WHITEPAPER

Februrary 1995

Second Edition

Compaq Computer Corporation

CONTENTS

Desktop Management

Businesses increasingly view local area networks (LANs) as strategic resources on which to develop and deploy business critical applications. Downsizing and rightsizing are growing trends as businesses strive to capitalize on the improved economies obtained through the deployment of LANs. As a result of rapid growth and importance of LANs, businesses are finding that hiring, training, and keeping skilled network administrative personnel is increasingly difficult. LANs are growing in size and complexity while their cost of management is increasing. Therefore, businesses demand improved LAN management tools to control the rising costs of LAN administration while increasing the dependability of network environments.

Today's network administrators have sophisticated management tools for network resources such as bridges, routers, and concentrators, as well as network protocols. Compaq has led the industry in bringing the benefits of server manageability to these network administrators — demonstrated by the Compaq Systempro with the Compaq Intelligent Drive Array Controller and the Compaq Server Manager/R, followed by the Compaq ProLiant and Compaq Insight Manager. Realizing the benefits of manageable servers have now caused our customers to demand easy-to-manage desktop PCs.

Compaq is responding to this customer need for easy-to-manage desktop PCs, demonstrated by its industry-leading implementation of desktop management, called Intelligent Manageability, the Compaq Desktop Management Solutions Partners Program, and its position as a Steering Committee Member in the Desktop Management Task Force (DMTF).

Compaq is poised to leverage its history of delivering manageable servers to desktop PCs.

This white paper discusses Compaq's Desktop Management strategy and provides you with a basic understanding of the technology. A separate white paper describes the specific management features and benefits of the new Compaq desktop PCs.

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.

Desktop Management

Second Edition (February 1995)
199A/0395

COMPAQ DESKTOP MANAGEMENT STRATEGY

Intelligent Manageability

Compaq is focused on delivering the easiest-to-manage desktop PCs. To achieve this end, Compaq will:

1. Enhance PC hardware to provide the richest set of management capabilities.
2. Partner with leading management tool providers to ensure that the hardware enhancements are integrated and compatible with the widest range of management tools.
3. Support the widest range of network management standards.

This strategy is called Intelligent Manageability. The following sections describe each component of the Intelligent Manageability strategy in detail.

Enhancing PC Hardware

Key hardware subsystems, such as hard disk and video, in Compaq desktop PCs, will have a robust set of capabilities designed-in that address one or more of the four aspects of Desktop Management . The four aspects of Desktop Management are inventory/configuration, fault, security, and performance (see Management Overview, on page 4, for additional information). Management software can take advantage of these enhancements through the ROM BIOS.

Solutions Supported By The Widest Range Of Management Products

Compaq will take the initiative to proactively ensure the compatibility and integration of the PC hardware enhancements for manageability with the leading vendors of management products. This initiative is called the Compaq Desktop Management Solutions Partners Program. The Partners' products deliver features demanded by network administrators such as server monitoring, network protocol analysis, software distribution, and software and hardware inventory, to name a few. The broad vendor support will ensure that customers can easily manage Compaq PCs using their preferred management products—and they can do so more confidently and cost-effectively than with other PCs.

Compaq Insight Manager is the Compaq application for easily managing servers. Compaq Insight Manager monitors the health and performance of servers, alerting LAN administrators to potential or actual problems and provides remote control of servers for support and maintenance operations. In the future, Compaq Insight Manager will be enhanced to support Desktop Management.

Supporting The Widest Range Of Network Management Standards

There are two significant interoperability requirements that Compaq desktop PCs meet that ensure Compaq Desktop Management works in the customer's network. These requirements are:

1. Compaq desktop PCs must be manageable within the customer's preferred environments.

   Compaq is committed to strict standards adherence. Whether the standard is the Simple Network Management Protocol (SNMP) or the Desktop Management Task Force (DMTF), Compaq will support the standards to their fullest. This ensures that the customer's investment in standards-based network management tools and environments is secure. For further information on the Simple Network Management Protocol and the Desktop Management Task Force, see Management Standards on page 9.

2. Customers can manage network resources such as desktops and servers from other vendors, bridges, and routers all from a single management environment.

   Compaq is committed to ensure that Compaq Insight Manager will integrate with network management tools and work as an integral part of the customer's management environment. In the LAN management environment, Compaq Insight Manager integrates with the NetWare Management System and Microsoft Systems Management Server, providing LAN administrators with a single console to manage all LAN components. For enterprise-wide management environments, Compaq Insight Management Agents integrate with the leading SNMP-based management platforms including Hewlett Packard's OpenView, IBM's NetView/6000 and SunConnect's SunNet Manager.

Implementation Vision

The delivery of management technologies for Compaq desktop PCs will occur in phases. Initially, Compaq will deliver desktop PCs that are easy to inventory, easy to troubleshoot, and easy to protect — delivering great value to our customers and leading the industry. These capabilities will be enhanced continually while we expand our focus to delivering PCs that are also easy to performance tune.

Benefits that a customer may enjoy include the following:

- Accounting personnel can maintain effortlessly an accurate asset inventory of desktop PCs.
- Centralized support personnel and network administrators can proactively address fault and performance problems.
- Corporate MIS personnel can comfortably locate business critical data on PC networks.

Intelligent Manageability is designed to enable customers to deploy PC network solutions more cost-effectively and confidently.

MANAGEMENT OVERVIEW

The International Standards Organization (ISO) has formulated a management framework that provides a reference for coordinating development of management standards. *The Basic Reference Model of Open Systems Interconnection (OSI), ISO 7498* — Part 4 describes the functional areas of management. This ISO network management model identifies five functional areas of management. They comprise the following:

- Inventory and Configuration Management
- Fault Management
- Security Management
- Performance Management
- Accounting Management

Compaq has mapped the ISO framework into server and desktop management. In the case of PCs, Compaq defines management as the process of in-depth monitoring, analyzing, and controlling the inventory/configuration, fault, security, and performance aspects of the PC's operation.

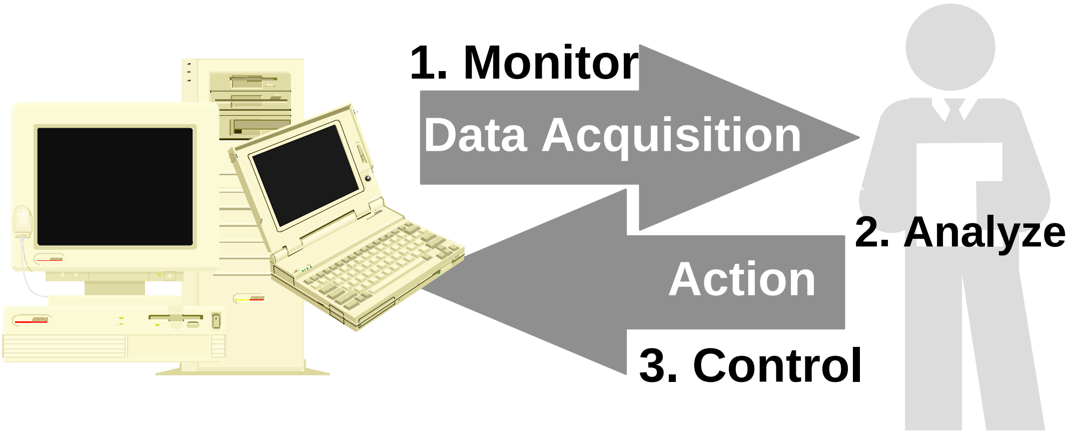
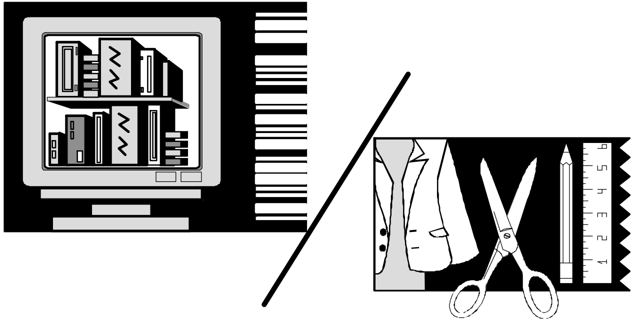


Figure 1. Management Definition

Monitoring is the process of acquiring inventory/configuration, fault, security, and performance data, analyzing is the process of making sense of the data, and controlling is the process of acting upon the data analysis. The sections that follow introduce you to Compaq's definition of the functional areas of management.

Note: The Compaq Intelligent Manageability white paper describes the specific management features and benefits of the new Compaq desktop PCs.

Inventory and Configuration Management



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

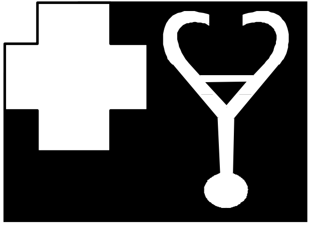
Inventory Tracking

Inventory tracking is a set of capabilities that provide comprehensive hardware and software component identification and configuration reporting to enable inventory and accounting procedures. This component identification (inventory data) is also a prerequisite to distributing data files and software, troubleshooting remote systems, and managing geographically dispersed assets. Without it, customers are forced to rely upon expensive on-site, manual support. End-user transparent inventory management is a requirement for effective utilization of networked PC computing. Such transparency will be achieved when all components, both hardware and software, provide a comprehensive set of “who am I?” data (for example: manufacturer, model, and serial number) to asset tracking application programs.

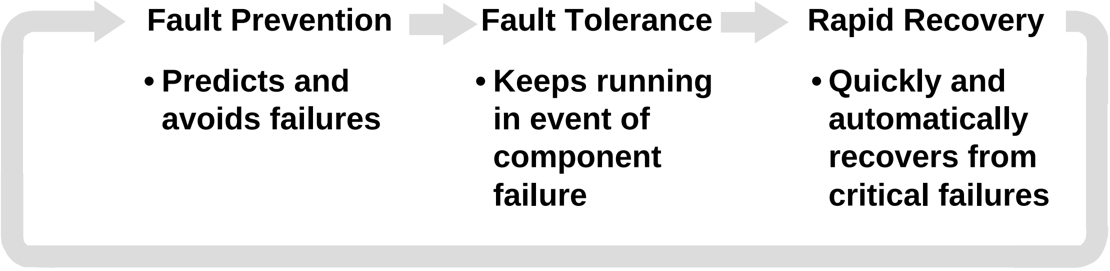
Automatic Configuration and Configuration Change Administration

Automatic configuration and configuration change administration is a set of capabilities that enable automatic and effective configuration to ensure minimum setup time. It also includes a set of capabilities that allow for a troublefree and repeatable upgrade process to enable fast use of the latest operational changes.

Fault Management



Detecting faults and notifying administrators of a fault occurrence is a basic function of network management. This function becomes essential in a business critical networking environment, particularly in an economic climate where shrinking budgets force MIS departments to become more efficient. Viewing a fault condition along the time axis leads to the realization that there are three distinct periods of importance. First, is the period before the fault. Second, is the period during the fault. Third, is the period after the fault. Compaq fault management, called Full-Spectrum Fault Management, is comprised of a set of fault prevention, fault tolerance, and rapid recovery capabilities designed to maximize uptime and data integrity.



Fault Prevention

- Predicts and avoids failures

Fault Tolerance

- Keeps running in event of component failure

Rapid Recovery

- Quickly and automatically recovers from critical failures

Figure 2. Compaq Full-Spectrum Fault Management

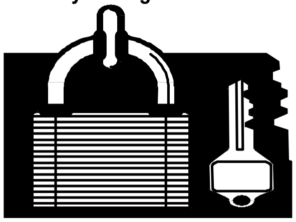
Fault Prevention

Fault prevention is a set of capabilities that provide an early warning of impending component or subsystem failure, so that preventive maintenance can be performed before the actual failure. For example, a hard drive that contains fault prevention capabilities would monitor how well its mechanical components and media are operating. Spin-up and seek times are attributes of the drive’s mechanical operation. Uncorrectable read and write errors are attributes of the media’s operation. A significant degradation in any of these attributes is an accurate predictive indicator of an impending drive failure. Conveying this information to the user and the administrator allows them to proactively replace the drive before a catastrophic data error occurs thereby preventing the failure.

Fault Tolerance
Fault tolerance is a set of capabilities that automatically corrects faults when they occur, maximizing uptime by ensuring continued operation in the event of component or subsystem failure. Fault tolerance, a capability typically found in network servers, is implemented as redundant hardware components, such as redundant arrays of inexpensive drives (RAID) or error correcting code (ECC) memory.

Rapid Recovery
Rapid recovery is a set of capabilities that provide notification, rapid identification of faults, and automated restart of failed systems or subsystems so that unplanned downtime is minimized. Error alerts, such as paging and administrator or sending “25th-line” messages to the user, nonvolatile health logs that hold error identification hints, and diagnostic software are all examples of rapid recovery features.

Security Management



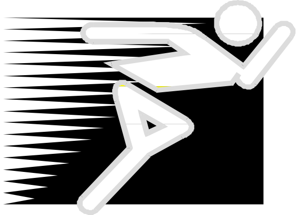
Networked PC computing has increased the quantity of easily accessible information that a corporation maintains. Ensuring that this information is accessed only by authorized personnel and that the integrity of the information and PC is maintained is critical in the information age. Security management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

Hardware and Software Security
Hardware and software security is a set of capabilities that secure the PC based on hardware, software, or a combination of both to prevent unauthorized access to the PC and safeguards the PC’s configuration.

Physical Security
Physical security is a set of capabilities that ensure against unauthorized access and theft. A key lock is an example of physical security.

Virus Detection
Virus detection is a set of capabilities that monitor the contents of critical data files, program files, and system memory to detect programmatic tampering of these critical resources.

Performance Management



Once the business critical PC networking environment becomes stable and dependable, maintaining and improving the peak performance of the networked PCs becomes key. As MIS departments become more efficient, they expand their focus to ensure that the PC network investment is maximized. Analyzing performance management needs leads to the requirement for two distinct capabilities. First, administrators need to tune current networked PCs and other devices. Second, they need to easily plan for future network growth. Performance management is comprised of a set of performance tuning and capacity planning capabilities designed to enable the cost-effective utilization and growth of the customer’s ever-changing network.

Performance Tuning
Performance tuning is a set of capabilities that assist in performance evaluation and modification to ensure peak performance levels for the targeted environment. For example, in-depth monitoring of the utilization of I/O buses, CPU, and network interface cards can be used by administrators to modify hardware and software configurations for maximum performance.

Capacity Planning
Capacity planning is a set of capabilities that provide “what-if” scenarios to assist in planning for network growth. Capacity planning is always embodied within a software application.

Elements of a Manageable Device

All PCs are inherently manageable. However, those PCs that are easy to manage are specifically designed with this customer requirement in mind: Easy to manage PCs contain hardware capabilities that expose in-depth inventory/configuration, fault, security, and performance aspects of the PC's operation. Along with the hardware capabilities, management tools (software) are required to provide an interface that allows an end-user or administrator to monitor, access, and control the management features of the PC.

Traditional Input/Output (I/O) Architecture

This section is intended to provide an overview of the input/output architecture of a typical PC. The architecture of a manageable PC builds upon the traditional I/O architecture.

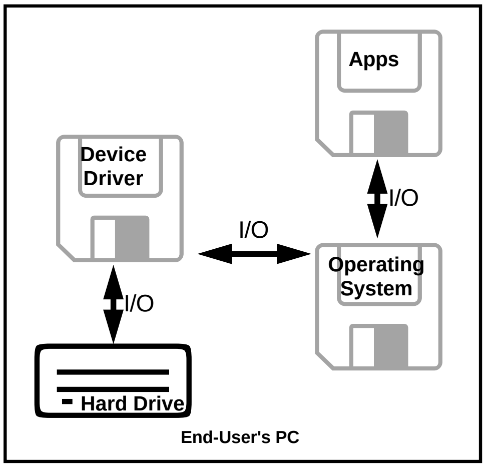


Figure 3. Traditional I/O Architecture

The traditional I/O architecture is comprised of the following:

- A *device*, for example, keyboard or hard drive, which allows application software to perform read and write operations. For example, read a key from the keyboard, or save a file to disk.
- A *device driver* that isolates the operating system from the complexity of controlling the device by providing a common interface to perform the read and write operations.
- An *operating system* that isolates the application software from the complexity of interacting with the device driver by providing an application programming interface (API).

Management Architecture

The architecture of a manageable PC builds upon the traditional I/O architecture.

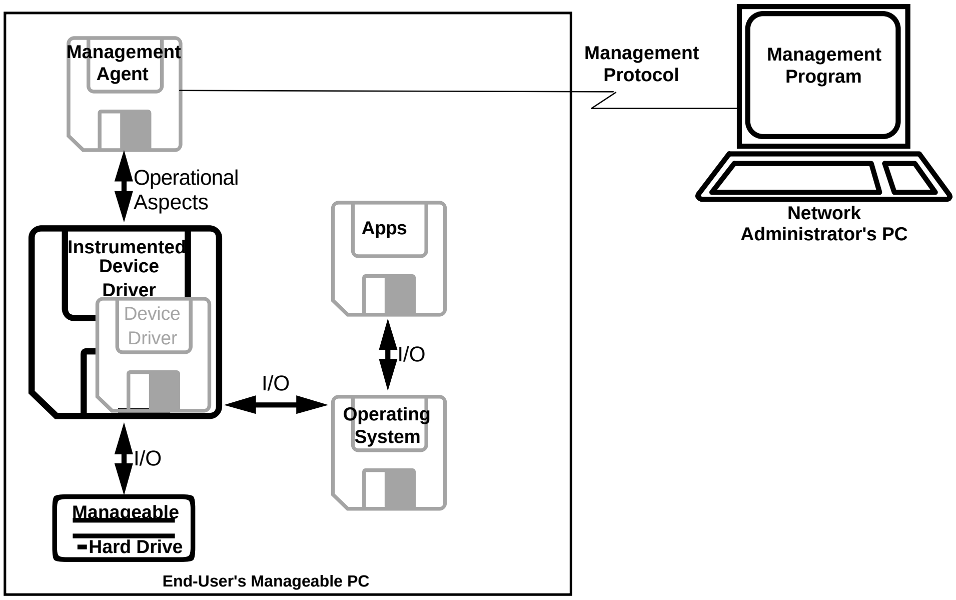


Figure 4. Management Architecture

The management architecture contains these additional elements:

- *Management hardware* is designed to provide a rich set of inventory/configuration, fault, security, and performance statistics.
- An *instrumented device driver* is designed to maintain management information (inventory/configuration, fault, security, and performance statistics) about the device’s operation along with providing the I/O services of the traditional device driver. For example, the instrumented hard drive device driver would maintain a count of the number of unrecoverable read and write errors to determine how well the drive is operating.
- A *management agent* takes the management information from the instrumented device driver and delivers the information to the management program using the management protocol.
- A *management protocol* defines the language that the management agent and management program use to communicate over a network.
- A *management program* provides the monitor, analysis, and control user interface of the management features in the device.

Fault Prevention Example

This section provides an overview of the interaction of the elements in the management architecture.

Hard drives are mechanical devices — they have components that move and spin. Each hard drive has a distinct way that it works that, when new, varies slightly within the drive manufacturer's specifications. A manageable hard drive might contain firmware that performs periodic analysis to determine how well the drive is operating at that moment. If the analysis determined that an aspect of the drive’s operation has degraded to the point that failure was impending then the drive could pass this information to its instrumented device driver.

The instrumented device driver passes the indication of failure and other management information (either acquired from the drive or maintained by the driver) to the management agent (agent). The agent stores the management information (information) in a database-like table. Besides storing the information in the table, the agent sends a message to the management program, such as Compaq Insight Manager. The message would tell the management program that the hard drive is likely to fail. The management program would alert the administrator (by way of a popup window, audible tone, or message to pager) that the user’s hard drive is likely to fail. *This alert, before the drive failed, enables the administrator to replace proactively the user's drive avoiding downtime*

This fault prevention example is analagous to watching the tread on your tires and replacing the tires before the tires are worn down.

MANAGEMENT STANDARDS

Standards-based network management is important because it provides interoperability between dissimilar environments and protect customers' investments by offering a common way of performing tasks across those environments. Protocols such as SMNP and Common Management Information Protocol (CMIP) allow network managers to monitor networks that include products from multiple vendors using multiple computers and operating systems.

Simple Network Management Protocol

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

SNMP Infrastructure

SNMP manageable network devices such as routers, bridges, clients, and servers contain several software components. This infrastructure consists of management agents, an SNMP protocol agent, a network transport protocol, and the information those agents make available. A functional block diagram of the SNMP infrastructure is shown below.

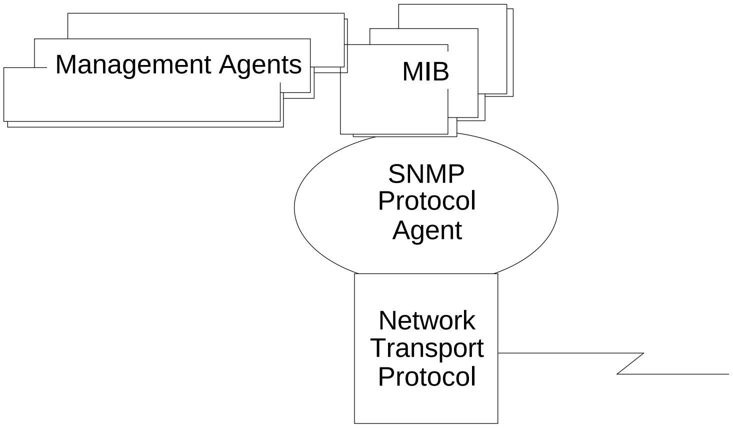


Figure 5. SNMP Infrastructure Functional Block Diagram

Management agents monitor various subsystems of the network device and store the inventory/configuration, fault, security, and performance information in a management information base (MIB) which is a database-like table. Due to the in-depth device knowledge required by the management agents, they are unique to the network device and must be provided by the network device vendor.

The **SNMP protocol agent** understands the SNMP language, as spoken over the network, and converts requests made by management applications into operations that must be carried out by the management agents. The application programming interface (API) of the SNMP protocol agent, the means through which the management agent and the SNMP protocol agent interact, are unique for each vendor's SNMP protocol agent implementation. However, bundling of SNMP protocol agents with operating systems is becoming the norm. Therefore, for each OS, a standard SNMP protocol agent API is emerging.

The **network transport protocol** is responsible for the end-to-end control of transmitted information and the optimized use of network resources. IP and IPX are examples of network transport protocols. SNMP is typically associated with TCP/IP and monitoring devices on Ethernet networks because of its long association with the Internet. However, you can use SNMP over other protocols such as IPX and AppleTalk.

SNMP Management Information Base

Conceptually, the management information base (MIB) is a database accessible by a management application using the SNMP protocol. There are two types of MIBs:

- Internet Management MIBs — This includes MIB-II, RMON, and others. These MIBs, standardized by the Internet community, represent the core objects that are common across the widest range of network devices implementing the Internet protocols. Examples of these objects include network protocols such as TCP/IP and network devices such as Ethernet and Token Ring network interfaces.
- Vendor MIBs — These MIBs represent objects that are unique to an individual vendor's product or product line. Over 500 vendors and organizations have created their own vendor MIBs. Compaq has created is own vendor MIB to represent servers and desktop PCs.

SNMP Protocol

The SNMP protocol specifies four operations that a management application can use to “speak to” the management agent. These are the GET, GET-NEXT, SET, and TRAP operations. A brief description follows:

- Management applications, such as Compaq Insight Manager, use the GET and GET-NEXT (read) operations to acquire data from management agents. This provides the mechanism for monitoring, or obtaining information from the MIB.
- Management applications use the SET (write) operation to change the data maintained by the management agents. This provides the mechanism for controlling.
- Management agents use the TRAP (unsolicited information) operation to notify management applications of important fault or performance events (for example, impending or actual hard drive failures). This provides an additional mechanism for monitoring.

Some users of SNMP have expressed concern over the security mechanisms employed. In response to that concern, the Internet community has recently completed SNMP-2. SNMP-2, the next version of the Simple Network Management Protocol, includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. At this time, SNMP-2 has not been implemented by vendors of network devices.

Desktop Management Task Force

The Desktop Management Task Force (DMTF) was formed in 1992 to create standards for the management of desktop computers. The goal of the DMTF was to establish an open process for specifying methods for managing desktop hardware and software components. As a result, the DMTF has defined two pieces of technology — the Desktop Management Interface software (DMI) and the Management Information Format (MIF) file.

DMTF Infrastructure
DMTF manageable desktop PCs may contain several software components. This infrastructure consists of optional management agents (called component agents), the Desktop Management Interface software (DMI), and the information that is made available. A functional block diagram of the DMTF infrastructure is shown below.

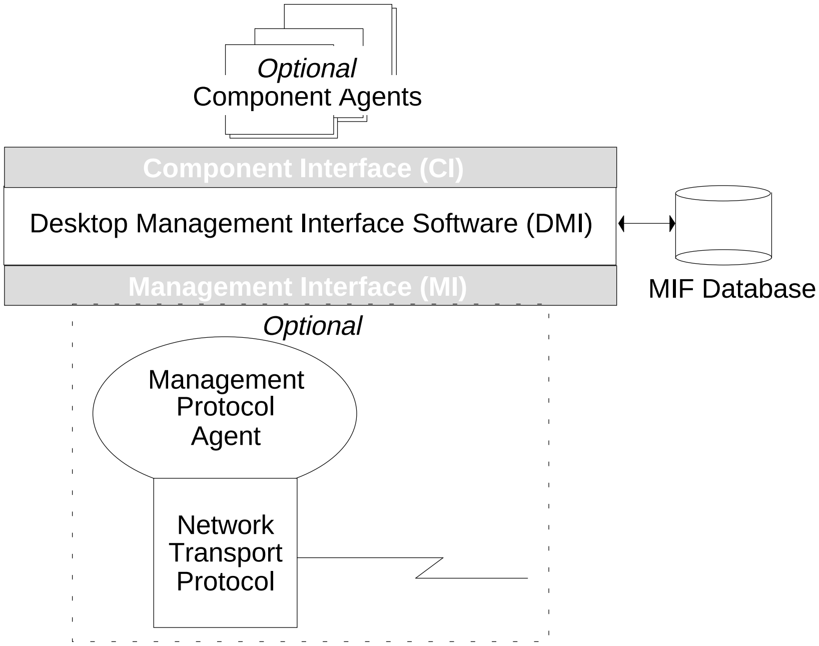

Optional
Component Agents
Component Interface (CI)
Desktop Management Interface Software (DMI)
MIF Database
Management Interface (MI)
Optional
Management Protocol Agent
Network Transport Protocol

Figure 6. DMTF Infrastructure Functional Block Diagram

If provided by the vendor, **component agents** perform a similar task as the SNMP management agents except that they store the inventory/configuration, fault, security, and performance information in a MIF. Component agents are required for the monitoring of dynamic information, such as sectors read from and written to a hard drive or impending and actual failure notifications. Access to purely static configuration data, such as amount of memory installed, manufacturer and model of computer, etc., is enabled solely through the MIF file which is why the component agents are optional.

The **Desktop Management Interface (DMI)** is a layer of *software* that brokers requests for management data from the components that provide the data. To accomplish this task, the DMI software provides two application programming interfaces (APIs). One API (the **component interface — CI**) enables components to provide management information to management applications. The other API (the **management interface — MI**) enables local management applications to extract the management information. Local management applications operate on the same PC as the components.

DMTF Management Information Format File
Conceptually, a management information format (MIF) file is similar to an SNMP MIB. However, a MIF can be implemented as a simple text file (for static configuration-only data) or implemented as a combination text file and component agents (for dynamic fault and performance data). Vendors select the implementation manner that suits their engineering budget and meets their customer’s needs. In every case, the support of a MIF does not mean that the PC has been enhanced for manageability. Regardless of whether the MIF is implemented as a simple text file or as a combination text file and component agents, there are two types of MIFs:

- Standard MIFs — Standardized by the DMTF but developed by working committees of companies, these MIFs describe the static attributes of an industry standard PC, network adapters, and printers. Leveraging our server management heritage, Compaq was the lead author of the Desktop System MIF. New working committees will be formed to develop standard MIFs for additional components such as server hardware, operating systems and application software.

- Vendor MIFs — These MIFs represent features that are unique to an individual vendor's product or product line.

DMTF Protocol
Unlike SNMP, the DMI software was designed to be a purely local management enabler. The DMI does not comprehend a network protocol. Some proponents of the technology label this protocol independence. In the short run, management tools that support the DMI software must provide a unique version of the DMI software integrated with the vendor's proprietary management protocol. Those customers desiring to use more than one management tool (each with a unique protocol) would be forced to (1) Sacrifice desktop PC RAM to load multiple protocols, and (2) Become the integration test bed for the compatibility of multiple protocols. In the future, the DMTF should define a standard management protocol to integrate with the DMI software. This move will spur widespread adoption of the DMI software by allowing PC manufacturers to preinstall the operating system, the DMI software, the remote management protocol, and component agents, in essence creating a manageable desktop PC out-of-the-box. Until this event occurs, the DMI technology is not appropriate for widespread adoption by customers.

DMI Compliance
DMI-compliance places no requirements upon desktop PC hardware. A PC manufacturer that markets its PCs as DMI-compliant typically has preinstalled the DMI software for DOS and Windows. However, this does not mean that the PC manufacturer has modified its hardware to ease inventory, troubleshooting, or security.

The DMI software and the PC Systems MIF was defined to handle legacy PCs and gets most of its data from well-known ROM interfaces and memory or I/O locations that are part of the industry-standard PCs by definition. Therefore, all industry-standard PCs, including the original IBM PC, are DMI-compliant.

DMTF Summary
The Desktop Management Task Force has made great strides to develop technology that provides a standard framework to manage desktop PCs. However, several key requirements for success still need to be met. These are:

1. Broad support by operating system vendors. Without such integrated support, the management information available through the DMI software will not enhance the configuration, installation, or troubleshooting capabilities of desktop PCs. In addition, lack of integrated support means that the DMI software, currently implemented as a DOS Terminate and Stay Resident (TSR) program, will inefficiently use precious system memory.

2. Standardization on remote management protocol suites. While SNMP is the defacto standard network management protocol, there is room in the marketplace for a PC LAN or workgroup management standard protocol. The standardization of such a protocol would allow system vendors to provide a manageable desktop PC out-of-the-box.

3. Broad support by management tool vendors. Without broad support, DMI-enabled desktop PCs can not be managed in the customer's preferred environment.

Until these requirements are met, the DMI technology is not appropriate for widespread adoption by customers. When these requirements are met, Compaq will:

1. Continue to enhance PC hardware for manageability.

2. Add value to the DMI.

3. Continue to work proactively with the leading vendors of management products to ensure tight integration and compatibility with these vendor's products.Compaq's desktop management strategy, both pre- and post-DMI, ensures that Compaq PCs will be the easiest-to-manage.

QUESTIONS AND ANSWERS

Management

Q1. What is Desktop Management?

A. Desktop Management is the process of in-depth monitoring, analyzing, and controlling the inventory/configuration, fault, security, and performance aspects of a PC's operation. Monitoring is the acquisition of data, analysis is the process of making sense of the acquired data, and control is the resulting actions.

Management maximizes the productivity of network support personnel and greatly improves PC network dependability. Management thereby enables customers to deploy PC network solutions more cost-effectively and confidently.

Q2. How does Desktop Management fit with network management?

A. Desktop Management is a subset of network management. It focuses upon the monitoring, analysis, and control of one type of device, the PC, within the broader network environment. Network management focuses upon the monitoring, analysis, and control of all LAN resources, including servers, bridges, gateways, clients, etc.

Q3. What is Intelligent Manageability?

A. Intelligent Manageability is Compaq's industry leading desktop management strategy to make networked PCs easier to manage today and tomorrow. With this strategy Compaq is making enhancements to the basic PC hardware to ensure that the PC is easier to inventory, easier to troubleshoot, and easier to protect. These hardware enhancements are then complimented by a wide range of PC LAN management software, integrated and compatible with Intelligent Manageability, to ensure that customers can easily manage Compaq PCs using the customer's preferred PC LAN management products—and they can do so more confidently and cost-effectively than with other PCs.

Q4. What is the Compaq Desktop Management Solutions Partners Program?

A. Compaq's reputation is built upon compatibility and quality. The Compaq Desktop Management Solutions Partners Program moves those elements of our success into the management domain. The program is a Compaq initiative to *proactively* ensure compatibility and integration of Intelligent Manageability with the leading vendors of PC LAN management products. Now, the benefits of Compaq's Intelligent Manageability are accessible to our entire customer base. The broad vendor support ensures that our customers can easily manage Compaq PCs using the customer's preferred PC LAN management products—and they can do so more confidently and cost-effectively than with other PCs.

Q5. What vendors are participating in the Compaq Desktop Management Solutions Partners Program?

A. Currently, the participating vendors are: Cheyenne Software Inc., Frye Computer Systems Inc., Intel Corp., McAfee Associates Inc., Microsoft Corp., Network Computing Inc., Novell Inc., Saber Software Corp., Symantec Corp., and Tally Systems Corp. These vendors will deliver products that are integrated and compatible with Intelligent Manageability.

Q6. Why is the Compaq Desktop Management Solutions Partners Program necessary?

A. There is a lot of confusion in the marketplace today. Too many management technologies are vying for the customer's mindshare (e.g. SNMP, DMI, Plug and Play, Windows Registry, etc.). Unfortunately, too few PC LAN management products that are well integrated with PC hardware are available today. Rather than market immature technologies that provide no useful benefits at this time, Compaq has chosen to work with PC LAN management vendors to provide customers with viable solutions today. The Compaq Desktop Management Solutions Partners Program lets customers focus on using their networks to solve business problems, thereby reaping the benefits of lower cost of ownership via these well integrated products. The program is also likely to make it unnecessary for customers to change the tools they're using today since many currently shipping products have been integrated into our plan. Without the program, customers would be spending the majority of their time making technology decisions.

Q7. Is Desktop Management different from server management?

A. No. Desktop Management and server management are both focused on lowering the total cost of ownership of these devices. However, the prioritized customer's needs are slightly different for these devices:

Priority	Desktop Management	Server Management
1.	Inventory	Fault
2.	Fault	Performance
3.	Security	Security
4.	Performance	Inventory

Simple Network Management Protocol

Q8. Is SNMP an appropriate protocol to use on a LAN to manage PC desktops and servers?

A. Yes. In fact, Compaq led the industry in using SNMP as the server management protocol. Compaq Insight Manager supports SNMP and has been available since 1992.

Q9. Doesn't SNMP generate a lot of network traffic?

A. No, but this is a common misperception. Vendors of internetworking devices such as bridges, hubs, and routers were the early implementors of SNMP and the Internet Management MIBs (for example, MIB-II). These vendors usually had a minimal amount of RAM on their device, in which to execute their SNMP management agent. So their agents provided only monitoring capabilities. Administrators are not capable of monitoring every attribute of every device simultaneously. Nonetheless, they need to know that the device is still operational. The administrator may know that when the number of receive errors exceeds a certain threshold that a failure is imminent. Therefore, the administrator can program an SNMP-compliant management platform (such as HP OpenView, IBM NetView/6000, Sun SunNet Manager, and NetWare Distributed Management System) to periodically poll the receive errors attribute and compare it with the threshold. If the attribute is greater than the threshold, the platform would notify the administrator. This platform polling causes SNMP traffic on the network — at least one and perhaps many SNMP GETs during each poll.

Fortunately, management agent technology has evolved. The paradigm for the administrator remains the same. However, it is the agent that polls the attribute and compares it with the threshold. This polling and comparison process occurs on the managed device without network traffic and without impacting the device's performance. Should the attribute exceed the threshold, then the agent generates an SNMP TRAP to notify the management platform of the event. To perform this operation required two network messages. The first was the platform commanding the agent to poll the attribute(s). The second was the agent alerting the management platform. No management protocol, standard or proprietary, can operate more efficiently. The Compaq Insight Management Agents have been designed to operate in this manner.

Desktop Management Task Force

Q10. What has the Desktop Management Task Force defined?

A. The Desktop Management Task Force (DMTF) has defined two pieces of technology - the Desktop Management Interface software (DMI) and the Management Information Format file (MIF). The DMI software is the set of APIs that enable the management of hardware and software components. A MIF is a text description of a hardware or software component that can be managed by using the DMI software. MIFs are created by component vendors to describe their product; the format and contents follow a specific set of rules in order to be understood by the DMI software.

Q11. Are there plans for standardizing MIFs?

A. In order to establish a set of standard MIFs, a number of working committees have been established within the DMTF. The PC Systems Group, composed of AST, Compaq, Dell and Hewlett-Packard have cooperated to develop a MIF that describes an industry standard PC. Other working committees include the Network Adapter Group, the Software Group and the Printer Group. The MIFs developed by the working committees will be available to the entire industry.

In addition to these standard MIFs, vendors have the option of extending the standard through the creation of vendor-unique MIFs. These MIFs represent features that are unique to an individual vendor's product or product line and are required for a complete management solution.

Q12. What is Compaq's role in the DMTF?

A. Compaq is a DMTF Steering Committee member, as well as a member of the Desktop System and Server working committees. Compaq led the authoring of the standard Desktop System MIF that describes basic industry standard desktop computers and intends to due likewise in the newly formed Server working committee.

Q13. What is Compaq's position on the DMTF?

A. Compaq, as a DMTF Steering Committee member, fully supports the DMTF's efforts to create standards for the management of networked PCs. However, Compaq believes that the Desktop Management Interface software (DMI)--the technology defined by the DMTF--is an emerging technology, not yet included as a standard feature in today's desktop PC operating systems or network operating systems. Therefore, the Partners Program is a pragmatic step that allows our customers to deploy well-integrated solutions without the need to worry about technology decisions.

The Desktop Management Task Force has made great strides to develop technology that provides a standard framework to manage desktop PCs. However, several key requirements for success still need to be met. These include broad support by operating system vendors, standardization on a remote management protocol, and broad support by management tool providers. Until these event occur, the DMI technology is not appropriate for widespread adoption by customers.

However, when these events occur, Compaq will add value to the DMI and continue to work with the members of the Compaq Desktop Management Solutions Partners Program to ensure tight integration and compatibility with these vendor's products.

Q14. What does DMI-enabled or DMTF-compliant mean?

A. At this point in time the DMTF has not placed restrictions on the use of these terms.

Q15. Does the DMI replace SNMP?

A. No. Unlike SNMP, the DMI was designed to be a purely local management enabler. The DMI does not comprehend a network protocol. Some proponents of the technology label this protocol independence. In the short run, remote management tools that support the DMI must provide a unique version of the DMI integrated with the vendor’s proprietary management protocol. In the future, the DMTF should define a standard management protocol to integrate with the DMI. This move will spur widespread adoption of the DMI by allowing PC manufacturers to preinstall the operating system, the DMI, the remote management protocol, and component agents, in essence creating a manageable desktop PC out-of-the-box. Until this event occurs, the DMI technology is not appropriate for widespread adoption by customers.

GLOSSARY

ARCNET
A network technology consisting of the token passing network access method and a bus network topology.

Bridge
An internetworking device that connects separate networks that have compatible addressing schemes, making them appear as one network.

Desktop Management Task Force
An industry consortium formed to create standards for the management of desktop computers. The current Steering Committee members include Compaq, Dell, Digital Equipment, Intel, Hewlett-Packard, IBM, Microsoft, Novell, SunConnect and SynOptics.

DMI
Desktop Management Interface.

DMTF
See Desktop Management Task Force.

Ethernet
A network technology consisting of the CSMA/CD network access method and a bus network topology.

Gateway
An internetworking device that is most often used to connect users on a LAN to minicomputers, mainframes, and other “foreign” host computers.

Internet
A large collection of connected networks, primarily in the United States, running the Internet suite of protocols. Internet is referred to as the DARPA (Defense Advanced Research Projects Agency) Internet, NSF/DARPA Internet, or the Federal Research Internet. The Internet suite of protocols is a collection of computer-communication protocols originally developed under DARPA sponsorship. The Internet suite of protocols is currently the de facto solution for open networking.

Internetwork Packet Exchange
A protocol developed by Novell, Inc. IPX is based on the XNS (Xerox Network Systems) protocol developed by Xerox Corporation.

IPX
See Internetwork Packet Exchange.

Management Information Base
A well-defined collection of information (database) that a managed network device (such as a desktop PC) maintains. The information within the MIB represents important device hardware and device software parameters, including inventory/configuration, fault, security, and performance .

Management Information Format
Conceptually, a management information format (MIF) file is similar to an SNMP MIB. However, a MIF can be implemented as a simple text file (for static configuration-only data) or implemented as a combination text file and component agents (for dynamic fault and performance data).

MIB
See Management Information Base.

MIF
See Management Information Format.

Network Access Method
The rules defined by the network to communicate among all the devices on the LAN. The two main types of access methods are token passing, and CSMA/CD (Carrier Sense Multiple Access/Collision Detection).

Network Technologies
Combinations of network topologies and access methods used to create a network solution. Some popular network technologies are Ethernet, Token Ring, and ARCNET.

Network Topology
The physical and/or logical layout of the LAN devices. The three basic topologies are bus, star, and ring.

Protocol
The language of networking. It is the rules by which bytes of information are packaged for transmission. Some popular network protocols are TCP/IP, IPX, and SNMP.

RAID
See redundant arrays of inexpensive drives.

Redundant Arrays of Inexpensive Drives
A group of two or more hard drives working together that provide increased performance and various levels of error recovery and fault tolerance.

Router
An internetworking device that connects networks that may (or may not) use different network technologies but share a common protocol.

Simple Network Management Protocol
The application protocol offering network management service in the Internet suite of protocols. SNMP is the defacto standard and has garnered a major share of the market with the support of over 20,000 products.

SNMP
See Simple Network Management Protocol.

TCP/IP
(Transmission Control Protocol/Internet Protocol) A standard protocol developed for the Department of Defense. Because the Department of Defense is such a large purchaser of computer equipment, TCP/IP is available for virtually all computing platforms.

Token Ring
A network technology comprised of the token passing network access method and a ring network topology.