



Cisco MDS 9000 Family Fabric Management

INTRODUCTION

One top item on the agendas of today's IT professionals is to reduce the costs associated with the deployment and scaling of critical enterprise applications. Factors contributing to these costs include the licensing, provisioning, and maintenance of the applications themselves. However, a major cost component also includes the application back-end infrastructure including the input/output (I/O) channel hardware, actual physical storage, and storage services including those used for business continuance.

The growing trend towards the adoption of storage area networks has helped reduce costs associated with growing and maintaining enterprise applications. Building an infrastructure that facilitates the sharing of physical storage and storage services allows enterprises to raise utilization levels of this existing infrastructure. This cost reduction is attributed to higher utilization rates related to storage and server consolidation around a storage network.

However, this optimization opportunity does not come without a series of challenges and associated costs. As storage network environment continue to grow, the need for comprehensive management services of the storage network environment becomes more apparent. Although many storage networking environments are usually built using the equipment and services from the disk subsystem company, this trend is beginning to change. For the enterprise to gain a negotiating advantage and not become locked in to one vendor, many enterprise customers look to multiple vendors to compete for their business. As such, storage networks consisting of many vendors' equipment are prevalent and are further complicating the management task. Even within one subsystem vendor's solution may exist four or five different original equipment manufacturer (OEM) vendors' equipment.

With this challenge of managing heterogeneous storage networking environment comes a host of new applications and services to fill the need. Some of these solutions are provided by the subsystem vendor or storage switch vendor and some are provided by 3rd party companies. Storage and storage network management solutions have become as numerous as the vendors' equipment they are trying to manage. While each management software solution offers its own set of features and benefits, most solutions can be categorized into three to four main categories. These categories are outlined in this paper with examples of the type of services provided by these categories of applications.

While Cisco is not positioning itself with products to compete with these comprehensive management application suites, there are several features and services offered with the Cisco MDS 9000 Family of products that offer assistance to such applications. Generally speaking, the features and services offered with the Cisco MDS 9000 Family of products for storage network management are targeted towards two end goals. The first goal is to provide a set of services that help a customer bring up and manage and initial deployment of Cisco MDS 9000 Family products. In some cases, the tools and services provided may be enough to manage the deployed Cisco MDS 9000 based network ongoing depending on the size of the deployment. However, the second goal of the features provided in the Cisco MDS 9000 product family is to offer interfaces to data about the storage network to higher-level applications that can use this information to consolidate and co-relate this information to other aspects of the application environment. This paper outlines these services and their application in achieving the goals stated above.

MANAGEMENT SOLUTIONS ARCHITECTURE

There are many facets to storage and storage network management in terms of the services that are provided and the scope of their application. To better understand where various services are applied, the following model in Figure 1 is provided to help classify such features. While the model presented in Figure 1 shows an overall comprehensive set of services for the storage environment, the features provided by the Cisco MDS 9000 Family do not necessarily apply to all categories. As the various management features of the Cisco MDS 9000 Family are outlined throughout this paper, a reference will be made to this model for clarification purposes.

Figure 1. Management Solutions Architecture

Data Bases	ERP	...	File Systems
Application Management			
Data Management			
Resource Management			
Fabric Management			
Device Management			
Physical Elements			

DEVICE MANAGEMENT

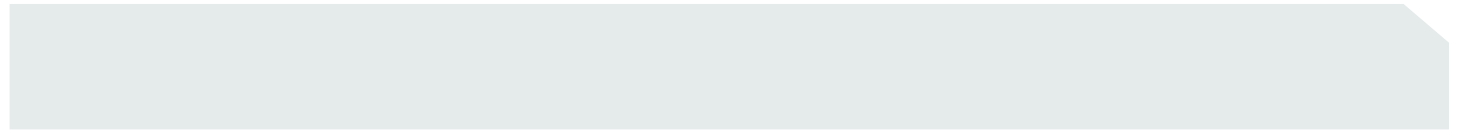
Device management consists of the most basic set of tools used to configure and manage a device within a system or a fabric. As any such system or fabric commonly consists of devices from multiple vendors, each vendor typically provides their own device manager.

A device manager is designed to perform tasks on one device at a time. The functions performed by a device manager generally revolve around configuration. Specifically such functions include initial device configuration, setting and monitoring thresholds, and managing device system images or firmware.

The Cisco MDS 9000 Series device manager and its functionality are presented later in this document.

FABRIC MANAGEMENT

Fabric management consists of a set of tools designed to take a more system-oriented view of a fabric and its devices. As a fabric can consist of numerous devices from multiple vendors, many such fabric management tools have evolved to manage 'heterogeneous fabrics'. Without any standard application programming interfaces (APIs) or information interfaces defined, a heterogeneous fabric represents a complex maze of devices and differing interfaces and APIs.



Fabric management applications commonly provide three general services, namely fabric discovery, fabric monitoring and reporting, and fabric configuration. Fabric discovery is the ability of the application to discover the devices of a fabric including their asset information, configuration, and statistical information using whatever APIs or interfaces that are available for the particular device. Commonly the fabric manager will draw the connected topology based on the discovered device configurations. Fabric monitoring and reporting involves using whatever information that can be gathered from the fabric devices and provide a correlated system-wide view of the fabric's health, configuration, and inventory. This view can be provided as a set of reports or as a real-time snapshot view. Fabric configuration can appear in two forms. To provide fabric configuration services, the fabric manager can simply call each individual device manager as needed to configure the actual devices of the fabric. Another more intelligent form of fabric configuration is for the fabric manager to configure multiple devices automatically based on user input or automated determination using the provided device APIs. In either case, the fabric manager can validate the intended configuration changes against known best practices or installed policies to provide an extra layer of control.

RESOURCE MANAGEMENT

Resource management consists of a set of tools designed to manage resources within a system or a fabric that are consumed by users or the devices themselves. Such resources may include fabric bandwidth, connected paths, disks, I/O operations per second (IOPS), CPU, and Memory. These resources could be physical in nature or a virtual representation as in the case of storage virtualization. Trending and capacity planning are activities that typically reside in a resource management system.

Resources can be managed in terms of their allocation, provisioning, monitoring, and reporting. Each of these aspects can be managed manually or automated through installed policy. For example, a policy may dictate when a particular database requires additional storage capacity. This same policy could invoke an automated process to allocate additional storage from a particular class of disk and make it ready for use by the application.

Access to such resources by users and system managers is also the responsibility of the resource management system. New users and their associated scope of resource control or use is managed by the resource management system.

DATA MANAGEMENT

Data management consists of a set of tools designed to ensure the availability of data within a system regardless of the semantics of the data. Data management generally relates to the integrity, availability, and performance in terms of access to the data itself.

Data management services commonly include attributes such as Redundant Array of Independent Disks (RAID) schemes, data replication practices, backup/recovery requirements, and data migration tasks. RAID schemes relate to the availability of data through disk mirroring or the performance of data through disk striping techniques. Data replication practices refer the task of maintaining real-time replicated copies of data over metropolitan distances or greater for business continuance reasons. Backup/restore requirements relate to the required frequency and method used for the backup of data and the followed procedure for data restore. Finally, data migration tasks refer to the requirement to move original or copies of data to different locations based on requirements of the user or the application.

APPLICATION MANAGEMENT

Application management consists of a set of tools designed to manage the overall system consisting of the devices, the fabric, the resources, and the data from the system's root, namely the application. The infrastructure consisting of devices, fabrics, resources, and data is created to support the deployment of applications. Application management ties all such components of the system back to the applications and helps to bring into context each of these deployed components.

The knowledge of how application organizes, accesses, and uses its data along with the context of the data can greatly help in making decisions on how storage should be provisioned, connected, organized, and managed. Application management tools provide this visibility to the system manager.

The above mentioned management components all contribute to the overall Storage and SAN management system. While each Cisco MDS 9000 Family management feature or service can easily be categorized according to the definitions above, Cisco provides tools for a subset of the categories mentioned above. There are many well-established vendors in the marketplace that have developed solid management suites that cover one or more of the categories above. Many enterprises today have implemented such management suites, or in some cases, have created their own tools to provide a component of the overall management system. Therefore, it is the intent of Cisco to provide a suite of tools used to deploy and manage a Cisco MDS 9000 Family switched network. However, it is equally important to Cisco to provide open interfaces and comprehensive APIs on the Cisco MDS 9000 Family products to storage and SAN management vendors to further enable their existing tools to manage a Cisco MDS 9000 based storage network.

The tools and APIs provided by Cisco for the Cisco MDS 9000 Family products are outlined later in this document.

THE CISCO MDS 9000 FAMILY MANAGEMENT SUITE

Along with the Cisco MDS 9000 Family of Multiprotocol storage switches comes a comprehensive set of management tools and features designed to aid in the provisioning and ongoing management of a Cisco MDS 9000 Family solution. The suite of tools provided can be categorized as device, fabric, and resource management tools.

Before providing a detailed outline of the management feature set within the Cisco MDS 9000 Family products, a brief overview of the product family and its management interfaces is provided.

The Cisco MDS 9000 Family is a series of multiprotocol storage switches designed to offer advanced scalability and resiliency for today's storage networks. The product line consists of three configurations of director-class switches, namely 6, 9, and 13 slots along with 2 configurations of 2-slot fabric switches and 2 configurations of 1-slot fabric switches. The multiprotocol nature relates to the Cisco MDS 9000 Family products' ability to support Fibre Channel, iSCSI (Ethernet), Fibre Channel over IP (FCIP) (Ethernet) and Fibre Connectivity (FICON) simultaneously. All of these platforms are equipped with several management or protocol interfaces to support access from various tools for management purposes. In addition, these interfaces serve as a method of the switches discovering their own environments in which they are situated.

CISCO MDS 9000 FAMILY MANAGEMENT INTERFACES AND PROTOCOLS

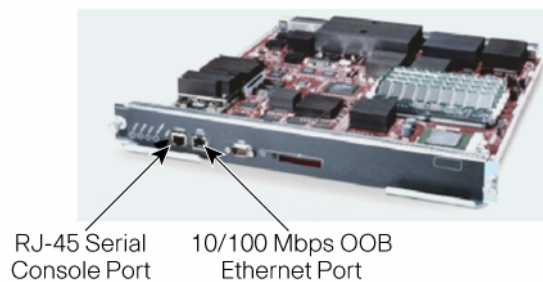
The Cisco MDS 9000 Family of switches offers three primary management interfaces through which a variety of management protocols are used.

The first primary management interface is an Out-of-Band (OOB) 10/100Mbps Ethernet connection on the Supervisor module. This OOB Ethernet connection can be connected to a management network to access the switch via IP/Ethernet. Each Supervisor module has its own 10/100Mbps connection; however the two Ethernet connections in a redundant Supervisor system operate in active/standby mode. The active Supervisor module also hosts the active OOB Ethernet connection. When a failover event occurs to the standby Supervisor module, the IP address and media access control (MAC) address of the active OOB Ethernet connection are moved to the standby OOB Ethernet connection thereby alleviating any need for management stations to relearn the location of the switch. This interface is shown in Figure 2.

The second primary management interface is a serial RJ-45 console connection on the Supervisor module. This console connection provides access to the Cisco MDS 9000 Family command-line interface (CLI) interface. From the CLI, many management and troubleshooting features can be enabled. This connection along with the console connections from other switches are commonly connected to a terminal server for ease of access. This interface is shown in Figure 2.

The third primary management interface is via an in-band connection over Fibre Channel to the Supervisor module itself. This in-band connection is unique in that it can support management protocols via Fibre Channel or via IP embedded within Fibre Channel. The capability to support IP management in-band over Fibre Channel stems from the fact that the Cisco MDS 9000 Family supports RFC2625-IP-over-Fibre Channel which allows IP to be transported between Fibre Channel devices via the Fibre Channel protocol. As some host bus adapters (HBAs) support IP drivers, this capability allows for a completely in-band management network. However, the in-band interface can also be used by the switch to discover its own environment including directly-connected and fabric-wide devices. This discovery capability is discussed later in the paper.

Figure 2. Management Interfaces on Cisco MDS 9000 Family Supervisor Module



There are several management protocols that are used to both in-band and OOB to gather or provide information to the management applications. Each protocol that is supported by the Cisco MDS 9000 Family of products is described below.

TELNET/SSH/FTP/SFTP/TFTP

These protocols are common networking protocols are mainly used to access the CLI of the Cisco MDS 9000 Family switches. Telnet provides a way to connect to the CLI remotely over TCP/IP and Secure Shell Protocol (SSH) provides a secure encrypted means of doing the same. Trivial File Transfer Protocol (TFTP) provides a no-frills way of transferring files to and from the Cisco MDS 9000 Family over UDP/IP and is commonly used in other Cisco products. File Transfer Protocol (FTP) and Secure File Transfer Protocol (SFTP) provide TCP-based methods of transferring files with SFTP providing a secure encrypted method of moving files.

SNMP V1, V2, AND V3

Simple Network Management Protocol (SNMP) provides a standardized method of passing control information and retrieving statistics and configuration from individual devices. SNMP is a UDP protocol that is used to transfer data. SNMP Management Information Bases (MIBs) are schemas or APIs that provide tree-like maps used to reference specific data to be placed or retrieved from a device. In the case of the Cisco MDS 9000 Family of switches, they support over 100 different MIBs, each referencing a specific category of information (eg. Zoning MIB, Interface MIB, iSCSI MIB).

SNMP V1 and V2 provided relatively unsecured transports for MIB information. Access is granted to SNMP information based on a shared password or 'community string' that must be used when requesting or placing information. Community strings could either grant Read-Only or Read-Write access to a particular device. As this password is shared, it can be easily spread to other users thereby opening up access to a wider audience.

SNMP V3 improved on V1 and V2 by adding security in terms of providing partitioned views and authenticated access to the data. In addition, the data transferred by SNMPv3 is encrypted for enhanced security. Users who wish to access an device via SNMPv3 are first assigned to an SNMPv3 role. This role is a grouping that is assigned a level of access to various SNMP MIBs (authenticated) including the ability to simply view or possibly change MIB values and may also be given access to only a subset of information provided by a MIB (authorized). As SNMPv3 provides a more secure method of accessing and managing MIB data, SNMPv3 is the default Read-Write SNMP access within the Cisco MDS 9000 Family of products.

SNIA STORAGE MANAGEMENT INITIATIVE (SMI-S)

The Storage Management Initiative (SMI) was created by the Storage Networking Industry Association (SNIA) to develop and standardize interoperable storage management technologies for storage, networking, and end-user communities. The SMI-Specification (SMI-S) is a vendor-neutral application programming interface (API) specification that can be built into networked storage devices and management applications. SMI-S is a way to develop and standardize interoperable storage management technologies. Based on the Common Information Model (CIM) and Web-Based Enterprise Management (WBEM) technologies from the Distributed Management Task Force (DMTF) and extended specifically for storage (as a SAN management interface).

The Cisco MDS 9000 Family switches embed the SMI-S provider on the switch, which is the preferred solution. The SMI-S provider supports the Service Location Protocol version 2 (SLPv2), Server Profile, Switch Profile, Fabric Profile which includes Zoning and Enhanced Zoning subprofiles. In addition the SMI-S provider has been extended to support additional Cisco MDS 9000 Family specific features not covered by the standard SMI-S profiles. These extensions include VSAN, TE Port, Port Channel, FCIP, iSCSI, Fabric and Zone Profile extensions.

The Cisco MDS 9000 Family SMI-S provider supports HTTPS which uses Secure Socket Layer (SSL) for enhanced security by encrypting communications between the SMI-S server and the SMI-S client.

HTTP

Hypertext Transfer Protocol (HTTP) is used very little within the Cisco MDS 9000 Family solution. Although there is a web interface on the Cisco MDS 9000 Family switches, it is simply used to provide download access to a switch-embedded java-based device and fabric management application which is then run locally on users' workstations. The HTTP connectivity is also utilized by clients to talk to the embedded SMI-S provider.

ANSI T11 FC-GS-4

FC-GS-4 is a Fibre Channel in-band management facility defined by the American National Standards Institute (ANSI) T11 working group. It provides what are referred to as generic services that may be utilized by any upper layer protocol making use of Fibre Channel as a transport. Primarily of interest here is the use of FC-GS-4 by the Fibre Channel Protocol (FCP) which is the most common upper layer protocol embedding the SCSI protocol within Fibre Channel. The generic services refer to a set of services that facilitate the transfer of status and configuration information between Fibre Channel devices in a solicited or unsolicited manner. *Name Service*, *Alias Service*, *Management Service* and *Time Service* are provided via FC-GS-4. In addition, FC-GS-3 services are fully supported.

Of particular interest are the *Management Service* and the *Name Service* which can both provide management information to connected devices such as the Cisco MDS 9000 Family switches. Within the Cisco MDS 9000 Family of switches, information retrieved from both of these sources is used to map the topology of the fabric as it is seen from a Cisco MDS 9000 Family switch. In addition, information from these sources provides a view into device manufacturer, model, and other inventory-related information. Naturally this information can only be gathered from devices that support the FC-GS-3 or FC-GS-4 ANSI standard. While not all devices support this standard, it is growing in popularity and most newer devices, including fabric switches and HBAs do support the standard.

The *Name Service* provides a distributed directory facility to Fibre Channel connected devices whereby devices can register their existence within the fabric and information about themselves. The information within the *Name Service* can then be polled by other devices to help determine the configuration of the fabric. This is by far the most common service of the set of FC-GS-4 generic services.

The *Management Service* provides access to discovered configuration information including inventory-related items as well as zoning configuration. Specifically, the sources of this information are the *Fabric Configuration Server* and the *Fabric Zone Server* within the *Management Service*. The *Fabric Configuration Server* provides access to fabric configuration information which can then be used to create a topology view of the fabric and its attributes. The information housed by the *Fabric Configuration Server* is actually maintained in a distributed database within each FC-GS-4 supporting node within the fabric. The *Fabric Zone Server* houses information about the zoning configuration within each fabric switch. In addition, zoning configuration can be changed also through the Fabric Zone Server. Therefore, the Fabric Zone Server represents a common interface that can be used to read and manipulate zoning configuration within a fabric across multiple vendors' fabric switches.

Within the Cisco MDS 9000 Family of switches, all FC-GS-4 generic services are supported. In addition, the information gathered from the *Name Server*, and *Fabric Configuration Server* is provided via SNMP MIBs and SMI-S provider to management applications that wish to retrieve and use this information. The Cisco *Fabric Manager* management tools embedded within the Cisco MDS 9000 Family switches also uses these MIBs for mapping topology. More information on the Cisco Fabric Manager tools is provided later in this document.

IPV6

The Cisco MDS SAN-OS supports IPv6 which extends the address space by quadrupling the number of network address bits from 32 bits (in IPv4) to 128 bits, which provides many more globally unique IP addresses. By being globally unique, IPv6 addresses enable global reachability and end-to-end security for networked devices, functionality that is crucial to the applications and services that are driving the demand for more addresses. The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while providing services such as end-to-end security, quality of service (QoS), and globally unique addresses.

ACCESS CONTROL LISTS

Access Control Lists (ACL) provide basic network security to all switches in the Cisco MDS 9000 Family. ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied.

ACLs can be applied to VSAN interfaces, the management interface, Gigabit Ethernet interfaces on IPS modules and MPS-14/2 modules, and Ethernet PortChannel interfaces. As the ACL filters are sequentially applied to the IP flows, only the first match determines the action taken. Subsequent matches are not considered. Configure the most important condition first. If no conditions match, the packet is dropped.

ACLs functionality is available for IPv4 and IPv6. Each switch in the Cisco MDS 9000 Family can have a maximum of 64 IPv4 or IPv6 ACLs and each ACL can have a maximum of 256 filters.

CISCO DISCOVERY PROTOCOL (CDP)

The Cisco Discovery Protocol is a layer-2 protocol that is embedded virtually in every Cisco platform, including the Cisco MDS 9000 Family. CDP allows for the periodic advertisement and discovery of a device's identity and attributes over a Layer-2 network. Currently CDP is not supported over Fibre Channel, however within the Cisco MDS 9000 Family, CDP is supported over the OOB Ethernet connection on the Supervisor module.

Using CDP, devices discover other CDP-enabled devices that are directly adjacent to them on a Layer-2 network. The type of information discovered includes the device name, model number, management IP address, capabilities, and other attributes. Each CDP-enabled device caches the discovered information and presents it in an SNMP MIB for retrieval and use by management applications.

CISCO MDS 9000 FAMILY DEVICE MANAGEMENT CLI-BASED TOOLS

The Cisco MDS 9000 Family of switches comes with a series of device management tools and facilities that can be used to configure and manage the switch along with the ability to troubleshoot and diagnose problems. These tools are configured or invoked from the CLI. They also are presented in GUI-form in the Cisco Fabric Manager which is discussed later in this paper. The following section outlines these CLI-based device management tools and how they can be used to help configure or diagnose problems.

Figure 3.



CISCO MDS 9000 FAMILY COMMAND-LINE-INTERFACE (CLI)

The Cisco MDS 9000 Family CLI is a robust interface providing extensive capability to configure and monitor the system. With a command structure similar to Cisco IOS® Software, the Cisco MDS 9000 Family offers a text-based, context-driven, hierarchical CLI that allows multiple users to simultaneously access the system.

Every facility within the Cisco MDS 9000 Family is configurable from the CLI. In addition, help menus are available by simply pressing '?' at any prompt or level to assist with commands or parameters of commands. An extensive 'show command' facility exists to display detailed statistics for every function within the switch.

Access to the CLI is granted through a roles-based permission system. Each user is assigned to a role or a grouping which is given a specific access level. This access level dictates which commands, or more specifically, which nodes of the CLI command parser tree the particular role has access to. Therefore, one could create a role which is called 'no_debug' that allows users assigned to the role to execute any command with the exception of any debug commands. The granularity of this permission system can be 2 levels deep within the parser tree. Therefore a role could even be defined called 'no_debug_fspf' which would allow a user to execute any system command, including debug commands with the exception of Fibre Channel Shortest Path First (FSPF) debug commands. Roles can be defined and assigned locally within a switch by using CLI commands. Role assignments can even be centralized in a RADIUS server for easier management. Two default roles are provided and up to 64 custom roles can be defined by the user. CLI activity can even be audited and accounted using RADIUS or Syslog facilities with timestamps and user identification.

SNMP AND RMON FACILITIES

The Cisco MDS 9000 Family of switches supports an extensive SNMP facility including traps. As previously mentioned, the Cisco MDS 9000 switches support SNMPv1, v2, and v3 for extended security. Each switch can be selectively configured for SNMP service.

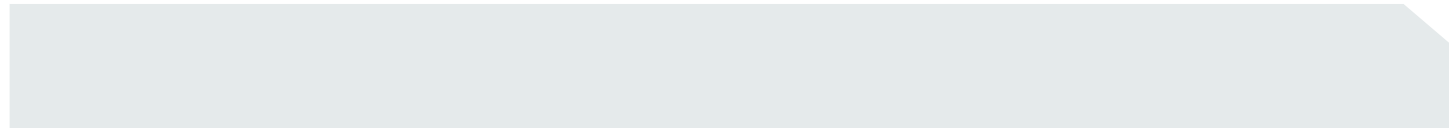
The Cisco MDS 9000 Family of switches supports a large list of MIBs, well over 100, which can be categorized as any of the following:

- **IETF Standards-based Entity MIBs (eg. RFC273—ENTITY-MIB)**—These MIBs are used to report information on the physical devices themselves in terms of physical attributes etc.
- **Cisco-Proprietary Entity MIBs (eg. CISCO-ENTITY-FRU-CONTROL-MIB)**—These MIBs are used to report additional physical device information about Cisco-only devices such as their configuration.
- **IETF IP Transport-oriented MIBs (eg. RFC2013—UDP-MIB)**—These MIBs are used to report transport-oriented statistics on such protocols as IP, TCP, and UDP. These transports are used in the management of the Cisco MDS 9000 Family through the OOB Ethernet interface on the Supervisor module.
- **Cisco-Proprietary Storage and Storage Network MIBs (eg. NAME-SERVER-MIB)**—These MIBs were written by Cisco to help expose information that is discovered within a fabric to management applications not connected to the fabric itself. In addition to exposing configuration details for features like zoning and Virtual SANs (VSANs) via MIBs, discovered information from sources like the FC-GS-3 Name Server can be pulled via a MIB. Additionally, MIBs are provided to configure/enable features within the Cisco MDS 9000 Family. There are over 20 new MIBs provided by Cisco for this information and configuration capability.
- **IETF IP Storage Working Group MIBs (eg. ISCSI-MIB)**—While many of these MIBs are still work-in-progress, Cisco is helping to draft such MIBs for protocols such as iSCSI and Fibre Channel-over-IP (FCIP) to be standardized within the IETF.
- **Miscellaneous MIBs (eg. SNMP-FRAMEWORK-MIB)**—There are several other MIBs provided in the Cisco MDS 9000 Family switches for tasks such as defining the SNMP framework or creating SNMP partitioned views.

Through the use of SNMPv3, roles can be assigned to SNMP capabilities. The SNMPv3 roles can be synchronized with the CLI-based roles and each user of the system can be assigned a role.

The Cisco MDS 9000 Family switches also support Remote Monitoring (RMON) for Fibre Channel. RMON provides a standard method to monitor the basic operations of network protocols providing connectivity between SNMP management stations and monitoring agents. RMON also provides a powerful alarm and event mechanism for setting thresholds and sending notifications based on changes in network behavior. For the Cisco MDS 9000 Family switches, RMON has been adapted to Fibre Channel to offer similar services as with Ethernet.

While RMON and RMON version 2 (RMON2) provide several groups of functionality, specifically the *AlarmGroup* and *EventGroup* have been implemented into the Cisco MDS 9000 switches. The *AlarmGroup* provides services to set alarms. Alarms can be set on one or multiple parameters within a device. For example, one could set an RMON alarm against the CPU utilization or crossbar utilization of the switch. Once a parameter is chosen to monitor, its sample type (*deltaValue* or *absoluteValue*), type of alarm (*risingAlarm*, *fallingAlarm*, etc.), and polling interval are specified for the alarm. Using the RMON alarm capability alleviates the user from having to continually poll a set of parameters to verify the existence of an alarm condition. The *EventGroup* allows us to configure events that are actions to be taken based on an alarm condition. The types of events that are supported include logging, SNMP traps, and log-and-trap. So, if a particular alarm condition were to be triggered, a message could be logged locally in an event log, and/or an SNMP trap could be sent to registered receivers with the details of the alarm. Here is a simple overview of the process:

- 
- Step 1.** Set an event in the eventTable by specifying the type of event, its description, and parameters required for the event (trap receivers, etc)
 - Step 2.** Create an alarm for each object that is to be monitored. Along with the alarm parameters is entered an index value to link the alarm to an event
 - Step 3.** In the case of SNMP trap events, ensure that the trap receivers are registered
 - Step 4.** Monitor the event log table and SNMP trap notifications for events

The RMON capability is very powerful considering the amount of status and information that can be monitored in a relatively automated way.

DEBUG FEATURE SET

One thing missing from today's fabric switch products is a set of tools to facilitate in-depth and detailed troubleshooting within a storage network. In most other products today one is only able to view various counters but there is no facility for providing active monitoring of control protocols and their associated activity.

The Cisco MDS 9000 Family of switches includes an extensive debugging feature set for actively troubleshooting a storage network. From the CLI, a user has the ability to enable various debugging modes for each switch feature and view a real-time updated activity log of the control protocol exchanges. Differing levels of detail are provided based on the user requirements. Each log entry is time-stamped and listed in chronological order using a user-friendly description of the event. Because the debug feature set is enabled from the CLI, its access can be limited through the CLI roles mechanism. Access to debug command can be partitioned on a per-role basis.

Figure 4 below shows a sample debug session invoked by a user. In this session, the user is debugging the FSPF protocol. First off, by using the '?' option, a user can see what options are available for debugging FSPF. As you can see in the output, a log entry is created for each entered command in addition to the actual debug output. The debug output shows a time-stamped account of the FSPF activity occurring between this switch and other adjacent switches.

Figure 4. Sample Output from Debug Session

```
switch> debug fspf ?
all                Configure debugging of FSPF
database           Configure debugging of FSPF database
error              Configure debugging of FSPF Errors
event              Configure debugging of FSPF Events
fc                 Enable dump of FC Packets and Headers
flood              Configure debugging of FSPF flooding events
ha                 Configure debugging of FSPF HA
mts                Enable dump of MTS Packets and Headers
retrans            Configure debugging of FSPF retransmit
route              Configure debugging of FSPF route computation
show_all           Show all debugging flags of FSPF
timer              Configure debugging of FSPF timer

switch> debug fspf all
Jul 23 07:55:18 sup-101 % LOG_ACCOUNTINGD-6-ACCOUNTING_MESSAGE:
update:/dev/pts/1_1027435623:tnosella:debug fspf all Successful
Jul 23 07:55:30 fspf: Updating LSR age for runtime data in PSS for vsan 1
Jul 23 07:55:35 fspf: Age timer expired for VSAN 1
Jul 23 07:55:35 fspf: FC2 IU Header: handle: 03AA1F93, usrhandle:00000000
Jul 23 07:55:35 fspf:  R_CTL:02      D_ID:FDFFFF00
Jul 23 07:55:35 fspf:  CS_CTL:00      S_ID:FDFFFF00
Jul 23 07:55:35 fspf:  TYPE:22      F_CTL:380000
Jul 23 07:55:35 fspf:  SEQID:AA DF_CTL:00 SEQCNT:0000
Jul 23 07:55:35 fspf:  OX_ID:0FCC RX_ID:1F93
Jul 23 07:55:35 fspf:  PARAM:00000000
Jul 23 07:55:35 fspf: 68 5D 09 08 28 00 00 00 00 00 00 00 20 BF 02 00
Jul 23 07:55:35 fspf: 67 6E 3D 3D 9D 67 07 00 20 00 00 00 00 00 00
Jul 23 07:55:35 fspf: 00 00 00 00 00 00 00 00
switch> no debug fspf all
switch> Jul 23 07:55:40 sup-101 % LOG_ACCOUNTINGD-6-ACCOUNTING_MESSAGE:
update:/dev/pts/1_1027435623:tnosella:undebg all no debug all
```

AAA

The authentication, authorization, and accounting (AAA) mechanism verifies the identity of, grants access to, and tracks the actions of users managing a switch. All Cisco MDS 9000 Family switches support.

Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) protocols to provide solutions using remote AAA servers.

Authentication refers to the authentication of users to access a specific device. Within the Cisco MDS 9000 Family switches, AAA can be used to centralize the user accounts for the switches. Therefore, when a user tries to log into the switch, the switch will validate the user via information gathered from the central AAA server.

Authorization refers to the scope of access that a user has once they have been authenticated. Within the Cisco MDS 9000 Family, assigned roles for users can be stored in a AAA server along with a list of actual devices that the user should have access to.

Once the user has been authenticated, then switch can then refer to the AAA server to determine the extent of access the user will have within the switch network. Accounting refers to the ability to log all commands entered by a user, the user's identity, and a timestamp of when the user entered the command. These command logs are sent to the AAA server and placed in a master log. This log can then be parsed to trace a user's activity and create usage reports or change reports. All exchanges between a AAA server and a AAA client can be encrypted using a shared key for added security. This security mechanism provides a central management capability for AAA servers.

Authentication, Authorization, and Accounting (AAA) are fully supported in the Cisco MDS 9000 Family of switches.

The following is an account of the type of information that would be reported, and in the case of the Cisco MDS 9000 Family, reported in the AAA output:

- **A user logs into the switch**—A AAA record is created with the user's identity and the time the user logged in.
- **The user enters configuration mode 'config terminal'**—This command is logged in AAA with the user's identity and a time-stamp added.
- **The user changes an FSPF parameter**—This command is logged in AAA with the user's identity and a time-stamp added.
- **The user logs out of the switch**—A AAA record is created with the user's identity and the time of user logged out.

AUTHENTICATION VIA FC-SP AND DHCHAP

Fibre Channel Security Protocol (FC-SP) capabilities provide switch-switch and host-switch authentication to overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol that provides authentication between Cisco MDS 9000 Family switches and other devices. DHCHAP consists of the CHAP protocol combined with the Diffie-Hellman exchange.

All switches in the Cisco MDS 9000 Family enable fabric-wide authentication from one switch to another switch, or from a switch to a host. These switch and host authentications are performed locally or remotely in each fabric. As storage islands are consolidated and migrated to enterprise-wide fabrics new security challenges arise. The approach of securing storage islands cannot always be guaranteed in enterprise-wide fabrics. For example, in a campus environment with geographically distributed switches someone could maliciously or accidentally interconnect incompatible switches, resulting in Inter-Switch Link (ISL) isolation and link disruption. This need for physical security is addressed by switches in the Cisco MDS 9000 Family.

DHCHAP is an authentication protocol that authenticates the devices connecting to a switch. Fibre Channel authentication allows only trusted devices to be added to a fabric, thus preventing unauthorized devices from accessing the switch.

DHCHAP is a mandatory password-based, key-exchange authentication protocol that supports both switch-to-switch and host-to-switch authentication. DHCHAP negotiates hash algorithms before performing authentication. It supports MD5 and SHA-1 algorithm-based authentication.

SYSLOG

Syslog is another valuable tool for troubleshooting tasks within the Cisco MDS 9000 Family. Using Syslog, a chronological log of system messages can be stored locally or sent to a central Syslog server. Syslog messages can also be sent to the console for immediate view by the user. These messages can vary in detail depending on the configuration entered by the user. Syslog messages are categorized into 7 severity levels spanning from *debug* to *critical* events. The user also has the ability to limit which severity levels are reported for specific services within the switch. As an example, a user may wish only to report *debug* events for the *FSPF* service but wish to record all severity level events for the *Zoning* service.

A unique feature within the Cisco MDS 9000 Family switches is the ability to send RADIUS accounting records to the Syslog service. The advantage of this feature is to be able to consolidate the messages for easier parsing and correlation. For example, if a user were to log into a switch and change an FSPF parameter, Syslog and RADIUS would yield very complimentary information to formulate a complete picture of the event. The following is an account of the type of information that would be reported, and in the case of the Cisco MDS 9000 Family, reported in the same Syslog output:

- **A user logs into the switch**—A AAA record is created with the user's identity and the time the user logged in and this record is sent also to the Syslog service.
- **The user enters configuration mode 'config terminal'**—The AAA record for this command is also sent to the Syslog service.
- **The user changes an FSPF parameter**—The AAA record for this command is also sent to the Syslog service. If any output is generated from the command such as an interface changing state or an error condition, this too is logged to the Syslog service.
- **The user logs out of the switch**—The AAA record for the log out event is also sent to the Syslog service.

So as you can see from the above example, by tying AAA and Syslog together, a detailed account can be recreated showing the user's activity (AAA) along with the response of the switch to command inputs (Syslog). In addition, by enabling debug mode for FSPF and sending that to the Syslog service, one now has a very detailed account of the reaction of the switch to the command inputs.

USER-SPACE FILE SYSTEM

Another valuable feature that aids in the management of the Cisco MDS 9000 Family switches is a 'workspace' file system that can be leveraged by users to store outputs of commands, scripts, or system images. The file system has a quota and can have its access controlled based on the assigned role of the user in the system. For example, a user may wish to take a copy of the output of a *show or debug* command. The user could simply direct the output of the command to a file within this shared file system. From there, the user could use TFTP, FTP, or SFTP to move the file off of the switch. Although users are restricted to a particular root directory, they can create subdirectories to better organize their files. All the standard file system management commands such as move, copy, rename, and delete are available. Using the available file system helps users gather statistics and protocol data to help in managing and troubleshooting a storage network.

SCRIPT-ABLE CONFIGURATION

The Cisco MDS 9000 Family offers a robust CLI with many commands each with many options. However, in most deployments, many of the commands that are entered to configure the switch are the same across multiple switches or have slight variations. To alleviate the need of constantly re-entering configuration details at each switch, the Cisco MDS 9000 Family supports the ability to use scripts to enter configuration details. From the CLI, a user can invoke a customized script that will enter configuration details into the switch.

The script facility can be used in two ways. The first primary use is to reduce the need from constantly entering the same configuration details across multiple switches. For the common sections of configuration, a user can execute a script that will automatically enter the appropriate configuration details such as SNMP contact information, RADIUS configuration, and Syslog configuration. After this has been completed, a user simply has to enter the unique pieces of the configuration either through the CLI or through the Cisco Fabric Manager tool.

However, in the day of automated provisioning, a far more powerful solution can be achieved. Automated provisioning systems can leverage the script-able nature of the switch and automatically generate scripts to configure the entire switch based on some inputted parameters or perhaps a predetermined topology. Using the script facility, an automated system could be devised to take host connectivity requirements and generate a topology, naming, configuration and all associated configuration files for the required switches. The generated configuration files could then automatically be loaded into the appropriate switches using the script facility. Using the script facility such as this helps eliminate user errors often introduced into device configurations.

FC PING AND FC TRACEROUTE

Arguably the two most used tools within the IP networking world are two simple programs, namely *Ping* and *Traceroute*. For those readers who are not familiar with these tools, the *Ping* tool provides the ability to generate a series of echo packets to a destination across an IP routed network. When these echo packets arrive at the destination, they are re-routed and sent back to the source. Using *Ping*, users can verify connectivity and latency to a particular destination across an IP routed network. *Traceroute* on the other hand operates in a similar fashion; however *Traceroute* can also determine the specific path that a frame takes to its destination on a hop-by-hop basis.

These tools have been migrated to Fibre Channel within the Cisco MDS 9000 Family switches. *FC Ping* and *FC Traceroute* are the Fibre Channel equivalents to their IP counterparts. *FC Ping* allows a user to 'ping' a Fibre Channel *N_Port* or end device. By specifying the *FC_ID* or Fibre Channel address, a user can send a series of frames to the target *N_Port*. Once these frames reach the outgoing *F_Port*, they are looped back to the source and a time-stamp is taken. *FC Ping* helps a user verify the connectivity and latency to an end *N_Port*.

FC Traceroute is slightly different than the IP equivalent in that the outbound and return paths are both recorded as they may differ. The result of an *FC Traceroute* command is two path descriptors that identify the path taken on a hop-by-hop basis including a timestamp at each hop in both directions.

Both *FC Ping* and *FC Traceroute* are powerful tools in verifying connectivity and zone permissions within a large connected fabric.

SCSI TARGET DISCOVERY

The Fibre Channel name service is a distributed service in which all connected devices participate. As new devices attaches to the fabric, they register themselves with the name service which is then distributed amongst all fabric switches. This information can then be used to help determine the identity and topology of nodes connected to the fabric. Although the name service can provide such information, it is at a Fibre Channel level only. As for Fibre Channel-connected devices such as SCSI targets, there is no additional information offered by the name server.

However, within the Cisco MDS 9000 Family of switches, a unique feature has been added to provide added insight into connected SCSI targets. The *SCSI Target Discovery* feature allows the switch to briefly log into connected SCSI target devices and issue a series of SCSI inquiry commands to help discover additional information. The additional information that is queried includes logical unit number (LUN) details including the number of LUNs, the LUN IDs, and the sizes of the LUNs. This information is then compiled and made available to the user via various methods. The collected information is provided directly through CLI commands, through the Cisco Fabric Manager, and also via an embedded SNMP MIB which allows the information to be easily retrieved by an upstream management application. Using the *SCSI Target Discovery* feature, a user can have a much more detailed view of the fabric and its connected SCSI devices.

FULL FC-GS-4 SUPPORT

As mentioned previously, FC-GS-4 is a Fibre Channel in-band management facility defined by the ANSI T11 working group. It provides what are referred to as generic services, particularly for use by the Fibre Channel Protocol (FCP). The generic services refer to a set of services that facilitate the transfer of status and configuration information between Fibre Channel devices in a solicited or unsolicited manner.

Within the Cisco MDS 9000 Family of switches, all generic services of FC-GS-4 are supported. The ability to support all services allows for the discovery and understanding of other attached devices that support the FC-GS-4 standard such as other fabric switches or HBAs. It also allows other management software packages that understand and use FC-GS-4 to discover and understand the Cisco MDS 9000 Family switches.

The added bonus with the Cisco MDS 9000 Family switches is the ability for non-FC-GS-4-aware systems to still retrieve the gathered information via SNMP MIBs. Embedded within the Cisco MDS 9000 Family switches is the support for a series of custom SNMP MIBs that expose all details discovered via FC-GS-4 such as the list of registered fabric devices and the attributes of connected fabric switches. In addition, information can also be provided that gives a view into device manufacturer, model, and other inventory-related details. Naturally this information can only be gathered

from devices that support the FC-GS-4 ANSI standard. While not all devices support this standard, it is growing in popularity and most newer devices including fabric switches and HBAs do support the standard.

So, whether using a 3rd party application, or writing custom in-house applications to manage the storage network, the detailed device and topology information that can be gathered via these FC-GS-4 related MIBs allows the user to accurately create and audit a fabric topology and its registrants.

FIBRE CHANNEL SPAN, RSPAN

When there is a problem in a storage network that cannot be solved by a configuration change, usually there is a requirement to take a look at the protocol level. While debug commands in the Cisco MDS 9000 Family switches can help look at the control traffic between an end node and a switch, many times a deeper look is required to focus in on all traffic originating or destined to a particular end node such as a host or a disk. In this case, one typically would resort to using an analyzer of sorts to capture protocol traces for deeper analysis. In using a protocol analyzer, one must insert the analyzer in-line with the device under analysis thereby requiring a disruption in I/O from the device. This problem gets worse if the point of analysis is on an Inter-Switch Link (ISL) link between two switches. In this case, the disruption may be widespread depending on what devices are downstream from the severed ISL link.

Cisco has adapted a very popular feature from its Cisco Catalyst® Family of Ethernet switches to the Fibre Channel world, namely *SPAN*. Simply put, the Switched Port Analyzer (SPAN) feature allows a user to take a copy of all traffic and direct it to another port within the switch. This copy is non-disruptive to any connected devices and is facilitated in hardware thereby alleviating any unnecessary CPU load. Therefore, using the *SPAN* feature, a user could connect a Fibre Channel analyzer such as a Finisar analyzer to an unused port on the switch and then simply *SPAN* a copy of the traffic from a port under analysis to the analyzer in a non-disruptive fashion.

The *SPAN* feature is highly customizable as well. A user can create up to 16 independent *SPAN* sessions within the switch. Each session can have up to four unique sources and one destination port. In addition, the user has the capability to filter the *SPAN* source based on received-only, transmitted-only, or bi-directional traffic. A user can even *SPAN* traffic from a particular Virtual SAN (VSAN) only*.

Using the *SPAN* feature, detailed troubleshooting can be conducted on a particular device without any disruption. In addition, a user may want to take a sample of traffic from a particular application host for proactive monitoring and analysis, a process that can easily be accomplished with the *SPAN* feature.

The Remote SPAN (RSPAN) feature enables ability to remotely monitor traffic for one or more SPAN sources distributed in one or more source switches in a Fibre Channel fabric. The SPAN destination port is used for remote monitoring in a destination switch. A destination switch is usually different from the source switch(es) but is attached to the same Fibre Channel fabric. One can replicate and monitor traffic in any remote Cisco MDS 9000 Family switch or director, just as you would monitor traffic in a Cisco MDS source switch. The RSPAN feature is nonintrusive and does not affect network traffic switching for those SPAN source ports.

* A Virtual SAN (VSAN) is a feature within the Cisco MDS 9000 Family switches that allows for the virtual connected fabrics to be created and overlaid on one physical infrastructure through a tagging and trunking procedure. More info can be found on this feature in the Cisco MDS 9000 Family product documentation.

CISCO FABRIC MANAGER (CFM)

One of the most powerful tools in the Cisco MDS 9000 Family for management is the Cisco Fabric Manager. This tool actually consists of two separate tools, namely a device manager for the switch and a fabric manager. Both tools that comprise the Cisco Fabric Manager are embedded in the switch itself. These tools are designed to run using the Sun Microsystems Java Web Start environment. Using Web Start, all the functionality of Java can be leveraged without the incurred delay associated with plain Java applets. To use the Cisco Fabric Manager, one simply has to point a web browser to the management IP address of any Cisco MDS 9000 Family switch. The resultant web page gives simple instructions on how to download the Web Start environment, a step that only has to be done initially. Once Web Start has been installed, the user simply invokes the Cisco Fabric Manager from the previous web page and the application will dynamically be downloaded to the local machine, cached, and started. For repeated use, a user only has to click on the Cisco Fabric Manager icon that is installed on the local machine.

SNMP PROXY SERVICES

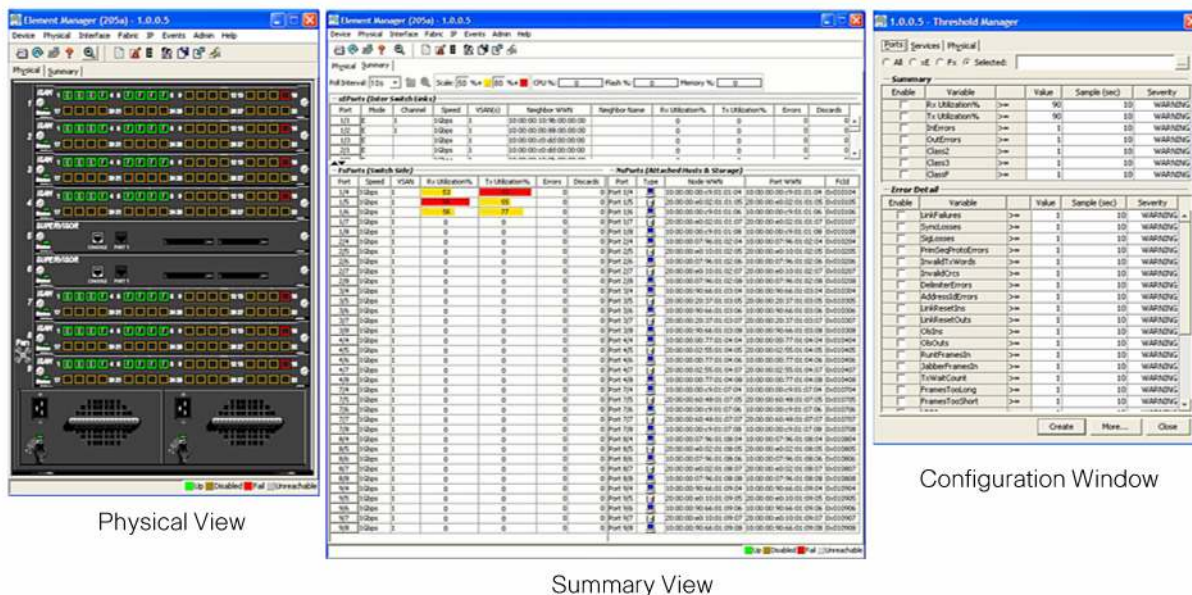
The Fabric Manager Client and Device Manager use SNMP to communicate with the Fabric Manager Server. In typical configurations, the Fabric Manager Server may be installed behind a firewall. The SNMP proxy service available in Cisco Fabric Manager provides a TCP-based transport proxy for these SNMP requests. The SNMP proxy service allows blocks all UDP traffic at the firewall and enables the Fabric Manager Client to communicate over a configured TCP port. Cisco Fabric Manager uses port 8080 for SNMP proxy services.

CISCO DEVICE MANAGER

One component of the Cisco Fabric Manager is the embedded device manager. The device manager is designed to allow a user to use a GUI-driven tool for configuration of an Cisco MDS 9000 Family switch. All configuration capabilities of the switch are represented through the device manager GUI including such items as roles definitions and RMON alarm and event configuration. The device manager tool has three primary components, namely the physical view, the summary view, and statistic and configuration windows. In the physical view, the actual switch is depicted along with graphical icons representing the states of the actual switching modules and ports. The summary view shows a real-time updating chart listing all the ports within the switch and a quick view of their statistics and configuration. The statistics and configuration windows are pop-ups used to configure and monitor specific details of the switch. Figure 5 shows an example of the three components of the device manager.

The device manager is also equipped with features that help the user track statistics and events. One such tool is a 'Save' button that allows the user to quickly save the text output of a statistics window to a local text file. Additionally, a graphing tool allows the user to create a graph based on any statistics window output which will update itself at the predefined polling interval. This graph can also be saved to the local machine.

Figure 5. Three Cisco Device Manager Views



Despite the powerful set of features, the device manager is designed to be a very easy tool to use. It is targeted towards those users that are not familiar with the Cisco MDS 9000 Family CLI or prefer to use GUI interfaces. The device manager can aid in deploying new switches or making quick changes to existing switches. For smaller storage networks of 5-10 switches, some users may prefer to use CFM as their sole configuration and management tool. For larger fabrics, users may prefer to use 3rd party tools that integrate more capability in terms of reporting and 3rd party device configuration.

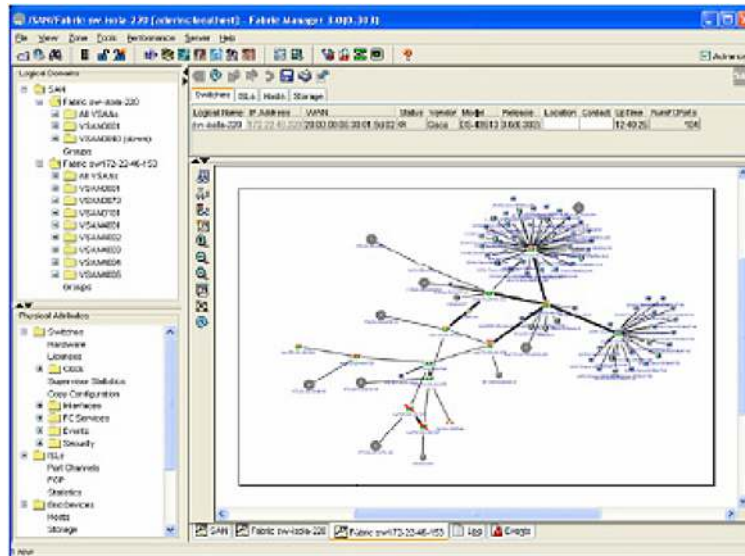
The Cisco Fabric Manager suite uses SNMP to communicate with the Cisco MDS 9000 Family switches. Although the user has the ability to use SNMPv1,v2, or v3 for this communication, SNMPv3 offers additional security and support of roles. By using SNMPv3 as the transport protocol, users will be restricted to certain features of CFM based on their SNMPv3 role assignment. Therefore by creating SNMPv3 and CLI roles for users, they can be given access to the same features whether they use the CLI or CFM.

CFM FABRIC MANAGEMENT

Another major component of the Cisco Fabric Management suite is the fabric management itself. Installed as an additional Web Start application, the fabric manager provides the capability to manage the fabric as a collection or network of devices. The fabric manager application is built upon a topology representation of the fabric. Once the fabric manager is invoked, a topology discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch including *NameServer* registrations and FC-GS-4 *Fabric Configuration Server* information, the fabric manager can recreate a fabric topology and represent it for the user in a customizable map. Because of the source of this information, any 3rd party devices such as other fabric switches that support the FC-GS, FC-GS-3 and FC-GS-4 standards shall be discovered and mapped as part of the topology. Vendor organizational unique identifier (OUI) values are also translated to derive the manufacturer of any 3rd party devices such as QLogic, EMC, or JNI. An added bonus is the ability to map SCSI-level target information based on information polled from the Cisco MDS 9000 Family switches. The Cisco MDS 9000 switch has the ability to log into targets that are discovered as connected to it and issue SCSI inquiry commands to determine LUN configurations. This information is then retrieved by the fabric manager and included in the presented inventory.

The fabric manager consists of three major components including the topology window, the inventory window, and the tools window. The topology window displays the discovered topology in a form that can be customized and easily navigated by the user. The inventory window displays a tree-like structure of all devices, both physical such as fabric switches, and virtual such as zones or VSANs. This inventory can then be used by the tools to perform configuration tasks. Finally, the tools window displays a series of fabric-oriented tools that are used to configure, monitor, or troubleshoot a fabric of Cisco MDS 9000 Family switches. Figure 6 shows these three windows.

Figure 6. Fabric Management Views with Cisco Fabric Manager



The tools provided within the fabric manager are fabric-wide tools with the ability to manage and troubleshoot multiple devices. The fabric manager has wizards to configure Virtual SAN (VSAN), Dynamic Port VSAN Membership (DPVM), Zones, Inter VSAN Routing (IVR), Port Channel, FCIP, iSCSI, QOS, ACL, Software Installation, and License Installation. In addition to the configuration wizards, the fabric manager provides troubleshooting tools such as a fabric configuration auditor, a Zone-merge analysis tool, a Fabric path verification tool, end-to-end connectivity verification tool and Switch Health Analysis. In addition, the fabric manager tool allows for the ability to apply configuration changes to multiple switches simultaneously. For example, if a user wished to change the R_A_TOV value on all fabric switches, the user could simply select all fabrics and make the change only once. The fabric manager would then propagate that change to all selected fabrics. The user can also invoke the device manager and/or a Telnet session to the switch from the fabric manager topology map.

The fabric manager provides a very complementary tool to the device manager within the Cisco Fabric Manager suite. The CFM suite helps users manage a fabric comprising multiple Cisco MDS 9000 Family switches. These tools provide a very fast interface to making quick changes to the Cisco MDS 9000 based fabric as necessary.

CISCO FABRIC SERVICES

Many features in the Cisco MDS switches require configuration synchronization in all switches in the fabric. Maintaining configuration synchronization across a fabric is important to maintain fabric consistency. In the absence of a common infrastructure, such synchronization is achieved through manual configuration at each switch in the fabric. This process is tedious and error prone. Cisco Fabric Services (CFS) provides a common infrastructure for automatic configuration synchronization in the fabric. It provides the transport function as well as a rich set of common services to the applications.

The CFS functionality is independent of the lower layer transport. Currently, in Cisco MDS switches, the CFS protocol layer resides on top of the FC2 layer and is peer-to-peer with no client-server relationship. CFS uses the FC2 transport services to send information to other switches. CFS uses a proprietary SW_ILS (0x77434653) protocol for all CFS packets. CFS packets are sent to or from the switch domain controller addresses. CFS can also use IP to send information to other switches. Applications that use CFS are completely unaware of the lower layer transport.

CFS supports two distribution modes to support different application requirements: coordinated and uncoordinated distributions. Both modes are mutually exclusive. Only one mode is allowed at any given time. Uncoordinated distributions are used to distribute information that is not expected to conflict with that from a peer. An example is local device registrations such as iSNS. Parallel uncoordinated distributions are allowed for an application. Coordinated distributions can have only one application distribution at a given time. CFS uses locks to enforce this. A coordinated distribution is not allowed to start if locks are captured by other application in the fabric. An example is port security configuration.

CISCO FABRIC MANAGER SERVER (FMS)

Cisco Fabric Manager Server (FMS) is a platform for advanced MDS monitoring, troubleshooting, and configuration capabilities. No additional software is required. The server capabilities are an integral part of the Cisco Fabric Manager software.

We recommend that FMS be installed on a dedicated computer to provide centralized MDS management services and performance monitoring. SNMP operations are used to efficiently collect fabric information. The FMS, including the server components requires about 20 MB of hard disk space on your workstation. Cisco Fabric Manager Server runs on Windows 2000, 2003, XP, Solaris 8.x or later and Red Hat Linux. The FMS can monitor up to 16 Fibre Channel SAN fabrics. By default 16 clients can connect to a single Cisco Fabric Manager Server concurrently.

Cisco Fabric Manager Server has the following features:

- **Multiple Fabric Management**—Fabric Manager Server monitors multiple physical fabrics under the same user interface. This facilitates managing redundant fabrics. FMS maintains up-to-date discovery information on all configured fabrics so device status and interconnections are immediately available when an Fabric Manager client is connected to the fabric.
- **Continuous Health Monitoring**—Cisco MDS switch(es) health is monitored continuously. Even when no client is running, FMS continues to collect the events and presents the events to clients that connect in future.
- **Roaming User Profiles**—FMS uses the roaming user profile feature to store your preferences and topology map layouts on the server, so that user interface will be consistent regardless of computer used to manage the storage networks.

CISCO PERFORMANCE MANAGER

Performance Manager gathers network device statistics historically and provides this information graphically using a web browser. It presents recent statistics in detail and older statistics in summary.

Performance Manager also integrates with tools such as Cisco Traffic Analyzer which will be discussed later.

The Performance Manager has three operational stages—Definition, Collection and Presentation:

- **Definition**—The Flow Wizard, one can select flows to be monitored and the Collection Wizard creates a collection configuration file.
- **Collection**—Reads the configuration file and collects the desired information via SNMP.
- **Presentation**—Generates web pages to present the collected data.

Performance Manager can collect statistics for ISLs, hosts, storage devices, and configured flows. Flows are defined based on a host-to-storage (or storage-to-host) link. Performance Manager gathers statistics from across the fabric based on collection configuration files. These files determine which SAN devices and SAN links Performance Manager gathers statistics for. Based on this configuration, Performance Manager communicates with the appropriate devices (switches, hosts, or storage devices) and collects the appropriate information at five-minute intervals.

Performance Manager uses a round-robin database to hold the statistical data collected from the fabric. This data is stored based on the configured parameters in the collection configuration file. At each polling interval, Performance Manager gathers the relevant statistics and stores them in the round-robin database. This database is a fixed size and will not grow beyond its preset limits.

Performance Manager creates a series of archived data to hold summarized information present in the real-time round-robin database. This archived data is used to generate daily, weekly, monthly, and yearly consolidated reports. In this way, Performance Manager maintains significant historical data without the cost of an ever-increasing database size.

A unique feature of Performance Manager is its ability to interpolate data when statistical polling results are missing or delayed. Other performance tools may store the missing data point as zero, but this can distort historical trending. Performance Manager interpolates the missing data point by comparing the data point that preceded the missing data and the data point stored in the polling interval after the missing data. This maintains the continuity of the performance information.

Performance Thresholds

The Performance Manager Configuration Wizard has ability to define up two thresholds that will trigger events when the monitored traffic exceeds the percent utilization configured.

Absolute value thresholds apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are compared to the percent utilization configured for the threshold type. If the statistics exceed either configured threshold, an event is shown on the Fabric Manager web client Events tab.

Baseline thresholds create a threshold that adapts to the typical traffic pattern for each link for the same time window each day, week, or every two weeks. Baseline thresholds are set as a percent of the average (110% to 500%), where 100% equals the calculated weighted average.

CISCO FABRIC MANAGER WEB SERVICES

Fabric Manager Web Services provides a web client to view MDS switch events, performance manager reports, inventory, and perform minor administrative tasks. Fabric Manager Web Services need to be installed on the same workstation as the Fabric Manager Server. By default Fabric Manager Web Services uses TCP port 80. If security is a concern, Fabric Manager Web Services can also be configured to run over HTTPS (TCP port 443) which uses SSL.

The web client provides the following reports:

- Events by Fabric, Switches, ISLs, Hosts or Storage
- Syslog messages
- Performance Reports by Summary, End Devices, ISLs, Flows, Traffic Analyzer, Prediction

Performance Prediction

To plan storage network changes, it is necessary to determine when configuration changes (such as re-zoning) may be needed to meet growing performance demands. Fabric Manager Server provides a performance prediction report to anticipate storage network connections that are over utilized. The prediction is based on the period of time in the past to predict the future performance along with acceptable threshold values and time into the future.

CISCO TRAFFIC ANALYZER

Cisco Traffic Analyzer is based on network top (ntop) software, a public domain software enhanced to support Fibre Channel and SCSI. Performance Manager works in conjunction with Cisco Traffic Analyzer to monitor and manage the fabric traffic. Cisco Traffic Analyzer with Performance Manager requires the following components:

- A configured Fibre Channel Switched Port Analyzer (SPAN) destination (SD) port to forward Fibre Channel traffic.
- A Port Analyzer Adapter 2 (PAA-2) to convert the Fibre Channel traffic to Ethernet traffic.
- Cisco Traffic Analyzer software to analyze the traffic from the PAA-2.

Performance Manager collects Fibre Channel level performance statistics using SNMP to access counters on Cisco MDS 9000 Family switches. To view detailed SCSI I/O statistics, one needs to look at the data on an SD port with the help of Cisco Traffic Analyzer, which uses the Cisco Port Analyzer Adapter 2 (PAA-2). Cisco Traffic Analyzer provides real-time analysis of SPAN traffic or analysis of captured traffic through a Web browser user interface. Traffic encapsulated by one or more Port Analyzer Adapter 2 products can be analyzed concurrently with a single workstation running Cisco Traffic Analyzer.

Cisco Traffic Analyzer monitors Round-trip response times, SCSI I/Os per second, SCSI read or traffic throughput and frame counts, SCSI session status, and management task information. Additional statistics like Fibre Channel frame sizes and network management protocols are available too.

CISCO FABRIC ANALYZER

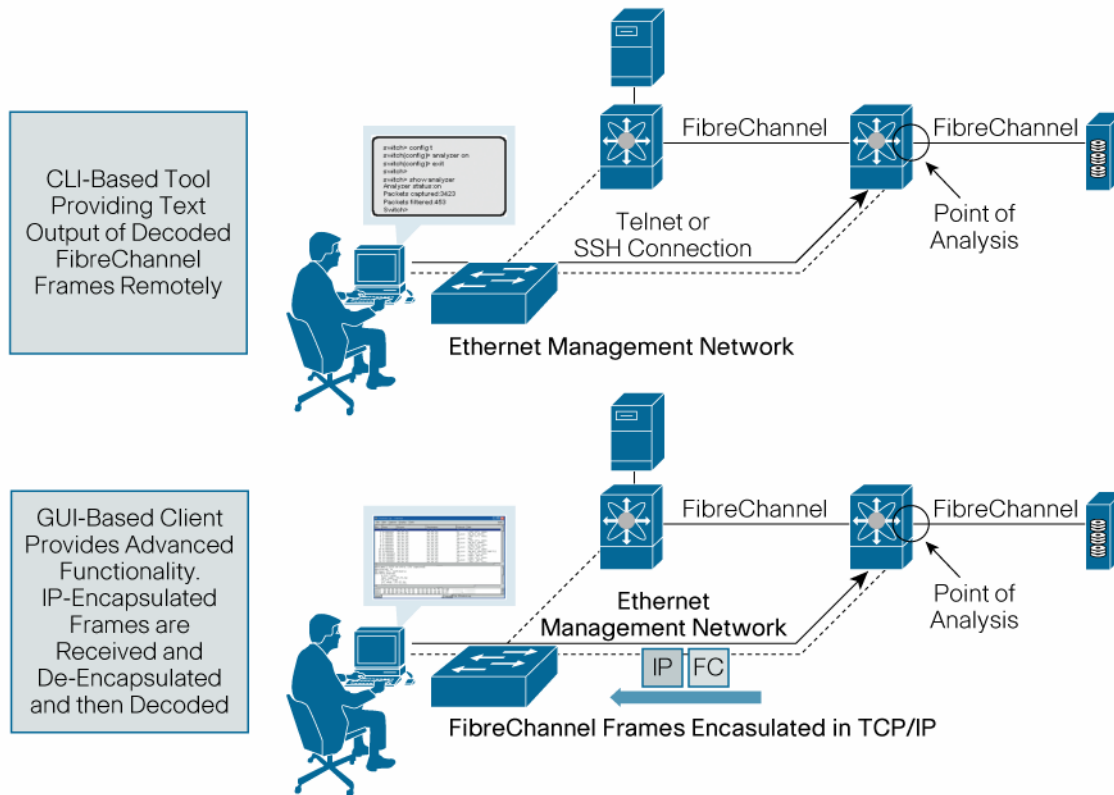
The ultimate tool for troubleshooting any sort of network protocol problem has always been the protocol analyzer. These devices have the ability to promiscuously capture network traffic and completely decode the captured frames down to the protocol level. Using the analyzer, users can conduct very detailed analysis by taking a sample of a storage network transaction and completely map the transaction from a frame-by-frame basis complete with very accurate timestamps. This information allows the user to pinpoint a problem with a high degree of accuracy thereby reducing the resolution time. However, the downside of protocol analyzers is that they are expensive, and they must be installed local to the point of analysis within the network.

Cisco has brought protocol analysis within a storage network to a new level of capability. Using the *Cisco Fabric Analyzer*, users can capture Fibre Channel control traffic from a switch and decode it without having to disrupt any connectivity, and without having to be local to the point of analysis.

The *Cisco Fabric Analyzer* comprises three main components. The first component is an agent embedded in the Cisco MDS 9000 Family switches that can be selectively enabled to promiscuously capture designated control traffic. The second component is a text-based interface to the control and decoded output of the analyzer. The third component is a GUI-based client package that can be installed on a user's workstation and provide a more full-function interface to the decoded data. Figure 7 outlines the three components of the *Cisco Fabric Analyzer* system and the two supported configurations, namely the CLI-based facility and the GUI-based client software.

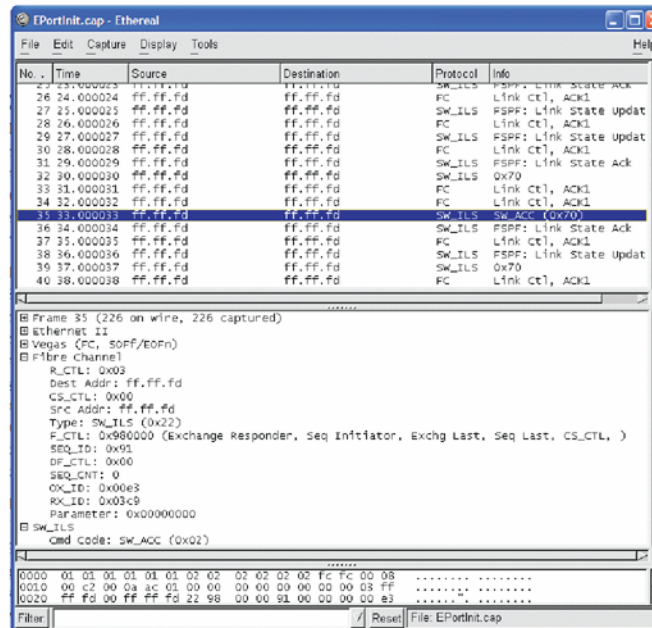
The text-based interface to the *Cisco Fabric Analyzer* is a CLI-based facility to control the analyzer and output the decoded results. Using the CLI-based interface, a user can remotely access an Cisco MDS 9000 Family switch via a secure method such as Secure Shell (SSH) and capture and decode Fibre Channel control traffic via the text-based CLI. This capability offers a convenient method for conducting remote detailed troubleshooting. In addition, since the tool is CLI-based, it is also covered under the roles-based policies defined in the switch which can limit access to this tool as desired.

Figure 7. Cisco Fabric Analyzer CLI-based and GUI Client Configurations



The GUI-based interface implementation is based upon a supplied software package that can be installed on a user's workstation. Through the GUI, the user has access to a more user-friendly and customizable interface to the captured and decoded Fibre Channel traffic. The GUI interface allows users to easily sort, filter, crop, and save traces to their local workstation. Figure 8 shows a screenshot from the *Cisco Fabric Analyzer* GUI. Although this client package is designed to allow remote access to captured and decoded Fibre Channel control traffic, it does not require a Fibre Channel connection in the remote workstation itself. The most powerful capability of the *Cisco Fabric Analyzer* package is the ability to capture and decode Fibre Channel traffic remotely, however over Ethernet! The *Cisco Fabric Analyzer* supports a revolutionary capability in Fibre Channel protocol analysis to promiscuously capture Fibre Channel traffic, encapsulate it in TCP/IP, ship it externally to a remote client connected via Ethernet, de-encapsulate, and fully decode the resultant Fibre Channel frames. This capability provides extreme flexibility in troubleshooting problems in remote locations. No longer does a user have to pick up a heavy protocol analyzer, travel to the point of analysis, insert the analyzer in-line, and capture traffic. All of these functions can be conducted remotely in a non-disruptive manner. The *Cisco Fabric Analyzer* completes the trio of troubleshooting features within the Cisco MDS 9000 Family of switches. CLI-based debug capability, along with Fibre Channel SPAN, and the *Cisco Fabric Analyzer* offer the system administrator a powerful and flexible toolset for troubleshooting storage network problems accurately and efficiently.

Figure 8. Cisco Fabric Analyzer Screenshot



CISCOWORKS RESOURCE MANAGEMENT ESSENTIALS

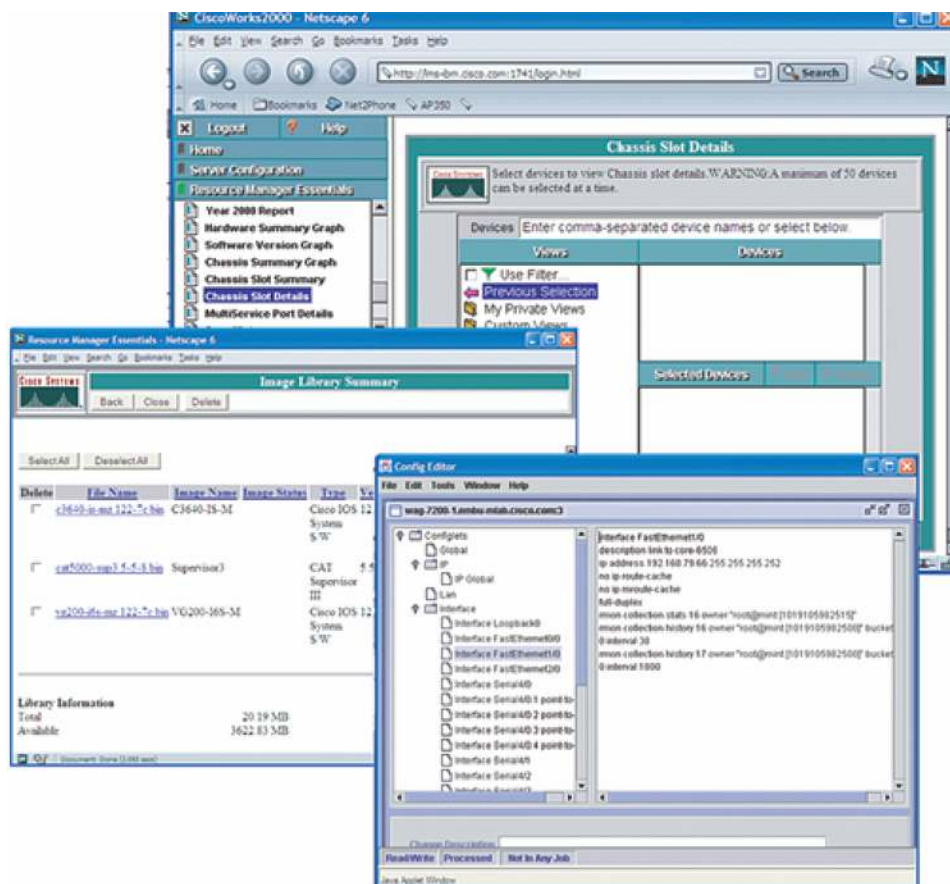
CiscoWorks Resource Manager Essentials (RME) is an application within the CiscoWorks umbrella of management applications that provides comprehensive resource management capabilities for a Cisco Powered Network (CPN). With the introduction of the Cisco MDS 9000 Family of switches, CiscoWorks RME has been extended to provide resource management services to a Cisco MDS 9000 Family storage network.

CiscoWorks RME comprises a set of resource management services. The following list outlines the services provided by CiscoWorks RME for the Cisco MDS 9000 Family of switches.

- **Inventory Manager**—provides a facility to gather and audit a detailed hardware and software inventory of all Cisco MDS 9000 Family devices deployed in the storage network. A reporting facility is included to generate inventory reports
- **Configuration Manager**—maintain an active repository of device configuration files for devices that are managed. It provides facility to upload and download configuration files to/from devices and a facility to log a record in the Change Audit log database when a new version of the configuration file is archived. Standard reports can be generated for configuration management inventory and activity.
- **Configuration Editor**—provides a powerful web-based editor that allows multiple configuration files to be checked out of the configuration archive, be updated or changed, and then either saved locally or downloaded to the device.
- **Net Show**—is a simplified web-based show command interface, allowing show commands to be run against multiple switches or routers to enhance and simplify network troubleshooting.
- **Software Image Manager**—a tool to greatly simplify the version management and routine deployment of software updates to Cisco devices through wizard-assisted planning, scheduling, downloading, and monitoring of software updates
- **Syslog Analyzer**—a tool that filters Syslog messages logged by Cisco devices and display explanations of probable causes and recommended actions. This tool also helps facilitate manual parsing of Syslog files for reporting purposes.

By including support for the Cisco MDS 9000 Family of switches into CiscoWorks RME, customers now have a system that can manage hardware, software, and configuration inventory across multiple infrastructures including storage networks, LANs, MANs, and WANs. Figure 9 shows a set of screenshots from the CiscoWorks RME applications.

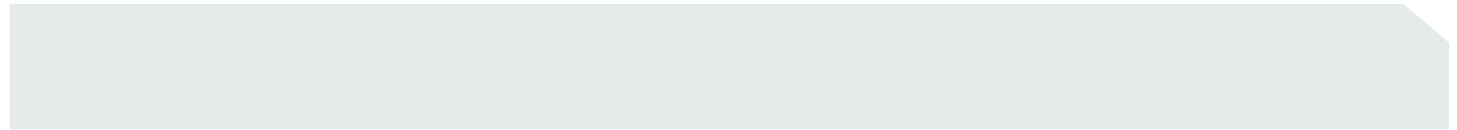
Figure 9. CiscoWorks Resource Manager Essentials Screenshots



3RD PARTY INTEGRATION

The key to providing a solid management solution is not only to provide a set of tools to manage the product, but to open interfaces to raw performance and configuration information within the product for 3rd party use. Many enterprises have already standardized on storage and storage network management platforms. Therefore, to integrate into a customer's environment, Cisco has opened access to extensive amounts of information that can be retrieved from the Cisco MDS 9000 Family switches for use in these applications.

The most common and widely used management protocol today for network management is SNMP. SNMP provides a simple and comprehensive way of sending commands and data back and forth between management stations and the devices they manage. The MIBs used by SNMP provide a very granular access to performance and configuration information within a networking device. Within the Cisco MDS 9000 Family of switches, numerous new storage network-related MIBs have been included to give access to 3rd party applications, or in-house developed applications to device and fabric-centric data. These new MIBs are in addition to many IETF-standardized and Cisco proprietary MIBs incorporate into the platforms. In addition, Cisco has implemented SNMPv3 within the Cisco MDS 9000 Family to offer secure connections to the data and commands provided by the MIBs.



The Cisco MDS 9000 Family switches also support standard in-band configuration facilities such as the Fibre Channel *Name Service* and the *FC-GS-3 and FC-GS-4 Fabric Configuration Server*. Any 3rd Party fabric management applications that utilize in-band information from the FC-GS-3 and FC-GS-4 generic services will discover the Cisco MDS 9000 Family switches. The Cisco MDS 9000 Family switches will in-turn discover other FC-GS-3 compliant devices in the fabric. In addition, the Cisco MDS 9000 Family switches will discover connected SCSI targets and their visible LUN layouts.

The Cisco MDS 9000 Family switches also support SNIA SMI-S 1.1 specification. Any 3rd party fabric management applications can communicate to the embedded provider via HTTP or HTTPS.

Cisco has gone one step further by providing an OOB access to this in-band information. Using SNMP, a 3rd-party application can retrieve fabric-oriented information such as the contents of the *Name Server* or the orientation of SCSI targets and their associated LUNs via MIBs. Cisco has written and included several new MIBs that allow outside applications to retrieve information that was formerly only available in-band over Fibre Channel.

Cisco continues to work with many of its partners to further integrate support for the Cisco MDS 9000 Family switches into popular management products.

CONCLUSION

The Cisco MDS 9000 Family of switches includes a robust toolkit of features and services for enabling storage network management. From device to fabric to resource management, the Cisco MDS 9000 Family offers a set of tools that can be used to independently manage a fabric, or provide interfaces for 3rd party tools to gain access to fabric configuration and statistics for seamless management. While providing access to statistical information, the tools provided with the Cisco MDS 9000 Family also provide a comprehensive set of troubleshooting tools for the fabric, something desperately lacking from today's switch product offerings.

Cisco has taken an open approach to storage network management with the Cisco MDS 9000 Family of switches. The open policy now gives the user choices on how they choose to manage their storage network environment. Whether a user relies solely on the tools provided with the Cisco MDS 9000 Family switches, or integrates the switches into their existing management software suite, or uses both, it is completely open. Cisco will continue to develop and extend its management services and interfaces based on customer requirements while maintaining its openness in enabling any and all storage network management offerings.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

