Tools and Trends
in
Storage Area Network Management

by

Jeff Bain
and
Jennifer Miller

Hewlett-Packard Company
Storage Organization / Data Protection
700 71st Ave.
North Campus, M/S E3
Greeley, CO 80634
(970) 350-4238
fax: (970) 350-4675

jeff_bain@hp.com
jennifer_miller@hp.com

Tools and Trends
in
Storage Area Network Management

Table of Contents

Tools and Trends
in
Storage Area Network Management

Abstract

A new paradigm in storage and backup management has emerged in which backup devices are no longer linked to a single server via a single SCSI bus. In today's data center, storage devices are often shared by many servers and applications in a Storage Area Network (SAN). This SAN may contain any number of heterogeneous servers, stand-alone storage and backup peripherals, automated libraries, Fibre Channel arbitrated loop hubs, and fabric switches.

Management "frameworks" such as OpenView Network Node Manager, CA Unicenter TNG, and TopTools can assist in monitoring and managing a heterogeneous SAN; but in order to take full advantage of these frameworks, storage devices themselves must be network-enabled and tightly integrated. Network-enabled storage devices are freed from unnecessary dependencies on specific hardware platforms and operating systems, and system administrators are freed from having to install, maintain, and upgrade multiple OS-specific agents and drivers in order to manage their network. When storage devices can be directly monitored and configured via the web, the true potential of SAN manageability can be realized.

This "how-to" presentation will show attendees how to set up and use network management frameworks – such as Unicenter and TopTools – to get a big-picture view of the network-enabled backup devices on their SAN. Current trends and futures in network-enabled backup manageability will also be discussed, with particular emphasis on the Distributed Management Task Force's Common Information Model (DMTF CIM) and the SNIA Storage Media Library Group's Management Information Base (SNIA-SML MIB).

Introduction

This paper describes the tools and technologies that have been available, and are becoming available today, to monitor and manage a Storage Area Network (SAN) and, by extension, the enterprise as a whole. Three stages of SAN and enterprise evolution will be described: a server-centric stage, a SAN stage, and a network-enabled storage stage. For each stage, a model will be described, tools and technologies will be highlighted, and challenges will be pointed out.

It is important to note that the figures shown in this paper focus on the management-centric aspects of the enterprise. Buses and topologies generally associated with "real" data transfer – such as SCSI and Fibre Channel – are shown only if they also serve as a path to retrieve status and asset information from devices. Further, automated tape libraries are often used as convenient examples of SAN storage devices, though the topics discussed apply equally to all storage devices, including RAID arrays, NAS disks, magneto-optical libraries, and stand-alone drives.

Yesterday's Enterprise: Server-Centric Storage

Historically, device management has meant local – rather than remote – management. A device's front panel has been the primary means for configuring and monitoring the device. Backup applications have provided an additional, limited means of device monitoring, but the use of such applications has tied storage devices to a single server. A typical server-centric management path is shown in Figure 1.

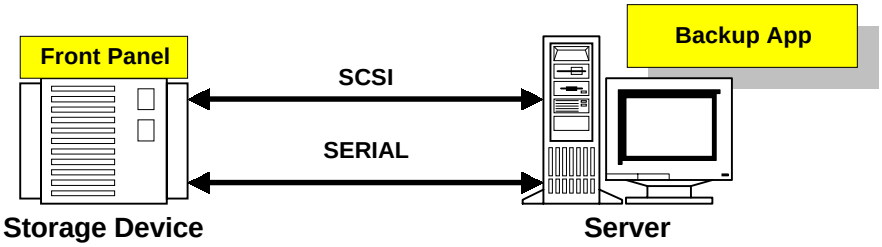

Figure 1: Typical Server-Centric Management Path

Here, we have a server connected to a storage device using a SCSI bus and serial connection. Any management of this device is done primarily through the device's front panel, through a serial port, or through a backup application on the server. The front panel will allow users direct access to the device, and will often include a type of error indicator, such as a red light. Unfortunately, a user must be physically near the device in order to view this error indication. A backup application can also report errors that occurred during a backup, but generally provides no information regarding the true nature of failures associated with the storage device. As with the front panel, remote notification of backup failures is often not available.

A slightly more sophisticated management path is shown in Figure 2.

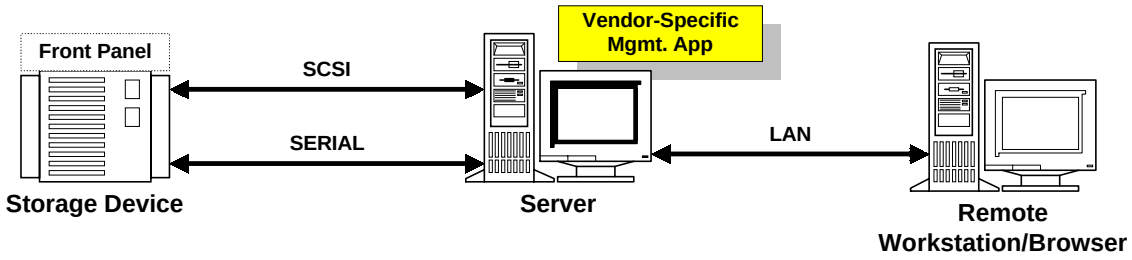

Figure 2: More Sophisticated Management Path

Here, a vendor-specific management application has replaced the backup application and front panel as the primary means of device management. While the front panel has not entirely disappeared, use of a host-based management application provides a better user interface. Such an application might also provide a means of remote – though indirect – access to the device. Remote users can point their browsers at the workstation on which the management application resides, and the application will communicate with the storage device over the SCSI bus – or via another physical connection – on the remote user's behalf.

Despite the advantages of this model over that shown in Figure 1, the disadvantages of vendor-specific, host-based management applications should not be overlooked:

- Users are tied to a specific vendor and device family by the vendor-specific nature of the management application
- Users are often tied to a specific operating system by the host-based nature of the management application
- Users are tied to a particular physical server for their device management needs. Connecting the storage device to a different server requires reinstallation of the management application and redirection of remote browsers

It should also be obvious that Figure 2 is a not a realistic picture of a data center. Generally, a data center consists of many more servers and storage devices, often from different vendors or running different operating systems. These differences between systems yield further management difficulties:

- No central point of management; multiple devices must be monitored independently
- Vendor-specific nature of applications makes interoperability difficult
- Tools from multiple vendors need to be evaluated, purchased, monitored, and upgraded individually

Today's Enterprise: Storage Area Networks

As the size and complexity of the enterprise increases, it becomes increasingly difficult to track the status and health of individual devices. Devices can be logically dispersed across multiple subnets, as well as physically dispersed across multiple sites. The creation of storage area networks (SANs) has contributed to this physical dispersal by allowing devices to be shared by multiple hosts separated by long distances. To track the health of all devices in a SAN, centralized device management is required. A typical picture of device management in a SAN is shown in Figure 3.

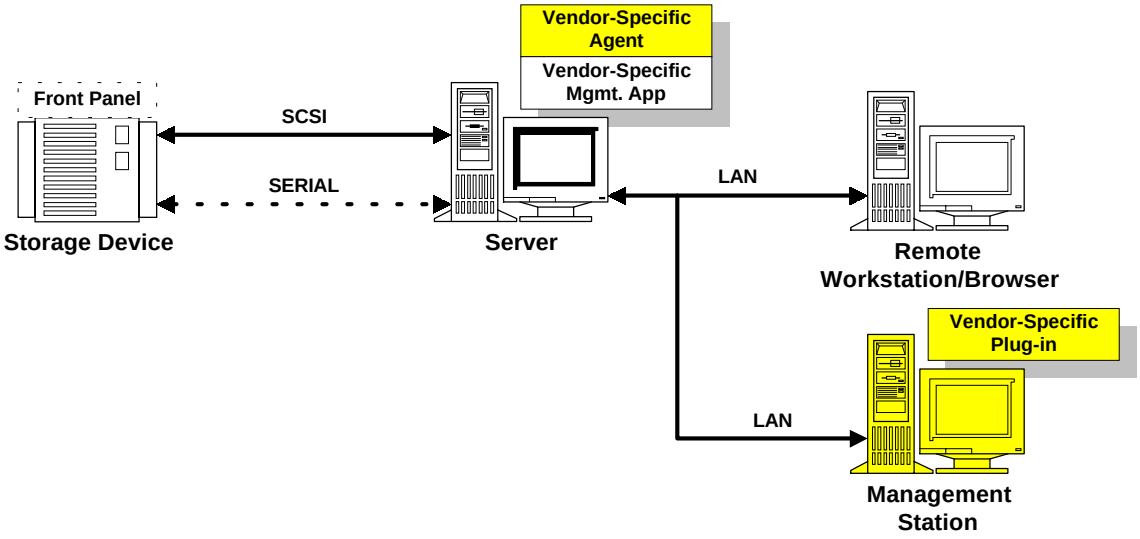

Figure 3: Typical Storage Area Network Management Path

Though only a small portion of a SAN is shown in Figure 3, the management path shown is representative: a storage device is attached to a server, or, as discussed later, to multiple servers. In Figure 3, a vendor-specific agent has been installed on a server that serves as a bridge between the storage device's SCSI (or Fibre Channel) connection and the LAN. Information about the storage device is retrieved by the agent and sent – usually using Simple Network Management Protocol (SNMP) – to a management station, where that information is interpreted using a vendor-specific decoder called a *plug-in*. As in the model of Figure 2, the server agent may also allow some level of (indirect) remote access to the storage device.

In today's SAN environments, multiple storage devices are usually shared between multiple servers. However, a single management station running a *framework tool* can monitor multiple servers and storage devices simultaneously. By using such a tool, a degree of centralized management can finally be achieved. What may not be apparent from Figure 3 are the disadvantages inherent in using an agent/plug-in mechanism to achieve centralized management:

- The vendor-specific nature of agents and plug-ins allow for management of only a single vendor-specific device family (per agent/plug-in pair)
- An agent must be installed on at least one server to which each storage device is connected
- Plug-ins and agents are often operating-system-specific, requiring a different agent and/or plug-in for each server type

- Vendors' development costs for agents and plug-ins are often passed on to customers
- The availability of multiple framework tools results in multiple agent/plug-in flavors, requiring further development and maintenance time for engineers, yielding increased cost for customers

In short, the proliferation of vendor-, operating-system-, and framework-tool-specific agents and plug-ins can make installation and upgrading of management utilities quite difficult. One improvement in this area can be made by eliminating the server-side agent software from the picture and moving the communications intelligence inside the storage device, which can then be connected directly to the LAN. This improved model is show in Figure 4.

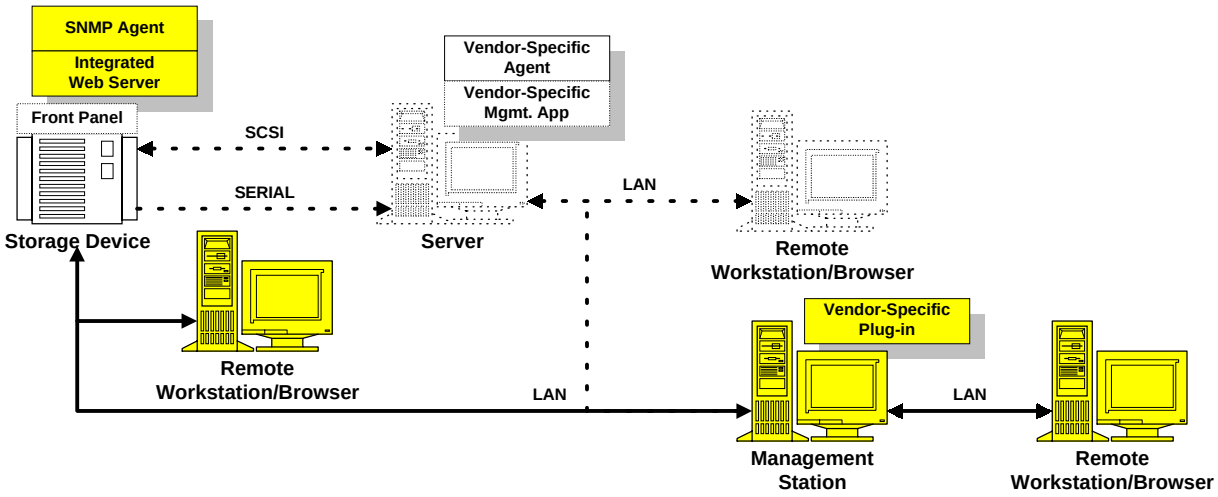

Figure 4: Improved Management by Elimination of Host-Based Agents and Addition of an Integrated Web Server

By adding networking ability to a storage device, remote device management can be done directly. If a company allows dial-up access to their LAN, remote management can even be done outside the office using a PC, laptop, or palmtop with a modem. Moving device management directly to the LAN eliminates management traffic from the SCSI/Fibre data path, and also eliminates the possibility of access conflicts between backup applications and server-based management agents. Storage devices are no longer tied to a specific server, and vendor- and OS-specific agents do not need to be installed and maintained (though plug-ins for framework tools are often still required). The management model of Figure 4 is becoming quite common today, and a more detailed discussion of centralized management stations and framework tools is merited.

Framework Tools for Managing Today's Enterprise

Framework tools are commonly used today to monitor and manage even the largest networks. Though several competing tools are available, all have several features in common:

- Discovery, in which manageable devices are found
- Topology Mapping, in which the physical or logical connections between devices are displayed, usually graphically

- Device Status Display, in which an indication of individual or group device status is reported
- Asynchronous Event Reception and Logging, in which updated device information is received without the need for constant polling
- Drill-Down/Application Launch, in which one or more applications are used to provide additional status and diagnostic information about a device

To these five basic features, two more advanced features are often added:

- Event Correlation/Tracking, in which polled information and event logs are analyzed in order to discover trends and make predictions
- Remote Notification, in which an email or page is sent from the management station to a user in order to flag important events

HP OpenView Network Node Manager

One framework tool incorporating the above features is HP's Network Node Manager (NNM). As the name suggests, NNM is focused more on LANs than SANs. However, when used in conjunction with plug-ins and network-enabled storage devices, NNM can be a powerful tool for a variety of storage management tasks.

Part of a typical NNM screen is shown in Figure 5.

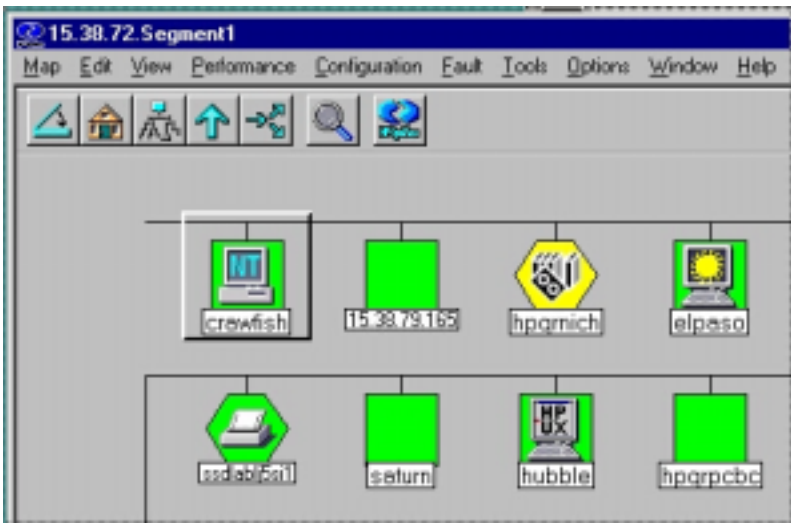

Figure 5: Typical NNM Screen

Several device types are shown in Figure 5: *ssdlablj5si* is a printer, *hubble* is an HP-UX workstation, *crawfish* is a Windows NT system, *elpaso* is a Sun workstation, *hpgrnich* is an HP tape library, and *saturn* has not been identified as a specific device type (and so retains its generic box icon). Each of these devices has been discovered by NNM using TCP/IP *ping*s. Once a device answers to a *ping*, it is queried using SNMP. Generally, a particular SNMP "object" called *sysObjectID* is queried. NNM uses the *sysObjectID* to associate a device type with a particular icon. Many standard device types are recognized, such as NT, HP-UX, or Solaris workstations. Devices that do not return a known *sysObjectID* – or do not respond to SNMP requests at all – are shown with the generic box icon.

For newer devices with new *sysObjectID*s, NNM can make use of vendor-unique plug-ins to add functionality. As mentioned above, a plug-in is a small piece of code or series of files that modify or add to a framework tool's functionality in some way. A simple plug-in might allow NNM to recognize a new *sysObjectID* and associate a new icon with devices responding with that *sysObjectID*. In Figure 5, a plug-in has been used to allow NNM to recognize *hpgrnich* as an HP DLT tape library and associate a new icon with that device. Without this plug-in installed, *hpgrnich* would show up as a blank square, just like *saturn*.

Plug-ins for many management packages can also be used to create menu items or functions specific to certain device types. For example, Figure 6 shows the difference between standard NNM menu items for generic devices and enhanced menu items created by a tape library plug-in for *hpgrnich*.

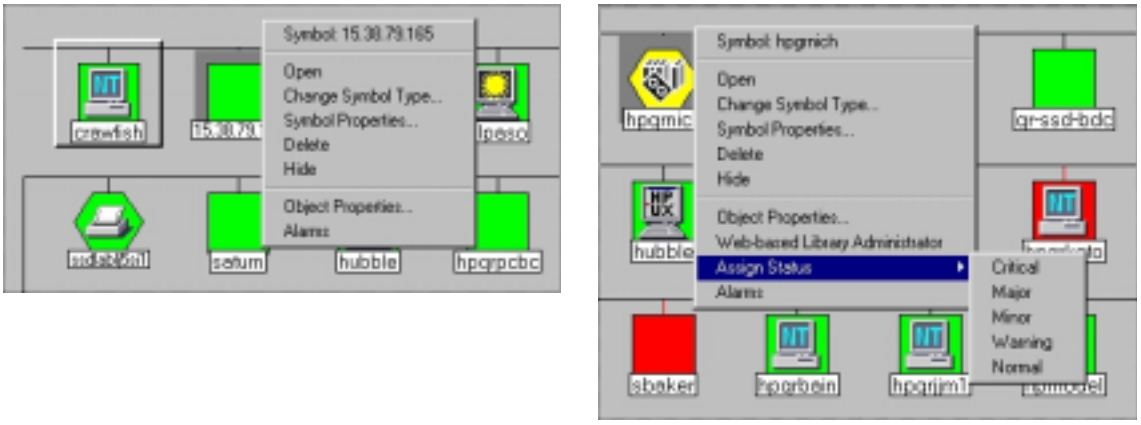

Figure 6: General and Plug-in Enhanced Menu Items in NNM

The additional menu items shown in Figure 6 provide device status monitoring and control – through the Assign Status option – and drill-down capability – through the Web-based Library Administrator option – for the *hpgrnich* tape library.

A final NNM screen shot is shown in Figure 7.

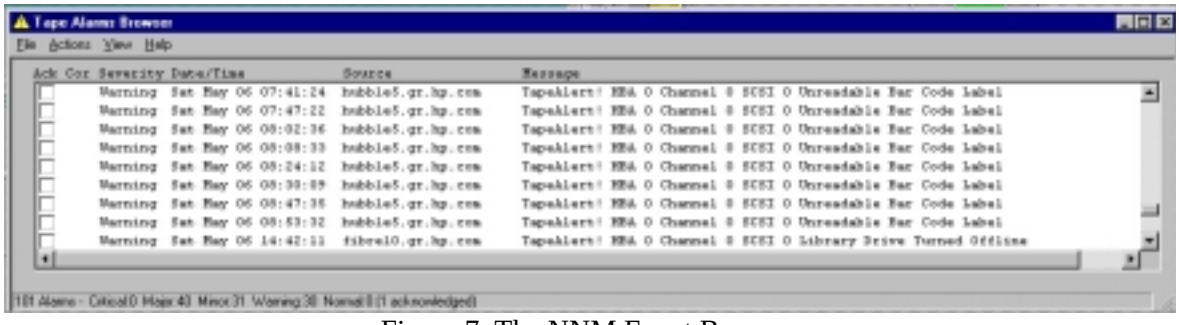

Figure 7: The NNM Event Browser

Figure 7 shows a list of asynchronous events that have been sent by various devices to NNM. NNM understands and decodes certain events automatically, while some events need to be decoded using a plug-in. The TapeAlert events shown in Figure 7 have been decoded using the same plug-in that provided other new functionality for *hpgrnich*.

CA Unicenter TNG

Computer Associate's Unicenter TNG provides similar functionality to NNM. Part of a typical Unicenter screen is shown in Figure 8.

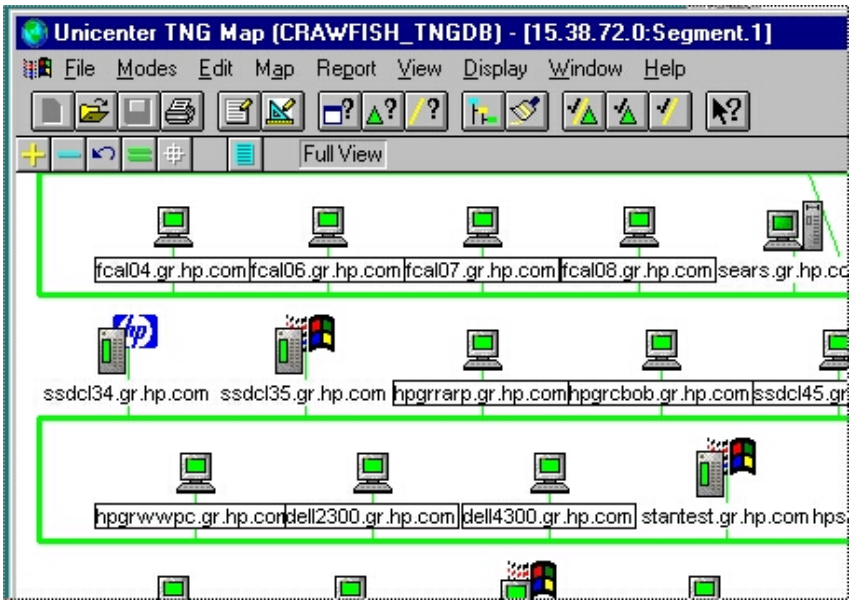

Figure 8: Typical CA Unicenter TNG Screen

As with NNM, Unicenter can identify a variety of device types: *fcal04* is a workstation, *ssdcl34* is an HP server, and *ssdcl35* is a Windows server. Although not shown in Figure 8, Unicenter also discovers and identifies printers, switches, and other standard device types. For new device types, plug-ins are again required. Additional details and status information for individual devices is available through Unicenter menus. Detailed information on *hpssdstv* is shown in Figure 9.

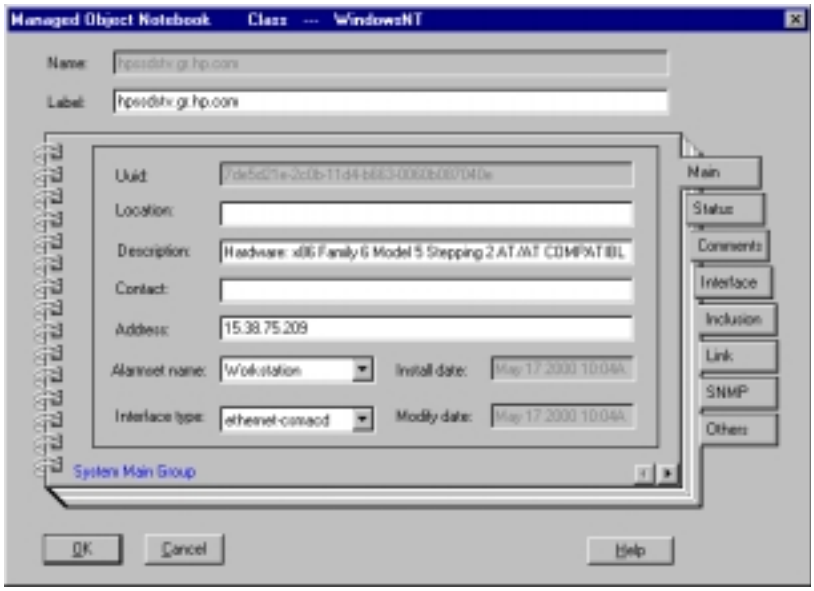

Figure 9: Detailed Device Information in CA Unicenter TNG

The device description shown in Figure 9 ("Hardware: x86 Family Model 5") was retrieved from *hpssdstv* using SNMP, as in NNM. Other standard Unicenter functions include asynchronous event reception, drill-down capability, event correlation, and remote notification.

HP TopTools

A third tool for network-based device management is HP's TopTools, a free, web-based framework tool providing similar functionality to NNM and Unicenter, though on a slightly smaller scale. A typical TopTools screen is shown in Figure 10.

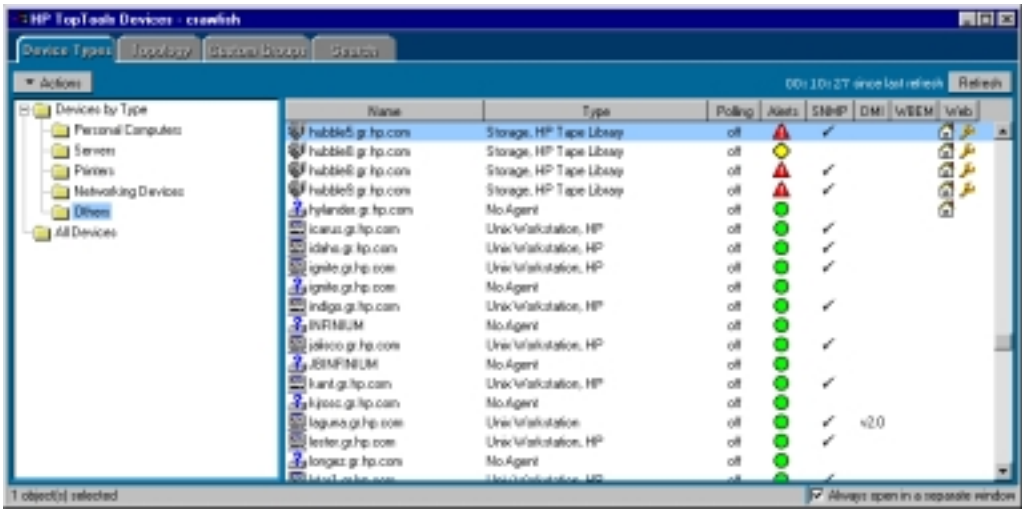

Figure 10: Typical TopTools Screen

Here, discovered devices are listed in tabular format. Whenever possible, a device type is listed, an overall status is shown, and the various protocols supported by each device are listed. As with other framework tools, asynchronous events can be received by TopTools and correlated in an intelligent manner. Figure 11 shows the TopTools event viewer screen for a tape library device.

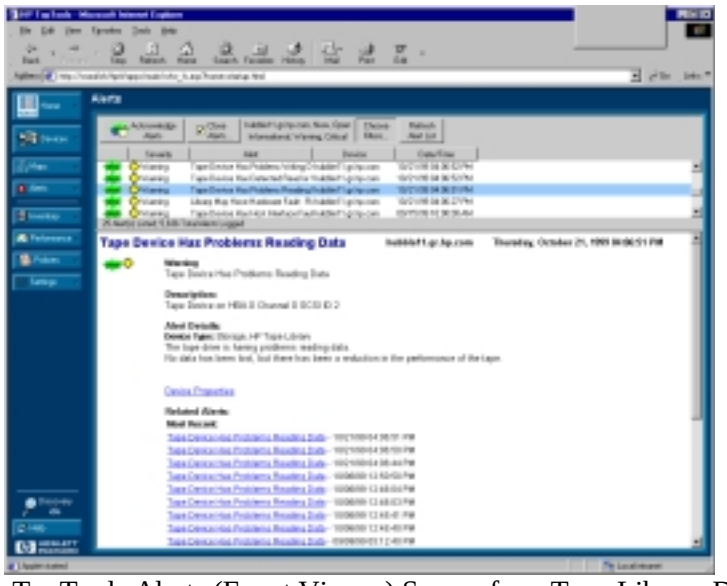

Figure 11: TopTools Alerts (Event Viewer) Screen for a Tape Library Device

In Figure 11, one alert in the list has been selected, and detailed information regarding that event is shown in the lower part of the screen. Previous occurrences of the same event are also listed. Though a tape library has been used in this example, similar functionality is available for printers, switches, servers, and other device types.

HP SAN Manager DM

One important piece of information not shown in any of the previous figures is data path topology. Management path connections between switches, hubs, and devices on a LAN are shown while SCSI and Fibre Channel connections between servers and peripherals are not. NNM, Unicenter, and TopTools, having been created for LAN-based enterprise management, are not easily extended to included SAN-based storage management. However, tools are becoming available that focus specifically on SANs and their data path topologies. One such tool is HP's SAN Manager DM, shown in Figure 12.

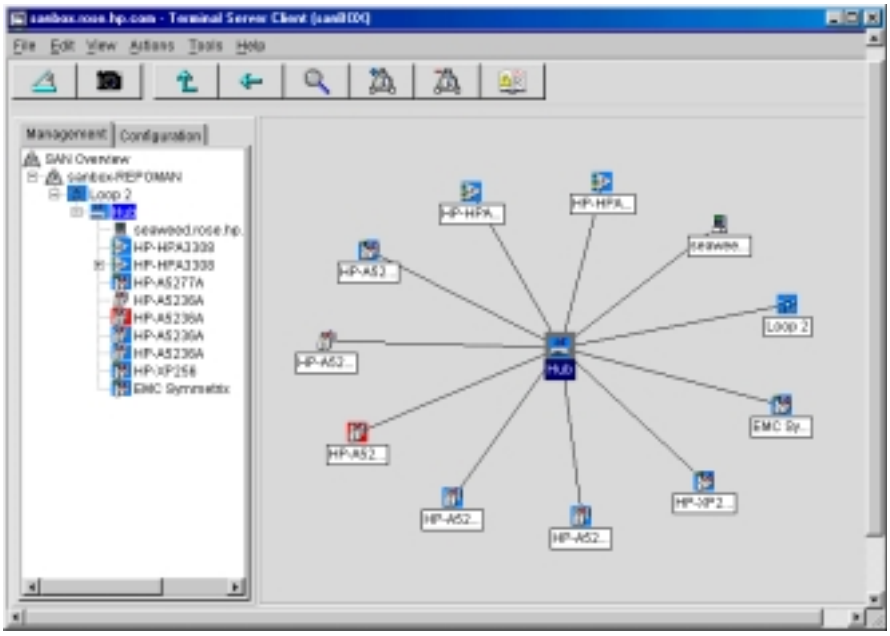

Figure 12: SAN Manager DM

SAN Manager DM discovers and illustrates a SAN topology in much the same manner as NNM, Unicenter, and TopTools illustrate a LAN topology. SAN Manager DM uses both LAN-based *ping*/SNMP discovery and SAN-based SCSI/Fibre discovery to draw a more complete picture of manageable devices. Storage devices connected to servers via SCSI or Fibre Channel are discovered using standard SCSI *inquiry* commands issued by SAN Manager DM agents installed on the servers. Inquiry data for discovered devices is passed back to a central management station as was shown in Figure 3. In addition, SAN Manager DM uses *ping*/SNMP discovery to detect network-enabled storage devices as shown in Figure 4. By correlating the device data received through these two paths, SAN Manager DM is able to draw a very complete picture of the enterprise. Figure 12, for example, shows several devices connected via a Fibre Channel hub in the center of the picture. The hub has been discovered using LAN-based mechanisms, while the other devices were discovered using SAN-based mechanisms. The connections between the hub and the other devices were derived by using SNMP to gather additional information from the hub on which devices were connected to it.

As with other framework tools, more detailed information on each device can be displayed, as shown in Figure 13.

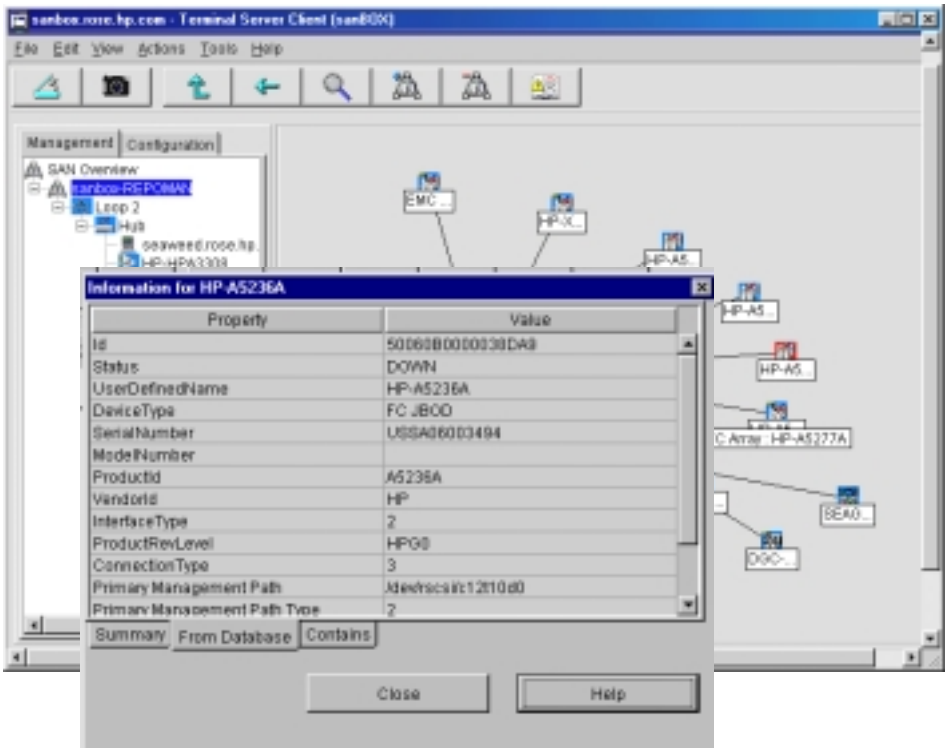

Figure 13: Detailed Device Information in SAN Manager DM

For many device types, external applications or web-based tools can be launched to diagnose device-specific conditions. Plug-ins can be installed to provide support for new device types.

Web-Based Drill-Down and Application Launching

Each of the framework tools discussed so far provides high-level, centralized management of servers, workstations, printers, switches, hubs, and storage devices. Each allows users to monitor their LAN/SAN, and each provides remote notification of important asynchronous events. However, no tool can be completely familiar with every device in the enterprise. In order to support the unique features of each device type, framework tools usually provide a way to launch a device-specific application that gives the user more direct control of that device. Many applications in this category are web-based, allowing for completely remote management of a device from any location. Without remote management capability, a user might be notified of an important event pertaining to a specific device, but still be unable to handle that event without being in close physical proximity to that device. In today's growing enterprise, the inability for a device to be managed and configured remotely is becoming unacceptable.

Examples of web-based device management tools are given in this section.

ATL WebAdmin

ATL's WebAdmin library administrator is a host-based application that allows remote management of ATL libraries from Windows NT- and Windows 2000-based servers. A screen shot of WebAdmin 3.0 is shown in Figure 14.

Figure 14: ATL's WebAdmin

WebAdmin gives both logical and physical views of an ATL library, allows configuration of library parameters, logs important events, provides diagnostics for troubleshooting, and can send email messages to administrators. However, WebAdmin is a host-based tool that must be installed and maintained on a server connected to the library over SCSI or Fibre Channel. Because of this, it is subject to certain architectural constraints already discussed in conjunction with Figure 3.

StorageTek Horizon Framework Library Monitor

StorageTek's Horizon Framework Library Monitor is a web-based application integrated into StorageTek tape libraries, including the L180 and L700. Two screen shots of Horizon are shown in Figure 15.

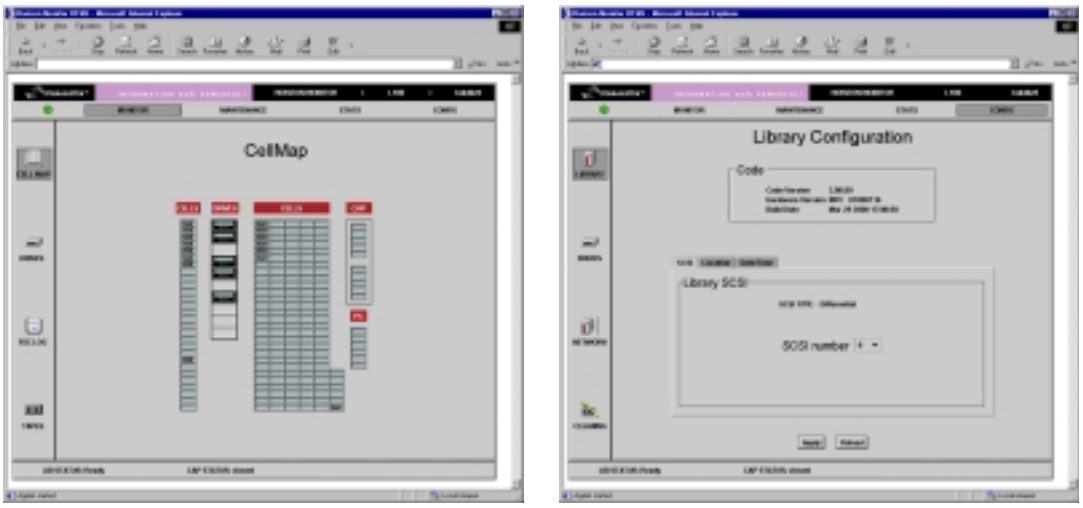

Figure 15: StorageTek's Horizon Framework Library Monitor

Horizon displays the status of the library's drives, robotics, and cartridge access ports. It also logs events, runs diagnostics, allows firmware upgrades, and forwards events on to management framework tools. The Horizon software is served up through an integrated web server, and therefore requires no host-based agent. However, Horizon is implemented in Java 1.2, and requires that an operating-system specific plug-in or Java 1.2 Runtime Environment (JRE) be installed on each host where a web browser will be run. As Java 1.2 becomes more widely used, it is possible that newer browsers will be shipped with this plug-in or JRE standard, eliminating the need for extra installation steps.

HP Web-Based Library Administrator

HP's SureStore 2/20, 4/40, 6/60, and 6/140 tape libraries contain an integrated Remote Management Card which includes a web server and SNMP agent. The web server serves a Web-Based Library Administrator, shown in the two screen shots of Figure 16.

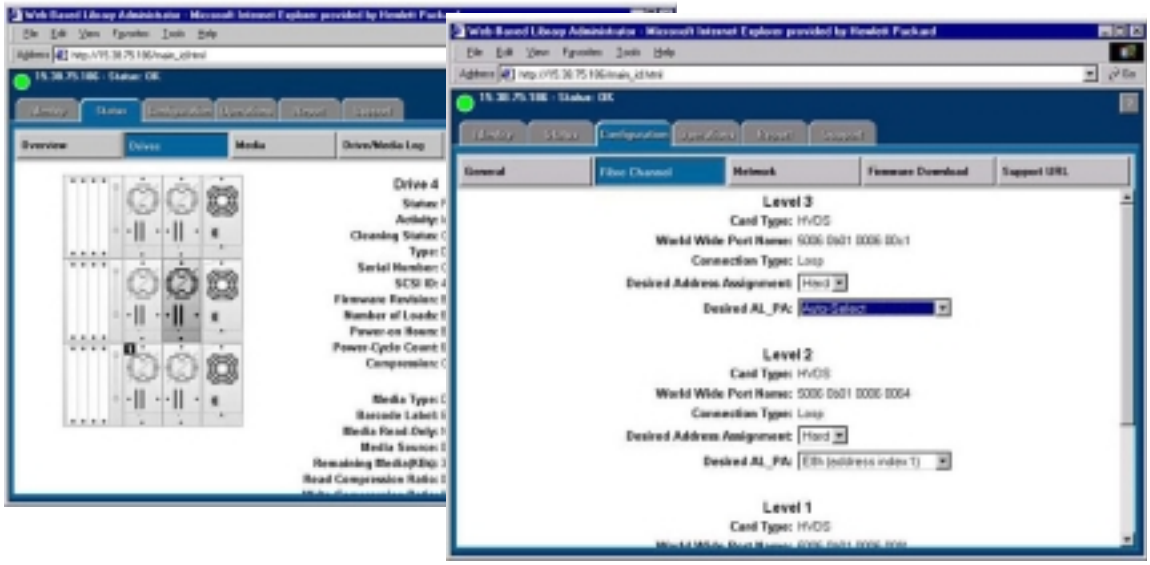

Figure 16: HP's Web-Based Library Administrator

Using the Web-Based Library Administrator, users can view library and drive status, download firmware, run diagnostic tests, configure SCSI, Fibre Channel, and network parameters, generate a summary report, view logs, and link to HP's support site. The Web-Based Library Administrator is compatible with any Java-enabled browser and requires no additional plug-ins or installation.

HP SureStore NetStorage 6000 Web Interface

The HP NetStorage 6000, a network-attached storage (NAS) device, also comes with a standard web interface, shown in Figure 17.

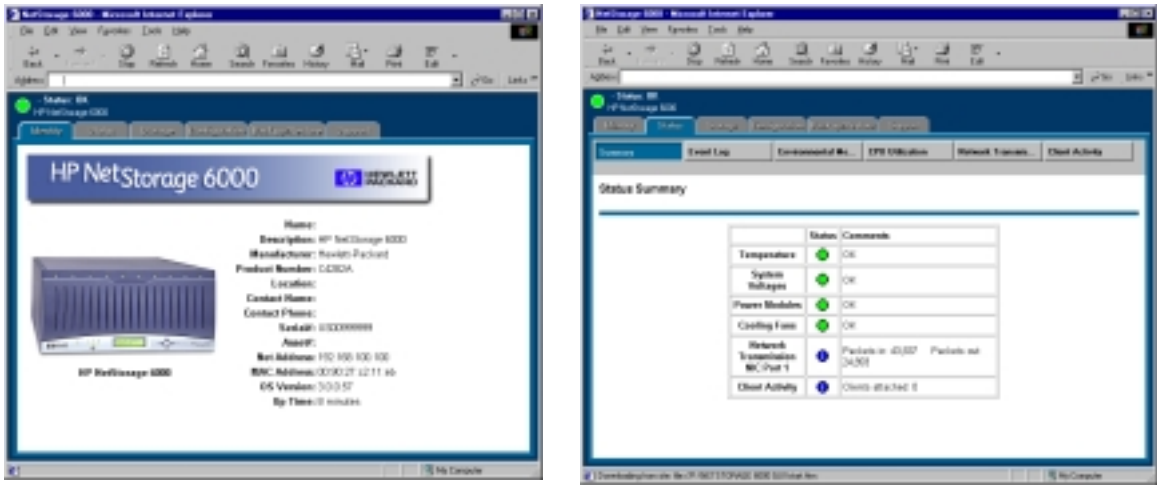

Figure 17: NetStorage 6000 Web Interface

Through the HP NetStorage 6000 Web Interface, users can monitor the device's environmental conditions, CPU utilization, network activity, and overall health. Users can also view logs, configure network and tape backup parameters, download firmware, and link to HP support. As with the Web-Based Library Administrator, no software installation is required; the web interface is a standard, built-in feature.

HP ProCurve Switch Web Interface

As a final example of network-enabled devices with built-in diagnostic tools, consider HP's ProCurve network switch. A screen shot of its web interface is shown in Figure 18.

Figure 18: ProCurve Switch Web Interface

Using this interface, each port on the switch can be monitored and configured individually, and a variety of other administrative and diagnostic functions can be performed.

Other Devices with Web-Based Management

The tools and products listed above are only a sampling of what is available today in terms of remote, web-based device management. Other devices with web interfaces include Brocade's Fibre Channel fabric switch, Crossroads 4200 family of Fibre-to-SCSI bridges, HP's XP256 disk array, Overland Data's WebTLC interface device for their automated storage libraries, and HP's Web JetAdmin for printers.

Using these tools, devices can be monitored and (re)configured from any location with network access. Administrators are no longer required to be at the device to keep track of its status. Not only can management be centralized, it can be centralized wherever the administrator happens to be.

Recommendations for Managing Today's Enterprise

Each of the devices described above offers a remote interface through one of three methods:

1. a host-based software agent that interfaces with a device through SCSI or RS232
2. an external box that interfaces with a device through SCSI or RS232
3. an integrated card or processor built directly into a device.

It is our claim that *built-in* management tools with broad browser and framework tool compatibility offer the greatest degree of flexibility available today. Reasons include:

- Zero installation: the remote management tool is a standard built-in part of the device
- Absolute physical independence: the device does not have to be connected to a specific host or other external device to be managed
- Operating system independence: the device can be managed from any system with a browser interface, including dial-up and laptop/palmtop systems

When purchasing your next disk array, NAS device, storage library, hub, or switch, ask your vendor the following questions:

- What management and diagnostic capabilities are built into the device? SNMP for discovery and event notification? HTTP for remote diagnostics and drill-down?
- Is remote, web-based management available for the device?
- Is additional software installation or hardware cabling required to take advantage of management and diagnostic features?
- What operating systems or browsers are compatible with the device's management and diagnostic tools? Are patches or browser plug-ins required? Do these compatibility constraints limit the device's manageability in your environment?
- What framework tools is the device integrated with? Are plug-ins available for the framework tool you use?
- What additional features do framework plug-ins offer for this device? Browser-based drill-down? Asynchronous event/error notification? Status polling? Event correlation?

In addition, ask yourself or your data center personnel to consider the following:

- If a backup fails during the weekend, or in the middle of the night, how long will it be before I find out? What risks are involved in this delay?
- If I'm away from the office, how can I keep track of critical devices in my SAN?
- How accurately can individual device failures be pinpointed?
- Can I easily change device configurations and diagnose problems myself, or do I have to wait for service personnel to arrive?
- Can I easily get a big-picture view of the health of my enterprise, or do I have to walk around and examine each device individually?

Through considering these questions, the importance of device manageability, particularly *remote* manageability should become clearer. How do you manage the devices in your SAN/enterprise today?

Tomorrow's Enterprise: Network-Enabled Storage

It should be obvious from the numerous web-based management tools described that each device has its own vendor-specific interface. Though some devices share a common look and feel, the manageability features available in each device are very different. Plug-ins for framework tools continue to be tied to a particular device, and often a particular operating system. Overall, the *data* available from a device is closely linked to the *presentation* of that data. For these reasons, interoperability between devices can be as much of a problem in the management path as it is in the data path. Though a management solution for multiple heterogeneous devices can be

constructed, it is often done in an ad hoc manner: a far cry from the plug-and-play architecture desired by data center personnel.

To reach a truly plug-and-play management environment, industry standards are required. The mechanisms most often used by framework tools are those which are industry standards. For example, *ping* is used by most tools for discovering devices on a network. If network devices did not support *ping*, most framework tool vendors would be hesitant to support this method of discovery. Instead, device-specific plug-ins would need to be installed in order to discover each new device type. Fortunately, all network-enabled devices support *ping*, and framework tools have no problem discovering devices in a heterogeneous environment.

In this section, examples are given of technologies and initiatives that seek to improve interoperability and manageability between heterogeneous devices on a SAN or in the enterprise as a whole.

HP's Network Managed Storage Initiative

When using a framework tool for centralized device management, identification of specific device types can be a problem. Plug-ins can be used to improve recognition of newer devices, but these plug-ins are vendor- and/or OS-specific and require installation and upgrading. HP's Data Protection organization is crafting an initiative to make device identification and information gathering more standard, particularly among network-enabled storage devices. This initiative, called the Network Managed Storage initiative, or NMS, describes a standard way for storage devices to communicate the following:

- Device type
- Device description
- Overall device status
- Device firmware revision(s)
- URL for drill-down management of the device
- Who to send important events to (i.e. "trap destination" configuration)

If framework vendors provide support for the NMS initiative, a management path model similar to Figure 19 would be possible.

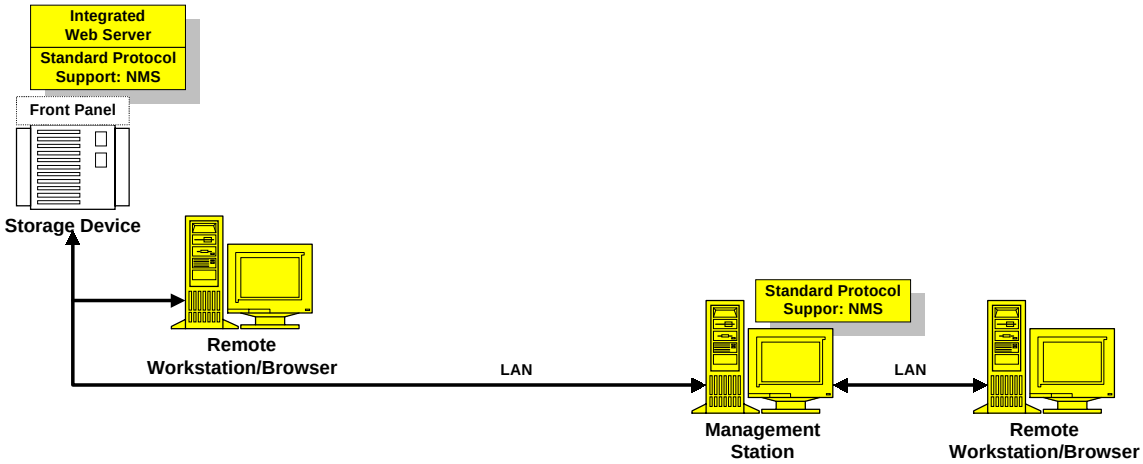

Figure 19: Management Path with Standard Protocol Support

In this model, no framework plug-ins are required to enable centralized device management. A framework tool – running on the Management Station of Figure 19 – would, by default, support a standard information gathering mechanism such as the NMS initiative. Users would no longer be required to install and maintain vendor-specific plug-ins, and full integration of network-enabled storage devices with framework tools could be achieved.

The DMTF, SNIA, CIM, and XML

Similar standardization efforts are proceeding on a variety of fronts. The Distributed Management Task Force (DMTF) has defined a Common Information Model (CIM) that describes a large number of devices in the enterprise. For example, CIM provides a standard set of information about storage libraries, disk and tape drives, SCSI buses and LANs, displays, power supplies, and many other devices and components. In contrast, vendors today generally serve up vendor-unique information in a device-specific, proprietary format. The use of a standard data model like CIM could eliminate the need for vendor-unique information sets (and plug-ins).

In order for CIM to be truly useful, network-enabled devices must be able to exchange CIM information with management tools in a standard way. Extensible Markup Language (XML) is one such way. XML is a textual "language" – similar to HTML – that can be used to model and exchange a wide variety of information. XML can be served up like standard web pages (via HTTP), but XML contains no formatting information, like font size, colors, or frames. XML is pure data that can easily be parsed and understood by applications. Standard CIM information exchanged using XML can yield a management picture similar to Figure 20.

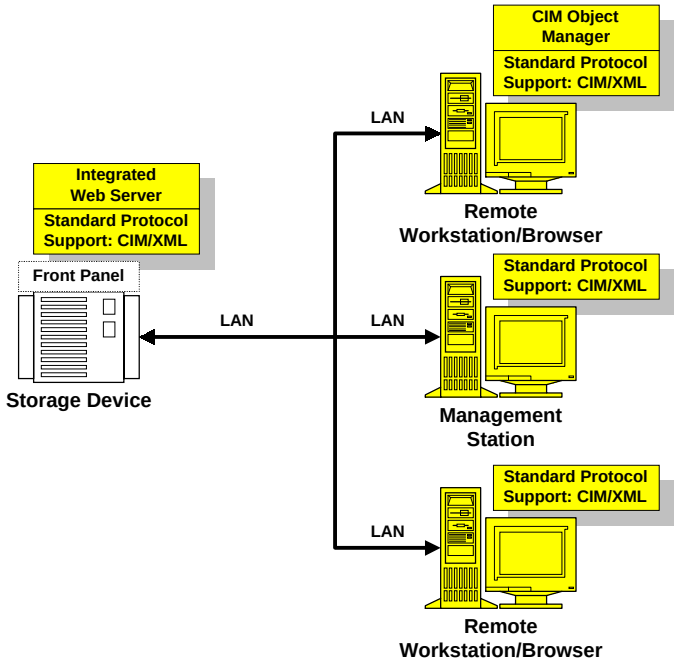

Figure 20: Plug-and-Play Management Using Standard Data and Transport

In Figure 20, CIM and XML provide the "Standard Protocol Support" shared by the Storage Device, Management Station, and Remote Workstation/Browsers. No plug-ins or other software installations are required; devices simply connect to the LAN and talk together.

A second method of exchanging CIM data is through a CIM Object Manager, or CIMOM. A CIMOM is a centralized application that collects CIM data from devices and makes it available to other applications through API calls. In some ways, a CIMOM is similar to a framework tool with some standard services but no plug-ins. In order for applications to retrieve device data through a CIMOM, the CIMOM must use a "Provider" that knows how to interface with a specific device type. In this way, a Provider functions in the same way as a framework tool plug-in, helping to discover devices and providing a proxy through which the application can gather information from a device. CIMOMs are available today for Microsoft's Windows and Sun's Solaris platforms. The Storage Networking Industry Association (SNIA) also provides an open-source CIMOM for public use. SNIA's CIMOM is written in Java, and uses the same interfaces as Sun's CIMOM.

CIM integration efforts are currently under way at the Storage Networking Industry Association (SNIA), particularly in the Storage Media Library (SML) working group. The SML group has created new CIM data models for automated library devices, and is working on an analogous SNMP model – the first of its kind – that devices would use to send information to CIMOMs via a Provider. Using this SNMP Management Information Base (MIB), framework tools could also retrieve information about library devices in an open, standard way.

Sun's Federated Management Architecture and JINI

Also known as Jiro, Sun's Federated Management Architecture (FMA) provides an infrastructure for the development of management applications. FMA provides a three-tiered architecture for device management. The top tier consists of the management applications themselves. The middle tier consists of distributed Java components – called FederatedBeans™ – and services that make features and interfaces available to higher-level applications. The bottom tier consists of manageable devices. By creating distributed Java "beans", developers can craft a management solution specific to a particular class of devices. Higher-level beans can build on the services of other beans to provide more intelligent functionality. As with CIMOM implementations, FMA can be thought of as a generic framework tool into which devices can be integrated. Rather than using CIMOM Providers to interface with devices, FMA uses Java beans called "Management Facades". Like framework tools, FMA also provides a set of services – such as event posting and retrieval, task scheduling, and polling – that may be useful to application developers. If a device needs to communicate an asynchronous event to an FMA management application, it would send that event to the Management Facade, which would publish the event using the FMA event service. A management application "subscribing" to that event service would then receive the event coming from the device.

An important component of FMA is JINI, a Java-based connection technology that allows Management Facades and other beans to discover each other and use each others' services. If a Management Facade supports a particular class of device, management applications would use JINI to discover the services provided by that Management Facade, and use those services to gather information from the device.

Using the services of CIMOM Providers or FMA Management Facades, these infrastructures can provide the features common to most framework tools:

- Discovery
- Device Status
- Event Notification
- Remote Notification
- Topology Mapping
- Drill-down/Application Launch
- Event Correlation

Ancor, a manufacturer of Fibre Channel switches and switch management products, has recently produced the first commercial Management Facade for FMA. The work done by SNIA's SML working group could also lead to the production of a Management Facade supporting automated library devices.

Tools, Trends, and Challenges in Tomorrow's Enterprise

Device management in tomorrow's enterprise will move toward broad interoperability through the implementation of industry standards. The use of XML to transport CIM data between devices and management applications is especially promising since it provides a level of independence from vendors, devices, and operating systems that can simply not be matched by other technologies. Even FMA and CIMOM implementations add a level of middleware that ties device management back to a particular operating system and technology that can increase development time and cost while decreasing interoperability.

On the other hand, CIM/XML does not provide some of the features common to framework tools. In particular, CIM/XML does not provide an asynchronous event notification system. For the time being, SNMP traps (alerts) would need to be used to communicate events without polling. This coupling of CIM, XML, and SNMP could work as shown in Figure 21.

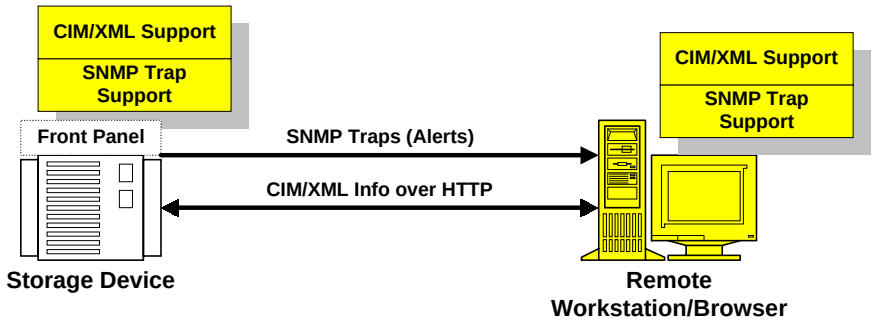

Figure 21: Using CIM/XML and SNMP for Device Management

Here, *ping* and HTTP requests are used to discover devices that support CIM/XML. Device status is polled using CIM/XML, and topology mappings are performed by applications after gathering CIM information from various devices. Drill-down/application launch can be performed by pointing a browser at a device, which already has an integrated web server to support CIM/XML transactions. Event notification is performed using SNMP traps, and events can be correlated at the remote workstation. Remote notification – via email/SMTP or web/HTTP – can be performed either directly by the storage device or from the remote workstation upon receipt of important events. Most importantly for end-users, no software – other than a browser and/or framework tool – is required for management of multiple devices.

Several steps must be taken before such a level of interoperability and vendor/platform independence can be achieved:

- Continued development of the CIM model
- Adoption of the CIM model by device and application vendors
- Implementation of the CIM/XML standard
- Development of an event mechanism for CIM

Watch for continuing development in the areas of vendor-, and platform-independent device management, and talk to your storage device vendor about their plans for support of CIM/XML.

Summary

Three stages of LAN/SAN development have been described from a management-centric point of view. In the first stage, storage devices are closely linked to a server and are managed primarily through a front panel or backup application. In this stage, remote management of single devices is difficult and centralized management of multiple devices is not possible. These difficulties arise primarily because management applications are closely tied to specific vendors, devices, and operating systems.

In the second stage, storage devices are shared between multiple hosts and can be managed from a central location using framework tools. Device-specific information and diagnostics are made available directly from network-enabled devices or through framework plug-ins. Despite these improvements, the sheer number of devices, vendors, operating systems, and framework tools results in increased development time for engineers and higher purchase and maintenance costs for end-users.

In the third stage, additional intelligence is built directly into storage devices, and the implementation of industry standards allows applications to talk directly to these devices without the need for host-based agents, plug-ins, or other middleware. XML and HTTP can be used to transfer standard CIM information between devices and applications, providing a management mechanism that is truly independent from vendors, operating systems, and middleware technologies.

For each stage, one or more models have been described, tools and technologies have been highlighted, and additional advantages and challenges have been pointed out. In addition, several examples of framework tools, plug-in capabilities, and web-based drill-down utilities have been provided.

Websites with further information on the technologies and products discussed in this paper can be found in Appendix A.

Appendix A: Where to Find Out More

SNMP: Simple Network Management Protocol

RFC 1157: The SNMP standard: http://www.cis.ohio-state.edu/htbin/rfc/rfc1157.html

Understanding SNMP MIBs
by David Perkins and Evan McGinnis,
Prentice-Hall, Inc., 1997

HP OpenView Network Node Manager

HP's OpenView site: http://www.openview.hp.com

HP's Network Node Manager site: http://www.openview.hp.com/nnm

CA Unicenter TNG

Computer Associates' main site: http://www.cai.com

Computer Associates' Unicenter TNG site: http://www.cai.com/unicenter

HP TopTools

HP's TopTools site: http://www.hp.com/toptools

HP SAN Manager DM

Info and datasheets: http://www.enterprisestorage.hp.com/san_value_device.html

SAN Manager DM main page:
http://www.hpsanmanager.com/ssmo2/ESBU_PROD_SAN_DM.htm

ATL WebAdmin

ATL's WebAdmin site: http://www.atlp.com/webadmin/webadmin30.html

StorageTek Horizon Framework Library Monitor

StorageTek's Horizon site:
http://www.storagetek.com/StorageTek/software/horizon/frameworkmonitor/

HP Web-Based Library Administrator

HP's Remote Management Card site: http://www.automatedbackup.com/fs_features.htm
Click on the Remote Management Card link

HP SureStore NetStorage 6000

HP's NetStorage site: http://www.hp.com/NAS/NetStorage6000/

HP ProCurve switch

HP's ProCurve site: http://www.hp.com/rnd/

Brocade Fibre Channel switches

Brocade main site: http://www.brocade.com/

Crossroads Fibre-to-SCSI Bridges

Crossroads main site: http://www.crossroads.com
Click on the Products link

HP XP256 disk array

HP's XP256 site:
http://www.enterprisestorage.hp.com/products/disk_array/sse_disk_array_mc256_pb.html

Overland Data WebTLC

Overland's Products page:
http://www.overlanddata.com/Overland.nsf/Pages/prd_frame.htm
Click on the links under WebTLC

HP Web JetAdmin

HP's Web JetAdmin info site: http://www.hp.com/net_printing/ppss/wja_info.html

DMTF: Distributed Management Task Force

DMTF main site: http://www.dmtf.org

CIM: Common Information Model

DMTF's CIM site: http://www.dmtf.org/spec/cims.html
SNIA's "CIM and DRM" site: http://www.snia.org/groups/CIMprototype.html

XML: eXtensible Markup Language

DMTF's WBEM/XML site: http://www.dmtf.org/spec/wbem.html

SNIA: Storage Networking Industry Association

SNIA main site: http://www.snia.org
SNIA SML working group site: http://www.snia.org/groups/sml/index.html

Sun's FMA/Jiro

Sun's Jiro site: http://www.jiro.com

JINI

Sun's Jini site: http://www.jini.com

Ancor

Ancor's site: http://www.ancor.com