Utilization - One Hour	cpqHeSysUtilEISABusHour	2.8.5	*CPQHLTH.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232.6. to construct the full ASN.1 number for the item.

Fault Identification

The attributes in this category provide the information recorded by the fault recording features of your system. Consult the referenced MIB file for more information on these attributes.

Table A-14
Fault Identification Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Critical Error Type	cpqHeCriticalErrorType	2.2.4.1.3	*CPQHLTH.MIB*
Critical Error Description	cpqHeCriticalErrorDesc	2.2.4.1.6	*CPQHLTH.MIB*
Correctable Memory Error Description	cpqHeCorrMemErrDesc	2.3.4.1.6	*CPQHLTH.MIB*
POST Error Code	cpqHePostMsgCode	2.7.2.1.2	*CPQHLTH.MIB*
POST Error Description	cpqHePostMsgDesc	2.7.2.1.3	*CPQHLTH.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232.6. to construct the full ASN.1 number for the item.

Condition Attributes

To help you focus on the important factors that ensure server reliability, Compaq has developed *condition* MIB attributes. These attributes are a composite of several attributes related to a specific subsystem. If you monitor the condition variables, you receive an accurate picture of the health of your server.

Drive Array

The attributes in this category provide information on the general condition of your Compaq Drive Array Subsystem. When one of these status items become set to "Degraded" or "Failed," you should then query the items specified in the "Hard Drive Errors" section in this appendix to pinpoint the error. Consult the referenced MIB file for more information on these attributes.

Table A-15
Drive Array Status Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Drive Array Index	cpqDaCntlrIndex	2.2.1.1.1	*CPQIDA.MIB*
Controller Condition	cpqDaCntlrCondition	2.2.1.1.6	*CPQIDA.MIB*
Drive Array Accelerator Index	cpqDaAccelCntlrIndex	2.2.2.1.1	*CPQIDA.MIB*
Drive Array Accelerator Condition	cpqDaAccelCntlrCondition	2.2.2.1.9	*CPQIDA.MIB*
Spare Drive Controller Index	cpqDaSpareCntlrIndex	2.4.1.1.1	*CPQIDA.MIB*
Spare Drive Index	cpqDaSparePhyDrvIndex	2.4.1.1.2	*CPQIDA.MIB*
Spare Drive Condition	cpqDaSpareCondition	2.4.1.1.6	*CPQIDA.MIB*
Drive Controller Index	cpqDaPhyDrvControllerIndex	2.5.1.1.1	*CPQIDA.MIB*
Drive Index	cpqDaPhyDrvIndex	2.5.1.1.2	*CPQIDA.MIB*
Drive Condition	cpqDaPhyDrvCondition	2.5.1.1.37	*CPQIDA.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232.3. to construct the full ASN.1 number for the item.

SCSI Disk

The attributes in this category provide information about the general condition of the SCSI disks attached to the SCSI channel(s) of your system. When one of these status items become set to "Degraded" or "Failed," refer to "Hard Drive Errors" section in this appendix. Consult the referenced MIB file for more information on these attributes.

Table A-16
SCSI Disk Status Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
SCSI Controller Index	cpqScsiCntlrIndex	2.2.1.1.1	*CPQSCSI.MIB*
SCSI Controller Bus Index	cpqScsiCntlrBusIndex	2.2.1.1.2	*CPQSCSI.MIB*
SCSI Controller Status	cpqScsiCntlrStatus	2.2.1.1.7	*CPQSCSI.MIB*
SCSI Controller Condition	cpqScsiCntlrCondition	2.2.1.1.12	*CPQSCSI.MIB*
SCSI Drive Controller Index	cpqScsiPhyDrvCntlrIndex	2.4.1.1.1	*CPQSCSI.MIB*
SCSI Bus Index	cpqScsiPhyDrvBusIndex	2.4.1.1.2	*CPQSCSI.MIB*
SCSI Drive Index	cpqScsiPhyDrvIndex	2.4.1.1.3	*CPQSCSI.MIB*
SCSI Drive Status	cpqScsiPhyDrvStatus	2.4.1.1.9	*CPQSCSI.MIB*
SCSI Drive Condition	cpqScsiPhyDrvCondition	2.4.1.1.26	*CPQSCSI.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232.5. to construct the full ASN.1 number for the item.

SCSI Tape Drive

The attributes in this category provide information about the general condition
of the SCSI tape drive(s) attached to the SCSI channel(s) of your system. When
one of these status items becomes set to "Degraded" or "Failed," refer to the
"SCSI Tape Drive Errors" section in this appendix. Consult the referenced MIB
file(s) for more information on these attributes.

Table A-17
SCSI Tape Drive Status Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
SCSI Controller Index	cpqTapePhyDrvCntlrIndex	5.4.1.1.1.1	*CPQSCSI.MIB*
SCSI Tape ID	cpqTapePhyDrvScsiIdIndex	5.4.1.1.1.3	*CPQSCSI.MIB*
SCSI Tape Drive Condition	cpqTapePhyDrvCondition	5.4.1.1.1.6	*CPQSCSI.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232. to construct
the full ASN.1 number for the item.

System Environment

The attributes in this category provide information about the general condition of the environment associated with your system and external storage system. Consult the referenced MIB file(s) for more information on these attributes.

Table A-18
System Environment Status Attributes

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Overall Thermal Condition	cpqHeThermalCondition	6.2.6.1	*CPQHLTH.MIB*
System Temperature Status	cpqHeThermalTempStatus	6.2.6.3	*CPQHLTH.MIB*
System Fan Status	cpqHeThermalSystemFanStatus	6.2.6.4	*CPQHLTH.MIB*
CPU Fan Status	cpqHeThermalCpuFanStatus	6.2.6.5	*CPQHLTH.MIB*
Storage System Type	cpqSsBoxType	8.2.1.1.3	*CPQSTSYS.MIB*
Storage System Index	cpqSsBoxBusIndex	8.2.1.1.2	*CPQSTSYS.MIB*
Storage System Fan Status	cpqSsBoxFanStatus	8.2.1.1.7	*CPQSTSYS.MIB*
Storage System Temperature Status	cpqSsBoxTempStatus	8.2.1.1.9	*CPQSTSYS.MIB*
Storage System Side Panel Status	cpqSsBoxSidePanelStatus	8.2.1.1.10	*CPQSTSYS.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232. to construct the full ASN.1 number for the item.

Fault Identification and Recovery

The attributes in this category provide information about the general condition of the fault identification and recovery features of your system. The logs that record any events are described by the items in the "Fault Identification" section in this appendix. Consult the referenced MIB file for more information on these attributes.

<div align="center">

Table A-19
Fault and Recovery Features Status Attributes

</div>

Data Item Description	MIB Attribute Name	ASN.1 No.	MIB File Name
Automatic Server Recovery Status	cpqHeAsrCondition	2.5.17	*CPQHLTH.MIB*
POST Error Message Recording Status	cpqHePostMsgCondition	2.7.1	*CPQHLTH.MIB*
Correctable Memory Log Status	cpqHeCorrMemLogCondition	2.3.2	*CPQHLTH.MIB*
Critical Error Log Condition	cpqHeCritLogCondition	2.2.2	*CPQHLTH.MIB*

NOTE: The ASN.1 numbers should be prefixed by 1.3.6.1.4.1.232.6. to construct the full ASN.1 number for the item.

Using the MIB Information

The primary usage of the condition attribute is to provide a high-level status of major subsystems within your system. You can monitor these items on a periodic basis. Any change in status indicates that you should investigate the subsystem further. The following sections provide some examples of the types of activities that can be supported by using the MIB information.

Environment

The environment condition attributes provide information on the environmental conditions in and around your system. If one of the attributes become set to "Degraded" or "Failed," you should examine the conditions surrounding your system for a lack of cool air flow or a possible failure of a cooling fan.

System Performance

You can use the attributes in the Hard Drive Read/Write/Seek and Network Interface Controller categories to monitor general system usage. Since many of these attributes are counts, you might want to monitor them on a periodic basis and convert them to rates to better use this information. If you notice continuous high rates, it might be an indication of a potential system overload.

Resource Usage

The usage of system resources can be seen by monitoring the Operating System Resource Utilization and Hardware Utilization categories. If you notice that the operating system file system usage is approaching your acceptable minimum for available space, you might want to plan to archive some files, examine the file systems for unused files that might be candidates for deletion, or consider adding more physical disk drives to increase disk space.

Appendix B
Compaq Trap Overview

Insight Agents generate traps to notify you of events that require action. Some traps enable you to be proactive by warning you of status changes or degraded states. Others require immediate attention.

Depending on the version of Insight Agents loaded on a particular server, you could receive a version 1.*x* type trap or a version 2.*x* type trap.

The version 1.*x* traps defined in the MIBs have a different base identifier, called the *enterprise ID*, for each MIB file (Intelligent Drive Array, SCSI Devices, and so on). The MIB enterprise IDs are the "Object ID" items in the descriptions of the MIBs shown in Table 4-1. For example, the version 1.*x* trap for Intelligent Drive Array is 1.3.6.1.4.1.232.3. The version 2.*x* traps have the same enterprise ID (1.3.6.1.4.1.232) for all traps defined in all of the MIBs.

The enterprise ID combined with the specific trap ID uniquely identify the trap.

Each trap message lists the trap name, the identification number, the description, and the values for the trap variables. The trap variables appear in alphabetical order with a descriptive title indicating an important event has occurred. Immediately following the title is the numerical equivalence for the trap variable listed. By providing you with this message, you can quickly and easily translate the trap variables you receive from your management platform to determine if the trap requires immediate attention.

NOTE: Insight Agents for NetWare (versions 1.0, 1.1, and 1.2) generate version 1.*x* traps. Insight Agents for NetWare (above version 1.2), Windows NT, SCO UNIX, UnixWare, and OS/2 generate version 2.*x* traps.

The Compaq traps described in the following tables are grouped by subject as well as Trap IDs.

Table B-1
Drive Array Traps

Trap Name: cpqDa2LogDrvStatusChange
Trap ID: 3001
Description:

A logical drive status change has occurred. The current status is indicated by the included status variable.

"Bad Connection" status (9) - The physical drive in a Compaq Drive Array is not responding to commands from the array controller. Several causes are possible:

- A drive was removed from the system.
- The data cable connecting the drive to the array has failed.

IMPORTANT: Do not attempt to re-seat any cables while the server is on. Damage to the drives or array controller will result.

- The cable connecting the drive to the array has become loose at either end and must be reseated.
- The cable connecting an external storage subsystem to the server has become loose.
- The power to the drive has been interrupted. This can be caused by a loosened drive power supply cable or a failed power supply in the server or disk subsystem.

Drive Array Traps *continued*

"Failed" status (3) - One or more physical drives have failed. Data is no longer protected on the drive array.

"OK" status (2) - This alarm is typically issued upon completion of repairs to a Compaq Drive Array logical drive. This alarm occurs whenever the logical drive status has returned to a normal state from any other state. In fault tolerant configurations, it is issued following the resolution of the Drive Array Logical Drive Status Change - Rebuilding alarm. In non-fault tolerant configurations, it is issued following the Drive Array Logical Drive Status Change - Failed alarm, after the failed drive has been replaced.

"Overheating" status (10) - The temperature inside an external drive array enclosure has risen above factory preset levels. If the temperature continues to rise, damage to the drives within the enclosure may result. Elevated temperatures may cause erratic operation of a physical drive within the array, causing data loss. This alarm may be caused by the removal of the enclosure cover, which impairs the cooling system performance significantly, or by a cooling fan failure in the drive array enclosure.

NOTE: Do not operate Compaq server and storage products with the chassis covers removed. Airflow inside the unit is interrupted, and proper cooling is not possible. Running with the chassis cover removed also violates the FCC certification and UL listing.

"Ready for Rebuild" status (6) - A failed drive has been replaced, and the system is ready to begin Automatic Data Recovery on the logical drive. This alarm is issued after a failed drive has been replaced or if a drive that previously failed appears to work again after the power is turned on.

NOTE: The system is ready to begin Automatic Data Recovery. Perform an orderly shutdown of the operating system and server, and turn the server off. Turn it on again to begin Automatic Data Recovery.

"Rebuilding" status (7) - Automatic Data Recovery is underway.
"Recovering" status (5) - A physical drive failed within the Compaq Drive Array. The drive array is in a recovery mode. No data has been lost, due to the fault tolerant mode currently in use.

NOTE: At the first available opportunity, replace the failed drive.

continued

Drive Array Traps *continued*

"Shutdown" status (11) - The external drive array has stopped operating because of elevated temperatures. Do not attempt to operate the disk storage subsystem while temperatures are elevated. Severe damage to the disk drives will occur. Elevated temperatures will cause erratic operation of a physical drive within the array, causing data loss. The elevated temperatures can cause physical changes to a hard drive, leading to data corruption. This alarm may be caused by the removal of the enclosure cover, which impairs the cooling system performance significantly, or by a cooling fan failure in the drive array enclosure.

IMPORTANT: If a logical drive shuts down due to high temperatures, data may no longer be available from the server or storage subsystem containing the logical drive. In this case, you may need to physically examine the server or storage subsystem to understand the cause of the alarm. Do not operate Compaq server and storage products with the chassis covers removed. Airflow inside the unit will be interrupted, and proper cooling is not possible. Running with the chassis cover removed also violates the FCC certification and UL listing.

"Wrong Drive" status (8) - During remedial hardware maintenance, the incorrect physical drive was replaced in an array.

IMPORTANT: Do not return the removed drive or the drive indicated as "wrong" for repair. Perform an orderly shutdown of the system, and run Compaq Drive Array Advanced Diagnostics if you need further assistance in identifying failed drives and/or drives installed in the wrong location. You must bring the system down, turn it off, and return the removed drive to its original location. Turn the system back on. After you reinstall the removed drive, identify the correct failed drive.

Drive Array Traps *continued*

"Inactive" status (4) - This alarm signifies that the spare is in a ready state. This alarm is typically issued if you install or replace a spare drive in a Compaq Drive Array. It is issued after you replace a failed spare drive with a new one. This alarm may also occur when a drive fails and the spare becomes active, the failed drive is replaced, and the spare eventually becomes inactive again. In fault tolerant configurations, when a drive fails and a spare drive is available, the storage subsystem begins building data onto that spare. If the failed drive is replaced before restoration has completed, the process halts and the data is restored to the replacement drive instead. If the failed drive is replaced after the build process is complete, the system reconstructs the data to the replacement drive, and the spare will revert to its original inactive state. This keeps a spare drive available. If you have installed or replaced a failed drive in the drive array, this alarm is to be expected.

Trap Name:	cpqDa2PhyDrvStatusChange
Trap ID:	3003

Description:

A physical drive status change has occurred. The current status is indicated by the included status variable.

"Failed" status (3) - A physical drive has failed in a mass storage subsystem. In configurations that are not fault tolerant, this alarm is critical. The mass storage subsystem failed, and server operation stopped. You must replace the failed drive before system operation can begin again. In a fault tolerant configuration, the overall system condition is degraded, but still operational. You may receive additional alarms, such as Drive Array Logical Drive Status Change - Recovering, or Drive Array Spare Drive Status Change - Active.

"OK" status (2) - This alarm indicates an improving condition. This alarm is issued after a physical drive fault has been corrected or when you add a new hot pluggable physical drive.

Drive Array Traps *continued*

Trap Name:	cpqDa2PhyDrvThreshPassedTrap
Trap ID:	3004

Description:

The server issuing this alarm has a drive that exceeded one or more factory preset thresholds for functional degradation. Many Compaq high performance drive array hard drives are "stamped" by the drive manufacturer with minimum functional characteristics. As a result of normal wear and tear, the operation of a hard drive may gradually deteriorate. If certain thresholds are exceeded, the drive may not perform to specified levels, and may be subject to hardware failure sometime in the future. Drives that exceed these thresholds are considered "failed," although true catastrophic failure has not yet occurred. Compaq will replace drives that have exceeded these thresholds, if these drives are still under warranty.

Trap Name:	cpqDa2AccelStatusChange
Trap ID:	3005

Description:

This trap indicates a status change event concerning the drive array accelerator. The current status is indicated by the included status variable.

"Enabled" status (3) - This alarm typically occurs when a Compaq Array Accelerator battery set has fully recharged from a discharged condition. The array accelerator is ready to accept posted writes.

"Permanently Disabled" status (5) - The write cache operations of the Array Accelerator are permanently disabled. Consult the cpqDaAccelErrCode MIB item for further information about why this trap occurred. You can perform an orderly shutdown, and run Compaq Drive Array Advanced Diagnostics if you need further information.

"Temporarily Disabled" status (4) - The Array Accelerator on the drive array controller has been temporarily disabled, due to one of the following reasons:

- The accelerator is holding data, and is configured for a different Drive Array Controller. Make sure the accelerator is installed on the original controller.
- Battery charge level is below 75 percent.
- Sufficient resources to perform posted writes are not available. This may be due to a current rebuilding process.
- The accelerator has failed or has been detached from the IDA-2 Controller.
- The host operating system has temporarily disabled posted writes.

Consult the cpqDaAccelErrCode MIB item for further information about why this trap occurred.

Drive Array Traps   *continued*

Trap Name: cpqDa2AccelBadDataTrap
Trap ID: 3006
Description:
This trap indicates an event concerning the contents of the drive array accelerator. The current accelerator data status is indicated by the included status variable.

"None" status (2) - A power loss to the server occurred. The battery-backed Array Accelerator functioned properly and saved all data stored in the cache. When the system is restarted, the stored data will be written to disk.

"Possible" status (3) - When the system was powered up, the battery set was not sufficiently charged. When the batteries are not sufficiently charged, and the system resumes power, the board does not retain stored data. If no data was stored, no data was lost.
Several causes of this alarm are possible:

- If the system was without power for eight days, and the battery packs were on (battery sets activate only if the system loses power unexpectedly), any data stored in the cache was lost.
- The battery set may have a problem. Check the Battery Status for more information.
- The Array Accelerator board has been replaced with a new board that has discharged batteries. No data is lost, and the Array Accelerator will automatically be enabled when the batteries reach full charge.

Trap Name: cpqDa2AccelBatteryFailed
Trap ID: 3007
Description:
This trap signifies that the Insight Agent has detected a battery status change associated with the array accelerator. The current battery status is indicated by the included status variable.

"Charging" status (3) - The battery set power is below 75% of nominal and is being charged.

Drive Array Traps   *continued*

"Degraded" Status (5) - The battery set in the Array Accelerator is operating, but one of the batteries has failed to recharge correctly. This condition jeopardizes the integrity of the battery-backed cache. Replace the Array Accelerator as soon as possible. If allowed to continue, the battery set might fail, and the drive array controller will no longer write data to the Array Accelerator. Server performance may be affected during this time. After the Array Accelerator is replaced, the Drive Array Accelerator Battery Status - Recharging alarm is issued. Once recharged, the alarm Drive Array Accelerator Battery Status - OK is issued, indicating that the array accelerator subsystem is operational.

"Failed" Status (4) - The Array Accelerator can no longer protect data in the cache in the event of a power interruption to the server. Replace the Array Accelerator as soon as possible. The replaced Array Accelerator batteries must reach full charge before the controller will allow data to be written to the Array Accelerator subsystem. Server performance may be affected during this time.

"OK" status (2) - The battery set has reached a fully charged condition.

Table B-2
SCSI Traps

Trap Name: cpqScsi2CntlrStatusChange
Trap ID: 5001
Description:
A SCSI controller status change has occurred. The current status is indicated by the included status variable.

"Failed" status (3) - A SCSI Controller failed. This alarm may be issued with physical drive alarms if the controller cannot communicate with the system.

"OK" status (2) - A SCSI Controller has been replaced. This alarm indicates an improving condition.

SCSI Traps *continued*

Trap Name:	cpqScsi2LogDrvStatusChange
Trap ID:	5002

Description:

A logical drive status change has occurred. The current status is indicated by the included status variable.

"BadConnect" status (9) - Indicates that a physical drive is not responding. Check the cables connected to it.

"Failed" status (3) - Indicates that more physical drives have failed than the fault tolerance mode of the logical drive can handle without data loss.

"OK" status (2) - Indicates that the logical drive is in normal operation mode. No user action is required.

"ReadyRebuild" (6) - Indicates that the logical drive is ready for Automatic Data Recovery. The physical drive that failed has been replaced, but the logical drive is still operating in Interim Recovery Mode.

"Rebuilding" status (7) - Indicates that the logical drive is currently doing Automatic Data Recovery. During Automatic Data Recovery, fault tolerance algorithms restore data to the replacement drive.

"Recovering" status (5) - Indicates that the logical drive is using Interim Recovery Mode. In Interim Recovery Mode, at least one physical drive has failed, but the logical drive's fault tolerance mode lets the logical drive continue to operate with no data loss. You shuld replace the failed drive as soon as possible.

"Unconfigured" status (4) - Indicates that the logical drive is not configured. Insure all of the drive switches are properly set and run the Compaq Configuration Utility.

"WrongDrive" status (8) - Indicates that the wrong physical drive was replaced after a physical drive failure. You need to return the drive incorrectly replaced and replace the failed drive.

continued

SCSI Traps *continued*

Trap Name:	cpqScsi2PhyDrvStatusChange
Trap ID:	5003

Description:

A status change has occurred to a physical drive attached to the SCSI controller. The current status is indicated by the included status variable.

"Failed" status (3) - A physical drive failed in a SCSI mass storage subsystem. Replace the drive.

"OK" status (2) - This alarm indicates an improving condition. When a physical drive error is corrected, this alarm is issued.

"Removed while Failed" status (7) - A SCSI drive installed in the mass storage subsystem has been removed. The removed drive has failed and must be replaced to restore the system to its original configuration. This alarm may be issued if the removed drive was not replaced prior to the time the status was polled by the software.

"Removed while OK" status (6) - A SCSI drive installed in the mass storage subsystem has been removed while operating properly. If the drive was inadvertently removed, return it to its original position.

Trap Name:	cpqTapePhyDrvStatusChange
Trap ID:	5004

Description:

A status change has occurred to a tape drive attached to the SCSI controller. The current status is indicated by the included status variable.

"Degraded" status (3) - This alarm indicates that a reread or rewrite threshold has been exceeded; backup integrity might have been compromised. Follow steps listed under "Failed" status.

"Failed" status (4) - A SCSI tape drive failed. For additional details, check the error status of the backup application. Follow these steps:

1. Clean the tape drive head and try the backup again (refer to your tape hardware user manual for more details on this procedure).
2. If step #1 fails, replace the tape media with new tape media and try the backup again.
3. If step #2 fails, cycle the power on the tape drive and try the backup again.
4. If the above steps fail, replace the drive.

"OK" status (2) - A SCSI tape drive has been replaced. This alarm indicates that the tape drive is now ready for operation.

Table B-3
System Health Traps

Trap Name: cpqHe2CorrectableMemoryError
Trap ID: 6001
Description:
This alarm indicates that a block of memory has failed or is failing and must be replaced
soon. This condition is not generally critical since the memory controller is able to correct
the problem; however, an error of this type indicates that a memory component is failing or
has failed in the server issuing the alarm. The system continues to correct any errors it can.
Correct the problem as soon as possible. Further degradation of the memory components
may occur, and then errors may no longer be correctable.

Trap Name: cpqHe2CorrectableMemoryLogDisabled
Trap ID: 6002
Description:
Correctable memory error tracking has been disabled due to excessive alerts. Logging of
correctable memory errors ceases when the error count exceeds a factory preset value
since continuing to log errors after the preset number is reached affects performance of the
server. This alarm indicates a failing or failed memory module. Though this alarm is not
critical, an error of this type indicates that a memory component is failing or has failed in
the server issuing the alarm. The system continues to correct any errors it can.

Trap Name: cpqHeThermalTempFailed
Trap ID: 6003
Description:
The temperature status has been set to "Failed." The server will be gracefully shut down.
You should monitor the room temperature and air conditioning. Verify that the covers to the
servers are properly installed as this ensures proper air flow within the server box. Verify
that all fans within the server unit are operational.

continued

System Health Traps *continued*

Trap Name:	cpqHeThermalTempDegraded
Trap ID:	6004

Description:

The temperature status has been set to "Degraded." The server's temperature is outside of the normal operating range. The included status variable indicates how the system will react to this temperature degradation.

"Continue" status (2) - The system is configured to continue operation when this alarm is received. **NOTE:** If the system continues to operate in this degraded condition, the hardware may initiate an immediate and unexpected shutdown.

"Shutdown" status (3) - The system has been configured to initiate a system shutdown when this alarm is received to protect hardware and data from damage or loss.

Trap Name:	cpqHeThermalTempOk
Trap ID:	6005

Description:

Previously abnormal temperatures have returned to a normal state. This is an improving condition.

Trap Name:	cpqHeThermalSystemFanFailed
Trap ID:	6006

Description:

A required system fan status has been set to "Failed." The included status variable indicates how the system will react to this failure.

"Continue" status (2) - The system is configured to continue operation when this alarm is received.

NOTE: If the system continues to operate in this degraded condition, the hardware might initiate an immediate and unexpected shutdown.

"Shutdown" status (3) - The system has been configured to initiate a system shutdown when this alarm is received to protect hardware and data from damage or loss.

continued

System Health Traps *continued*

Trap Name: cpqHeThermalSystemFanDegraded
Trap ID: 6007
Description:
The system fan status has been set to "Degraded." An optional system fan is not
operating properly.

Trap Name: cpqHeThermalSystemFanOk
Trap ID: 6008
Description:
A system fan returned to a normal state from a failed state. This alarm is to be expected
after you replace a failed system fan.

Trap Name: cpqHeThermalCpuFanFailed
Trap ID: 6009
Description:
A system CPU fan failed. The system is configured to continue operation when this alarm
is received.

Trap Name: cpqHeThermalCpuFanOk
Trap ID: 6010
Description:
The CPU fan status has been set to OK. Any previous non-operational processor fans have
returned to normal operation.

Trap Name: cpqHeAsrConfirmation
Trap ID: 6011
Description:
This alarm indicates a return to normal operation. Automatic Server Recovery (ASR) shut
the system down and then restarted the server, which has returned to normal operation.
Other alarms that were issued before this alarm may require action.

NOTE: An ASR reboot does not mean the system is free of faults. The server may be
running in a degraded condition, and must be corrected soon to prevent the fault condition
from escalating into a critical event. If the fault is not corrected, expect another Automatic
Server Recovery reboot at any time.

continued

System Health Traps *continued*

Trap Name: cpqHeThermalConfirmation
Trap ID: 6012
Description:
This alarm is issued when server temperature has returned to acceptable levels, and the
server automatically resumed operation. Ensure that you have corrected the problem that
caused the elevated temperature.

Trap Name: cpqHePostError
Trap ID: 6013
Description:
A Power-On Self Test error occurred during a reboot of the server. This error may have
been noted during the Automatic Server Recovery reboot. The subsystem responsible
for the error may also be responsible for the ASR reboot. The error might include
non-correctable memory errors, fatal hard drive and/or controller failures, and system
board failures. It may not be possible to view the server issuing the alarm, as the network
operating system may have failed to load properly.

Trap Name: cpqHeFltTolPwrSupplyDegraded
Trap ID: 6014
Description:
The redundant power supply subsystem has become degraded. Although the server will
continue to operate, take corrective action soon to restore power redundancy.

Table B-4
Storage Systems Traps

Trap Name: cpqSs2FanStatusChange
Trap ID: 8001
Description:
The status of a storage system fan has changed. The current status is indicated by the included status variable.

"Failed" status (3) - The storage subsystem's internal fan(s) failed. The temperature may soon rise beyond factory preset levels. The storage system may shut down automatically to prevent damage to hardware and data loss.

"OK" status (2) - This alarm is issued when a change occurs in the operating condition of a monitored server's external storage system fan. A fan has been replaced, or has otherwise returned to normal operation. This alarm typically follows the Storage System Fan Status Change - Failed alarm.

Trap Name: cpqSsTempFailed
Trap ID: 8002
Description:
The internal temperature has risen beyond factory preset levels and the storage system may shut down automatically to prevent damage to hardware and data loss. One or more fans may have failed, or a cover is off the storage system issuing the alarm.

NOTE: This alarm is unlikely to occur. If temperatures rise beyond factory preset safety levels, the storage system may shut down. In this case, no data is available to view.

Trap Name: cpqSsTempDegraded
Trap ID: 8003
Description:
The temperature inside a storage subsystem is outside normal operating range. A fan may have failed. If a fan failed, an additional alarm, Storage System Fan Status Change - Failed may also be issued. The storage subsystem is operating without the proper cooling capacity, and internal unit temperatures may soon rise beyond safe levels.

---

continued

Storage Systems Traps *continued*

Trap Name:	cpqSsTempOk
Trap ID:	8004

Description:

Previously abnormal temperatures inside a storage subsystem returned to a normal state. This is an improving condition, and generally requires no further action.

Trap Name:	cpqSsSidePanelInPlace
Trap ID:	8005

Description:

The side panel status has been set to "In Place." The storage system's side panel has returned to a properly installed state.

Trap Name:	cpqSsSidePanelRemoved
Trap ID:	8006

Description:

The side panel status has been set to "Removed." The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.

Trap Name:	cpqSsPwrSupplyDegraded
Trap ID:	8007

Description:

The storage system redundant power supply subsystem has become degraded. Although the storage system will continue to operate, take corrective action soon to restore power redundancy.

Table B-5
User Threshold Traps

Trap Name: cpqMeRisingAlarm
Trap ID: 10001
Description:
Rising Threshold passed. One of the monitored objects has passed the rising threshold. The instances of those objects contained within the variable list are those of the alarm entry that generated this trap.

Trap Name: cpqMeFallingAlarm
Trap ID: 10002
Description:
Falling threshold passed. One of the monitored objects has passed the falling threshold. The instances of those objects contained within the variable list are those of the alarm entry that generated this trap.

Table B-6
Uninterruptible Power Supply Traps

Trap Name: cpqUpsLineFailed
Trap ID: 12001
Description:
The AC power has failed. Once this alarm is issued, power to the server is provided by the Compaq Uninterruptible Power Supply (UPS). Depending on the capacity, the load, and the battery charge level of the UPS, the amount of time the UPS can supply conditioned AC power will vary. If you have enabled Automatic Shutdown, the UPS support software will begin an automatic orderly shutdown of the system when the UPS batteries reach the Shutdown Threshold limit. At this time, the UPS Shutdown in Progress alarm is issued to indicate the shutdown process has begun. If Automatic Shutdown is not enabled, the UPS continues to operate until the power returns or the battery power is exhausted.

---

continued

Uninterruptible Power Supply Traps   *continued*

Trap Name: cpqUpsLineOk
Trap ID: 12002
Description:
The AC line is now active. All electrical devices previously supported by the Compaq
Uninterruptible Power Supply (UPS) are now reconnected to the main AC line. The Compaq
UPS indicates that it is no longer operating on internal batteries.

Trap Name: cpqUpsShutdown
Trap ID: 12003
Description:
This alarm is the result of an extended power loss. The Compaq Uninterruptible Power
Supply (UPS) is about to shut down. If the operating system is configured for automatic
shutdown, this process has begun and should be inspected to make sure it will complete
prior to the shutdown of the UPS.

Trap Name: cpqUpsConfirmation
Trap ID: 12004
Description:
The Compaq Uninterruptible Power Supply (UPS) has returned to normal operation. A power
failure occurred, and the system was shut down. Commercial power was restored, and the
network operating system restarted.

Trap Name: cpqUpsBatteryLow
Trap ID: 12005
Description:
The battery set in the UPS is getting low.

Table B-7
Standby Recovery Server Traps

Trap Name: cpqRsPartnerFailed
Trap ID: 13001
Description:

The Recovery Agent reports that the partner server has failed. This server has taken over the operations of the partner server.

Actions

One of the two servers of a Recovery Server pair has failed. The surviving server has assumed the role of the failed server. A service event should be scheduled to repair the failed server and to restore the Recovery Server pair to its original configuration.

Trap Name: cpqRsStandbyCableFailure
Trap ID: 13002
Description:

The Primary server in a Standby Recovery Server configuration has detected a cable fault condition. This can be caused by disconnecting the serial interconnect cable from the Primary server. Other causes may include failure of the serial port in the Primary server.

Disconnecting the serial cable from the Primary server will cause loss of the heartbeat message at the recovery server. The loss of heartbeat will cause the recovery server to assume that the Primary server has failed. The recovery server will then switch the disks from the Primary server to the recovery server. The recovery server will then boot from the disks. In anticipation of this event, the Primary server operating system will be shutdown in an orderly fashion to prepare for the switchover to the recovery server. A service event should be scheduled to repair the failure and to restore the Recovery Server pair to its original configuration.

Standby Recovery Server Traps *continued*

Trap Name:	cpqRsStandbyFailure
Trap ID:	13003

Description:

The Recovery Server Option Driver reports that the Standby server has failed or the serial interconnect cable to the Standby server is not connected.

Actions:

This trap indicates that the Primary server is no longer receiving an acknowledgment message from the Standby server. This error indicates one of the following possible conditions:

   A. The recovery server has failed.
   B. The recovery server has been powered off.
   C. The serial interconnect cable has been disconnected from the recovery server.

A service event should be scheduled to repair the failure condition and to restore the Recovery Server pair to its original configuration.

**Table B-8
Server Manager/R Traps**

Trap Name: cpqSmBoardFailed
Enterprise ID: 1.3.6.1.4.1.232.4
Trap ID: 1
Description:
Server Manager/R board failure. Schedule maintenance time to run Compaq Diagnostics to determine the problem.

Trap Name: cpqSmBoardReset
Enterprise ID: 1.3.6.1.4.1.232.4
Trap ID: 2
Description:
Server Manager/R board reset. If the board and the software were not able to recover, schedule maintenance time to run the Compaq EISA Configuration Utility to ensure the proper board configuration.

Trap Name: cpqSmServerManagerAlert
Enterprise ID: 1.3.6.1.4.1.232.4
Trap ID: 3
Description:
Threshold exceeded on Server Manager/R monitored item. Monitor which threshold is exceeded to determine what actions to take.

Trap Name: cpqSmCommFailed
Enterprise ID: 1.3.6.1.4.1.232.4
Trap ID: 4
Description:
Server Manager/R asynchronous communications failure.

continued

Server Manager/R Traps   *continued*

Trap Name:	cpqSmBatteryFailed
Enterprise ID:	1.3.6.1.4.1.232.4
Trap ID:	5
Description:	

Server Manager/R battery failure. Schedule maintenance time to replace the failed battery or to replace the board.

Trap Name:	cpqSmBoardTimeout
Enterprise ID:	1.3.6.1.4.1.232.4
Trap ID:	6
Description:	

Server Manager/R board time-out. If the problem persists, run Compaq Diagnostics at the next scheduled maintenance down time.

Trap Name:	cpqSmAlertDestinationBlacklisted
Enterprise ID:	1.3.6.1.4.1.232.4
Trap ID:	7
Description:	

The Server Manager/R is unable to complete a call to a designated alert phone number. Verify the proper Server Manager/R alert configuration.

NOTE: Server Manager/R trap IDs 1 - 7 apply only to Insight Agents for NetWare.

For more details on traps, refer to the *READMIB.TXT* file included on the Insight Agents diskette for the appropriate server operating system.

Appendix C
Multivendor Integration
from Compaq

To help you successfully integrate and optimize your network or multivendor system, Compaq has developed a library of systems integration TechNotes for the NetWare, Microsoft Windows NT, SCO UNIX, and OS/2 operating system environments. TechNotes provide you with important information on topics such as network performance management, server management, and operating system interconnectivity.

You can obtain a copy of a particular TechNote in electronic format by:

■   Downloading the files from the Internet at:

http://www.compaq.com

■   Accessing online files from the SmartStart CD

Pricing

Compaq TechNotes   U.S. $15   (CND $20)*

*Plus shipping & handling

How to Order

To order by PHONE (credit card orders only), call:

■   1-800-952-7689 (In U.S.: 7 a.m. - 7 p.m. C.S.T.)

■   1-800-263-5868 (In Canada: 24 hours)

■   1-317-364-7281 (From outside U.S. & Canada:
     7 a.m. - 7 p.m. C.S.T.)

To order by MAIL or FAX, send complete order information to:

Worldwide:
(except Canada &
France)

Compaq Fulfillment Center
P.O. Box 4100
Crawfordsville, Indiana 47933

FAX: 1-317-364-0787

Canada:

Compaq TechNotes
Compaq Canada, Inc.
111 Granton Drive, Suite 101
Richmond Hill, ON L4B 1L5

FAX: 1-800-668-1835

France:

Compaq TechNotes
Compaq Computer S.A.R.L.
5, Avenue de Norvege
91959 LES ULIS Cedex
France

FAX: 1-331-64-46-51-81

Current TechNotes

Table C-1 lists the current TechNotes available online and in print.

Table C-1
Compaq TechNotes

TechNote Name	Available on SmartStart	Part Number
Compaq Insight Management		
Integrating Compaq Insight Management with Enterprise Management Platforms (8/95)	√	145806-003
Integrating Compaq Insight Management with Microsoft Systems Management Server (8/95)	√	184720-001
Integrating Compaq Insight Management with ManageWise (8/95)	√	182074-001
NetWare		
Performance Management in a NetWare v3.1x Environment (4/93)		133399-002
NetWare Tape Backup Management Using ARCserve from Compaq (4/93)	√	137535-001
NetWare 4 Performance Management (7/94)	√	137989-001
ORACLE Server Planning in a NetWare v3.11 Environment (5/93)		145143-001
NetWare Server Management (9/92)		145231-001
Compaq IDA-2 Configuration for NetWare (12/92)		145536-001
Compaq ProSignia Configuration Guidelines for NetWare v3.x (12/92)		145537-001
Compaq Answers to Technical Support Questions for NetWare Environments (2/95)		145710-002
NetWare SFT III v3.11 Installation (9/93)		145905-001
NetWare Migration from 2.x to 3.12 (6/94)	√	181069-001
NetWare Migration from 3.12 to 4 (11/94)	√	181152-001

continued

Compaq TechNotes *continued*

TechNote Name	Available on SmartStart	Part Number
NetWare (continued)		
SYBASE SQL Server 4.2.2 for NetWare: Tuning and Performance (2/95)	√	184429-001
Performance of Lotus Notes 3.1 on Compaq ProLiant Servers with NetWare 3.1x (2/95)		184430-001
Configuration and Tuning of Oracle7 for NetWare on Compaq Servers (11/94)	√	Not available in bound format
Microsoft		
Implementing Lotus Notes on Compaq Servers with Microsoft LAN Manager (9/92)		145201-001
Microsoft SQL Server and Novell NetWare Requester for OS/2 (9/92)		145376-001
Drive Subsystem Performance with Microsoft LAN Manager 2.1 (11/92)		145517-001
Configuration and Tuning of Microsoft SQL Server for Windows NT on Compaq Servers (7/94)		184207-001
Migrating from Microsoft Windows NT Advanced Server 3.1 to Microsoft Windows NT Server 3.5 (2/95)		184669-001
Compaq Backup and Recovery for Microsoft SQL Server (3/95)		184489-001
Implementing Microsoft Windows NT Server RAS, DHCP, and WINS on Compaq Servers (8/95)		184488-001

continued

Compaq TechNotes *continued*

TechNote Name	Available on SmartStart	Part Number
UNIX		
SCO UNIX in an SNA Environment Using CLEO DataTalker U/X (5/92)		145081-001
SCO UNIX in an SNA Environment Using Computone LYNX (7/92)		145116-001
SCO UNIX Database Servers in Novell Networks (10/92)		145402-001
Printing in SCO UNIX and NetWare Integrated Environments (3/93)		145538-001
SCO UNIX Connectivity to SNA Environments Over X.25 Networks (1/93)		145583-001
Disk Mirroring with VERITAS VxMirror (12/93)		145656-001
SCO UNIX IP Routing Over X.25 Networks (4/93)		145711-001
Performance Tuning for SCO UNIX on Compaq Systems (5/93)		145730-001
Configuration and Tuning of Oracle7 for SCO UNIX on Compaq Servers (11/94)	√	184329-001
The Compaq, SCO UNIX, and ORACLE7 Database Server (9/93)		195818-001
IBM		
Compaq Answers to Technical Support Questions for OS/2 Environments (11/94)	√	Not available in bound format
Performance of Lotus Notes 3.1.5 on Compaq ProLiant Servers with OS/2 2.11 (3/95)		184655-001
Technology Overview		
Configuring Compaq RAID Technology for Database Servers (7/94)	√	184206-001

Glossary

Advanced Error Checking and Correcting (ECC) Memory	A fault tolerance feature that detects and corrects all single-bit memory parity errors, as well as detecting 2-bit and 3-bit memory errors. Ensure that common memory errors including the failure of an entire DRAM chip can be corrected without interrupting system operation.
Alarm	Notification that Compaq Insight Manager displays when certain events happen. For instance, if a monitored item changes, Insight Manager displays an alarm to notify you of the change. Insight Manager stores alarms in the Alarm Log. Alarm is synonymous with Trap. *See also* Trap.
Alarm Forwarding Destination	The pager that you configured to receive the alarms using the alarm forwarding feature. The alarm forwarding feature sends Compaq Insight Manager alarms to an alarm forwarding destination pager.
Alarm Log	Log of all the alarms received at this workstation. If the Alarm Log is full and another alarm occurs, Compaq Insight Manager adds the alarm to the Alarm Log and deletes the oldest entry from the list.
American National Standards Institute (ANSI)	An organization that acts as the national clearing house and coordinator for voluntary standards in the United States. ANSI is the organization representing the United States to the International Standards Organization (ISO). *See also* ISO.
ANSI	*See* American National Standards Institute.
ASR-2	*See* Automatic Server Recovery-2.

AssetControl	Comprehensive set of hardware and software component information reported through integrated hardware, firmware, software, and third-party management tools. AssetControl provides detailed component information including manufacturer, model, and serial number for system, monitor, and hard drive(s). Also provides revision level information for system board, system ROM, Compaq option ROM, and device drivers developed by Compaq.
Asynchronous Management	Management by way of modems and Point-to-Point Protocol (PPP) to communicate with a management PC. For instance, Compaq Insight Manager can use PPP to dial into a server and manage it as if it were part of a local network. The Compaq Insight Management Agents can be configured to send traps through a Point-to-Point connection allowing complete remote management.
Automatic Server Recovery-2 (ASR-2)	Feature designed to restart your server automatically after a critical hardware or software error has occurred. If a critical error occurs, the server records the error in the Server Health Logs, reboots the system, and pages you. *See also* Server Health Logs.
Bridge	Device that connects LANs with compatible addressing schemes, which usually means LANs of the same technology type; for example Ethernet-to-Ethernet, Token Ring-to-Token Ring, Ethernet-to-Token Ring.

Btrieve	A key-indexed record management system designed for high-performance data handling and improved programming productivity. It allows your application to retrieve, insert, update, or delete records either by a key value or by sequential or random access methods.
Community String	A password-like string with a 32-character maximum which is to be used for read/write access to the SNMP attributes.
Compaq Insight Management Agents	Compaq specific software that can query a manageable device and provide information that responds to SNMP requests for data. *See also* SNMP.
Compaq Insight Management MIB	Vendor MIB that describes the fault, performance, and configuration aspects of Compaq products. *See also* MIB.
Corrected Memory Log	A list of corrected memory errors which is stored in non-volatile RAM.
Critical Error Log	A log file that records catastrophic errors, such as non-correctable memory, expansion board, and expansion bus arbitration errors. This file is stored in non-volatile RAM.
Corrected Error Log	A log file that contains the date, time, frequency, and unique information about errors that the various subsystems have automatically corrected, such as Advanced ECC Memory errors. This file is stored in non-volatile RAM.
DHCP	*See* Dynamic Host Configuration Protocol.

Dynamic Host Configuration Protocol (DHCP)	A client-server model that simplifies assigning and maintaining the IP address information and databases. It provides a reliable TCP/IP network configuration, ensures address conflicts do not occur, helps conserve the use of IP addresses through a centralized management address allocation, and allows dynamic configuration of IP addresses for any computer connected to the network.
ECC	*See* Advanced Error Checking and Correcting Memory.
EISA	*See* Extended Industry Standard Architecture.
Element Manager	A software component that monitors and controls a particular type of device on the network, such as a hub.
End-User Desktop Management	Tools which allow a user to view critical system information at the desktop (on the PC).
Enterprise Management	Management of a geographically distributed network containing a wide range of network devices such as computers, bridges, routers, gateways, and modems.
Enterprise Management Platform	A program designed to manage the infrastructure of large corporate networks that have an extensible database and Application Programmers Interface so independent software vendors can write applications to provide enhanced device management.
Enterprise MIB	*See* Vendor MIB.
Ethernet	Network cabling and signaling scheme with a 10 megabits per second rate that works over a wide variety of cabling.

Extended Industry Standard Architecture (EISA)	Open extension to the industry-standard expansion bus architecture, allowing the use of 8-/16-bit peripherals as well as 32-bit devices.
Gateway	Computer that controls the exchange of information between a LAN and a "foreign" computing environment such as a mini-computer or mainframe.
Hub	Device used to connect several network interface controllers (NICs) to a network. The hub is also called a Multi-Access Unit (MAU).
IETF	*See* Internet Engineering Task Force.
Intelligent Manageability	Compaq's industry-leading desktop management strategy enabling desktop PC management capabilities that make networked PCs easier to manage today and tomorrow
IntelliSafe Hard Drives	Compaq hard drives which use a combination of hardware and firmware to predict hard-drive failures before they occur. These drives issue a warning to the user when a drive is likely to fail.
International Organization for Standardization	*See* International Standards Organization.
International Standards Organization (ISO)	An organization which coordinates national standards bodies to promote standardization worldwide. It develops and publishes international standards. The United States representative to the ISO is ANSI. This organization is also called the International Organization for Standardization.
Internet Engineering Task Force (IETF)	The standards oriented group which under the direction of the Internet Architecture Board develops the specifications that become Internet standards.

Internet Packet Exchange (IPX)	NetWare LAN communication protocol; moves data between server and/or workstation running on different network nodes.
Internet Protocol (IP)	The connectionless datagram delivery protocol used by the upper layers of the suite of Internet protocols.
IP	*See* Internet Protocol.
IPX	*See* Internet Packet Exchange.
ISO	*See* International Standards Organization.
LAN	*See* Local Area Network.
LANDesk Desktop Manager	A comprehensive set of desktop management tools that enable you to control and monitor desktops that are attached to the network. These management tools are part of the ManageWise product and reside on the console.
LANDesk Inventory	A ManageWise component that resides on the server which maintains the inventory database and the client inventory scanning components.
LANDesk Inventory Manager	A ManageWise component that resides on the console that displays, queries, and modifies hardware and software inventory information.
LANDesk Virus Protect	A ManageWise component that prevents viruses from being introduced into NetWare servers and desktop PCs. It provides continuous and on-demand scanning on both file server and local desktop drives.
Local Area Network (LAN)	A communications network that serves users within a confined geographical area. A LAN can consist of servers, workstations, a network operating system, and a communications link.

Managed Device	Any network device (router, hub, server) that provides management data; typically one or more management agents execute on the device.
Managed Object	Component of a device that is manageable (for example, network interface, storage subsystem, operating system, active applications, or hardware configuration).
Managed Server	Server with the Compaq Insight Management Agents installed.
Management Agent	Software (for example, Compaq Insight Management Agents) that executes on the managed device, which allows management information to be retrieved or modified by a management application.
Management Application	Software (for example, Compaq Insight Manager) that executes within the context of a management platform, or the native operating system of the management PC, that interacts with management agents.
Management Information Base (MIB)	A set of monitored items that management applications and management agents use to monitor, analyze, and control the operation of managed devices.
Management PC	A network device on which a management platform and management applications execute.
Management Platform	Software providing an open environment for multiple management applications to execute simultaneously; for example, ManageWise, NetView for AIX, HP OpenView, and SunConnect SunNet Manager.
Management Protocol	Set of rules for the network that defines a format and procedures for data transfer.
MAU	*See* Multi-Access Unit.

MIB	*See* Management Information Base.
Monitored Item	A unique attribute that describes a fault, performance, configuration, or security aspect of a component of the managed device, for example, Read Error Count or I/O Bus Utilization.
Multi-Access Unit (MAU)	A central hub in a token ring local area network. *See also* Hub.
Naming Service	Software that converts a name into a physical address on a network, providing logical to physical conversion. Names can be user names, computers, printers, services or files. The transmitting station sends a name to the server containing the naming service software, which sends back the actual address of the user or resource.
NetExplorer	The ManageWise discovery engine that has the ability to discover all devices within an entire network.
NetExplorer Manager	A ManageWise component that resides on the console and controls the timing and duration of updates from the NetExplorer components.
NetExplorer Plus	The NetWare Management System software that provides information to the NetExplorer system about users logged in or attached to the server.
NetWare LANalyzer Agent	A ManageWise component that is a remote monitor that analyzes network segments, provides dynamic data about segments, discovers devices on a segment, and captures packets.
NetWare Management Agent	A ManageWise component that provides real-time server performance data and information about server alarms from the server.
NetWare Virtual Terminal (NVT)	Application that performs offline in-band management.

Network Interface Controller (NIC)	A controller installed in a PC, workstation, or server that allows the PC or workstation to communicate with other devices connected to the same network. This term usually implies a local area network (LAN) controller.
Network Management	Term describing the monitor and control of the network infrastructure (wire and internetwork devices).
Network Transport Protocol	The network protocol used for communicating management information.
NVT	*See* NetWare Virtual Terminal.
NIC	*See* Network Interface Controller.
Open Systems Interconnection (OSI),	An internationally accepted framework of standards for communication between different systems made by different vendors. OSI was developed by the International Standards Organization.
OSI	*See* Open Systems Interconnection.
Out-of-Band	Refers to the capacity to deliver information via a modem or other asynchronous connection.
Point-to-Point Protocol (PPP)	A set of industry standard framing and authentication protocols, which negotiates operation over asynchronous or synchronous serial links.
POST	*See* Power-On Self Test.
Power-On Error Log	A log file that records any errors that occur during Power-On Self Test (POST). This file is stored in non-volatile RAM. *See also* Power-On Self Test.
Power-On Self Test (POST)	A set of tests that compares hardware versions of the server and its options to the stored configuration. POST runs each time the server is turned on.

PCI	*See* Peripheral Component Interconnect.
Peripheral Component Interconnect (PCI)	A system bus architecture specification that supports 32-bit bus-mastered data transfer. It is designed to support plug-and-play configuration of optional peripherals.
PPP	*See* Point-to-Point Protocol.
Rapid Recovery Engine	The term used to describe the diagnostic and recovery capabilities built into Compaq servers and some Compaq desktops.
Revision History Table	Stores board revision information in nonvolatile memory. It logs the system board revision first and then logs other boards that support the Revision History Table.
Router	Interconnecting device that selects the appropriate communication path and routes a message accordingly. The router examines the destination address and determines the most efficient route.
SAP	*See* Service Advertising Protocol.
Service Advertising Protocol	A NetWare protocol used to identify the services and addresses of servers attached to the network. The responses are used to update a table in the router known as the Server Information Table.
Simple Network Management Protocol (SNMP)	Industry-standard protocol for the exchange of management data between management applications and management agents.
Snap-In Application	Third-party management application that integrates with a management platform.
SNMP	*See* Simple Network Management Protocol.

SNMP Trap	*See* Trap.
Subsystem	Major components of a device (for example, disk subsystem, storage subsystem, memory subsystem, and processor subsystem).
TCP	The part of TCP/IP protocol set that controls the transfer of data. *See also* Transmission Control Protocol and Internet Protocol.
TCP/IP	*See* Transmission Control Protocol and Internet Protocol.
Terminate-and-Stay-Resident (TSR)	A term for loading a software program in an MS-DOS computer in which the program loads into memory and is always ready for running by using a combination of keys.
Threshold	A limit that you can set to produce an alarm if it is reached or exceeded.
Token Ring	Networking topology that uses a token-passing scheme. A logical token passes from a station to its nearest neighbor; and stations can send data only when they have the token.
Topology	The physical layout of network components (cables, stations, gateways, hubs, etc.). The three basic interconnection topologies include star, ring, and bus networks. On a star network, workstations are connected directly to a file server but not to each other. On a ring network, the file server and workstations are cabled in a ring; however, a workstation's messages might have to pass through several other workstations before reaching the file server. On a bus network, all workstations and the file server are connected to a central cable, usually called a trunk or bus.

Transmission Control Protocol and Internet Protocol (TCP/IP)	Protocol that manages the transmission of packets on a network and checks for errors.
Trap	Unsolicited message generated by the management agent that indicates that an important event has occurred; either a monitored item exceeded a set threshold or changed status. Trap is synonymous with alarm. *See also* Alarm.
TSR	*See* Terminate-and-Stay-Resident.
Vendor MIB	Management objects that are unique to an individual vendor's product or product line.
Version Control	A database of Compaq software products provided on the Compaq SmartStart CD and the Compaq Support Software CD. The code queries servers for the software version levels to see if an upgrade is needed.
WAN	*See* Wide Area Network.
Wide Area Network (WAN)	Network of LANs connected by routers or bridges, usually covering a large geographic area.
Windows Internet Name Service (WINS)	Dynamic database maintenance that supports computer name registration and name resolution.
WINS	*See* Windows Internet Name Service.
X.25	Network that implements the internationally accepted CCITT standard governing the operation of packet-switching networks.

Index

COMPAQ TECHNOTE ORDER FORM

Ship To:

Name: _____ Company:_____

Address: _____ Dept/Mail Code: _____

City: State/Province:_____

ZIP/Postal Code: _____ Country: _____

Phone:_____

Payment Method:

❑ Company Check   ❑ Cashier's Check   ❑ VISA   ❑ MasterCard   ❑ American Express

❑ Personal Check (Driver's License Number/State -- USA only): _____

Card Number:_____ Expiration:_____

Card Holder Name (please print): _____

Card Holder Signature: _____

Part Number	Title	Qty	Unit Price	Total Price

Shipping/Handling*	
Subtotal	
Sales tax**	
Total	

**For U.S orders, add applicable sales tax.

  For Canadian orders, add 7% GST.

*SHIPPING AND HANDLING	U. S.	Canada	Outside U.S. and Canada
Compaq TechNote (per order)	$3.00	CDN $2.50	U.S. $15.00

For more information, call: **1-800-952-7689 (USA)**
                               1-800-263-5868 (Canada)
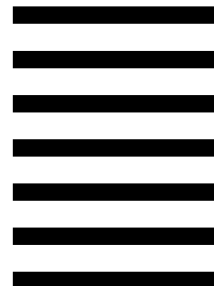   **1-317-364-7281 (Worldwide)**

(Fold Here)

Please Tape Here   Please Tape Here

USER SURVEY

Please help us provide quality documentation by completing and returning this postage-paid form.

TechNote Title: _____

1. Overall rating of the document:
   ❏ Excellent   ❏ Satisfactory   ❏ Fair   ❏ Poor

2. Does this document contain all the information you need?   ❏ Yes   ❏ No
   If not, what information is missing? _____
   _____

3. Is the information appropriate to your experience?   ❏ Yes   ❏ No
   Explain: _____

4. Are the checklists, charts, etc., provided useful?   ❏ Yes   ❏ No
   What additional items would be helpful? _____
   _____

5. What part of this document do you use the most? _____
   _____

6. How often do you anticipate referring to this TechNote?
   ❏ Never   ❏ Once   ❏ Occasionally   ❏ Often

7. How did you first learn about Compaq TechNotes?
   ❏ Compaq advertising   ❏ Compaq Reseller/Distributor
   ❏ Compaq salesperson   ❏ Compaq Customer support
   ❏ Other: *(explain)* _____

8. Does your company own any Compaq products?
   ❏ Server   ❏ Desktops   ❏ Portables   ❏ Network laser printers

9. What operating system(s) does your company use?
   ❏ Microsoft Windows NT   ❏ NetWare   ❏ SCO UNIX   ❏ Oracle7
   ❏ IBM LanServer   ❏ Banyan VINES   ❏ UnixWare
   ❏ Other *(specify)* _____

10. What is your role in the acquisition of computer products at your company?
    ❏ VP Finance   ❏ Manager/Information Systems   ❏ Network Administrator
    ❏ Purchaser   ❏ User   ❏ Other_____

(Optional) If you would like to receive future information about Compaq TechNotes, complete the following:
Name: _____Title: _____
Company: _____
Address: _____
City:_____State: _____Zip:_____

If mailed outside of the U.S.A. please affix proper postage to ensure delivery.
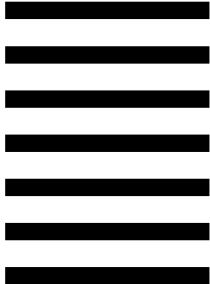
Please fold card over and tape closed. Do not staple.

BUSINESS REPLY MAIL

FIRST CLASS MAIL   PERMIT NO. 400   HOUSTON, TEXAS

POSTAGE WILL BE PAID BY ADDRESSEE

MAILCODE 090307
COMPAQ TECHNOTES
COMPAQ COMPUTER CORPORATION
PO BOX 692000
HOUSTON TX 77269-9976

(Fold Here)

Please Tape Here   Please Tape Here