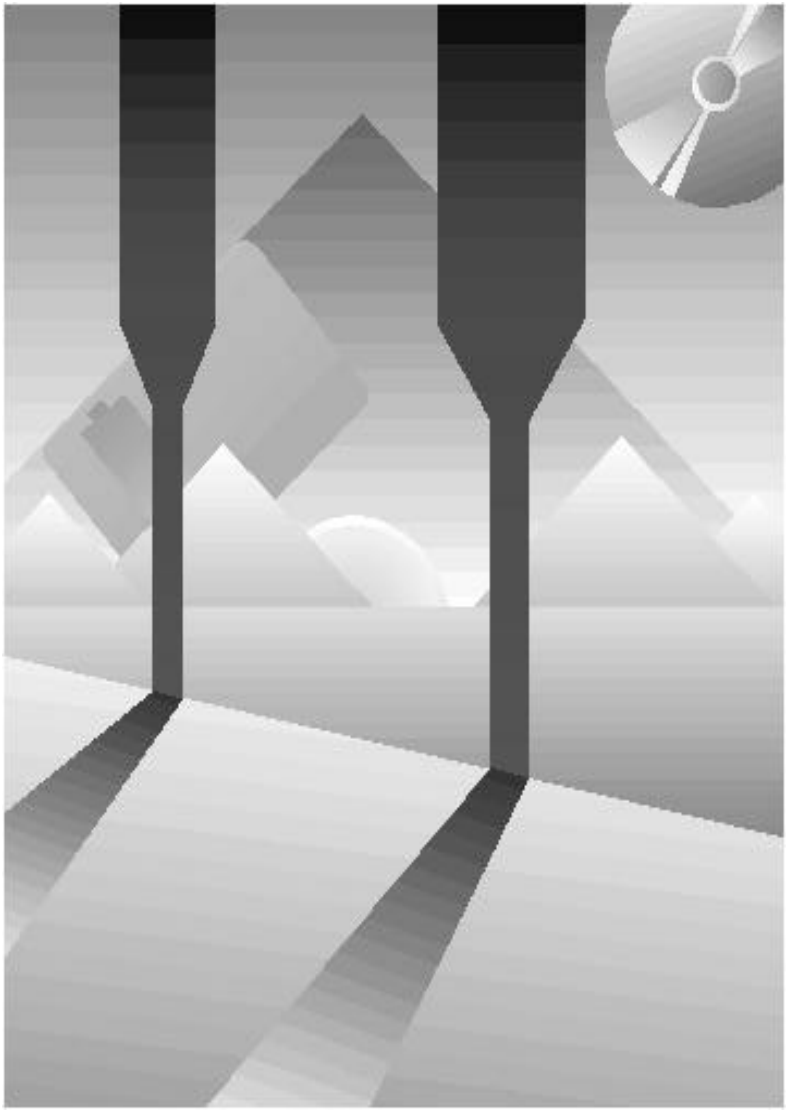
COMPAQ

NetWare Server Management

Compaq TechNote

Includes information on:

- Increasing network administrator productivity
- Compaq Insight Manager
- Compaq Server Manager/R



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 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.

COMPAQ, DESKPRO, SYSTEMPRO, SLT, LTE, FASTART
Registered U.S. Patent and Trademark Office.

EZ Help and INSIGHT Manager are trademarks of
Compaq Computer Corporation.

COMPAQ TECHNOTE FOR NETWARE

NETWARE SERVER MANAGEMENT

First Edition (September 1992)
Part Number 145231-001

Compaq Computer Corporation

CONTENTS

COMPAQ INSIGHT MANAGER (*Continued*)

Chapter 3
COMPAQ SERVER MANAGER/R

COMPAQ SERVER MANAGER/R (*Continued*)

Chapter 4
INCREASING PRODUCTIVITY USING SERVER MANAGEMENT TOOLS

INCREASING PRODUCTIVITY USING SERVER MANAGEMENT TOOLS (*Continued*)

Appendix A
GENERATING INSIGHT MANAGER AD HOC REPORTS

GENERATING INSIGHT MANAGER AD HOC REPORTS (*Continued*)

FIGURES

TABLES

Chapter 1
SERVER MANAGEMENT OVERVIEW

As a network administrator, you face formidable challenges every day, including decisions about:

- Server configuration management
- Preventive maintenance and network status changes
- Recovery from catastrophic network events
- Remote network management

For example, you might be considering an additional hard drive subsystem or network interface card (NIC) for your local area network server. Do you have to bring the server down to find out if it has any open slots? How do you know what expansion boards are in the server, and at which interrupts the boards are set?

You have discovered a possible security breach, and you want to know if Network Server Mode is set for that server. Do you have to bring down the server to check its security configuration?

You have a question about system performance, so you call your Authorized COMPAQ Computer Service Provider. The representative asks you the ROM revision on the system board. Do you have to bring down the server to run COMPAQ Diagnostics software?

You have a critical server used by the accounting department. A failed hard drive in the middle of the quarterly budget cycle could be costly. How can you monitor the server hard drives for errors that might indicate a potential problem?

During an overnight report run, your server fails. You discover the failure the next morning, losing several hours of valuable time. How could you be alerted as the failure happened?

You need tools to help you face these daily challenges. Compaq Computer Corporation has pioneered a technology framework, COMPAQ INSIGHT Server Management, that shows you the status and condition of your server hardware, and presents that information clearly, concisely, and graphically.

True server management includes much more than a simple software application. It begins with the server hardware itself. A robust server management solution includes intelligent server hardware that reports data on system activity and system errors or anomalies. It includes tools to collect, interpret, and display this data in a useful and understandable way. It is based on industry standards such as Simple Network Management Protocol (SNMP). Compaq combines all of these facets of server management into the COMPAQ INSIGHT Server Management technology framework. The framework provides you, the network administrator, with the information you need to make sound decisions on server optimization, management, and problem prevention in your network environment.

Compaq offers two tools as part of the COMPAQ INSIGHT Server Management framework: COMPAQ INSIGHT Manager and COMPAQ Server Manager/R.

These two server management tools complement a variety of other tools, including NetWare Services Manager from Compaq. In the past, network management tools have provided information about the network operating system, not about the server hardware. INSIGHT Manager and Server Manager/R allow you to manage your server configurations, monitor the status of your servers, and receive alerts when a status change occurs.

SERVER MANAGEMENT: A TWO-PART SOLUTION

This TechNote discusses ways to increase your productivity by using two unique products that can operate independently or together for a complete server management solution:

- COMPAQ INSIGHT Manager v1.00a
- COMPAQ Server Manager/R v1.11

COMPAQ INSIGHT Manager and COMPAQ Server Manager/R monitor and report information about your network server hardware. Both products allow you to look at both real-time and historical data. Server Manager/R also reports selected information about the network operating system.

INSIGHT Manager monitors the server hardware configuration and its status, notifying you at the management console of any alert conditions. A scheduled reporting feature allows you to automatically generate hourly, daily, weekly, or monthly customized health reports that show a comprehensive overview of your server subsystems. These reports highlight subsystems that have changed significantly since the last report. Using third-party report writing software, you can enhance the generated ad hoc reports. The information provided by INSIGHT Manager helps you schedule preventive maintenance for your servers before hardware failures occur, allowing you to be proactive and more productive in managing your network servers.

Like INSIGHT Manager, Server Manager/R monitors server hardware, its environment, and selected items in the operating system software, notifying you of any alert conditions. You can also make changes to your server configuration through the Remote Console feature of the Server Manager board. Any function you can perform from the NetWare Server Console screen can be done with the Server Manager board from a remote location.

Server Manager/R allows you to:

- Edit files, such as *AUTOEXEC.NCF* and *STARTUP.NCF*, using *INSTALL.NLM*.
- Load and unload NLMs.
- Change SET parameters.
- Bring the server down and restart it.
- Reset the system (both warm and cold boots).
- Run COMPAQ Diagnostics software, the COMPAQ Inspect Utility, or the COMPAQ EISA Configuration Utility.

You can connect the local management console to the server using a null modem cable or a "dial-up" connection using modems. See Chapter 3 for more information on communication options.

ON-THE-NETWORK AND REMOTE OR OFF-THE-NETWORK OPERATIONS

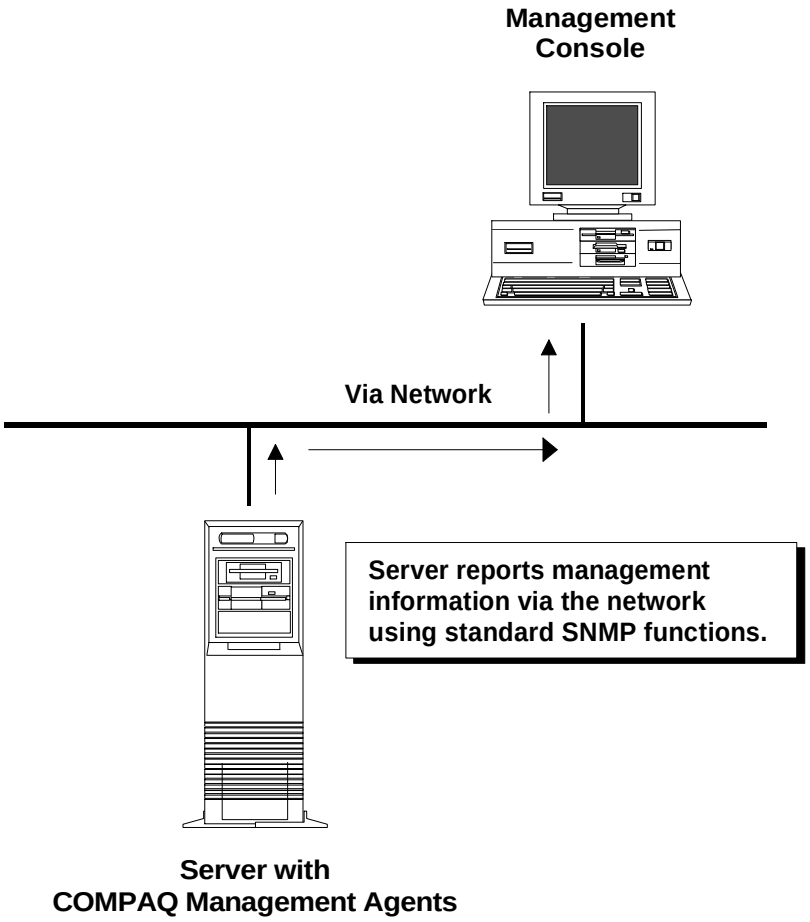
Using INSIGHT Manager and Server Manager/R together allows you to achieve an enhanced level of alert delivery fault tolerance. These two applications provide different methods by which you can communicate with and receive alerts from your server.

INSIGHT Manager and Server Manager/R report much of the same information, but the different reporting methods give each its distinct advantages. These two reporting methods are "on the network" and remote, or "off the network."

On-the-network reporting means that the server reports collected information and alerts via the network cabling (Ethernet or Token Ring, for example) using the Simple Network Management Protocol (SNMP). This type of connection relies on the integrity of the network. The advantage of on-the-network reporting is that any server attached to your network can report information to the management console. INSIGHT Manager offers on-the-network reporting.

Figure 1-1 illustrates on-the-network reporting.

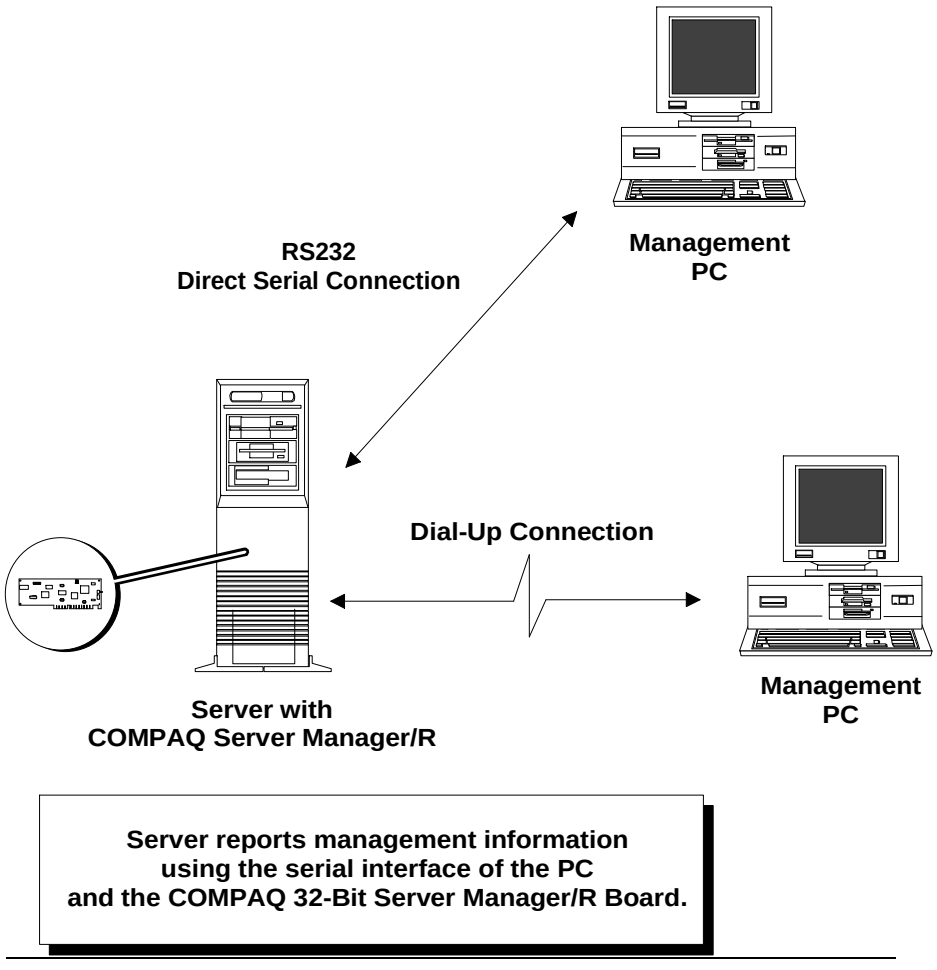
Figure 1-1
On-the-Network Reporting



Remote or off-the-network reporting means that the server reports management information and alerts via a serial connection. This connection can be a direct connection between the server and the management PC (using a null modem cable), or a dial-up connection (using modems). Serial connections are separate and independent of the network cabling; therefore, they do not depend on the integrity of the network to communicate. Server Manager/R offers remote or off-the-network reporting.

Figure 1-2 illustrates remote or off-the-network reporting.

Figure 1-2
Remote or Off-the-Network Reporting



SUMMARY

Server management is a key element in any network management scheme, and involves monitoring and alerting capabilities for both hardware and the operating system. With reliable and effective management tools, you can increase network uptime, optimize server performance, and quickly analyze any problems that may occur on the network.

INSIGHT Manager and Server Manager/R focus on monitoring server hardware. INSIGHT Manager operates on the network to provide convenient day-to-day monitoring and reporting capabilities with an easy-to-use Microsoft Windows interface. Server Manager/R provides remote network management capabilities, monitors environmental parameters, such as server temperature and power, and reports important operating system information. Because it operates remotely, or off the network, it can provide alerting and analysis capabilities even when the network is down.

INSIGHT Manager and Server Manager/R used together offer the most complete server management solution available today. See Chapter 4 for detailed examples of the effective use of these tools.

ABOUT THIS COMPAQ TECHNOTE

This TechNote discusses two products that can operate independently or together for a complete server management solution:

- COMPAQ INSIGHT Manager
- COMPAQ Server Manager/R

! **IMPORTANT:** This TechNote refers you to COMPAQ Server Manager/R documentation. These references also apply to COMPAQ System Manager documentation. Though the name of the product has changed, both sets of documentation are applicable.

Terminology associated with these products is listed and defined in Tables 1-1 and 1-2.

Table 1-1 lists INSIGHT Manager terms.

Table 1-1
INSIGHT Manager Terminology

Managed server	A NetWare server with the COMPAQ Management agents installed.
Management agents	A collection of COMPAQ Instrumentation Agents.
Instrumentation agent	Software that can query manageable devices and respond to management protocol requests for data.
SNMP	Simple Network Management Protocol. An industry-standard management protocol that provides data across the network.
Btrieve	Object information gathered over time by INSIGHT Manager will be stored in Btrieve database files allowing access from other programs running on the workstation.
Management console	A management and control center for the network. Managed server information is reported here.
Monitored items	The actual items that INSIGHT Manager manages or monitors, or the information that INSIGHT Manager collects.
Alert	A notification when certain events occur. It is also referred to as an SNMP trap.
COMPAQ Enterprise MIB	COMPAQ Enterprise Management Information Base. A MIB is a description of a set of items that management applications and agents use to report and control managed devices.

Table 1-2 lists Server Manager/R terms.

Table 1-2
Server Manager/R Terminology

Monitored server	A COMPAQ EISA-based system with a COMPAQ 32-Bit Server Manager/R Board installed.
Management PC	Personal computer running the SMF and SMC software.
Server Manager Collector/R (SMC)	Microsoft Windows-based application that collects information from the Server Manager board. You can export information retrieved from Server Manager/R into an analysis program (such as a spreadsheet).
Server Manager Facility/R (SMF)	Microsoft Windows-based application that communicates with the Server Manager board. You can set alert thresholds, configure alert destinations, view monitored items, and operate servers configured with Server Manager boards.
Class	The highest level of organization that the SMF uses to display information. Classes are divided into objects.
Object	The middle level of organization that the SMF uses to display information. A group of related objects make up a class, and each object consists of one or more monitored items.
Monitored items	The lowest level of organization that the SMF uses to display information. Items are individual parameters monitored by the SMF.
Remote Console feature	The ability of the management PC to access the monitored server so that you can operate the monitored server from the management PC.
Alert	A notification when certain events occur.
Default alert	A preset alert for a monitored item. These alerts have thresholds set and alerting enabled.

Chapter 2
COMPAQ INSIGHT MANAGER

COMPAQ INSIGHT Manager is a server management tool that provides valuable information about your server configuration, status, and activity. INSIGHT Manager operates on the network, and can monitor multiple servers from a central location.

INSIGHT Manager provides a list of servers on the network. When you select an "instrumented" server (a server with the COMPAQ Management Agents loaded), you are presented with a illustration of that server, as well as its system configuration, security configuration, and hardware subsystem (hard disk, expansion boards, and system board) information.

Many of today's network management solutions provide information about the traffic flowing across the network, but specific information about the status of the server hardware has not been as easily available. INSIGHT Manager provides management and alerting information specific to the server hardware. INSIGHT Manager allows you to use network administrator resources more efficiently; one administrator can monitor many servers from a single location.

In addition to alerting, INSIGHT Manager provides comprehensive reporting that allows you to track the health of each server and predict potential failures before they occur.

This chapter covers the following topics:

- Understanding the application architecture
- Interpreting management data
- Alerting
- Reporting
- Modifying INSIGHT Manager

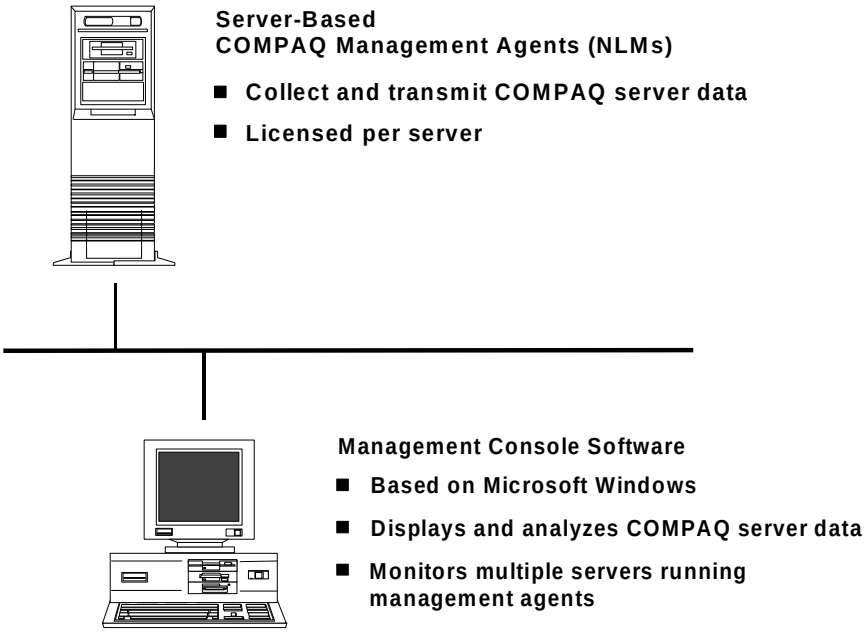
UNDERSTANDING THE APPLICATION ARCHITECTURE

COMPAQ INSIGHT Manager comprises two parts:

- Management console application
- COMPAQ Management Agents (NLMs running on the server)

INSIGHT Manager uses Simple Network Management Protocol (SNMP) agents residing on the managed servers to transmit data from the managed servers to the management console. See Figure 2-1.

Figure 2-1
COMPAQ INSIGHT Manager



COMPAQ MANAGEMENT AGENTS

The COMPAQ Management Agents, *CPQBSSA.NLM*, *CPQDSKSA.NLM*, and *CPQSMBSA.NLM*, are modular, and are used to instrument specific server subsystems. These management agents are based on the COMPAQ Enterprise Management Information Base (MIB). A MIB is a description of a set of items that management applications and agents use to report and control managed devices.

The management agents gather information from hardware subsystems and pass this information to the management console, which runs INSIGHT Manager. A server with the appropriate management agents loaded is said to be "instrumented." INSIGHT Manager polls the management agents and reports that information through the graphic representation of the data, or through printed reports. INSIGHT Manager, running on a single workstation, can monitor many different servers. Each managed server, however, must have the agents installed to gather the appropriate information.

Each network administrator needs a copy of INSIGHT Manager to monitor the managed servers. For example, if you have 15 managed servers and 3 network administrators, you need 3 copies of INSIGHT Manager, which comes with a single copy of the management agents, and 12 additional copies of the management agents to instrument the servers on the network.

SNMP TRANSMISSION OF DATA

INSIGHT Manager adheres to network management standards to provide access to open environments and a pathway for future enhancements. It uses SNMP to transmit data from the managed servers to the management console, using the SNMP agent residing on the managed servers. The NetWare SNMP agent is an NLM for NetWare v3.11 (*SNMP.NLM*) and is included with the INSIGHT Manager diskettes.

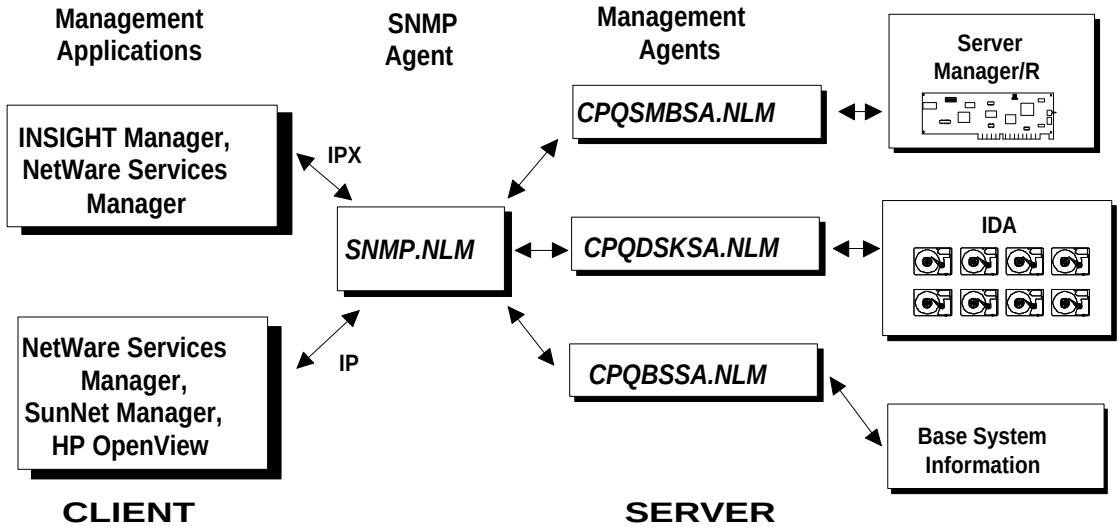
SNMP is a widely adopted management protocol that manages the components of a Transport Control Protocol/Internet Protocol (TCP/IP) network, such as gateways, hubs, concentrators, and hosts. Since SNMP was first implemented over TCP/IP, it is often considered a transport protocol-specific management tool. However, SNMP is actually independent of TCP/IP, and can be implemented over different transport protocols.

Novell has implemented an extensible SNMP agent over IPX and IP networks with *SNMP.NLM*. It is an extensible agent, which means it allows other agents, such as the COMPAQ Instrumentation Agents, to communicate with it. The instrumentation agents are also protocol-independent, relying on the NetWare SNMP agent to communicate over both IPX and IP (see Figure 2-2). The NetWare SNMP agent routes requests for information to the correct instrumentation agent and remembers the original protocol of the request (IPX or IP), so it can return information correctly.

! **IMPORTANT:** The *SNMP.NLM* that ships with NetWare v3.11 is not an extensible agent. When installing INSIGHT Manager, use the *SNMP.NLM* included with INSIGHT Manager.

INSIGHT Manager currently supports the IPX transport protocol and requests information via IPX. Applications that support IP (for example, NetWare Services Manager, Hewlett Packard HP OpenView, and Sun Microsystems, Inc. SunNet Manager) can request and receive information from the instrumentation agents by using the COMPAQ Enterprise MIB.

Figure 2-2
COMPAQ Server Management Architecture



The management console requires specific hardware and software to communicate with the managed servers. For detailed information, refer to the *COMPAQ INSIGHT Manager User Guide* or the *README.WRI* files included on the INSIGHT Manager diskettes. Print the *README.TXT* files and read them carefully. (Both *README.WRI* and *README.TXT* files are included on the diskettes.)

! **IMPORTANT:** INSIGHT Manager requires a NetWare Open Data Link Interface (ODI) shell for DOS at the management console. Ensure that your NIC has an ODI shell for DOS before you install INSIGHT Manager. Novell recommends ODI drivers for multiprotocol stack support. Non-ODI drivers are neither tested nor supported.

ODI NIC drivers are provided with NetWare v3.11 on the WSGEN diskette in the \DOSODI subdirectory and on INSIGHT Manager Disk 2. If the driver you require is not on either diskette, contact your NIC manufacturer.

HARDWARE AND SOFTWARE REQUIREMENTS

The following hardware and software are required for installing INSIGHT Manager on a management console:

- 386 (or higher) system processor
- 6 megabytes of system memory
- 12 megabytes of available disk space (monitoring fewer than 10 servers may reduce this requirement)
- VGA (or higher) color graphics controller supported by Microsoft Windows (INSIGHT Manager uses color to indicate status)
- NIC with compatible NetWare ODI workstation driver
- Microsoft Windows-compatible mouse
- Microsoft Windows-compatible graphics printer to print reports
- Microsoft Windows 3.x (386 Enhanced mode required)
- Minimum of 30 file handles for DOS, set in the *CONFIG.SYS* file as FILES=30

The following software and hardware are required for installing INSIGHT Manager on a managed server:

- NetWare v3.11 or later
- Drives must be properly initialized or "stamped" for Intelligent Drive Array (IDA)
- Minimum COMPAQ Intelligent Drive Array Controller firmware 1.26
- Minimum COMPAQ Intelligent Drive Array Controller-2 firmware 2.40
- Minimum COMPAQ 32-Bit IDA Expansion Controller firmware 1.16

NOTE: Most server configurations do not require additional memory to support the management agents. The agents require 200 Kbytes or less of system memory, depending on your hardware configuration.

MANAGED SERVER CONFIGURATION

The following sections outline important information for installing and configuring managed servers.

Drive Stamping

Much of the managed server's monitored hard drive information is dependent on the drive being properly initialized, or "stamped," for IDA. Stamping is the process of writing information, such as the drive manufacturer and the drive type, to a reserved area of the disk.

NOTE: Stamping does *not* destroy data on the disk.

Disk initialization may contain drive manufacturer and model information, such as "COMPAQ 210MB CP3201." All arrayed COMPAQ drives manufactured after February 1992 are factory-stamped. If your drives were manufactured before February 1992, or you are not sure of the manufacture date, run the COMPAQ Diagnostics software (minimum version 8.05 2/12/92) and select *Quick Check* or *Monitor and Performance* to initialize the disk.

Installing COMPAQ Management Agents and SNMP Support

The following steps outline installation of the COMPAQ Management Agents on the managed server. Refer to the *COMPAQ INSIGHT Manager User Guide* and the *README.TXT* files in the \COMPAQ and \NOVELL subdirectories on the Management Agents diskette for more details on managed server setup.

1. From the Management Agents diskette, copy the agents from the \COMPAQ directory to the NetWare server SYS volume in the \SYSTEM directory. For example:

   ```
   COPY A:\COMPAQ\CPQBSSA.NLM  F:\SYSTEM\CPQBSSA.NLM
   COPY A:\COMPAQ\CPQBSSA.TXT   F:SYSTEM\CPQBSSA.TXT
   COPY A:\COMPAQ\CPQDSKSA.NLM   F:\SYSTEM\CPQDSKSA.NLM
   COPY A:\COMPAQ\CPQSMBSA.NLM   F:\SYSTEM\CPQSMBSA.NLM
   COPY A:\COMPAQ\CPQSYSMN.NLM   F:\SYSTEM\CPQSYSMN.NLM
   ```

   NOTE: This example assumes that drive F: is mapped to the server's SYS volume. *CPQSYSMN.NLM* is the device driver for the Server Manager board. See Chapter 3 for more information on COMPAQ Server Manager/R.

2. From the Management Agents diskette, copy the SNMP support files from the \NOVELL\SYSTEM directory to the NetWare server SYS volume in the \SYSTEM directory. For example:

   ```
   COPY A:\NOVELL\SYSTEM\AFTER311.NLM  F:\SYSTEM\AFTER311.NLM
   COPY A:\NOVELL\SYSTEM\SNMP.NLM  F:\SYSTEM\SNMP.NLM
   ```

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

4. Copy the SNMP configuration files in the \NOVELL\ETC directory of the COMPAQ Management Agents diskette to the \SYS:ETC directory of the NetWare server to be instrumented. For example:

   ```
   COPY A:\NOVELL\ETC\SNMP.CFG F:\SYSTEM\ETC\SNMP.CFG
   COPY A:\NOVELL\ETC\TRAPTARG.CFG F:\SYSTEM\ETC\TRAPTARG.CFG
   ```

5. Use the LOAD INSTALL command and select *System Options* to edit your *AUTOEXEC.NCF* file. Include load statements for the NLMs listed in step 1 (see the following sample *AUTOEXEC.NCF* file).

NOTE: COMPAQ Management Agents are modular. If your managed server does not contain a Server Manager board or a COMPAQ Intelligent Drive Array (IDA) subsystem, you may choose not to load *CPQSYSMN.NLM, CPQSMBSA.NLM* (Server Manager/R), and/or the *CPQDSKSA.NLM* (drive arrays) management agents.

The COMPAQ Management Agents diskette also contains updated SNMP support from Novell in the *SNMP.NLM*. Refer to the *README.TXT* file in the \NOVELL directory for information about this NLM and its installation.

The following is a sample NetWare *AUTOEXEC.NCF* file:

```
FILE SERVER NAME COMPAQ
IPX INTERNAL NET  123456
LOAD NE3200 SLOT=3 frame=ETHERNET_802.3  name=IPXLAN
BIND IPX to NE3200 NET=E1
**********Start COMPAQ INSIGHT Manager**********
LOAD AFTER311
LOAD SNMP
LOAD CPQBSSA
LOAD CPQDSKSA
LOAD CPQSMBSA

LOAD MONITOR
```

Establishing Alert Delivery Addresses

You must provide an alert destination address for the management console to receive alerts from the managed server. The alert destination address is the network and node address of the workstation or workstations (management consoles) that will receive the alerts.

You can obtain this address information by using the command line utility USERLIST/A or by selecting *Connection Information* at the Monitor screen. Include the network and node address in the *TRAPTARG.CFG* file, located in the SYS:\ETC directory on each instrumented server. Edit the *TRAPTARG.CFG* file and add a line under the IPX section using the following format:

```
network_address:node_address
```

For the example shown in Figure 2-3, this line would resemble the following:

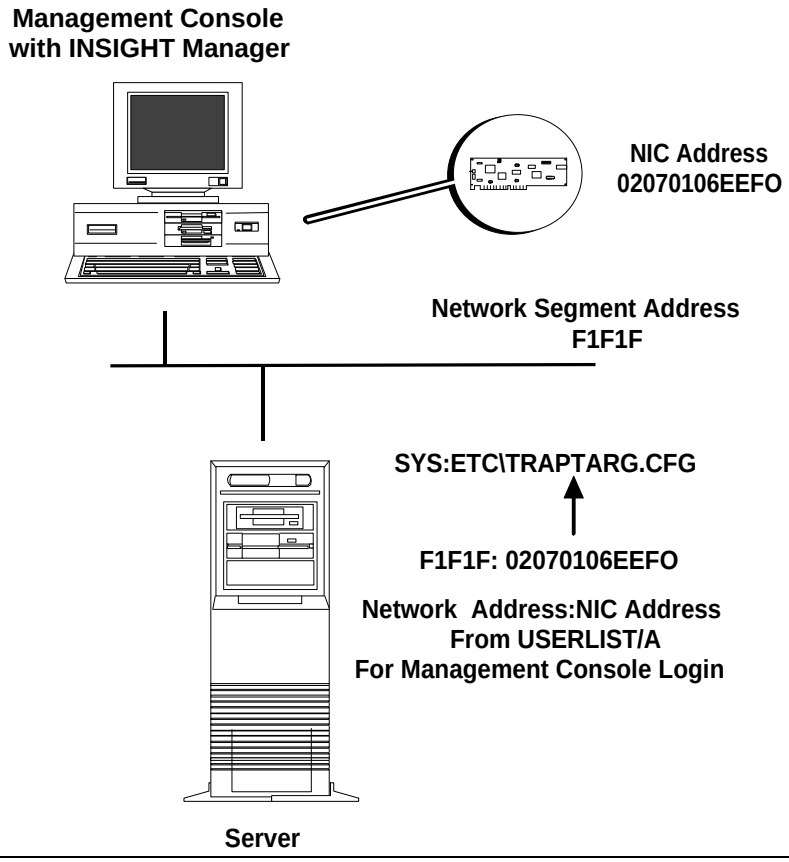
```
F1F1F:02070106EEF0
```

Add additional addresses as required for other management consoles to receive alerts.

! **IMPORTANT:** This procedure must be performed on *each* instrumented server from which you want to receive alerts.

Figure 2-3 illustrates providing an alert destination address.

Figure 2-3
Setup of Alerting



MANAGEMENT CONSOLE CONFIGURATION

Installing an INSIGHT Manager management console includes:

- Setting up workstation DOS ODI shell and network connection.
- Setting up Microsoft Windows to be NetWare-aware.
- Installing INSIGHT Manager from within Microsoft Windows.

Table 2-1 shows the minimum software versions required for NetWare and Microsoft Windows to be used with INSIGHT Manager.

Table 2-1
Required Software Versions*

\ODI	\WINDOWS\SYSTEM
LSL.COM v1.20	*VNETWARE.386* 3/10/92 3:10 a.m.
IPXODI.COM v1.21	*VIPX.386* 3/10/92 3:10 a.m.
NETX.COM v3.26	

* Use the version of *NWIPXSPX.DLL* that ships with INSIGHT Manager.

NOTE: The management console requires Novell DOS ODI drivers. In addition, Microsoft Windows must be installed to be NetWare network-aware. Windows SETUP allows you to select the network operating system and inserts the necessary entries into the *SYSTEM.INI* file.

The following steps outline the management console installation procedure.

1. Configure the DOS ODI shell for the management console. For detailed information, refer to the Novell document *Novell NetWare ODI Shell for DOS*, which ships with NetWare. Configure the NIC, and record the settings to add to the *NET.CFG* configuration file.

2. Create a batch file to load the required shell files. This file can be added to the end of your existing *AUTOEXEC.BAT* file or can be a separate batch file that is called from your *AUTOEXEC.BAT* file. An example of this batch file follows:

```
CD C:\ODI
LSL
NE2000
IPXODI
NETX
REM The following LOGIN is optional.
F:
LOGIN COMPAQ
C:
WIN
```

   In this example, C:\ODI directory on the local drive is used for all NetWare shell files. A path includes a pointer to the Windows subdirectory.

   NOTE: You are not required to log into a network server for INSIGHT Manager to run; however, it is recommended. Your Windows setup includes adding NetWare support. Whether you should log into the network server depends on the network services or applications that you may use at this management console. If you configure Windows to be NetWare network-aware, and you do not log in, Windows reports an error.

NET.CFG is a control file that contains section headings and options that deviate from the defaults of the workstation boot process. The *SHELL.CFG* file also contains network configuration information. Options from the *SHELL.CFG* file can be specified in the *NET.CFG* file. The *Novell NetWare ODI Shell for DOS* documentation discusses rules to help you determine whether to use *SHELL.CFG* or *NET.CFG*. The revision level of your shells also influences your decision.

The following is a sample *NET.CFG* file for a management console with an NE2000 NIC:

```
#
# PROTOCOL STACK SECTION:
#
PROTOCOL STACK IPX
        Bind NE2000
#
# Link Driver Section: Remove the '#' sign where appropriate
# Required fields: Port, Int, Mem.
#
LINK DRIVER NE2000
        port 300
        Int 3
#       Mem D000
#       Frame Ethernet_II
        Frame Ethernet_802.3
#
# Personal preferences
#
PREFERRED SERVER=COMPAQ
SET STATION TIME=OFF
SHOW DOTS=ON
```

This example does not include all the hardware and software commands available within the *SHELL.CFG* or *NET.CFG* files. For a complete list of these commands, refer to *Novell NetWare ODI Shell for DOS.* This example does include load options for both the *SHELL.CFG* and *NET.CFG* files. Novell recommends that SHOW DOTS be set to ON when using Microsoft Windows. The default is OFF.

The following steps outline INSIGHT Manager installation on the management console.

1. Attach or log into the server, start Windows, and ensure that Windows is NetWare-aware.
2. To install INSIGHT Manager, insert INSIGHT Manager Disk 1 - Install into drive A.
3. Select *File* and *Run*, and type the following command:

   A:INSTALL

During installation, the INSIGHT Manager software attempts to detect the Server Manager Facility on the installation drive. If INSIGHT Manager finds the Server Manager/R software, it adds a path entry to the *CIM.INI* file, and a Server Manager Facility button is added to the Tool Bar. The SMF button allows you to launch the Server Manager Facility/R from INSIGHT Manager.

If it does not find the Server Manager/R software, you are asked if Server Manager/R will be used. If you answer *Yes*, then you are prompted for a path for the Server Manager/R software directory.

NOTE: If you want to launch Server Manager/R from INSIGHT Manager at a later date, you must specify a path in the *CIM.INI* file. For details, refer to the *CIMINI.TXT* file.

By editing the *CIM.INI* file, you can add applications to the Tools menu, such as SYSCON, FCONSOLE, or others on your local hard drive. Add this information to the TOOLS section of the *CIM.INI* file. See Chapter 4 for more information.

Once INSIGHT Manager is installed, four icons display in the Windows group:

- Release Notes - *README.TXT*
- Read Me - *README.WRI*
- SNMP Data Server
- INSIGHT Manager

Read both README files for the latest information on INSIGHT Manager.

! **IMPORTANT:** You *must* start the SNMP Data Server to run as a background task before you start INSIGHT Manager. SNMP Data Server provides SNMP services over IPX for INSIGHT Manager.

Once INSIGHT Manager starts, a server list screen displays, allowing you to select the server to be monitored and the information category to view.

INTERPRETING MANAGEMENT DATA

INSIGHT Manager provides information to help you predict potential subsystem failures. This predictive analysis information, such as hard drive subsystem data, allows you to take preventive measures before a failure occurs.

SERVER INFORMATION

INSIGHT Manager provides information on virtually every aspect of server hardware operation. Understanding the data available and how to interpret it is key to using INSIGHT Manager effectively.

INSIGHT Manager supplies information in the following categories:

- Configuration
- I/O Ports
- Disk Storage
- System Board
- Expansion Boards
- Security Configuration and Setup

If a COMPAQ 32-Bit Server Manager/R Board is installed in the managed server, the status of that board and the environmental information it gathers are also available through INSIGHT Manager.

INSIGHT Manager also provides information about non COMPAQ hardware, primarily from system information stored in EISA non-volatile system memory or ISA CMOS. Table 2-2 outlines the information monitored by INSIGHT Manager and indicates the items available for COMPAQ and non COMPAQ servers.

Table 2-2
COMPAQ and Non COMPAQ Hardware Information
Reported by COMPAQ INSIGHT Manager

Information Reported	EISA		ISA	
Category	**COMPAQ**	**Non COMPAQ**	**COMPAQ**	**Non COMPAQ**
Configuration				
Bus Type	✔	✔	✔	✔
Processor Type	✔	✔	✔	✔
Processor Speed	✔	*	NA	NA
Coprocessor Type	✔	✔	✔	✔
Coprocessor Speed	✔	*	NA	NA
Serial Port Addresses	✔	✔	✔	✔
Parallel Port Addresses	✔	✔	✔	✔
Pointing Device Status	✔	NA	✔	NA
Video Description	✔	✔	✔	✔
Keyboard Type	✔	✔	✔	✔
ROM Version	✔	✔	✔	✔
ROM Family	✔	NA	✔	NA
ROM Type	✔	NA	✔	NA
Base Memory	✔	✔	✔	✔
Total Memory up to 16 MB	✔	✔	✔	✔
Total memory above 16 MB	✔	✔	NA	NA
Diskette Drives Installed	✔	✔	✔	✔
Security Features Status	✔	NA	✔	NA
System Configuration Memory (EISA NVRAM, ISA CMOS)	✔	✔	✔	✔

Legend

✔ Available
* Vendor-Dependent
** Available only with COMPAQ Server Manager/R installed
*** Model-Dependent
NA Not Available

Continued

Table 2-2 *Continued*

Information Reported	EISA		ISA	
Category	**COMPAQ**	**Non COMPAQ**	**COMPAQ**	**Non COMPAQ**
I/O Ports				
Serial Port Addresses	✔	✔	✔	✔
Parallel Port Addresses	✔	✔	✔	✔
Keyboard Type	✔	✔	✔	✔
Video Description	✔	✔	✔	✔
Pointing Device Status	✔	NA	✔	NA
Serial Port Statistics **				
Carrier Detect	**	NA	NA	NA
Overrun Errors	**	NA	NA	NA
Parity Errors	**	NA	NA	NA
Framing Errors	**	NA	NA	NA
Parallel Port Status	**	NA	NA	NA
Disk Storage				
Hard Drives	✔	*	✔	*
Intelligent Drive Array (IDA)	✔	NA	NA	NA
Expansion IDA	✔	NA	NA	NA
System Board				
Processor Type	✔	✔	✔	✔
Processor Speed	✔	*	NA	NA
Coprocessor Type	✔	✔	✔	✔
Coprocessor Speed	✔	*	NA	NA

Legend *Continued*

✔ Available
* Vendor-Dependent
** Available only with COMPAQ Server Manager/R installed
*** Model-Dependent
NA Not Available

Table 2-2 *Continued*

Information Reported	EISA		ISA	
Category	**COMPAQ**	**Non COMPAQ**	**COMPAQ**	**Non COMPAQ**
***System Board** (continued)*				
Firmware Version	✔	✔	✔	✔
Firmware Family, Type	✔	NA	✔	NA
Serial Number	***	NA	***	NA
Bus Type	✔	✔	✔	✔
I/O Check **	**	NA	NA	NA
Base Memory	✔	✔	✔	✔
Total Memory up to 16 MB	✔	✔	✔	✔
Total Memory above 16 MB	✔	✔	NA	NA
Memory Parity **	**	NA	NA	NA
Expansion Boards				
Slot Number	✔	✔	NA	NA
Board ID	✔	✔	NA	NA
Board Name	✔	*	NA	NA
Resources Used	✔	✔	NA	NA
COMPAQ Server Manager/R				
Board Name	**	NA	NA	NA
Board ID	**	NA	NA	NA
ROM Date	**	NA	NA	NA
Board Status	**	NA	NA	NA
Modem Settings	**	NA	NA	NA
Alert Destination List	**	NA	NA	NA

Legend *Continued*

✔ Available
* Vendor-Dependent
** Available only with COMPAQ Server Manager/R installed
*** Model-Dependent
NA Not Available

Table 2-2 *Continued*

Information Reported	EISA		ISA	
Category	**COMPAQ**	**Non COMPAQ**	**COMPAQ**	**Non COMPAQ**
Security Configuration ***				
Network Server Mode	***	NA	***	NA
Power-on Password	***	NA	***	NA
Prevent Diskette Boot	***	NA	***	NA
QuickLock	***	NA	***	NA
QuickBlank	***	NA	***	NA
Serial Port	***	NA	***	NA
Parallel Port Control	***	NA	***	NA
Diskette Control	***	NA	***	NA
Hard Drive Control	***	NA	***	NA
Server Manager Dial-Back	**	NA	NA	NA
*Environment ***				
Current Temperature	**	NA	NA	NA
Temperature Change	**	NA	NA	NA
Voltage	**	NA	NA	NA

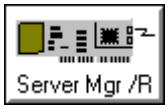
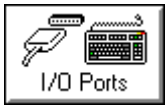
Legend
✔ Available
* Vendor-Dependent
** Available only with COMPAQ Server Manager/R installed
*** Model-Dependent
NA Not Available

NOTE: INSIGHT Manager presents IRQ 2 as IRQ 9. COMPAQ EISA Configuration Utility and COMPAQ Inspect Utility present it as IRQ 2 (9). IRQ 2 and IRQ 9 are the same IRQ.

INFORMATION FROM INSIGHT MANAGER AND SERVER MANAGER/R COMBINED

Table 2-3 shows the additional information that INSIGHT Manager reports with COMPAQ Server Manager/R present. INSIGHT Manager uses its own reporting agents to collect information on the network. When Server Manager/R is not present, some icons are grayed out, or the value appears as "N/A."

Table 2-3
INSIGHT Manager and Server Manager/R Information

Category	Item
	Server Manager Dial-Back Status
	ESDI/IDE I/O Errors ESDI/IDE ECC Errors Track Zero Not Found
	Expansion Bus I/O Check Memory Parity
	Board Name, ID, ROM Date, and Status Alert Destination List Modem Settings
	Carrier Detect Overrun Errors Parity Errors Framing Errors LPT# Status
	Current Temperature Temperature Change Voltage

PREDICTIVE ANALYSIS USING MONITORED DISK INFORMATION

Because the hard drive subsystem is one of the most important components of any server, INSIGHT Manager provides extensive monitoring capabilities for the internal and external hard drive subsystems. This includes configuration information for the hard drive controller, monitored items for the logical and physical drives, and advanced information for the physical drive. You can use this critical information in two ways: proactive server monitoring or performance tuning.

Each of the monitored disk areas provides key information on the health of the hard drive subsystem. Some of the monitored items reflect catastrophic disk failures, while many simply reflect a degradation in disk performance. If a warning disk counter increments, it does not necessarily mean that the drive has failed or is about to fail. By monitoring the items that reflect warnings, you can detect potential disk problems before they become catastrophic, and take necessary actions to minimize system downtime.

You can monitor the server in several ways: with the management console, through the alerting process, or by creating and reviewing a history report. You can monitor the Thresholds Exceeded item for the Physical Drive and Advanced Physical Drive windows as an overview, and determine at a glance whether an increment has occurred for any of the monitored disk items. If Thresholds Exceeded = Yes**,** review the monitored item list, and determine which parameter is causing the alert.

For example, if you receive one Seek Error increment over time, you should not be alarmed. This is a natural event with normal disk use over time. If you receive multiple Seek Error increments in a short period of time, monitor the Functional Tests items. Functional Tests indicate how well a physical drive is performing. These tests compare the way the physical drive currently operates with the factory settings. New drives operate at 100 percent. As the drives wear over time, the performance will decrease. A decrement in the Functional Tests means that drive performance is beginning to degrade.

If the drive performance appears to be degrading, run COMPAQ Diagnostics software. The Diagnostics software runs a series of tests, and indicates whether the drive should be replaced. When the Functional Tests value degrades past 80 percent, you should schedule time to run COMPAQ Diagnostics software to determine if the drive should be replaced. This proactive approach to server management helps you prevent catastrophic hard drive failures and increases your productivity by allowing you to schedule maintenance or downtime.

Table 2-4 lists and explains key disk items monitored by INSIGHT Manager. This table lists *key* items, not *all* items monitored.

Table 2-4
Key Disk Items Monitored
by INSIGHT Manager

Object Category	Item	Cause for Alerts	Comments
Device Driver	Corrected Reads/ Corrected Writes	A read or write was unsuccessful when first attempted; retries required. Corrected by the hard drive controller or the physical drive.	Warning alert; should be monitored. Value is reset when driver is unloaded. If increment is constant, check physical drives for errors.
Logical	Status	Multiple causes.	Logical drive status. Refer to online Help for details and action.
Physical	Thresholds Exceeded	Any monitored item within the Physical Disk Monitor List that exceeds the assigned threshold.	Review all physical drive monitored items to determine which error occurred. Run COMPAQ Diagnostics software.
	Functional Tests #1-#3	Wear from normal drive use over time.	Warning alert; indicates drive performance has degraded.
Physical/Advanced	Thresholds Exceeded	Any monitored item within the Advanced Physical Disk Monitor List that exceeds the assigned threshold.	Review all Advanced Physical Disk Monitor List items to determine which error occurred. Run COMPAQ Diagnostics software.

Continued

Table 2-4 *Continued*

Object Category	Item	Causes for Alerts	Comments
Physical/Advanced (continued)	Used Reallocation Sectors	Controller attempted to write data addressed for unusable sectors. Data was written to usable sectors in Reallocation area.	Warning alert. Monitor increment rate; if rapid, run COMPAQ Diagnostics software.
	Spin Up Time/Spin Up Retries	Wear from normal drive use over time.	Warning alert; indicates drive performance has degraded.
	Recovered Read Errors/ Recovered Write Errors	Wear from normal drive use over time. Corrected through physical drive retries.	Warning alert; indicates drive may be developing problems.
	Seek Errors	Wear from normal drive use over time.	Warning alert. Monitor Functional Tests item. If drive appears to be degrading, run COMPAQ Diagnostics software.

NOTE: COMPAQ Diagnostics software must report a failure before drives or other assemblies should be considered for replacement. Even if the drive exceeds certain preset thresholds, it may still be operational, as the thresholds are set to provide warnings of degraded performance before actual failures occur. In some cases, it may be more effective to continue to monitor the drive for further problems and schedule system maintenance when appropriate.

The Logical Drive screen displays a Status box that contains a text string. When the hard drives are under normal operation, this field reads "OK." If a problem with the drives is detected, this box contains a text string specifying the status of the logical drive. Ten different status items can be reported in this box. For a complete listing and explanation of all available status items that can be reported, refer to the online Help.

You can also further optimize server performance by using the reported data. The total read and write operations of each logical drive are available in the Device Driver screen. Click on the Logical Drive button, and then on the Device Driver button. The total number of read and write operations for that particular logical drive displays. By adding the total read and write operations for all of the logical drives, you can determine the total read/write ratio. Use this ratio in tuning the server with the NetWare SET parameters that pertain to the hard drive subsystem.

Two key SET parameters are involved in tuning hard drive performance:

- SET MAXIMUM CONCURRENT DISK CACHE WRITES
- SET DIRTY DISK CACHE DELAY TIME

The default values for both of these parameters are optimized for environments that have a 50/50 read-to-write ratio. Decreasing these values allows the disk to perform reads more quickly. Inversely, increasing these values favors a write-intensive environment. The principles used to determine whether you should adjust these values are explained in the COMPAQ TechNote for NetWare, *Performance Management in a NetWare v3.11 Environment*. Refer to this document before changing these SET parameters.

ALERTING

The Disk Storage and Server Manager/R buttons in the INSIGHT Manager Main System view have status indicators (red, yellow, or green bands around the box). INSIGHT Manager provides alerts on these two buttons, which represent the hard drive subsystem and the Server Manager board.

DISK ALERTS

INSIGHT Manager can provide alerts from the IDA subsystems (IDA, IDA-2, Array Expansion System) and the Server Manager board. You receive failure alerts, degraded condition alerts, and status alerts at the management console. Failure alerts notify you of critical problems, so you can take immediate action. Degraded condition and status alerts, however, allow you to take corrective action before you experience a failure. Table 2-5 provides a complete list of IDA alerts available from INSIGHT Manager.

Table 2-5
INSIGHT Manager IDA Alerts

Alert	Status	Indication
Logical Drive Status Change	OK	The logical drive is in normal operation mode.
	Failed	More physical drives have failed than the fault tolerance mode of the logical drive can handle without data loss.
	Unconfigured	The logical drive is not configured. Run the COMPAQ EISA Configuration Utility.
	Recovering	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 drive continue to operate without data loss.
	Rebuild Ready	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	The logical drive is currently performing Automatic Data Recovery. During Automatic Data Recovery, fault tolerance algorithms restore data to the replacement drive.
	Wrong Drive	The wrong physical drive was replaced after a physical drive failure.
	Bad Connect	A physical drive is not responding. Run COMPAQ Diagnostics software.
	Overheating	The enclosure that contains the logical drive is overheating. The array is still functioning, but should be shut down. Applies to the Intelligent Array Expansion System only.
	Shutdown	The drive array enclosure that contains the logical drive has overheated. The logical drive is no longer functioning. Applies to the Intelligent Array Expansion System only.
	Unknown	The instrumentation agent does not recognize the Logical Drive Status Change.

Continued

Table 2-5 *Continued*

Alert	Status	Indication
Spare Status Change (Intelligent Array Expansion System only)	Building	A physical drive has failed. Automatic Data Recovery is in progress to recover data to the online spare.
	Active	A physical drive has failed. Automatic Data Recovery is complete. The system is using the online spare as a replacement for the failed drive.
	Failed	The online spare has failed and is no longer available for use.
	Inactive	The monitored system has an online spare configured, but is not currently in use.
	Unknown	The instrumentation agent does not recognize the Spare Status Change.
Physical Drive Status Change	OK	The drive is functioning properly.
	Failed	The drive is no longer operating and should be replaced.
	Unknown	The instrumentation agent does not recognize the drive or that the physical drive status is unknown because the logical drive has failed.
Physical Drive Threshold Exceeded		When the drive is shipped, certain factory thresholds are set to monitor performance of the drives. If the monitored item exceeds the factory threshold, there may be a problem with one of the drives. Run COMPAQ Diagnostics software.
Array Accelerator Board Status Change (IDA-2 only)	Enabled	Write cache operations are currently configured and enabled for at least one logical drive.
	Temporarily Disabled	Write cache operations have been temporarily disabled. View the Array Accelerator Board Error Code monitored item to determine why the write cache operations have been temporarily disabled.
	Permanently Disabled	Write cache operations have been permanently disabled. View the Array Accelerator Board Error Code monitored item to determine why the write cache operations have been disabled.

Continued

Table 2-5 *Continued*

Alert	Status	Indication
Array Accelerator Board Status Change (IDA-2 only) (*continued*)	Unavailable	An Array Accelerator board has not been installed in this system.
	Unknown	The instrumentation agent does not recognize the status of the Array Accelerator.
Array Accelerator Board Bad Data (IDA-2 only)		At power-on, the battery packs were not sufficiently charged, and the board has not retained any data that may have been stored in the write cache. If no data was on the board, no data was lost. This message also appears if the Array Accelerator board is replaced with a new board that has discharged batteries. No data has been lost in this case, and posted writes are automatically enabled when the batteries reach full charge.
Array Accelerator Board Battery Status (IDA-2 only)	OK	Indicates that a particular battery pack is fully charged.
	Failed	The battery pack is below the sufficient voltage level and has not recharged in 36 hours. The battery needs to be replaced. Contact your Authorized COMPAQ Computer Reseller or Service Provider.
	Charging	The battery power is less than 75 percent and the Drive Array Controller is attempting to recharge the battery.
	Degraded	The battery is still operating, but one of the batteries in the pack has failed to recharge properly.
	Unknown	The instrumentation agent does not recognize battery status.

If you receive the Physical Drive Threshold Exceeded alert, the drive is still operational, but has degraded beyond one or more of the factory preset thresholds. The following preset thresholds are monitored for the Physical Drive Threshold Exceeded alert:

- Spinup Time
- Functional Tests #1 - #3
- Used Reallocation Sectors
- Other Timeouts
- Failed Recovery Read Error
- Failed Recovery Write Error
- Format Error
- Self Test Error
- Drive Not Ready Errors
- Reallocation Aborts

COMPAQ Diagnostics software must report a failure before drives or other assemblies should be considered for replacement. Even if the drive exceeds certain preset thresholds, it may still be operational, as the thresholds are set to provide warnings of degraded performance before actual failures occur. In some cases, it may be more effective to continue to monitor the drive for further problems and schedule system maintenance when appropriate.

! **IMPORTANT:** For more information and assistance with drive replacement, contact your Authorized COMPAQ Computer Reseller or Service Provider or call the Compaq Customer Support Center at 1-800-345-1518 in North America. In Canada, call 1-800-263-5868. Outside the United States and Canada, contact the local Compaq Computer Corporation office from which you normally receive support.

For more information, refer to "Interpreting Reports" later in this chapter.

SERVER MANAGER/R ALERTS

INSIGHT Manager receives on-the-network threshold alerts from the Server Manager board. These alerts carry information on the monitored item, when and why the alert occurred, the severity of the problem, and the threshold. Use the Server Manager Facility/R, which you can launch from INSIGHT Manager, to acknowledge and receive more information about the alert. INSIGHT Manager also monitors Server Manager board status and alerts you to board failures. See Chapter 4 for examples of using INSIGHT Manager and Server Manager/R together.

Table 2-6 provides a complete list of Server Manager board alerts.

! **IMPORTANT:** When INSIGHT Manager reports an alert listed in Table 2-6, you must also acknowledge the alert in the Server Manager Facility/R. Otherwise, the Server Manager board continues to attempt to deliver alerts to its Alert Destination list until the alert is acknowledged.

Table 2-6
INSIGHT Manager Server Manager/R Alerts

Alert	Indication
Board Failed	The Server Manager board may have a problem. Server Manager board commands are not being processed. *
Board Reset	The Server Manager board may have a problem, and you may lose threshold settings for some monitored items. The Server Manager board resets itself when it experiences an unrecoverable error. The Server Manager/R driver attempts to reload the configuration for the board. *
Board Timeout	The Server Manager/R driver has timed out waiting for a reply from the Server Manager board. The driver and the board are no longer communicating. *
Battery Failed	The battery on the Server Manager board is no longer working properly. You will lose your threshold settings when you turn the monitored system off. Back up the thresholds to diskette using the Server Manager/R support software. *
Asynchronous Communication Failure	The Server Manager board is no longer communicating with the external modem.
Blacklisting	Server Manager/R has detected a phone number that has been blacklisted. Blacklisting is a communications requirement for some countries outside North America. A blacklisting alert indicates that the Server Manager/R modem has blacklisted an alert destination phone number. Once blacklisted, that alert destination can no longer be called by the board. Blacklisting occurs only in international modems and is a requirement imposed by certain countries outside North America to prevent a phone number from being dialed multiple times without connecting. The number of attempts before a number is blacklisted is country-dependent.
Server Manager/R Alerts	Server Manager/R alerts that are translated into an SNMP alert (trap). You can also use Server Manager/R to receive more information and help on specific monitored items.

* If you suspect a problem with the Server Manager board, run COMPAQ Diagnostics software on the managed server. For more information and assistance, contact your local Authorized COMPAQ Service Provider or call the Compaq Customer Support Center at 1-800-345-1518 in North America. In Canada, call 1-800-263-5868. Outside the United States and Canada, contact the local Compaq Computer Corporation office from which you normally receive support.

ALERT MANAGEMENT

INSIGHT Manager sends alerts on the network to the management console. Depending on your operating environment, you may have one or many management consoles receiving alerts. Managing these alerts is important in order to use INSIGHT Manager effectively.

Alert Notification

You must establish alert delivery addresses for the management console to receive alerts from managed servers. See "Establishing Alert Delivery Addresses" earlier in this chapter.

INSIGHT Manager must be running (window or icon) to receive alerts. You can receive notification via Alert Popups (a popup window), Audible Alerts, or both. Toggle these features on and off at the Options menu. Every alert is automatically logged in the Alert Log, even if the Alert Popups and Audible Alerts are turned off.

NOTE: You are not required to view or acknowledge INSIGHT Manager alerts within a specified period of time, as is required with Server Manager/R. However, once the Alert Log is full, the oldest entries will be rolled off as new entries are added to the log.

If you receive a Server Manager/R alert at an INSIGHT Manager console that has been set up as the management console for both applications, you must acknowledge the alert in the Server Manager Facility/R console as well. If you do not acknowledge the alert in the Server Manager Facility/R console, the Server Manager board continues to contact alternative destinations in the Alert Destination list until the alert is acknowledged. Consider this when creating your Alert Destination list for each Server Manager board. Refer to Chapter 3 for more information on Server Manager/R, and Chapter 4 for a examples of using INSIGHT Manager and Server Manager/R together.

! **IMPORTANT:** If INSIGHT Manager is not running when an alert condition occurs, the alert is not logged.

NOTE: Alert Popups are not related to NetWare broadcast messages; therefore, the CASTON and CASTOFF commands do not affect Alert Popups.

Alert Delivery Using the NetWare SEND Command

Another alert delivery method uses the *CIM.INI* file and the NetWare SEND command to deliver line 25 broadcast alerts. The *CIM.INI* file has sections titled SERVER MANAGER TRAPS and IDA TRAPS. Seven traps are presented for each of these sections. These seven traps represent the actual software trap that would cause an alert.

The sections are presented in the *CIM.INI* file as follows:

```
[Server Manager Traps]
Trap1=
Trap2=
Trap3=
Trap4=
Trap5=
Trap6=
Trap7=

[IDA Traps]
Trap1=
Trap2=
Trap3=
Trap4=
Trap5=
Trap6=
Trap7=
```

Review the *CIMINI.TXT* file for trap definitions. The seven trap statements in each section are used to provide a path for a program that would be executed when that particular trap or alert is received.

You can use a different batch file for each of the different traps. A simple batch file can be created that uses NetWare to broadcast a message to individuals or a group of users when an alert occurs.

The two trap sections of the *CIM.INI* file can be edited as follows:

```
[Server Manager Traps]
Trap1=C:\ALERT\SM1.BAT
Trap2=C:\ALERT\SM2.BAT
Trap3=C:\ALERT\SM3.BAT
Trap4=C:\ALERT\SM4.BAT
Trap5=C:\ALERT\SM5.BAT
Trap6=C:\ALERT\SM6.BAT
Trap7=C:\ALERT\SM7.BAT

[IDA Traps]
Trap1=C:\ALERT\IDA1.BAT
Trap2=C:\ALERT\IDA2.BAT
Trap3=C:\ALERT\IDA3.BAT
Trap4=C:\ALERT\IDA4.BAT
Trap5=C:\ALERT\IDA5.BAT
Trap6=C:\ALERT\IDA6.BAT
Trap7=C:\ALERT\IDA7.BAT
```

The following are examples of batch files that execute at the alert:

SM1.BAT

```
F:\PUBLIC\SEND "SM BOARD FAILURE" TO COMPAQ/SUPPORT
```

SM2.BAT

```
F:\PUBLIC\SEND "SM BOARD RESET" TO COMPAQ/SUPPORT
```

IDA1.BAT

```
F:\PUBLIC\SEND "LOG DRV STATUS CHANGE" TO COMPAQ/SUPPORT
```

IDA2.BAT

```
F:\PUBLIC\SEND "SPARE DRV STATUS CHANGE" TO COMPAQ/SUPPORT
```

The batch files send messages to all members of the SUPPORT group on the server named COMPAQ. This message displays on the 25th line of monitors of all SUPPORT group members logged into server COMPAQ.

This method can also be used to call a pager, if you use a communications package allowing macro programs to be created. In this example, you could create a macro program to call a pager. This program would then be executed within the batch file. The batch file would include an entry to execute the pager program.

Requirements for the *CIM.INI* file to be used as an alternate method of alert delivery are listed below:

- INSIGHT Manager management console must be logged into the server that contains the individuals or group that will receive the alerts.
- INSIGHT Manager must be running on the management console.
- NetWare broadcast must be enabled at the workstation (using the CASTON command).
- All users to receive the broadcast message must be logged into the same server as the INSIGHT Manager management console.

  NOTE: When you send messages to groups, those group members who are not logged into the server do not receive the broadcast message. Broadcasts are controlled using the NetWare commands CASTON/CASTOFF. Refer to your NetWare documentation for details and syntax.

ALERT LOG

The Alert Log is a record of the alerts sent to the management console. These alerts can come from any instrumented server. The default number of alert entries in the Alert Log is 300. When the Alert Log is full, the oldest entries are rolled off from the list as new alerts are logged. You are notified that the log is full the next time you access it.

The default number of entries to the Alert Log is the optimum value for performance and for most circumstances. You can increase the number of entries in the Alert Log by editing the *CIM.INI* file, but this may affect INSIGHT Manager performance. For more information on editing the *CIM.INI* file, refer to the *CIMINI.TXT* file that was copied to the INSIGHT manager directory during installation.

When you access the Alert Log window, the number of unread alerts displays in the status bar at the bottom of the screen.

The Alert Log provides the following information about each alert:

- Description of the alert
- Date and time the alert was received
- Name of the server that produced the alert

Each item in the Alert Log is marked with an asterisk until you read its detailed information. This shows you the alerts you have acknowledged when you access the log.

REPORTING

INSIGHT Manager provides on-screen reporting through the management agents on the server. You can purchase separate agent packages to instrument additional servers. Once the server is instrumented, information about that server is reported online to INSIGHT Manager and collected in Btrieve databases for that server.

REAL-TIME INFORMATION

When you select a server from the Server List, bring up the Main System view, and click on a button such as Disk Storage, the information you receive is in real-time. When you click the button, INSIGHT Manager retrieves the information from the server. If you continue to leave the window open, the information on the screen will be updated in one minute intervals.

! **IMPORTANT:** If you are viewing windows for a server that goes off line, the open windows for that server automatically close. INSIGHT Manager will allow you to view the server information and will begin Automatic Data Collection once the server has come back on line.

The real-time information displayed on the screen is view-only. However, you can capture screens to Windows Clipboard, from which the screen can be printed or pasted into other applications.

Many of the disk storage, system board, I/O port, and environment items have a graph button. Select the graph button next to an item to display both Historical and Real-Time graphs. The Graph window appears. If you have enabled Automatic Data Collection at the Server Setup window, this window presents a historical graph on the selected items, showing performance over time, and a real-time graph showing the latest collected values. You can print graphs by clicking the Print button.

You can turn on grid lines parallel to the X (horizontal) and Y (vertical) axes by selecting the X Grid and Y Grid check boxes. These grid lines help you view the values more accurately. Click the Show Zero button to rescale the Y axis to show a zero.

For example, if you click the graph button on the Volts +5 item in the Environment window, the Y axis automatically scales to the maximum and minimum values collected up to the present. If the scale happened to be 4940 to 5000, the lines on the graph would appear more dramatic because the small variations in the voltage changes would be amplified. When you select Show Zero, the Y axis becomes rescaled starting at 0, causing the lines on the graph to become less detailed.

Similarly, the X axis automatically scales according to the number of data points being graphed (the Real-Time graph reflects 70 data points; the Historical graph reflects 200) and the amount of time to collect those data points. Depending on the item graphed, many changes over a shorter period of time (such as temperature) or a few changes over a longer period of time (such as physical drive seek errors) can display. As a result, different items graphed on the same server can have different X axis scales.

NOTE: Under conditions where the values of the monitored items fluctuate in short periods of time (for example, temperature and voltage), the Historical graphs may resemble a bar code. This is normal. It occurs when there are more data points to display than pixels available to display them, causing the graph display to become compressed.

The Reset button checks the server's Btrieve databases for the minimum and maximum values, determined by the lowest and highest values that have occurred since collecting began. Only the current values in the database are used to determine the minimum and maximum values. If the current minimum and maximum values are still in the database, the graph will not change.

HISTORICAL INFORMATION

Automatic Data Collection allows you to collect historical information about your servers. This information can be helpful with performance tuning, determining server health, and troubleshooting problems by providing information about your servers over time. For example, if you track total read and write operations for the server's logical drives, you can adjust SET parameters to favor read- or write-intensive environments. You can determine server environment problems by tracking temperature or voltage fluctuations.

Enable Automatic Data Collection on each server (up to ten servers per management console) for which you want historical information and report printing. Enable this feature for your critical servers. You may also require multiple management consoles if you need historical graphs or printed health reports for more than ten servers.

NOTE: The number of instrumented servers that you can view for real-time information is not limited by Automatic Data Collection.

Automatic Data Collection operates only while INSIGHT Manager is running. Keep the management console operational 24 hours a day to receive all alerts and collect complete databases. If INSIGHT Manager runs fewer hours than the servers on which it collects data, you may miss critical information.

If you have multiple management consoles running INSIGHT Manager, you have multiple sets of Btrieve databases, because these files reside by default on the console's local hard disk.

The default location or output path of the database files is in the INSIGHT Manager directory. You can change the location of the files by editing the *CIM.INI* file and specifying a new path. For more information on changing the initialization file, read the online Help, the *CIMINI.TXT* file, or "Modifying INSIGHT Manager" in this chapter.

INSIGHT Manager creates two Btrieve database files, *.BTP* and *.BTV* files, containing entries for a server's monitored items. You can estimate the size of the database files by following these formulas:

.BTP size = (n * c / 23 + 2 * c / 38) * 1024

.BTV size = (t + 2 * t / 46) * 1024

t = total items
c = total counter and gauges
n = number of points to store in database (default is 200 in *CIM.INI*)

.BTP files contain information on monitored items that change frequently, such as total reads and total writes, and historical information. *.BTV* files contain information on monitored items that do not change frequently, such as base memory, as well as the most recently collected values from the *.BTP* file.

The number of items reported on depends on your hardware configuration. For example, a COMPAQ SYSTEMPRO with two IDA controllers, eight internal drives, and two fully loaded COMPAQ Intelligent Array Expansion Systems would have more items on which to report than a COMPAQ SYSTEMPRO/LT with one IDA controller and four internal drives. The COMPAQ SYSTEMPRO would have a larger database.

To estimate the number of items reported with your specific hardware configuration, turn on Automatic Data Collection and print a health report using the Standard form.

Increasing the default value gives you more data points to report on, but has an adverse effect on the performance of INSIGHT Manager. It also significantly impacts the size of the Btrieve database file. This may be a potential problem if you have limited hard disk resources on the management console.

If you have increased the default value for data points collected, and later decrease the value, INSIGHT Manager performance improves, but the file size of the Btrieve database does not change. The number of sectors reserved does not decrease. To reclaim the disk space, delete the database file, and allow INSIGHT Manager to re-create the file. Remember that decreasing the number of data points can reduce the historical value of your printed health reports.

Another method for increasing the reporting period for historical information gathering is to use the default value for the number of data points, but increase the collection time period from the default of 30 minutes.

Historical information is updated differently than the real-time information displayed in the Main System view and other online windows. Automatic Data Collection collects information about the server every 30 minutes; real-time information is collected every 60 seconds while the window is open for that server. Thirty minutes is the default minimum value and can be increased in the *CIM.INI* file. Refer to "Modifying INSIGHT Manager" later in this chapter for more information.

Collected historical information is stored in a Btrieve database if a change occurred since the last data collection. For example, the first time the temperature value of 30 degrees Celsius is collected, it is added as a data point. Thirty minutes later, when the temperature value of 30 degrees is collected again, the value has not changed, so it is not added as a data point. However, the most recent *time* that this data was collected *is* changed.

GENERATING REPORTS

In addition to the on-line alerting and Alert Log, INSIGHT Manager allows you to print health reports on servers set up for Automatic Data Collection. A built-in scheduler allows you to run reports to be printed automatically. Print daily health reports to help you recognize important trends that may require ordering parts or scheduling preventive maintenance.

The Standard form prints all information that can be reported on a given server and its hardware configuration. You can also create and save custom forms that report only specific areas of interest on a daily, weekly, or monthly basis.

When you are editing or creating a custom report, you can choose, item by item, when a monitored item should print. The print options for a monitored item are always (A), never (N), when there is any change (C) in the monitored item, or only when there is a large change (L) in the monitored item. A large change occurs when the value for any item changes by more than two standard deviations from the average since the last report. (Information on standard deviations is available in the online Help.) You can also choose to print information in text or graphic forms for some items.

! **IMPORTANT:** The INSIGHT Manager print queue differs from the NetWare print queue. The purpose of the INSIGHT Manager print queue is to queue health reports that have been scheduled to print at the same time. For example, if you have three server reports scheduled to run at 8:00 a.m., these reports go into the INSIGHT Manager print queue.

In addition to the Standard form, six sample forms are included to report on specific areas of interest. You may also customize the following forms for your particular needs:

- **CONFIG** - Processor, bus type, ROM version, port addresses, memory, and so on
- **DRIVES** - Diskette and Hard Drive information, physical and logical drive status, and so on
- **ENVIRON** - Voltage and temperature information
- **SECURITY** - COMPAQ Security Configuration, such as Network Server Mode, Power on Password, and so on
- **SRVMAN** - Server Manager board settings and status
- **NOGRAPH** - Same as Standard form but without graphs

Interpreting Reports

INSIGHT Manager reports use the historical information of the monitored items collected in the database to provide the current value, the last reported value, the largest variation, the average value, and the standard deviation. The reports indicate changes that have occurred since the last report to draw your attention to the change. The header at the top of the page identifies the report with the following items:

- **System** - Name of the server
- **Database** - Name of the file where the managed data is stored
- **Date** - Date the report was printed
- **Time** - Time the information was processed
- **Report Period** - Time between this report and the last one specified
- **Form** - Name of the report form

The legend for the item types in the report is also in the header. The letters are used in the Type column to define the type of item on the report. The columns in the report are:

- **Item** - Identifies the managed item.
- **Type** - Identifies the item as one of the types listed in the legend.
- **Current** - Identifies the most recent value collected for that item.
- **Last Reported** - Last reported value associated with the previous printed report.
- **Largest Variation** - Difference between the minimum and maximum value since the last report of this item.

- **Average Since Rep**. - Average since the last time this item was printed in a report, calculated according to the Type. For counters, the average is the average rate of change. For gauges, the average is of the actual values.

- **Average** - Calculated according to the Type and based on all the values currently stored in the database for this item. For counters, the average is the average rate of change. For gauges, it is the average of the actual values.

- **Standard Deviation** - Indicates how much this item varies from the average, or normal value. This value is calculated according to the Type. For counters, it is the standard deviation of the rate of change. For gauges, the standard deviation is of the actual values.

An asterisk by an item indicates a change since the last time this particular report form was printed for that server. The asterisk marks items that have changed by more than two standard deviations from the average. This asterisk is a visual pointer to show unusual deviations.

Not all deviations are marked by an asterisk. For example, if the Temperature value increased a small amount each report, but it did not change by two standard deviations, it would not be marked by an asterisk.

Disk capacity is presented at the INSIGHT Manager console and in INSIGHT Manager reports. Remember that the value displayed is the actual available disk capacity, after DOS format (if used), NetWare partitioning, and Hot Fix Redirection Area creation.

Printing INSIGHT Manager Screens

In addition to standard printed reports, you can create printouts of any of the INSIGHT Manager screens by using Windows Clipboard and Paintbrush.

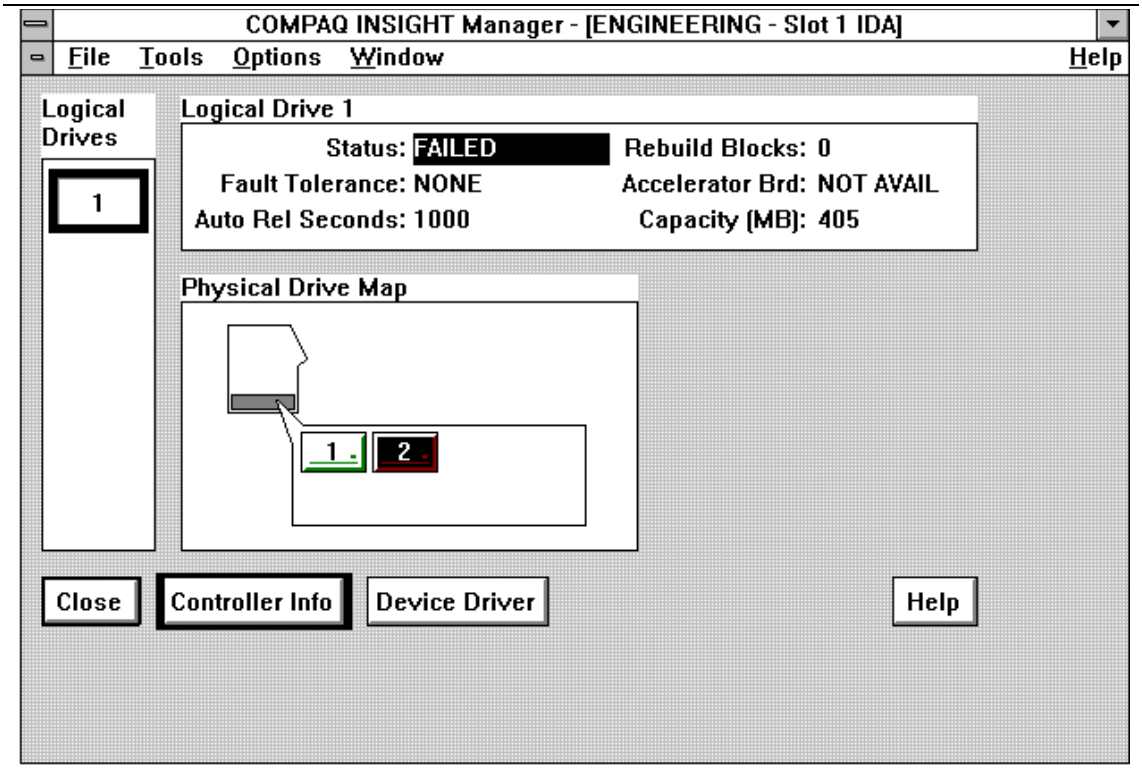
For example, in the case of a drive failure, you can print the IDA Logical Drive screen that shows the Physical Drive Map. This shows the location of the failed drive to be replaced. Printing this screen and attaching it to a work order gives the repair technician a clear picture of the drive to be replaced.

The following steps show how to print the screen mentioned in this example.

1. Select *Options* from the INSIGHT Manager menu bar, and turn off the Button bar.
2. Maximize the INSIGHT Manager IDA Logical Drive screen.
3. Press the **PRINT SCREEN** key on your keyboard to copy the screen contents to the Clipboard.
4. Start the Paintbrush application.
5. Select *View* from the menu bar and turn off the Tool Bar and Palette.
6. Select *Edit* and *Paste* from the Paintbrush menu bar. This will bring the contents of Clipboard into Paintbrush.
7. Select *File* and *Print* to send the IDA Physical Drive Map to your printer.
8. Select *Options* from the menu bar, and turn on the Button bar.

Figure 2-4 shows an example of an IDA Physical Drive Map that was captured and printed using these steps.

Figure 2-4
Example of Screen Printout



REPORTING INSIGHT MANAGER INFORMATION WITH THIRD-PARTY TOOLS

INSIGHT Manager reports are server-specific; each report covers one specific server. INSIGHT Manager cannot print a single report containing information from multiple servers. Because INSIGHT Manager stores historical data in Btrieve database files, you can use third-party products, such as Novell Xtrieve PLUS, to manipulate the INSIGHT Manager data and generate more customized reports. See Appendix A for more detailed information.

MODIFYING INSIGHT MANAGER

You can use a text editor, such as Microsoft Windows Notepad, to edit the *CIM.INI* initialization file and customize INSIGHT Manager. This file allows you to:

- **Add tools to the Tools menu.** To add applications such as SYSCON, FCONSOLE, or others on your local hard drive to the Tools menu, add this information to the TOOLS section of the *CIM.INI* file.

- **Set Alert Log size**. You can control the maximum number of alert entries kept in the log. The default value is 300; once this value is reached, the oldest entries are rolled off as new entries are added. Edit this information in the SETTINGS section of the *CIM.INI* file.

- **Specify the path to the Server Manager Facility/R.** By providing this information, you can launch SMF from the Tool Bar in INSIGHT Manager. This allows you to acknowledge Server Manager/R alerts passed to INSIGHT Manager without having to go to another window. Add this information to the SETTINGS section of the *CIM.INI* file.

- **Specify the output directory**. When Automatic Data Collection is turned on for a server, Btrieve database files are created and stored in the INSIGHT Manager directory. If you prefer to have the files located in a different directory, you can specify the path of the alternate directory in the SETTINGS section of the *CIM.INI* file. If you specify output paths to a server, and you have multiple management consoles running INSIGHT Manager, you must have different output paths for each INSIGHT Manager application.

- **Set collected server database size and update interval.** You can control the maximum number of servers set up for Automatic Data Collection and the time interval for the data collection. You can set the number of servers from 0 to 10; the default value is 10. You can set the time interval for data collection for 30 minutes or more. Change these settings in the DATABASE section of the *CIM.INI* file.

- **Set graph line colors.** You can control the colors used for the graphs in the online displays. Make these changes in the GRAPH section of the *CIM.INI* file.

- **Set printed report parameters, font style and size, and so on.** You can change the appearance of the printed health reports by adjusting the margins, font, font size, column types, and column widths. Make these changes in the REPORT section of the *CIM.INI* file.

- **Launch another application when an alert is received.** When you receive IDA or Server Manager/R alerts, you can launch other applications. For example, you can write an application to call a pager number, or run applications, such as Digital Communications Associates, Inc. Crosstalk, that launch a script. Add this information to the IDA TRAPS and SERVER MANAGER TRAPS sections of the *CIM.INI* file. You can also run different applications for different alerts as illustrated in "Alert Delivery Using the NetWare SEND Command" in this chapter.

INSIGHT Manager must be restarted for the changes to take effect. Refer to the *CIMINI.TXT* file for more information.

Chapter 3
COMPAQ SERVER MANAGER/R

COMPAQ Server Manager/R allows you to monitor local or remote server subsystems and receive alerts. You can also take control of the server and make required changes using the Remote Console feature. Server Manager/R is a remote or off-the-network server management product comprising the following:

- COMPAQ 32-Bit Server Manager/R board
- COMPAQ Server Manager/R software
  - Server Manager Support software
  - COMPAQ Server Manager Facility/R (SMF)
- COMPAQ Server Manager Collector/R (SMC) - Available from your Authorized COMPAQ Computer Reseller or Service Provider

The Server Manager board contains a battery that allows you to connect to the server, via modem or direct RS-232 cable, even when power to the server is out. You can use the modem on the Server Manager board or use an external modem.

To connect to the server, you must configure the management PC and load the appropriate software.

Both Server Manager Facility/R (SMF) and Server Manager Collector/R (SMC) are Microsoft Windows-based applications. SMF communicates with the Server Manager board and presents status information on the management PC. SMC allows you to collect information on all or selected monitored items at assigned times, and generates management reports accordingly.

The Server Manager board monitors the system in which it is installed. Each system has three monitored classes:

- System Board
- Disk Storage
- NetWare

Within each of these classes are object icons. Each icon represents a list of one or more monitored items that directly relates to the object icon. The information presented is static or dynamic. For example, configuration information is static, while incremental disk error counters are dynamic.

This chapter discusses the following topics:

- Server Manager/R configuration
- Server Manager Facility/R overview
- Destination management
- System security
- Key monitored items
- Remote Console feature
- Server Manager Collector/R
- Special notes

SERVER MANAGER/R CONFIGURATION

The Server Manager/R documentation includes detailed information for installation and configuration of the Server Manager board and the SMF and SMC applications. This TechNote does not provide specific Server Manager/R installation information, but does provide key technical information to help you install and configure Server Manager/R for optimal use.

INFORMATION TRACKING

Use the worksheets in Appendix C to track all pertinent Server Manager board configuration information. Use the first worksheet to record the required hardware and software components for the management PC, as well as configuration information. Use the second worksheet to record configuration information for the monitored server.

! **IMPORTANT:** Any configuration information entered on the worksheets should be considered confidential and handled accordingly.

REQUIRED FIRMWARE

All EISA-based COMPAQ PC Systems and PC Servers shipped after the introduction of the COMPAQ Server Manager/R (in October 1991) are capable of communicating with the Server Manager board. For Server Manager/R to report complete status information, your system may require a minimum system firmware revision.

! **IMPORTANT:** For more information on COMPAQ Intelligent Drive Array Controllers and system board ROM firmware upgrades, contact your local Authorized COMPAQ Computer Reseller or Service Provider, or call the COMPAQ Customer Support Center at 1-800-345-1518 in North America. In Canada, call 1-800-263-5868. Outside the United States and Canada, contact the local Compaq Computer Corporation office from which you normally receive support.

COMMUNICATION OPTIONS

You have several options available when you configure the communications connections for the Server Manager board. The Server Manager board is equipped with a 2400-baud internal modem and an external serial port.

Monitored Server

You can use a higher baud rate than the on-board 2400-baud modem by using an optional external modem. Also, a direct connection between the monitored server and the management PC supports 9600 baud. Connection to an external modem or a direct connection to the serial interface of a management PC is made through the serial interface of the Server Manager board. This interface supports speeds up to 9600 baud. A standard 9-pin RS-232 connector is required to use an external modem or direct connection with the serial interface. This cable must conform to the cable pinouts provided in Server Manager/R documentation.

Direct connection is convenient, but has some limitations: connection is limited by the length of the cable, and can only monitor a single server. Direct connection is useful if you are monitoring only one server or if you are resolving problems with Dial-Back connections. Refer to "System Security" later in this chapter.

While an external modem can provide faster data transfer rates than the integrated modem, a power failure may prevent connection to the Server Manager board.

The integrated enhanced 2400-baud modem uses speed buffering, which increases data transfer rates. Using the integrated modem and another enhanced 2400-baud modem at the management PC provides data transfer rates greater than 2400 baud. You can also achieve increased data transfer rates using the integrated modem and a 9600-baud modem at the management PC.

Because both methods of connection have advantages and disadvantages, the best solution is often a combination of direct connection and the integrated modem.

Once the Server Manager board has been physically installed in the monitored server and you have decided which type of communication to use, run the COMPAQ EISA Configuration Utility. Refer to the Server Manager/R documentation for detailed configuration information. Use the worksheet provided in Appendix C to record Server Manager/R configuration information. To maintain system security, this information should be considered confidential.

The internal modem settings section of the COMPAQ EISA Configuration Utility does not require any modification unless the management PC is using a 300-baud modem for communication. If the monitored server's integrated modem is set at the default of 2400-baud, and it attempts to connect with a management PC using a modem set at 300-baud, connection cannot be established. This is true whether the management PC modem is internal or external. In this case, you must set both modems at 300 baud. Avoid using a 300-baud modem at the management PC because of slow performance.

NOTE: During configuration, the Server Manager board uses IRQ 2 by default. IRQ 2 is commonly used by ISA NICs. For this reason, you must manually add all ISA boards during EISA configuration to avoid interrupt conflicts.

Once the Server Manager board is configured, begin installing the support software for the NetWare environment. This software includes five NLMs:

- *CPQCAGNT.NLM* - Collection agent that filters requests from the instrumentation agents to the Server Manager board.
- *CPQSYSMN.NLM* - Device driver for the Server Manager board.
- *CPQDAIA.NLM* - Instrumentation agent for COMPAQ Drive Array Controllers.
- *CPQNWAI.NLM* - Instrumentation agent that collects operating system data and reports it through the collection agent to the Server Manager board.
- *CPQCAUI.NLM* - Collection Agent User Interface that provides a NetWare console screen interface.

For complete installation details, refer to the Server Manager/R documentation. After the support software is installed, modify the *AUTOEXEC.NCF* file to include LOAD commands for the Server Manager/R NLMs.

NOTE: Failure to load all disk and NIC drivers and mount all drives before loading the Server Manager/R NLMs can result in incomplete reporting.

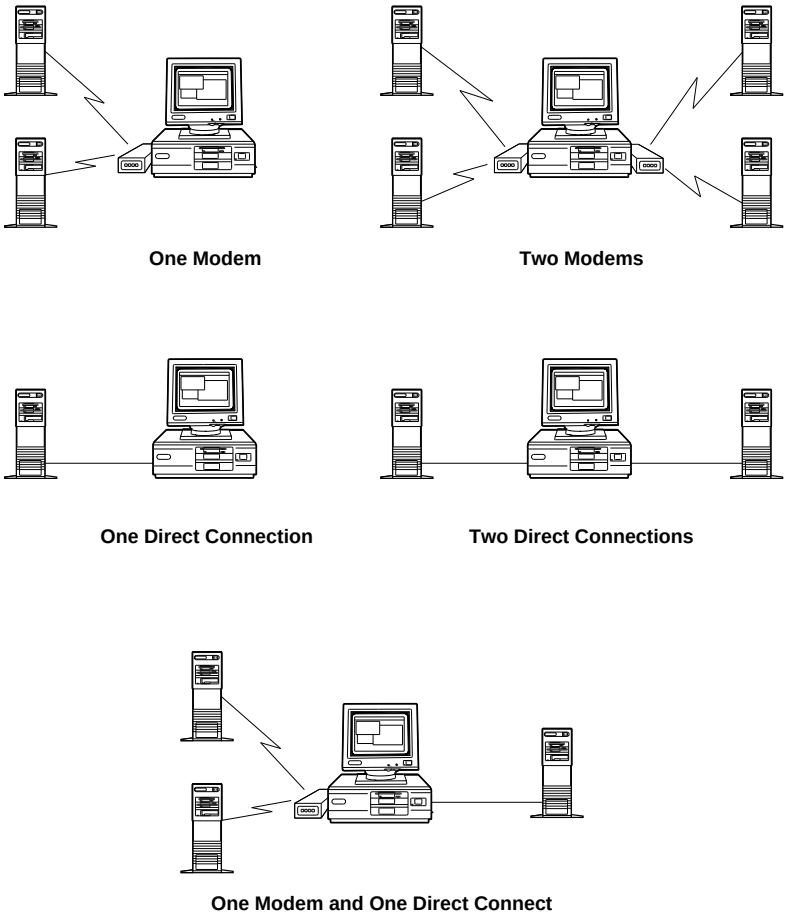
Management PC

The management PC communicates with the Server Manager board to obtain information for SMF to display. Two methods are available for communication:

- Modem - The management PC requires a modem supported by the Server Manager/R. You can use up to two modems at the management PC to receive alerts and communicate with monitored servers.
- Direct Connection - Direct connection requires a null modem cable conforming to the pin-out described in the Server Manager/R documentation.

If your management PC has two COM ports, you can use a combination of modems and/or direct connections to communicate with the monitored server(s). See Figure 3-1 for combinations of communication options.

Figure 3-1
Communication Options



Regardless of the communication configuration used at the management PC, the serial ports must be enabled and configured using the COMPAQ SETUP Utility for ISA computers, or the COMPAQ EISA Configuration Utility for EISA-based computers. The following table lists different ways to set up communications for the management PC.

Table 3-1
Communications Setup Configurations

Function	Description
One modem on the management PC	This option is appropriate for monitoring a limited number of servers.
Two modems on the management PC	If you plan to monitor many systems, having two modems on the management PC lets you communicate with one system while you use the other modem to receive alerts from other servers.
One direct connection between the management PC and the monitored server	Use a null modem cable to connect the management PC and the Server Manager board. This allows 9600-baud transmission, but you can monitor only one system.
Two direct connections on the management PC	Use two direct connections to devote the management PC to monitoring two servers. This allows 9600-baud transmission for both connections, but the management PC must be physically connected to both monitored servers.
One modem and one direct connection on the management PC	If you plan to monitor one local server and a limited number of remote servers, use this option.

After you decide on the communication method and configure the management PC, install the SMF software. Refer to Server Manager/R documentation for detailed installation information. Use the worksheets provided in Appendix C to record SMF configuration information. To maintain system security, this information should be considered confidential.

NOTE: If you plan to use two connections at the management PC, you must specify which one will be used to call monitored servers. In SMF, select one of the connections as the dial-out port. The dial-out port is used to call monitored servers. If only one connection is specified, use that connection as the dial-out port.

COLLECTION AGENT USER INTERFACE (CPQCAUI.NLM*)*

CPQCAUI.NLM is the Collection Agent User Interface NLM that provides a full-screen user interface and management functions at the NetWare server console. Placing a LOAD command for this NLM in the *AUTOEXEC.NCF* file is optional. You can load and unload *CPQCAUI.NLM* as needed. *CPQCAUI.NLM* provides the ability to toggle alerting and battery power. Use these options by selecting them within the *CPQCAUI.NLM* Available Options menu.

NOTE: Unloading *CPQCAUI.NLM* does not affect data collection or alerting.

BATTERY MAINTENANCE

Once the Server Manager board is installed and powered on, it begins charging its internal battery. The Status Indicator on the board mounting bracket is amber during the charging process. A green light indicates a full charge. Charging a new or completely discharged battery takes six hours.

At some point, you may choose to remove the Server Manager board from the monitored server. You *must* disable the battery first. Use the *CPQCAUI.NLM* console screen to disable the battery.

Δ **CAUTION:** Disable the Server Manager/R battery before removing the board, or damage to the board may result. If you disable the battery and remove the Server Manager board from the server, the board loses the contents of its memory. Run the COMPAQ EISA Configuration Utility to re-initialize the configuration.

Once you have reconfigured the board and loaded the software on the monitored server, the battery is automatically enabled.

SERVER MANAGER FACILITY/R

Once you have loaded and configured the SMF software, familiarize yourself with the monitored objects and their corresponding thresholds. Carefully determine the default state of each monitored item. Study the monitored items, determine which items you should enable for that particular server and site, and enable alerting for those items. Once you have enabled alerting for the monitored item, determine and set optimal threshold values.

! **IMPORTANT:** Alerting is *not* enabled by default for many monitored items.

THRESHOLD MANAGEMENT

Before you make any modifications to default threshold values, carefully study each item and its relation to the system. You may find it necessary to audit your system for a few days, using SMC to collect data about system use. Auditing your system allows you to determine baseline values for key monitored items. Understanding each monitored item, its threshold value, and system use helps you set optimal threshold values and avoid nuisance alerts. In many cases, the default values are appropriate. After you gain experience with the Server Manager board, you may choose to modify the threshold values or disable alerting for certain monitored items. Avoiding nuisance alerts is key to maximizing productivity.

For example, within the NetWare class of monitored items is the Network Interface Controller (NIC) object. The NIC object contains monitored items that directly relate to the General Statistics and Custom Statistics reported by that NIC driver to the NetWare *MONITOR.NLM*. The monitored item No ECB Count is directly related to the amount of network traffic and the value of the Minimum Packet Receive Buffers statistic.

During initial system growth and dynamic tuning by the NetWare operating system, this ECB counter is likely to increment if you use the default value (10) for the SET MINIMUM PACKET RECEIVE BUFFERS parameter, and you set the SET MAXIMUM PACKET RECEIVE BUFFERS parameter high enough to allow this growth. However, once the system reaches its normal settings, this counter should not increment except in times of extreme load. If the system is new and recently brought on line, you may choose to leave No ECB Count disabled. This eliminates nuisance alerts while the system is tuning.

Once the system has dynamically tuned itself and you have determined a baseline value, set a threshold that exceeds the baseline value, and enable No ECB Count alerting. Use this item as a key indicator to alert you if unusual loads are placed on that physical segment of your network.

! **IMPORTANT:** Always enable alerting and use the default threshold values for *all* Disk monitored items. Refer to Table 3-4 for more information.

Once you are familiar with Server Manager/R and have set the threshold values appropriately, save these values with a backup. Follow these steps:

1. At the server's *CPQCAUI.NLM* console screen, select the *Threshold Management* option under Available Options. You are prompted with four menu items.
2. Select *Backup Current Thresholds To A File*. A default filename, *CPQTHRSH.MSB*, is provided. You can choose to use a different filename.
3. Record the file name on the worksheet in Appendix C. Save the file to an alternate location.
4. If Server Manager/R data is lost, use this file to restore the desired threshold values. Select *Restore Thresholds From A Backup File* at the Threshold Management menu.

ALERT MANAGEMENT

Information reported by the Server Manager board falls into four categories:

- Informational
- State
- Rate counter
- Range

Informational items have no counter, and report monitored item information. Examples include server name, network number, and so on.

States are either ON or OFF. For example, the Serial Port monitored item within the System Board class provides a Carrier Detect item. If the state is zero, then Carrier Detect is not active. If the state is one, then carrier detect is active.

Rate counters are incremental. For some objects, a single increment can indicate a possible problem.

Ranges include temperature. If the current temperature of a server falls outside the specified range, an alert is generated.

Interpreting Alerts

For many objects, a single increment can indicate a possible problem. For other objects, the rate of incremental occurrences is key to understanding the severity of the alert.

For example, if you receive one Seek Error increment over time, you should not be alarmed. This is a natural event with normal disk use over time. If you receive multiple Seek Error increments in a short period of time, monitor the Functional Tests items. Functional Tests indicate how well a physical drive is performing. These tests compare the way the physical drive currently operates with the way it worked when it was new. New drives operate at 100 percent. As the drives wear over time, this percentage may decrease. A decrement in the Functional Tests means that drive performance is beginning to degrade.

If the drive performance appears to be degrading, run COMPAQ Diagnostics software. The Diagnostics software runs a series of tests, and indicates whether the drive should be replaced. When the Functional Tests value degrades to 80 percent, you receive an alert, and you should consider replacing the drive.

Specifying Alert Timeout

You can specify the amount of time that SMF waits for a response before disconnecting from the Server Manager board. By default, SMF waits five minutes. To adjust the amount of time that SMF waits for a response, follow these steps:

1. Highlight the Configure menu, and select the *Alert Timeout* option.
2. Use the **UP** and **DOWN ARROW** keys to increase or decrease the number of minutes (from 0 to 9) that SMF will wait for a response.
3. Select *OK* to close the dialog box.

If you respond within the timeout period, then that alert is not sent to other destinations. If you do not respond within the timeout period, the board sends the alert to the next destination.

Sending Alerts

In addition to sending alerts to the management PC, telephone, or pager, the Server Manager board can also send alerts to the following:

- NetWare server console display screen
- All members of the CPQCAGNT_OPERATORS user group
- NetWare system error log, which can be viewed with the NetWare SYSCON utility

Use the SYSCON utility to set up the CPQCAGNT_OPERATORS user group. All members of this group receive network-based alerts on line 25 of their workstations.

NOTE: If the CPQCAGNT_OPERATORS group is not configured, all network-based alerts go to users with SUPERVISOR-level access. If the group exists but contains no members, alerts go to the NetWare system error log only.

Disabling Alerts

Disable alerts during scheduled server maintenance or when adding components to the server. Alerts are not required when you know when and why the server is down. Disable alerting at the server using the *CPQCAUI.NLM* console screen.

> **!** **IMPORTANT:** Always remember to enable alerting once maintenance is completed.

DESTINATION MANAGEMENT

Destination management includes carefully planning the Alert Destination list, using scheduling, and testing alerts and the Alert Destination list.

For example, you may have six entries on the Alert Destination list. The primary administrator voice alert is the first entry after the management PCs, followed by several voice and pager destination entries. (See "Complex List" later in this chapter.) When a threshold is exceeded, the Server Manager board begins issuing alerts according to the Alert Destination list. The primary administrator receives a pager alert, and then a voice alert via his or her home phone. To respond to the alert, the administrator uses a management PC at home to dial into the Server Manager board and acknowledge the alert. This stops the alerting process and prevents additional personnel from being alerted.

Your ability to contact the Server Manager board is based on timing. The dial-in connection can only occur if the Server Manager board is *not* dialing out, or if you are using two modems, one for dialing in and one for dialing out. If the Alert Destination list specifies a high number of retries, it might take some time to connect with the Server Manager board and acknowledge the alert.

In the case of phone alerts, however, it can be beneficial to specify several retries. If the person answering the telephone is not aware of the Server Manager board function, he or she may not understand the meaning of the message. Several retries could be helpful in this situation.

Perform several short tests with the alerting procedure to become familiar with the Server Manager board before you implement it in a "live" environment. See "Testing Alerts and the Alert Destination list" later in this chapter.

ALERT DESTINATION LIST LENGTH

Plan the Alert Destination list carefully. Short, concise lists offer many benefits.

Too many destinations can cause unnecessary alerting and extend the time required for the Server Manager board to complete the alerting process. Remember that timing is critical to acknowledging the alert and ending further alert notifications. If the Retries option is set at zero for a destination entry and an alert occurs, the Server Manager board makes one attempt to contact that particular alert destination. If the Retries option is set at one, then the Server Manager board makes two attempts to alert that destination.

NOTE: The maximum number of retries that can be set for any alert destination entry is 31.

Having numerous destination numbers on the list or enabling an excessive number of retries can hinder your ability to respond to an alert. For example, an Alert Destination list of 16 phone numbers with 30 retries each can cause the Server Manager board to call its Alert Destination list for over 21 hours on a single alert, assuming that the last person on the Alert Destination list is the only one available to answer the call. If this situation occurs, and you can access SMF, abort the process and use SMF to modify the Alert Destination list. You can also disable alerting at the server and use the COMPAQ EISA Configuration Utility to modify the Alert Destination list.

SCHEDULING

The Alert Time Schedule window allows you to select specific times when the Server Manager board will use a particular destination. For instance, if you want to receive alerts on the management PC at your home only in the evenings, use this window to set a specific schedule for that management PC. By default, all times are valid. Select a block of time when the Server Manager board should *not* try to contact an alert destination. Select this block of time in one of two ways:

- Using a mouse, press the mouse button and drag the pointer to select times when alerts should not be sent to this destination.
- Using the keyboard, press the **SHIFT+ARROW** keys to highlight the area you want to select, then press the **SPACE BAR** to select times when alerts should not be sent to this destination.

  NOTE: If an "X" shows in a time block, the Server Manager board can send alerts at that time. To reschedule blocks of time, select the Scheduled Time option, then select the blocks of time that you want to reschedule.

Scheduling benefits networks with multiple servers and a large support staff, and may be especially beneficial if your network is supported by personnel working in multiple shifts. Scheduling can be simple or complex. You can also use scheduling to restrict multiple alerts for a single incident when using Server Manager/R and INSIGHT Manager together. Refer to Chapter 4 for more information on using Server Manager/R and INSIGHT Manager together.

You must base your decision to use scheduling on the hours of operation, site support policies, and whether you are using other server management tools.

ALERT DESTINATION LIST EXAMPLES

The following sections illustrate the three kinds of Alert Destination lists:

- Simple
- Semi-complex
- Complex

Simple List

A small, single server network that runs non-mission-critical applications with one support person would require a simple Alert Destination list. The list includes two destinations, no retries, and no use of scheduling.

		Retries
1.	Management PC	0
2.	Pager Number	0

Semi-Complex List

A somewhat more complex site has two or more servers. One of these servers runs a critical application that must be available until midnight. One support person is responsible for keeping that server available until midnight, so scheduling and retries have been incorporated. This example requires a semi-complex Alert Destination list.

		Schedule	**Retries**
1.	Management PC	8 a.m. - 5 p.m.	1
2.	Pager Number	24 hours	1
3.	Home phone	5 p.m. - 8 a.m.	2

Complex List

An example requiring a complex Alert Destination list is a large, multiple server site, running mission-critical batch applications during the night. These batch jobs must be completed before the start of business the following day. For this reason, multiple support personnel are listed, and scheduling and multiple retries are incorporated into the Alert Destination list. Note the retry count for the home/voice alerts.

		Schedule	**Retries**
1.	Management PC Primary	8 a.m. - 5 p.m.	1
2.	Management PC Secondary	8 a.m. - 5 p.m.	1
3.	Primary Pager	24 hours	2
4.	Secondary Pager	24 hours	1
5.	Primary Home/Voice	5 p.m. - 8 a.m.	3
6.	Secondary Home/Voice	5 p.m. - 8 a.m.	2

TESTING ALERTS AND THE ALERT DESTINATION LIST

Once you have configured SMF, test the Alert Destination list. Testing is discussed in detail in the Server Manager/R documentation.

To test the Alert Destination list, follow these steps:

1. Run COMPAQ Diagnostics software at the monitored server, and make sure that you are *not* using SMF to communicate with this monitored server.
2. From the list of test options for the Server Manager board, select *Generate Test Alert*. The Server Manager board sends an alert to all entries on the Alert Destination list. The alert message number displayed by pager or relayed by a voice message on a telephone is "057."

NOTE: When an alert is sent to the management PC, do *not* click on the Alert Log button or the Resume button until you are sure that all alert destinations have been tested.

You may encounter situations during testing in which an expected alert does not occur. Table 3-2 describes typical causes of testing problems and recommended actions.

Table 3-2
Causes and Recommended Actions
If An Expected Alert Does Not Occur

Cause	Recommended Action
Schedule for this destination entry indicates the time is not valid for delivery when the alert occurs.	View schedule for this destination entry, and alter as needed.
Destination entries alerted out of order.	View Alert Destination list, and confirm the order in which alerts should occur.
Alerting has been disabled at the host with the **CTL+ALT+END** keys or through application software interaction.	Reenter key sequence at host. Three long beeps indicate alerting was active but is now disabled. Three short beeps indicate alerting was disabled but is now active.
No pager alert is received when expected. The paging service could be down temporarily.	Contact pager service, or dial pager number directly to listen for carrier (instead of busy signal or no answer).
External modem used to reach destination entry, but inadvertently disconnected or power is turned off.	Examine external modem condition at server.
Lengthy Alert Destination list is causing excessive delay in reaching destination entry.	Wait until alerting is completed, or recompose list and generate test alert again.
SMF has an active session established with the board, but has left the Current Location field unassigned. Two problems result: SMF does not receive alerts, and the board is unable to disconnect in order to continue delivering alerts to valid destinations. Alerting is, in effect, completely disabled.	Set a Current Location at the SMF.
Only one delivery attempt has been allowed for the destination entry (for example, number of retries = 0) and the alert delivery attempt occurred while the line was busy.	Use COMPAQ Diagnostics software to generate TEST ALERT. For Voice and SMF case, both the Test alert and Failed alert should be delivered.
Board entered battery mode (for example, host power failed) without full charge. Reserve charge was exhausted before the alert could be delivered to destination entry.	Watch for expected alert when host power returns.
Expected alert is *not* Power Failed alert, but this alert occurs before expected alert can be delivered. In case of pager, *only* the Power Failed alert is delivered before host power returns.	Watch for expected alert when host power returns.

SYSTEM SECURITY

Record your security information on the worksheets in Appendix C when configuring the Server Manager board with the COMPAQ EISA Configuration Utility and during SMF setup. Once you have recorded this information, store it in a secure place. System security depends on your ability to maintain this level of confidentiality. Use most or all of the available passwords to protect system access.

SYSTEM PASSWORD

Set the system password during COMPAQ EISA configuration of the Server Manager board. Record this password on the worksheets provided in Appendix C. You will need it when adding systems to be monitored by SMF. This password is case-sensitive.

When adding a system to the SMF server list, enter the system password exactly as it was entered during configuration. If you do not enter the password correctly, connection between SMF and the monitored server cannot occur.

The system password is critical in controlling access to the Server Manager board and to your system. If you are unable to connect to a system, verify that this password was entered correctly during SMF setup. If you are monitoring multiple servers, you could use the same password for every Server Manager board or use the NetWare SUPERVISOR-level password for that particular server. This can help eliminate confusion when you have multiple monitored servers, each containing a Server Manager board.

APPLICATION PASSWORD

Set the application password in the SMF application. Although setting this password is not required to use SMF, it ensures that the information displayed is available only to users who know the password. Change this password regularly to maintain a high level of security. Record this password and treat it as confidential. To set the application password, select the *Configure* option in the SMF window and follow the instructions.

! **IMPORTANT:** Once you have installed the Server Manager board in a server and configured SMF, anyone with access to SMF also has access to your servers. For this reason, implement an application password at every management PC.

TONE PASSWORD

Tone Password is the numeric password used from a touch-tone telephone to confirm the proper recipient of a voice alert. The Tone Password has a maximum of four digits. If you do not enter the correct Tone Password during a voice alert, the Server Manager board considers the alert undelivered, and continues the alerting process. When you enter the correct Tone Password, you receive a voice message that states the monitored server ID and error code. Detailed error code information is provided in the Server Manager/R documentation.

DIAL-BACK

Dial-Back is a security feature that ensures unauthorized users do not gain access to system information. If Dial-Back is enabled, when a management PC attempts to dial in, the Server Manager board hangs up and verifies the identification number (ID) of that management PC. If the Server Manager board determines that the ID is valid and matches an entry in the Alert Destination list, the board calls that management PC, using the Alert Destination list entry phone number.

When Dial-Back is enabled, it pertains to *all* management PCs. It can also provide cost savings for remote site monitoring.

NOTE: You can enable Dial-Back for some servers, and not others, and still manage the servers from the same management PC. Dial-Back is set for each Server Manager board individually.

1. Before you enable Dial-Back, update the Alert Destination list to include all management PCs that will dial into the server.
2. To enable Dial-Back, each individual management PC that will be used to gain access to that server must dial in and connect to the Server Manager board.
3. Once connected, you must click on the Current Location box. The Alert Destination list is displayed in the Current Location box.
4. Select your respective entry (the entry for your management PC) in the Current Location box.
5. When you select your entry, the SMF assigns an ID to that management PC.
6. When all management PCs have been added to the Alert Destination list, and each management PC has selected its current location, the *last* management PC to dial in should enable Dial-Back.

With Dial-Back enabled, when a management PC dials in, the SMF software passes the ID information to the Server Manager board. The Server Manager board uses this information to validate the user as a member of the Alert Destination list. If the ID information matches, the Server Manager board hangs up and dials that phone number. If the ID information does not match, connection is refused.

NOTE: Do not enable Dial-Back before all users are added to the Alert Destination list. If you do, only those users already added to the Alert Destination list who have selected their Current Location have system access.

! **IMPORTANT:** Before enabling Dial-Back, verify that:

- All members have been added to the Alert Destination list.
- All members have selected their Current Location from each intended management PC.
- All Alert Destination list information is correct.

Suppose the Alert Destination list contains only one management PC and phone number. If Dial-Back is enabled and the phone number in the Alert Destination list is *incorrect*, the Current Location phone number is also wrong. When the management PC dials the Server Manager board, the Server Manager board hangs up and attempts to call the *incorrect* phone number. At this point, no modem can access the Server Manager board, and Dial-Back cannot be disabled.

Only two methods can fix this problem. In the first method, you can set up a direct connection and disable Dial-Back, and then go to the other management PCs and set the Current Location for each one. In the second method, you can disable the battery, and turn off the PC.

NOTE: Dial-Back can be enabled if a combination of direct connection and an internal modem is used at the management PC. With this configuration, Dial-Back would be in effect for alerts delivered via the modem. For the direct connection, Dial-Back would not be in effect. Direct connection between the management PC and the monitored server does not use Dial-Back.

An example of Dial-Back use involves a large corporation with multiple remote computer sites. It uses typical accounting practices, which implement site-specific cost centers at each remote site. One of the remote administrators has been having ongoing performance problems with a new application. Each remote site has implemented Dial-Back for local users and corporate support.

The remote site has requested corporate support for their server in an attempt to resolve the performance problem. Because Dial-Back hangs up and calls the management PC back when the Server Manager board is contacted, the remote site is billed for any long distance telephone charges incurred. This allows corporate support to lend assistance without incurring any long-distance charges for their services.

KEY MONITORED ITEMS

The Server Manager board reports system information in three different classes:

- System board (and related system components)
- Disk storage (hard drives)
- NetWare (operating system environment information)

When you select a Class icon, object icons are displayed. Each object icon represents a group of monitored items. Review the Server Manager/R documentation thoroughly to understand all of the monitored items. This will help you determine which items are critical to a particular server's monitoring and alerting. The following sections discuss key items monitored for system health and maintenance.

NOTE: This is not a complete explanation of all object icons or their inclusive monitored items.

SYSTEM BOARD

Table 3-3 lists and explains key system board items monitored by the Server Manager board. This table lists *key* items, not *all* items monitored.

Table 3-3
Key System Board Items Monitored by Server Manager/R

Object Category	Item	Causes for Alerts	Comments
System Memory	Memory Parity	Bad memory chip, memory corruption, or lack of refresh	Catastrophic alert. Always enable alerting and use default threshold settings.
EISA Bus	I/O Check Count	Error on expansion board	May require system reset.
Serial Port	Carrier Detect	1=active, 0=inactive	Does not necessarily indicate that the communications application is functioning correctly; simply indicates that the port is active.
Parallel Port	Out Of Paper	Printer requires paper	If no print server or spooler is set up on the monitored server, this item can be disabled.
Power	Volts ± 5 ± 12	Variance of EISA bus power	Catastrophic; disable during server maintenance to avoid nuisance alerts.
Temperature	Temp, Temp Chg	System overheating, environment beyond tolerance levels	Critical alarm; use default values; *do not* disable.

DISK STORAGE

The Server Manager board shows icons for the disk class only if you have the corresponding hardware and proper support software installed on the monitored server. SMF displays the proper icons for drive arrays when the following conditions are met:

- Drives have the appropriate IDA controller firmware version.
- Drives are properly initialized with COMPAQ Diagnostics software.
- COMPAQ Server Manager/R Support Software is installed on the monitored server.

NOTE: Enable all of the disk monitored items and use the default threshold values.

Physical drives are the individual drives that make up the logical drive. SMF shows a separate icon for each physical drive. This particular object icon has 16 monitored items. Serial numbers display for some, not all, drive arrays. If the model and drive firmware are listed as unavailable, you have improperly initialized the drive array, or the server contains a drive that the Server Manager board does not recognize.

NOTE: Use all of the factory default values for physical drives.

By monitoring the drive values, you can make decisions based on performance trends on when to schedule preventive maintenance.

Three items should always be enabled: Seek Errors, Read/Write Recovery, and Functional Tests. By monitoring these items, you can take preventive action in maintaining system health. Over time, a hard drive will produce Seek and Read/Write Recovery Errors. This is a natural event with normal disk use over time. If a rapid increase in these values occurs, monitor the Functional Tests items more closely to determine if the hard drive is degrading. If the drive performance appears to be degrading, run COMPAQ Diagnostics software. When the Functional Tests value degrades to 80 percent, you should consider replacing the drive.

NOTE: Server Manager/R does not send alerts for Seek Errors unless you set a threshold and enable alerting. See "Threshold Management" in this chapter.

Table 3-4 lists and explains key disk items monitored by the Server Manager board. This table lists *key* items, not *all* items monitored.

Table 3-4
Key Disk Items Monitored by Server Manager/R

Object Category	Item	Cause for Alerts	Comments
Disk/Logical	Status/ Failed Drive	Multiple causes	Logical drive status. Refer to online Help for details.
Disk/Physical	Functional Tests # 1 - #3	Wear from normal drive use over time	Warning alert; indicates drive performance has degraded.
	Used Reallocation Sectors	Controller attempted to write data addressed for unusable sectors	Warning alert; monitor increment rate. If rapid, run COMPAQ Diagnostics software.
	Recovered Read Errors/ Recovered Write Errors	Wear from normal drive use over time, corrected through physical drive retries	Warning alert; indicates drive may be developing problems.
	Seek Errors	Wear from normal drive use over time	Warning alert; indicates drive may be developing problems. Monitor Functional Tests.

NOTE: For more information and assistance with drive replacement, contact your local Authorized COMPAQ Computer Reseller or Service Provider, or call the Compaq Customer Support Center at 1-800-345-1518 in North America. In Canada, call 1-800-263-5868. Outside the United States and Canada, call the local Compaq Computer Corporation office from which you normally receive support.

NETWARE OPERATING SYSTEM

In addition to monitoring information about system hardware and hard drives, the Server Manager board also gathers information from the operating system. This allows a comprehensive view of overall system health.

This class displays four object icons:

- NetWare Server
- VOL SYS
- Log Partition
- NICs

Additional items may be displayed if users are logged into the monitored server and if Print Servers are active on the monitored server.

NetWare monitored items refer directly to the operating system environment. This object icon has 11 monitored items. Several of these items could be important when you are trying to determine the server load, the performance impact, and its capacity for growth.

Table 3-5 lists and explains key NetWare items monitored by the Server Manager board. This table lists *key* items monitored, not *all* items monitored.

Table 3-5
Key NetWare Items Monitored by Server Manager/R

Object Category	Item	Cause for Alerts	Comments
NetWare Server	CPU Utilization	Server Use	No alerting. Use SMC to graph history.
	Current Connections	User Login	Status information. Alerting can be disabled. Use SMC to graph history.
	Peak Connections	User Login	Status information. Alerting can be disabled. Use SMC to graph history.
	Users Locked Out	Network login attempted with the wrong password	Warning alert. Enable alerting; use as a security violation indicator.
VOL SYS	Available Megabytes	User's desired minimum disk space has been reached	Status information. Enable alerting or use % Space Available item.
	% Space Available	User's desired minimum disk space has been reached	Status information. Enable alerting or use Available Megabytes item.

If you are using SMC, the monitored items listed above are important in determining the average load on the server. Using SMC, monitor and track all of the items listed above. Once you have determined a baseline value for each item, set a threshold that exceeds the baseline value. If any of these values exceed the set threshold, it indicates unusual activity on the monitored server. The Users Locked Out item can indicate whether a system security breach was attempted.

To determine threshold values, disable the alerting function for these items, and then use SMC to collect information at peak load times. Calculate the average values. Once you have determined this value, use it to set the threshold values.

If nuisance alerts occur repeatedly, adjust the Server Manager board threshold values to reflect the current normal server use. This is especially true for CPU Utilization, Current Connects, and Peak Connects. Determine the average/typical values prior to setting the thresholds. Once you have determined a consistent value, monitor and readjust the values when any major changes to the network occur.

REMOTE CONSOLE FEATURE

Another key feature of the Server Manager board is Remote Console emulation. Remote Console lets you manage all monitored servers from one centralized management PC, and access and control monitored servers regardless of their location. Using SMF, you can emulate the console screen and keyboard of the monitored server. When using Remote Console, multiple functions are available, including

- COMPAQ EISA Configuration Utility
- COMPAQ Diagnostics software
- Warm Boot
- Cold Boot
- Any text-based application

Remote Console is powerful. It allows you to minimize travel time and cost, as well as downtime. Remote Console allows you to take complete control of the monitored server. Details of the utilities, their use, and considerations are in the Server Manager/R documentation.

NOTE: When you use Remote Console, the monitored server beeps at regular intervals. This alerts others that you are using Remote Console emulation and that the monitored server keyboard is locked. You can disable beeping using the COMPAQ EISA Configuration Utility by selecting *Audible Alert* and *Disable.*

Δ **CAUTION:** Before you select Warm Boot or Cold Boot, always perform a formal shutdown using the NetWare DOWN and EXIT commands on the system to be booted. Failure to do so can result in damage to user files that were open and in use.

SERVER MANAGER COLLECTOR/R

Server Manager Collector (SMC) collects and stores information from any Server Manager board installed in a network server. You can request SMC to dial each Server Manager board at periodic intervals and retrieve its monitored information. The information is written to a text file, which can be imported into most spreadsheet software packages for analysis. For example, Compaq provides a Microsoft Excel macro that prints and graphs the data.

SMC is a standalone program, separate from the SMF application. Use SMC to:

- Get a broad overview of events occurring on a single system or multiple monitored servers.
- Plot monitored items over specific time periods to maintain a historical log or note sudden changes.
- Track specific events and obtain reports.
- Generate daily, weekly, or monthly system reports for management.

You may not wish to report on all of the information that SMC collects. Use the Select feature within SMC to flag the items you wish to include in your report.

The reporting function can be scheduled. For example, network traffic is typically heavy between 8:00 and 11:00 a.m., and slightly lighter after the lunch hour. Traffic in the afternoon is usually somewhat lighter than in the morning. Given this information, track server utilization during high traffic periods. Select *Utilization* as an item to track. Schedule the "snapshot" to be taken multiple times in the morning and afternoon. Use the *Append* option of Output Type.

By capturing server utilization information at peak traffic periods, you can understand how your server is handling peak loads. This is useful in determining how much additional load your server can handle. Server utilization is constantly changing, and finding an average is difficult. By using SMC to track this value, you can create a report that shows trends in server utilization for historical analysis.

NOTE: The Server Manager board can monitor all available items, but your report does not have to include this information every time the report is generated. For example, you may not want to include configuration information in every report; however, you may want to always include server utilization.

Data collection is done in two different ways: by overwriting the previously collected information or by appending the previous collection. You must decide which option fits your needs. Two methods of reporting are also presented: tabular and graphical.

SPECIAL NOTES

The following sections list special tips or techniques to remember when using Server Manager/R.

PAGERS

Server Manager/R supports the Telocator Alphanumeric Input Protocol (TAP) to deliver messages in a standard format for pagers that display alphabetic or numeric characters. SkyTel and the National Dispatch Center (NDC) offer paging services compatible with this protocol. Contact your pager vendor to determine if your pager supports TAP. TAP is required to receive pager alerts from Server Manager/R.

Pager signals have varying signal strength. Some pagers have problems receiving pages inside buildings, in areas with electromagnetic interference, and so on. For this reason, we do not recommend that you use pagers as sole recipients of alert delivery. Verify the receiving ability of your pagers with the vendor.

If the pager uses the NDC paging system and the message-number-to-text translation, enter five digits for the server ID or the translation cannot be performed.

MODEM CONNECTIONS

Set the baud rate in SMF and the baud rate on the Server Manager/R modem (internal or external) to the lowest common denominator baud rate of both modems.

If you use an enhanced modem (for example, the Server Manager board's built-in modem) to connect to a non-enhanced modem (without built-in error correction and/or compression), append the following to both the Answer and Originate strings for the enhanced modem:

```
&Q6
```

This causes the enhanced modem to function like a non-enhanced modem, and improves connection rates between the modems. It also keeps speed-buffering enabled.

NOTE: Two non-enhanced modems perform better than two dissimilar modems.

If you are having problems connecting two enhanced modems, append the following to both the Answer and Originate strings:

```
S36=7
```

This eliminates a negotiation step when one modem may time out waiting for the other. Another solution is to append the following:

```
S9=2
```

This reduces the carrier debounce time, which is sometimes set too high.

! **IMPORTANT:** When entering Originate, Answer, and Dial strings in the COMPAQ EISA Configuration Utility, be sure *every* parameter you enter is supported by the modem. Otherwise, the modem responds with an error, and the Server Manager board flags an error and disables the modem.

MODEM BLACKLISTING

Blacklisting is a requirement imposed by some countries outside North America to prevent a phone number from being dialed multiple times without connection. The number of attempts before a number is blacklisted varies by country.

A blacklisting alert indicates that the Server Manager/R modem has blacklisted an alert destination phone number. Once an alert destination is blacklisted, the board can no longer call that number. You must shut off power to the Server Manager/R modem.

Follow these steps for an external modem:

1. Disable alerting by pressing the **CTL+ALT+END** keys on the numeric keypad or by using the *CPQCAUI.NLM* console screen.
2. Disable asynchronous communications using the *CPQCAUI.NLM* console screen.
3. Turn the modem off, and then back on.
4. Enable asynchronous communications using the *CPQCAUI.NLM* console screen.
5. Enable alerting by pressing the **CTL+ALT+END** keys on the numeric keypad or by using the *CPQCAUI.NLM* console screen.

Once power is cycled to the external modem, it clears its blacklist, and the board's alerting functions work for all destinations.

For an internal modem, follow these steps to force the board into dormant mode:

1. Disable alerting by pressing the **CTL+ALT+END** keys on the numeric keypad or by using the *CPQCAUI.NLM* console screen.
2. Disable asynchronous communications using the *CPQCAUI.NLM* console screen.
3. Bring the server down.
4. Exit to DOS.
5. Turn the server off.
6. After five minutes, turn the server on.
7. Enable asynchronous communications using the *CPQCAUI.NLM* console screen.
8. Enable alerting by pressing the **CTL+ALT+END** keys on the numeric keypad or by using the *CPQCAUI.NLM* console screen.

Once power is restored to your system, the modem clears its blacklist, and the board's alerting functions work for all destinations.

PATCH311.NLM

PATCH311.NLM affects Server Manager/R's ability to obtain NetWare information by fixing known problems in CLib v3.11. *PATCH311.NLM* is a dynamic patch; it is in effect only while it is loaded. (Static patches perform modifications on the program file itself before it is loaded.)

PATCH311.NLM requires the released CLib v3.11 (dated February 14, 1991 or later) to be loaded on the server. If an incorrect version of CLib is loaded, the patch utility terminates with an error message. Load *PATCH311.NLM* from the console.

This patch is available from NetWire on CompuServe. Download *PAT311.ZIP*.

Chapter 4

INCREASING PRODUCTIVITY USING SERVER MANAGEMENT TOOLS

COMPAQ INSIGHT Manager and COMPAQ Server Manager/R allow you to increase your efficiency and productivity. Tasks that once took time and effort can be managed quickly and easily with INSIGHT Manager and Server Manager/R. These tools allow you to manage configuration changes, track the health of key server subsystems, recover from catastrophic network events, and manage remote servers, all from a single management PC.

For example, if you have a question about a server's available slots, a server's security configuration, or the ROM revision levels, you do not have to visit the server site or bring the server down. You can use INSIGHT Manager or Server Manager/R to check the configuration.

You can avoid costly downtime by using the alerting capabilities of INSIGHT Manager and Server Manager/R. Changes in status, warning signs of subsystem wear or degradation, and any system failures can be reported instantly, allowing you to take corrective action immediately.

These tools are useful by themselves - INSIGHT Manager for day-to-day administration, and Server Manager/R for critical or remote servers. Together, or combined with NetWare operating system tools, they offer an even more powerful server management solution.

This chapter discusses some of the considerations in combining INSIGHT Manager and Server Manager/R, and offers examples of their effective use.

USING INSIGHT MANAGER AND SERVER MANAGER/R TOGETHER

When you combine INSIGHT Manager and Server Manager/R to manage your server, you achieve an enhanced level of fault tolerant alerting over the individual use of each application. INSIGHT Manager even alerts you to Server Manager board failures and passes Server Manager/R alerts over the network.

FAULT TOLERANT ALERTING

INSIGHT Manager delivers alerts on the network using network cabling, where Server Manager/R delivers alerts remotely, or off the network, using telecommunications or direct serial connections. Using the two together provides the best of both. If the network cabling fails, INSIGHT Manager is affected, but alerting is still delivered via Server Manager/R. If the telecommunications fail, Server Manager/R is affected, but alerting is still delivered via INSIGHT Manager.

LOADING NLMS

The management agents for INSIGHT Manager and Server Manager/R are modular, so you load only the NLMs you need. For example, if you have both products installed, you need to load *CPQSYSMN.NLM* once. If your instrumented server does not have a drive array subsystem, then do not load the *CPQDSKSA.NLM* for the INSIGHT Manager or *CPQDAIA.NLM* for Server Manager/R.

For more information about INSIGHT Manager NLMs and their functions, refer to "Understanding the COMPAQ Management Agents" in the *COMPAQ INSIGHT Manager User Guide.* For more information about the Server Manager/R NLMs and their functions, refer to the Server Manager/R documentation.

MANAGING MULTIPLE ALERTS

Since INSIGHT Manager and Server Manager/R can be used individually as well as in combination, you can receive multiple alerts for a single incident that both applications monitor. The multiple alerts are a combination of "native" alerts, which are generated within the specific application, and "passed" alerts, which are passed from one application to another.

INSIGHT Manager can generate native alerts and pass alerts from the Server Manager/R. Refer to Table 2-6. For example, if a physical drive on your server has degraded so that its current value for the Functional Test #1 equals 80 percent or below, an alert occurs. It is possible to receive three alerts from this single incident:

- INSIGHT Manager gives a Physical Drive Threshold Exceeded alert
- Server Manager/R gives a Functional Test #1 alert
- INSIGHT Manager gives a Server Manager/R alert

The first two alerts are native; the alert is generated within the application. The third alert is passed from one application to another.

INSIGHT Manager allows you to control disk alerts that are passed from Server Manager/R. To restrict passed disk alerts, load *CPQSMBSA.NLM* using the /D option by placing the following command in the *AUTOEXEC.NCF* file:

```
LOAD CPQSMBSA /D
```

Server Manager/R allows you to be flexible in controlling alerting by using the scheduling feature. When you use Server Manager/R in combination with INSIGHT Manager, you may want to restrict multiple alerts during regular business hours. When you create your Alert Destination list in SMF, use the scheduling feature to disable alerting during regular business hours. See Chapter 3 for more information on Alert Destination lists.

Some other ways to control alerting include:

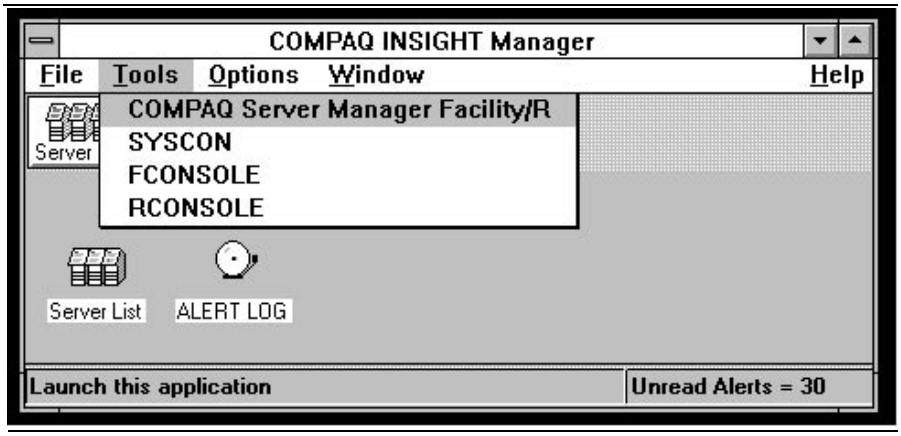
- Disabling alerts for each individual monitored item using SMF.
- Preventing all on-the-network alerts by not providing the workstation address in the *TRAPTARG.CFG*.

LAUNCHING OTHER APPLICATIONS

INSIGHT Manager provides a means to start, or "launch," other applications. This means you can access other applications without having to exit INSIGHT Manager. You can add SMF to the Button bar during INSIGHT Manager installation or add it later by editing the *CIM.INI* file. You can add other applications under Tools in the Options Menu bar. You may want to consider adding SYSCON, FCONSOLE, and RCONSOLE to your management console.

Figure 4-1 illustrates applications that can launch from INSIGHT Manager.

Figure 4-1
Launching Applications from INSIGHT Manager



For more information on modifying INSIGHT Manager, see "Management Console Configuration" and "Modifying INSIGHT Manager" in Chapter 2, and read the *CIMINI.TXT* file that is copied to the INSIGHT Manager directory during installation.

The following excerpt from the *CIM.INI* file shows how to set up SMF, SYSCON, FCONSOLE, and RCONSOLE to launch from INSIGHT Manager.

```
[TOOLS]
ToolName1=SYSCON
ToolPath1=z:\public\syscon.exe

ToolName2=FCONSOLE
ToolPath2=z:\public\fconsole.exe

ToolName3=RCONSOLE
ToolPath3=f:\system\rconsole.exe

[SETTINGS]
AlertDBSize=300
OutputDir=
SMFPath=c:\cpqsmf
```

SERVER MANAGEMENT EXAMPLES

The following sections illustrate using INSIGHT Manager and Server Manager/R as server management tools. Refer to the *Compaq and Novell Integration ToolKit* for information on backup strategies and verification and recovery procedures. The ToolKit also includes information on planning, installation, security, and performance optimization.

UPDATING SERVERS TO CURRENT REVISIONS

You can use the reporting capabilities of INSIGHT Manager for server configuration management as well as for monitoring server health. While configuration information has always been available through the COMPAQ EISA Configuration Utility and COMPAQ Inspect Utility, these tools require you to take the server off line. The following example illustrates time savings through online configuration management.

In this example, a business has a network of 200 users attached to 7 COMPAQ SYSTEMPROs or COMPAQ SYSTEMPRO/LT servers. Three of the servers are in a central administration building, and the other four are in remote warehouses throughout the city.

The network administrator reads about server performance enhancements in an industry publication. The performance improvements require a new driver release and a firmware upgrade, and the firmware upgrade applies only to certain older product models. The administrator needs to determine which servers require the firmware upgrade.

The administrator can physically inspect the server units, or use the COMPAQ Inspect Utility. These methods require either a site visit to each warehouse, or each server to be taken off line to run the COMPAQ Inspect Utility. Neither of these options is convenient or practical. Instead, the administrator can use INSIGHT Manager to retrieve and report the firmware revision of each server.

The administrator creates a custom form that lists the system ROM version number, the hard drive controller firmware revision level, NetWare 3.x driver name, and NetWare 3.x driver version number. This new report can run for each of the seven servers in only a few minutes.

The administrator can also create a custom report using a third-party reporting tool, such as Novell Xtrieve PLUS or Borland Quik Reports. Using one of these reporting tools with INSIGHT Manager databases requires some data preparation and manipulation. You may consider this process too time-consuming for a one-time report. This alternative is practical if the data files are already prepared and consolidated for other more frequently generated reports. For details on using third-party reporting tools with INSIGHT Manager databases, see Appendix A.

PREVENTIVE DISK MAINTENANCE

INSIGHT Manager's reporting capabilities can also monitor server health. The hard drive subsystem is one of the most important components of the server, and by generating a daily, in-depth report, you can be proactive in maintaining system reliability and data integrity.

Refer to Table 2-4 for a concise list of key disk monitored items that you should watch. The items on this list are disk "warning" items. By monitoring the "warning" items, you can prevent more serious problems. (Other disk items are monitored, but these are not "warning" items. If these items increment their counters, a major drive failure may have occurred.)

The administrator of a multiple-server site creates a custom disk report that includes many of the items illustrated in Table 2-4. The reports, one for each server, are scheduled to print during the evening to be available for review in the morning.

This evening, however, the support person on call receives an alert from the Server Manager/R installed in the Accounting department's server. The alert message number is 032, which indicates that a physical drive has had a Recovered Write Error during the month-end update process. This type of error occurs over time with normal drive wear. Mirroring is the fault tolerance method selected for this server. The administrator, to be on the safe side, dials into the Server Manager board and resets the threshold for that drive. The administrator on call does not receive any more alerts that evening.

The next morning, the printed Disk Report and the Alert Log from INSIGHT Manager confirm that a Recovered Write Error occurred. The administrator and the support staff continue to monitor the hard drive subsystem of this server throughout the day. As activity on this server increases, the disk continues to generate errors periodically.

At this point, the administrator schedules maintenance for this server and generates a picture of the drive array and the failing drive using Microsoft Windows Paintbrush (see the steps in "Printing INSIGHT Manager Screens" in Chapter 2). The administrator makes a service request, and attaches the picture to the work order.

After hours, the administrator runs COMPAQ Diagnostics software, and a failure is reported. Because the server had fault tolerance implemented, the regularly scheduled tape backup is able to begin. When the backup is complete, the technician replaces the failing drive and starts a disk rebuild. When the rebuild is complete, the technician does another backup. By 8:00 a.m. the next day, the system is restored to its original state. Proactive monitoring of the server prevented a hard drive failure, maintained data integrity, and minimized server downtime.

DISK FAILURE PRIOR TO SCHEDULED BACKUP

Server Manager/R alerts you in the event of a server subsystem failure. If a disk fails after hours, Server Manager/R can notify you at home, allowing you to begin recovery procedures immediately. You do not have to wait until morning to discover the problem and begin repairs. The following example illustrates how to use the Server Manager/R alerting and Remote Console features to minimize server downtime.

In this example, a COMPAQ SYSTEMPRO Model 2040 with two 1020-megabyte drive array pairs has Server Manager/R installed. This server is set up with distributed data guarding and two COMPAQ 1.3-/2.0-Gigabyte Digital Audio Tape Drives. A workstation is dedicated to run unattended backups with Cheyenne ARCserve.

Unattended backups are scheduled for 1:30 a.m. At 8:30 p.m., the Server Manager board detects a drive failure. Following the predetermined Alert Destination list, the Server Manager board notifies the system administrator at home via voice alert. Using the home-based management PC, the system administrator dials in with SMF, and verifies the drive failure. SMF identifies the failed drive number.

The system administrator contacts the technician on call, and asks the technician to replace the failed drive once a backup is completed. While the technician travels to the site, the administrator disconnects and exits SMF. The administrator uses Microcom Systems Inc. Carbon Copy to dial the office management PC and begins the ARCserve backup process from the ARCserve client. While the backup is in progress, the administrator dials in periodically to check on the backup status, using the Remote Console feature in SMF and the ARCserve server console screen.

Once the backup is complete, the administrator authorizes the service technician to replace the drive. The technician contacts the administrator when the drive replacement is complete. The administrator dials in, resets the system, and starts the rebuilding process when prompted during the Power-On Self-Test (POST). When the drive is rebuilt, the administrator brings the server back on line, and readies it for the following day's work.

By receiving the Failed Disk alert at home, the administrator could start the backup process early, call the service technician to replace the drive, and initiate the rebuild process. If the administrator had not been alerted during the evening, the failed drive would have caused degraded performance the next day. The server is up and running for normal business hours the next morning because the administrator could act on the alert when it occurred.

REMOTE SUPPORT TO MULTIPLE SITES

The following example illustrates benefits of the Server Manager/R Remote Console feature, which allows you to diagnose problems with the monitored server and make corrections and repairs from a remote site. The remote site can be an unlimited distance from the monitored server.

In this example, an enterprise-wide NetWare v3.11 network has multiple site locations, both at corporate headquarters and at remote offices. Each site holds one or more COMPAQ SYSTEMPRO servers, with a Server Manager board installed in each.

One of the remote sites requests network assistance with one of their servers, which is experiencing noticeable performance problems. The server is configured with one Ethernet segment and one 16-megabit Token Ring. The local administrator tells the system administrator that the only recognizable error condition is an abnormal increase in the NO ECB Error counter under LAN Statistics of the NetWare *MONITOR.NLM* server console screen.

The system administrator dials into the remote Server Manager board. Once connected, the administrator runs Remote Console emulation from within SMF to monitor the server. The NO ECB Error rate prompts the administrator to inspect the SET MINIMUM PACKET RECEIVE BUFFERS and SET MAXIMUM PACKET RECEIVE BUFFERS parameters.

The administrator discovers that these two parameters are equal. While the local administrator increased MINIMUM PACKET RECEIVE BUFFERS to help accommodate network needs, MAXIMUM PACKET RECEIVE BUFFERS remained at the default value. This meant that no additional buffers could be allocated when network traffic reached a level high enough to request more buffers. The system administrator, at the console, increases the MAXIMUM PACKET RECEIVE BUFFERS value by 150, and installs a permanent SET command in the server's *AUTOEXEC.NCF* file. This resolves the NO ECB Errors, and performance on the Ethernet segment shows noticeable improvement.

In addition to correcting the No ECB Count errors, the system administrator inspects other SET parameters to see if other operating system settings are optimal. The administrator notices that the SET MAXIMUM PHYSICAL RECEIVE PACKET SIZE parameter is not set at 4202, which is the optimal packet size when running at 16 megabits per second. The administrator discovers that no values have been set for this parameter in the *STARTUP.NCF* file, which indicates that the Token Ring is using the default physical packet size of 1130. The administrator adds the entry SET MAXIMUM PHYSICAL RECEIVE PACKET SIZE = 4202 to the *STARTUP.NCF* file. This change does not take effect until the server has been brought down and then up, so the administrator informs the local administrator of the changes, and requests permission to bring the server down and then up. Once the server is up again, the local administrator monitors its performance, and reports noticeable improvement.

In this example, the system administrator diagnosed the performance problems from a remote site, saving time and money. No travel was required, and the problems were identified and resolved quickly and efficiently.

MONITORING THE HEALTH OF A COMMUNICATIONS SERVER

The following example shows how the alerting feature of Server Manager/R can notify you of problems in a communications server.

A national company has multiple remote sites using NetWare servers. These servers run nightly sales totals and upload these totals to corporate headquarters using a dedicated phone line.

Server Manager/R, with alerting enabled, monitors Carrier Detect on the serial port. The Carrier Detect default is disabled; when alerting is enabled, the value is zero. If the carrier is active, this item is set to one and an alert occurs. During daily operations, this monitored item is set to zero, because the phone line is dedicated for nightly posting. For this reason, no alerts should occur during the day.

At night, however, an alert *should* occur when the sales posting process is completed and the upload begins. This notifies the system administrator that the serial port is active. This does not guarantee that the upload is functioning correctly, but it does inform the system administrator that the process has been initiated. The administrator expects an alert for this monitored item every work night. If the alert does not occur, the administrator knows that the upload process has not been initiated, and that there may be a problem.

ENVIRONMENT ALERTS

Server Manager/R monitors the physical environment of the server. When the physical environment of the server exceeds certain preset limits, the Server Manager board notifies you, allowing you to take protective action before your server is damaged. The Server Manager board can detect power fluctuations, power loss, and out-of-tolerance-range temperature variations. An alert in any of these categories might indicate the loss of power or air conditioning at the server site.

In this example, COMPAQ servers are located in a server room. Each server is on a Uninterruptable Power Supply (UPS) and has a Server Manager/R board installed. Each UPS is configured to issue the NetWare DOWN command after the servers have been on battery power for ten minutes.

If the building loses power for more than ten minutes after hours, the UPS brings the servers down. The system administrator receives a critical alert message # 51, Watchdog Alert for System Software, for each server. This alert indicates the Server Manager board is not receiving information from the Server Manager support software loaded on each server.

By dialing the servers, the system administrator can tell that each server is down. A call to the building's facilities personnel indicates that there was an emergency power shut-down. The system administrator returns to the office to start up all the servers once commercial power is restored.

REPORTING SERVER MANAGER/R ALERTS THROUGH INSIGHT MANAGER

The following example illustrates fault tolerant alerting, and the advantages of passing alerts between INSIGHT Manager and Server Manager/R. It also illustrates the flexibility of running other applications from INSIGHT Manager when these alerts occur.

A business' corporate headquarters keeps six servers and the management console secured in a restricted access area. The management console is dedicated to running INSIGHT Manager and is collecting historical information on all six servers for periodic reporting. A Server Manager board is installed in each server to provide after-hours alerting, remote server control, hardware configuration information, and diagnostic capabilities.

Since the management console is not manned continuously, INSIGHT Manager is set to broadcast alert messages to the ADMIN group using the NetWare SEND command for any disk or Server Manager alerts. Also, the Server Manager's Alert Destination list is scheduled to page members of the ADMIN group during normal business hours.

The Server Manager board fails on the Human Resources server. Since the board itself has failed, individuals on the Alert Destination list are not notified. However, INSIGHT Manager sends the following message to all members of the ADMIN group:

```
SM Board Failed on server HR01
```

The Server Manager board failure is also entered into the INSIGHT Manager Alert Log. The system administrator can schedule maintenance for the Human Resources server after hours so that COMPAQ Diagnostics software can be run to check the Server Manager board.

Then, the system administrator receives the following broadcast alert from the Accounting department's Server Manager board:

```
SM Alert on server ACCT
```

At this point, the system administrator knows there is an alert for the Accounting department's server, but does not know details about the alert. The system administrator clicks on the SMF icon at the secondary management PC, and connects to the ACCT Server Manager board. Once connected, the administrator receives the "Users Locked Out" warning message. The system administrator acknowledges the alert so that alternate destinations are not contacted, and then calls the accounting department. A temporary clerk has been attempting to log into the Accounting department's server, but has forgotten the user GUEST password. Once the user account is reset, the clerk can login with the correct password.

SUMMARY

Since the server is the most critical part of your LAN, you need management tools that help you keep server downtime to a minimum. Your servers must be managed with attention to configuration management and preventive maintenance, and they must recover quickly from any failures.

While many products provide information about the network itself, few provide information on the management and health of the server. COMPAQ INSIGHT Manager and COMPAQ Server Manager/R offer you the tools you need to efficiently manage your network server. Together, they provide a complete solution to meet your server management needs in today's network environments.

Appendix A
GENERATING INSIGHT MANAGER AD HOC REPORTS

This appendix is intended for the advanced user with an understanding of database technology.

COMPAQ INSIGHT Manager creates Btrieve database files of managed server information. Btrieve is a common format for database programs in the NetWare environment. Btrieve databases and INSIGHT Manager's use of the Simple Network Management Protocol (SNMP) standard allows you to use third-party reporting applications to gather and consolidate information into an ad hoc report.

The INSIGHT Manager database files are usually located in the INSIGHT Manager subdirectory. These files are identified by the extensions *.BTP* and *.BTV*. The first six characters of the database files are the first six characters of the NetWare server name. *.BTV* indicates an historical database; *.BTP* indicates an entry database.

This appendix discusses the use of Novell Xtrieve PLUS v4.01a and Borland Quik Reports to generate ad hoc reports.

! **IMPORTANT:** You must load Btrieve before Xtrieve PLUS. Use the following configuration command to start Btrieve:

```
BTRIEVE /M: 64 /P: 4096
```

where M = memory size in Kbytes
and P = page size in bytes

DATABASE SCHEMA

The following tables describe the schema in the INSIGHT Manager database. Use these schema to generate reports with Xtrieve PLUS.

Table A-1 lists the schema of the INSIGHT Manager historical database. This is the primary INSIGHT Manager database file, and contains all configuration information and the last recorded value of each parameter that is monitored by the INSIGHT Manager for an individual server. Each record in this table contains information about a different monitored item for that individual server. Each monitored server for which Automatic Data Collection has been enabled has an historical database associated with it.

Table A-1
Historical Database Schema

	Name	Type	Length	Description
*	MIBType	Integer	2	Type of MIB object
*	Reserved1	Integer	2	Reserved field
*	Reserved	Integer	2	Reserved field
*	Instance	Integer	2	Instance value
*	InstanceLow	Integer	2	Instance value
*	InstanceHigh	Integer	2	Instance value
*	InternalMIBNumber	Integer	2	Internal MIB Number
	asn1Size	Integer	2	Length of the ASN.1 Number
	asn1	String	128	ASN.1 Number
	desc	String	80	Text description of the MIB item
	type	Integer	2	Processing type
**	firstTime	Integer	4	First time this item was ever collected
**	lastTime	Integer	4	Last time this item was collected

* Indicates an indexed field. *Continued*

** Times are listed in number of seconds since 00:00:00 January 1, 1970.

Table A-1 *Continued*

	Name	Type	Size	Description
**	lastChangedTime	Integer	4	Last time this item changed
**	lastReportTime	Integer	4	Last time this item was reported
**	minMaxResetTime	Integer	4	Last time the min and max for this item was reset
	lastValue	Integer	4	Last value collected for this item
	minValue	Integer	4	Smallest value seen for this MIB item since minMaxResetTime
	maxValue	Integer	4	Largest value seen for this MIB item since minMaxResetTime
	stringLength	Integer	2	Size of the string
	string	String	256	Last string collected for string types

** Times are listed in number of seconds since 00:00:00 January 1, 1970.

The type field in Table A-1 indicates the classification of monitored item that each record describes. For example, some items, such as processor type, are static values, meaning that the item does not change frequently. Other items, such as total reads, are counter values, meaning that they increment continually. Table A-2 lists the INSIGHT Manager database element types that correspond with the value of the type field in the historical database.

Table A-2
Database Element Types

Value	Description
0	Counter value
1	Gauge value
2	Static value
3	Static Hex value
4	Enumerated value
5	String value
6	Octet string value

Many items monitored by INSIGHT Manager for each server increment or change frequently. Only the last recorded value is stored in the historical database for these items. The previously recorded values are kept in the INSIGHT Manager entry database.

Each entry database record contains monitored item information that includes the value of the item and the time the value was read from the server. The entry database contains detailed records only for monitored items that increment or change. It does not contain static data such as configuration information.

For example, the total reads monitored item increments frequently. If you monitored a constantly used server for 24 hours, the historical database would contain the last recorded value for total reads. The entry database would contain 48 records for total reads (one added every 30 minutes during Automatic Data Collection), each containing the number of total reads and the time the value was recorded.

Table A-3 lists the INSIGHT Manager entry database schema.

Table A-3
Entry Database Schema

	Name	Type	Size	Description
*	MIBType	Integer	2	Type of MIB object
*	Reserved1	Integer	2	Reserved field
*	Reserved	Integer	2	Reserved field
*	Instance	Integer	2	Instance value
*	InstanceLow	Integer	2	Instance value
*	InstanceHigh	Integer	2	Instance value
*	InternalMIBNumber	Integer	2	Internal MIB Number
	code	Integer	1	0 = Collected value 2 = Server went down
**	firstTime	Integer	4	Time of the entry
**	totalTime	Integer	4	Total time this entry is valid
	value	Integer	4	Value collected
	rate	Float	8	Rate of change of this item in values per second

* Indicates an indexed field.
** Times are listed in number of seconds since 00:00:00 January 1, 1970.

CREATING SINGLE SERVER REPORTS

Creating a simple historical report from the INSIGHT Manager historical database using a third-party tool, such as Xtrieve PLUS, involves several steps:

1. Building the data dictionary.
2. Building a database view.
3. Viewing or printing the report.

You may also wish to restrict your report to records that meet a given criteria.

BUILDING A DATA DICTIONARY

Xtrieve PLUS uses a data dictionary, which contains descriptive information about every data field and index in the Btrieve file. Before Xtrieve PLUS can recognize the data in your existing Btrieve file, you must add a definition to the Xtrieve PLUS dictionary that corresponds to the data in the Btrieve file.

To define a file in the Xtrieve PLUS dictionary, you must have a list of all the fields in your Btrieve file, in the order in which they are stored in the data record, along with the data type and length of each field. You must also know which of these fields are indexed. Refer to Table A-1 for a list of all the fields in the INSIGHT Manager historical Btrieve files.

To build an INSIGHT Manager historical database data dictionary, follow these steps:

1. Copy the INSIGHT Manager database file for your server (for example, *ACCTQ00.BTV*) to the Xtrieve PLUS subdirectory.

   NOTE: All INSIGHT Manager historical databases have a *.BTV* extension.

2. Select *Dictionary* at the Xtrieve PLUS Main menu.
3. Select *Define* at the Dictionary menu.
4. Enter the Location of the database file (for example, C:\XTRIEVE\ACCT00.BTV) and press the **ENTER** key.
5. At the File prompt, enter a descriptive file name (20-character maximum) and press the **ENTER** key. This is the name used within Xtrieve PLUS for that specific file (for example, "hist of cpq accting").
6. Enter the name, type, and size of each field in the database in the order in which they are located in the database. See Table A-1 for a list of the fields in the INSIGHT Manager historical database. Enter *all* the fields in the table.
7. When all the field information is entered, press the **ESC** key.
8. Select *Complete* from the Fields? menu.

   NOTE: If the table is not complete, select *Continue* to modify the fields, or *Abort* to begin again.

9. The Indexes menu displays. Select the field names in Table A-4 from the Indexes menu. Enter *Yes* or *No* according to the table, and using the default for Dup and Case.

Table A-4
Example Indexes Menu

Path	Field	Dup	Case	Asc	Seg
0	MIBType	Yes	No	Yes	Yes
	InternalMIBNumber	Yes	No	Yes	Yes
	InstanceHigh	Yes	No	Yes	Yes
	InstanceLow	Yes	No	Yes	Yes
	Instance	Yes	No	Yes	Yes
	Reserved	Yes	No	Yes	Yes
	Reserved1	Yes	No	Yes	No
1					

10. Press the **ESC** key and select *Complete* to save the field and index definitions.
11. Select *Finished - Don't Create* at the File Definition menu.

This process must be repeated for each individual database from which you wish to generate a report. Because the process of creating the data dictionary can be time-consuming, you may want to automate dictionary building, as illustrated in the next section.

AUTOMATING DICTIONARY BUILDING

You can automatically recreate building a dictionary using Xtrieve PLUS. The following sections illustrate automated dictionary building using a command file.

Creating a Command File

You can perform a series of Xtrieve operations automatically by running a command file. Command files can record and automate frequent operations. For example, since you must build a dictionary for every INSIGHT Manager server database, you can create a command file, build one dictionary, and use the command file with minor changes to build dictionaries for all other servers.

Follow these steps to create a command file to build a dictionary:

1. Select *Command* at the Xtrieve PLUS Main menu.
2. Select *Record* at the Command menu.
3. Select *Make* at the Record menu.
4. Enter a valid DOS file name (for example, *BUILDME*) when prompted for Location, and press the **ENTER** key. Xtrieve automatically appends the extension *.XTC* to the file name. Press the **ENTER** key at the Descriptive Name prompt.

   NOTE: RCD in the lower right corner of the screen indicates that your keystrokes are being recorded.
5. Enter the desired commands. To automate the dictionary-building process, follow the steps in "Using Xtrieve to Build a Dictionary."
6. To end your recording, press the **F7** key or select *Quit* at the Main menu.

Your command file, *BUILDME.XTC*, is complete. This file replicates the process of building a data dictionary, including the location and file names. The next sections outline modifying this command file to create a new data dictionary for different INSIGHT Manager databases.

Modifying a Command File

The command file (in this case, *BUILDME.XTC)* is unreadable. The Xtrieve PLUS utility program *XCFP.EXE* allows you to convert the command file to a readable text file, and vice versa.

Use the following procedure to convert a command file to a text file and modify it to create a new dictionary file for other INSIGHT Manager databases. The following example describes the process for converting a command file for an accounting server database, *ACCT00.BTV*, to a command file for an auditing server database, *AUDIT00.BTV*.

1. At the DOS prompt, enter:

   XCFP BUILDME.XTC BUILDME.XTA

   Xtrieve converts *BUILDME.XTC* to the text file *BUILDME.XTA*.

   An example of a command file for the accounting server follows:

   "d" .DICTIONARY. "d" .DEFINE. "acct00.btv" .ENTER. "hist of cpq accting" .ENTER. "MIBType" .ENTER. "i" .INTEGER. "2" .ENTER. "Reserved1" .ENTER. .INTEGER. "2" .ENTER. "Reserved" .ENTER. .INTEGER. "2" .ENTER. "Instance" .ENTER. .INTEGER. "2" .ENTER. "InstanceLow" .ENTER. .INTEGER. "2" .ENTER. "InstanceHigh" .ENTER. .INTEGER. "2" .ENTER. "InternalMIBNumber" .ENTER. .INTEGER. "2" .ENTER. "asn1Size" .ENTER. .INTEGER. "2" .ENTER. "asn1" .ENTER. "s" .STRING. "128" .ENTER. "desc" .ENTER. .STRING. "80" .ENTER. "type" .ENTER. "i" .INTEGER. "2" .ENTER. "firstTime" .ENTER. "4" .INTEGER. "4" .ENTER. "lastTime" .ENTER. .INTEGER. "4" .ENTER. "lastChangedTime" .ENTER. "4" .INTEGER. "4" .ENTER. "lastReportTime" .ENTER. .INTEGER. "4" .ENTER. "lastValue" .ENTER. .INTEGER. "4" .ENTER. "minValue" .ENTER. .INTEGER. "4" .ENTER. "maxValue" .ENTER. .INTEGER. "4" .ENTER. "stringLength" .ENTER. .INTEGER. "2" .ENTER. "string" .ENTER. .STRING. "256" .ENTER. .ESC. .DOWN. .COMPLETE. %MIBType % .YES. .YES. .UP. .YES. .INS. .DOWN. %Reserved1 % .YES. .UP. .YES. .DOWN. %Reserved % .YES. .UP. .YES. .DOWN. %Instance % .YES. .UP. .YES. .DOWN. %InstanceLow % .YES. .UP. .YES. .DOWN. %InstanceHigh % .YES. .UP. .YES. .DOWN. %InternalMIBNumber % .YES. .UP. .DOWN. .NO. .ESC. .DOWN. .COMPLETE. .CREATENOT. .ESC. "q" .QUIT.

2. Using the text editor, change "acct00.btv" and "hist of cpq accting" to the location and filename of the new server database; in this case, "audit00.btv" and "hist of auditing."

3. Save the modified file and exit the text editor.

4. At the DOS prompt, enter:

   ```
   XCFP BUILDME.XTA BUILDME.XTC
   ```

   The *XCFP.EXE* application converts the text file back to the unreadable command file *BUILDME.XTC*.

5. At the DOS prompt, enter:

   ```
   XTRIEVE BUILDME
   ```

6. Xtrieve PLUS then defines the second table. The *AUDIT00.BTV* file contains all the information for the auditing server as collected by INSIGHT Manager.

Once you have created the data dictionaries, you can view the data, as described in the next section.

VIEWING DATA

Follow these steps to view INSIGHT Manager data with Xtrieve PLUS:

1. Select *View* from the Main menu.
2. Select *File* from the View menu.
3. Select the database you wish to view from the File menu.
4. Select *Field* from the View menu.
5. Select *Add* from the Field menu. Xtrieve displays all of the defined fields.
6. Enter *Yes* at the Defaults? prompt.
7. Select the fields you wish to view from the available choices in the Add menu.

   NOTE: The first seven fields of the INSIGHT Manager databases contain reserved or encoded information that would not be useful to most network administrators. Do not include these in your view.

8. Press the **ESC** key twice to return to the View menu.
9. Select *Browse* to see the database file.

To limit the amount of data or number of records to view, follow these steps:

1. Select *Restrict* from the View menu.
2. Select *New* from the Restrict menu. Xtrieve displays the Operand 1 menu, listing the fields in the view.
3. Select the field to restrict. For example, select *desc*.
4. Select the condition from the Condition menu. For example, select *contains.*
5. Define Operand 2. For example, if you want to display records containing all physical hard drive information, select *Constant*, and enter *Fixed disk* at the Constant prompt. (This information, "Fixed disk," is provided on the INSIGHT Manager Standard report in the "Item" column, and should be entered exactly as it appears on the report.)
6. Select *Complete* from the Expression menu.
7. Press the **ESC** key at the Restrict menu.
8. Select *Browse* from the View menu.

NOTE: You can also save this specific view by selecting *Manage*, then Store the view with a name. You can Recall the saved view later.

CREATING MULTISERVER REPORTS

You can create a single report that contains data from several different servers, a useful way to track configuration information for all servers or to compare one server with another. Creating a multiserver report is slightly more complicated than creating a single server report and requires several additional steps:

1. Creating a temporary database to hold the consolidated data.
2. Loading data from several INSIGHT Manager databases into a single consolidated database.
3. Building a view for the consolidated database.
4. Viewing or printing the report.

The following sections outline the steps needed to build a multiserver report.

CREATING THE CONSOLIDATED DATABASE

The following steps illustrate creating a new, empty database with the *BUILDME.XTC* command file from the earlier example. The empty database will hold the data from your different INSIGHT Manager monitored server databases. The new consolidated database contains an extra field, ServerName, which identifies the server from which the specific data came.

1. Use the *XCFP.EXE* application to convert the *BUILDME.XTC* file to the *BUILDME.XTA* text file. (See "Modifying a Command File.")
2. Use a text editor to modify the converted command file *BUILDME.XTA* with the following changes:
   a. Change the location "audit00.btv" to "consol00.btv" (or a filename of your choice) and "hist of auditing" to "hist of consolidated" (or a name of your choice).
   b. Insert the following before "MIBType":

      "ServerName" .ENTER. "s" .STRING. "20" .ENTER.

   c. Change .CREATENOT. to .CREATE. This command causes the command file to create a new, empty database.
3. Save the modified file and exit the text editor.
4. At the DOS prompt, enter:

   ```
   XCFP BUILDME.XTA BUILDME.XTC
   ```

   The *XCFP.EXE* application converts the *BUILDME.XTA* text file to the unreadable command file *BUILDME.XTC*.
5. At the DOS prompt, enter:

   ```
   XTRIEVE BUILDME
   ```

You now have a new database called "hist of consolidated," with an extra field "ServerName." The command file exits Xtrieve.

LOADING DATA INTO THE CONSOLIDATED DATABASE

The following steps outline loading the data from your various server databases into the new, consolidated database, called "hist of consolidated." Repeat this process for each server you wish to add to the consolidated database.

1. Select *View* from the Xtrieve PLUS Main menu.
2. Select *File* from the View menu.
3. Select *hist of consolidated* (or the name you chose for the database).
4. Select *Field* from the View menu.
5. Select *Add* from the Field menu.
6. Select *Yes* from the Defaults? menu.
7. Select *hist of consolidated* (the first option of available fields).
8. Press the **ESC** key twice to return to the View menu.
9. Select *Manage* from the View menu.
10. Select *Retain* from the Manage menu. The Descriptive Name menu appears, listing "hist of consolidated" as the current view. Press the **ENTER** key to retain the "hist of consolidated" file.
11. Press the **ESC** key to return to the View menu.
12. Select *File* from the View menu.
13. Select one of the INSIGHT Manager historical databases. This is the first data to be loaded into the new database, called hist of consolidated.
14. Select *Field* from the View menu.
15. Select *Add* from the Field menu.
16. Select *Yes* from the Defaults? menu. Xtrieve presents a list of available fields in the Add menu.
17. Select the last option, *User Defined*. Xtrieve displays the Type menu.
18. Select *String* at the Type menu.
19. Enter 20 when prompted for the field size.
20. Enter 20 when prompted for the display width of the field.
21. At the Operand menu, select *Constant*, and enter the name of the server from which the database file is collected. For example,

    Accounting Server
22. From the Expression menu, select *Complete*.
23. Enter Server Name for the Heading at the Display prompt.
24. Enter 1 by Offset.
25. At the Justify menu, select *Left* alignment, and press the **ESC** key to return to the *Field* menu.

26. Select *Add* from the Field menu. Xtrieve displays all the defined fields.
27. Select *Yes* from Defaults? menu.
28. Select the first item in the fields list (for example, hist of cpq accting.*) to add all fields to the view.
29. Press the **ESC** key twice to return to the View menu.
30. Select *Translate* from the View menu.
31. Select *To View* from the Translate menu.
32. At the To View prompt, select the consolidated file (for example, hist of consolidated).
33. Repeat steps 12 through 29 until data from all designated INSIGHT Manager databases is copied to the consolidated database.

See "Viewing Databases" for instructions on viewing the database information.

MANAGING THE CONSOLIDATED DATABASE

Remember that you can create a command file to consolidate the server data for repeated applications, such as reporting daily drive errors from all servers.

To refresh the consolidated database (delete all records in the database while preserving the database format), follow these steps:

1. Select *Dictionary* from the Xtrieve PLUS Main menu.
2. Select *Reorganized* from the Dictionary menu. (You cannot reorganize information being used as a View. If you receive this error message, select another database to view or exit and re-enter Xtrieve PLUS.)
3. Select *hist of consolidated* from the Reorganize menu. Select *Yes* at the Replace? prompt.
4. Press the **ENTER** key at the Location prompt.
5. Press the **ENTER** key at the File prompt.
6. Press the **ESC** key and select *Complete* at the Fields? menu to retain the database structure intact.
7. Press the **ESC** key and select *Complete* at the Indexes? menu to retain the indexes intact.

8. Select *Finished-Create* at the Files Definition menu to rebuild a new database (you will have a new database without any records).
9. Repeat the steps from the previous section, "Loading Data Into the Consolidated Database," to load the new data from your server databases until all the desired servers are included.
10. See "Using Xtrieve PLUS to View Databases" for instructions on retrieving information.

The following example consolidated report shows a company's partial server inventory list. Many other items are also available.

Company Inventory Report - System ROM

Server Name	Description	ROM Information
Accounting	System ROM Version	06/05/91, Family E, Type 03
Publications	System ROM Version	05/13/91, Family E, Type 03
Personnel	System ROM Version	09/23/91, Family E, Type 03
Legal	System ROM Version	09/23/91, Family E, Type 03

CREATING A REPORT FROM THE ENTRY DATABASE

When you attempt to analyze a potential problem on the server, or you perform a trend analysis for a particular monitored item, you may want to report information stored in the INSIGHT Manager entry database. (See "Database Schema" for a description of the entry database.) The entry database does not contain text information to describe the name of the monitored items to which the values pertain. You must join this file with the server's historical database to get meaningful descriptions of the values.

The following sections outline the process in these steps:

1. Create data dictionaries for both the entry and the history databases.
2. Join the entry database to the historical database.
3. Create a view for the data.
4. Select the desired records by creating a restriction criteria (optional).

5. View the data.

CREATING THE DATA DICTIONARIES

If you have not done so already, follow the steps in "Building a Data Dictionary" to create the data dictionary for the historical database. The entry database has the same name as the historical database, but with a *.BTP* file extension.

Follow these steps to build the entry database data dictionary:

1. Copy the INSIGHT Manager database file for your server (for example, *ACCT00.BTP*) to the Xtrieve PLUS subdirectory.

   NOTE: All INSIGHT Manager entry databases have a *.BTP* extension.

2. Select *Dictionary* at the Xtrieve PLUS Main menu.
3. Select *Define* at the Dictionary menu.
4. Enter the Location of the database file (for example, C:\XTRIEVE\ACCT00.BTP) and press the **ENTER** key.
5. At the File prompt, enter a descriptive file name (20-character maximum) and press the **ENTER** key. This is the name used within Xtrieve PLUS for that specific file (for example, "entry cpq accting").
6. Enter the name, type, and size of each field in the database in the order in which they are located in the database. See Table A-3 for a list of the fields in the INSIGHT Manager entry database. Enter *all* the fields in the table.
7. When all the field information is entered, press the **ESC** key.
8. Select *Complete* from the Fields? menu.

   NOTE: If the table is not complete, select *Continue* to modify the fields, or *Abort* to begin again.

9. The Indexes menu displays. Select the field names in Table A-5 from the Indexes menu. Enter *Yes* or *No* according to the table, and using the default for Dup and Case.

Table A-5
Example Indexes Menu

Path	Field	Dup	Case	Asc	Seg
0	MIBType	Yes	No	Yes	Yes
	InternalMIBNumber	Yes	No	Yes	Yes
	InstanceHigh	Yes	No	Yes	Yes
	InstanceLow	Yes	No	Yes	Yes
	Instance	Yes	No	Yes	Yes
	Reserved	Yes	No	Yes	Yes
	Reserved1	Yes	No	Yes	No
1					

10. Press the **ESC** key and select *Complete* to save the field and index definitions.
11. Select *Finished - Don't Create* at the File Definition menu.

This process must be repeated for each individual database from which you wish to generate a report.

JOINING THE DATABASES

Use the following steps to join the databases.

1. Select *View* at the Xtrieve PLUS Main menu.
2. Select *File* at the View menu.
3. Select the server's history file (for example, hist of cpq accting) from the File menu.
4. Select *Join* from the View menu.
5. Select the server's entry file (for example, entry cpq accting).
6. Enter *Yes* at the Include All? prompt.
7. Select each of the first seven fields at the Primary menu by highlighting each field and pressing the **ENTER** key. The first letter of each selected field will blink.

8. Press the **ESC** key and the Secondary menu will display.
9. Press the **ENTER** key.

VIEWING DATA

To view the server data, follow the steps outlined in the earlier "Viewing Data" section. Note that you can select fields from both databases. Be sure to include the value field from the entry database to insure that you see the values collected for incrementing or changing monitored items.

BORLAND QUIK REPORTS

Borland Quik Reports for Windows v1.0 is compatible with Xtrieve PLUS. Quik Reports offers a Windows interface with computation capabilities. Refer to Quik Reports documentation for detailed instructions on using Quik Reports.

REQUIREMENTS

Apply the *BTRVDLL.EXE* patch program to enable Quik Reports to work with Btrieve databases. The patch is available from the Crystal Services technical support bulletin board at (604) 681-9516.

1. Download the file *BTRVDLL.EXE*. This is a self-extracting file.
2. Copy *BTRVDLL.EXE* to your Quik Reports directory.
3. Run *BTRVDLL.EXE* to expand to four more files:
   - *PDCTBTRV.DLL*
   - *WBTRVDEF.DLL*
   - *PDBBTRV.DLL*
   - *README*

GENERATING A REPORT

Before using Quik Reports, create the data dictionary using Xtrieve PLUS.

1. Select the Quik Reports icon from Windows.
2. Select *New Report* from the File menu.
3. At the Database File dialog box, enter:

   c:\xtrieve*.ddf

4. Select any one of the *.DDF* files on the Files menu (choosing one reads all the *.DDF* files). The Insert Database Field dialog box displays, listing all the databases defined in the dictionary as well as each field in the database.
5. Select the field(s) on which you wish to report. A shaded block displays.
6. Move the block(s) to the Detail line of the display area.
7. On the Page Header section, type heading information, such as Server Name, and align these with the value in the Detail section. These Page Header entries are your column headings. You may also enter Page Footer information.
8. Select *Save* from the File menu, and name the report.
9. To view the report before printing, select *Print to Window* from the Print menu.

To select specific records for the report, follow these steps:

1. Select *Edit Record Selection Formula* from the Print menu.
2. Build your formula by clicking on the Fields, Functions, and Operators sections. To repeat the example used in "Viewing Databases" to limit the number of records to view, enter

   Fixed disk

   in the Formula Text box.
3. Select the series operator *x in y*.
4. Select the description field for your report in the Fields section.
5. Select *Accept*.
6. Select *Print to Window* from the Print menu.

See the Quik Reports documentation for more information on selecting specific records within your database file.

Appendix B
COMPAQ ENTERPRISE MANAGEMENT INFORMATION BASE

> **!** **IMPORTANT:** This appendix is intended for developers or advanced users with an understanding of SNMP, and MIB syntax, formats, and compilers.

The COMPAQ Management Information Bases (MIBs) describe the information instrumented by the COMPAQ Management Agents for NetWare. Many SNMP management consoles allow you to incorporate third-party MIBs. With such a console, you can retrieve the information in the COMPAQ MIBs. These consoles differ in the amount of information they extract from MIBs, and in the flexibility that you have in displaying the information. These consoles can also extract information for decoding traps (alerts) that the server can send to the management console.

The COMPAQ MIBs provide detailed information that is necessary to obtain a complete picture of server configuration and status. COMPAQ INSIGHT Manager gathers and interprets this information and presents you with a complete picture of the server. To customize even the most flexible generic management console to provide the same level of sophistication may be possible, but probably would not be practical for even an expert user.

The COMPAQ MIBs can provide software developers the level of detail necessary to incorporate the ability to use the COMPAQ management information into a management console.

Software developers might also use the COMPAQ MIBs to customize a generic SNMP management console to get a few important data items showing a basic server's status. You can then monitor basic server functionality with the generic management console, and use INSIGHT Manager when specific information or more detail is required.

Generic SNMP management consoles that can use third-party MIBs typically provide a MIB compiler tool. The MIB compiler reads the SNMP MIB and extracts the information the console requires. Check the documentation for your SNMP management console for more details on its use.

The COMPAQ MIBs comply with the syntax for SNMP MIBs. Many MIB compilers also have additional rules for MIB formats. This may require you to customize the MIBs for your MIB compiler. Some management consoles only allow you to specify one MIB for any particular network device. You might need to combine all the COMPAQ MIBs, the standard SNMP MIB (MIB-II), and the MIBs of any other third-party agents that are loaded on the NetWare server. This customization or combining of MIBs requires a working knowledge of SNMP, MIB syntax, and the specific MIB compiler.

You can request a copy of the COMPAQ MIB License Proposal Form from COMPAQ PAQFax. Call the Compaq Customer Support Center at 1-800-345-1518 in North America, and select 1 on your touch-tone phone. Have the number of your fax machine ready. Follow the automated touch-tone instructions to receive the license proposal form.

Appendix C
WORKSHEETS

Use the following worksheets to record important Server Manager/R Management PC and monitored server information.

COMPAQ Server Manager Facility/R
Requirements and Configuration Worksheet

Management PC Hardware Requirements

386- or 486-based PC

2 megabytes of system memory

EGA, VGA or higher monitor

Serial Port or Modem

Data line (telephone line)

Date line cable (RJ11)

Management PC Software Requirements

_____ Microsoft Windows 3.x

_____ COMPAQ Server Manager Facility/R diskette

Configuration

Serial Ports:

COM Port:_____

Connectivity Type:_____

Application Password:_____

Alert Timeout:_____

Server Name:_____

Alert Destinations: #1 _____

#2_____

#3_____

#4_____

#5_____

#6_____

Threshold Backup File Name:_____

COMPAQ Server Manager/R
Monitored Server Configuration Worksheet

Monitored Server Type:_____

Server Name:_____
(Case Sensitive)

Server ID: _____

System Password:_____
(Case Sensitive)

Tone Password:_____

Internal Modem Status:_____

Internal Modem Baud Rate:_____

Direct Connect Serial Port Mode:_____

Direct Connect Serial Port Baud Rate:_____

Pager Baud Rate:_____

Remote Console Audible Indicator:_____

Host Interrupt:_____

Server Manager/R Phone Number:_____

COMPAQ TechNotes for NetWare

Technical Information for the NetWare Administrator

The COMPAQ TechNote Service can help you keep up with the latest integration technology for NetWare.

Each COMPAQ TechNote for NetWare provides advanced integration information on a specific NetWare topic, such as performance management, server management, and database services.

Subscribing to the COMPAQ TechNote Service entitles you to a full calendar year of COMPAQ TechNotes for NetWare, with a minimum of four issues.

To order, complete the order form and mail or fax it to:

COMPAQ TechNotes
Compaq Computer Corporation
P.O. Box 692000, Mail Stop 130102
Houston, TX 77269-2000

FAX: (713) 374-0668

For more information, call:

1-800-345-1518 (USA)
1-800-263-5868 (Canada)

(Outside the USA and Canada, contact your local Authorized COMPAQ Reseller or your local Compaq office.)

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

V

W

X

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)

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS MAIL PERMIT NO. 44 CRAWFORDSVILLE, INDIANA

POSTAGE WILL BE PAID BY ADDRESSEE

COMPAQ TECHNOTES
COMPAQ COMPUTER CORPORATION
PO BOX 4100
CRAWFORDSVILLE IN 47933-9940

(Fold Here)

Please Tape Here

Please Tape Here