CHAPTER 1

Product Overview

The Cisco MDS 9000 Family of multilayer directors and fabric switches offers intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. They combine robust and flexible hardware architecture with multiple layers of network and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9000 Family provides intelligent networking features such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

This chapter lists the hardware features for the Cisco MDS 9000 Family and describes its software features. It includes the following sections:

- Hardware Overview, page 1-1
- Software Features, page 1-4
- Tools for Software Configuration, page 1-14

Hardware Overview

This section provides an overview of the Cisco MDS 9000 Family of multilayer directors and fabric switches.

- Cisco MDS 9120 multilayer switches
- Cisco MDS 9140 multilayer switches
- Cisco MDS 9216 multilayer fabric switches.
- Cisco MDS 9216A multilayer fabric switches
- Cisco MDS 9216i multiprotocol fabric switches
- Cisco MDS 9506 multilayer directors
- Cisco MDS 9509 multilayer directors

Cisco MDS 9100 Series Fixed Configuration Fabric Switches

Cisco MDS 9100 Series includes two multilayer, fixed configuration (non-modular) switches:

- Cisco MDS 9120 with 20 ports (4 full-rate ports, 16 host-optimized ports)
- Cisco MDS 9140 with 40 ports (8 full-rate ports, 32 host-optimized ports)

These fixed configuration switches are packaged in 1 RU enclosures and have the following features:

- Two redundant, hot-swappable power supplies have AC connections, each of which can supply power to the entire chassis.
- Two hot-swappable fan modules with two fans each manage the airflow and cooling for the entire switch.
- The 1-Gbps or 2-Gbps autosensing Fibre Channel ports support Inter-Switch Links (E ports), Extended Inter-Switch Links (TE ports), loops (FL and TL ports), and fabric (F ports) connectivity. Besides Telnet access, a 10/100BASE-T Ethernet port provides switch access.
- Hot-swappable, small form-factor pluggable (SFP) ports can be configured with either short or long wavelength SFPs for connectivity up to 500 m and 10 km, respectively.

Note Switches in the Cisco MDS 9100 Series do not have a COM1 port (RS-232 serial port).

Refer to the *Cisco MDS 9100 Series Hardware Installation Guide*.

Cisco MDS 9200 Series Fabric Switches

The Cisco MDS 9200 Series includes two multilayer switches and one multiprotocol switch:

- The multilayer Cisco MDS 9216 and Cisco MDS 9216A switches share a consistent software architecture with the Cisco MDS 9500 Series in a semi-modular chassis and consists of the following major hardware components:
  -
  -
  -
  -
-
  -
  -

–
–

•
•
•
•
•

Cisco MDS 9216 Switch Hardware Installation Guide *Cisco MDS 9200 Series Hardware Installation Guide*

Cisco MDS 9500 Series Multilayer Directors

- The Cisco MDS 9506 Director addresses the stringent requirements of data center storage environments and consists of the following major hardware components:
  - The chassis has six slots, two of which are reserved for the supervisor modules.
  - Up to four hot-pluggable switching or services modules that provide Fibre Channel or Gigabit Ethernet services.
  - The backplane has direct plug-in connectivity to four switching or services modules, two supervisor modules, two clock modules, and two power supplies.
  - The hot-swappable fan module has six fans managing the airflow and cooling for the entire switch.
- The Cisco MDS 9509 Director addresses the stringent requirements of large data center storage environments and consists of the following major hardware components:
  - The chassis has nine slots, two of which are reserved for the supervisor modules.
  - Up to seven hot-pluggable switching or services modules that provide Fibre Channel or Gigabit Ethernet services.
  - The backplane has direct plug-in connectivity to seven switching or services modules, two supervisor modules, two clock modules, and two power supplies.
  - The hot-swappable fan module has nine fans managing the airflow and cooling for the entire switch.

These multilayer directors have the following features:

- Two redundant, hot-swappable power supplies have AC or DC connection, each of which can supply power to the entire chassis.
- Two supervisor modules ensure high availability and traffic load balancing capabilities. Each supervisor module can control the entire switch. The standby supervisor module provides redundancy in case the active supervisor module fails.
- The 1-Gbps or 2-Gbps autosensing Fibre Channel ports support Inter-Switch Links (E ports), Extended Inter-Switch Links (TE ports), loops (FL and TL ports), and fabric (F ports) connectivity. Besides Telnet access, a 10/100BASE-T Ethernet port provides switch access and an RS-232 serial port allows switch configuration.
- Hot-swappable, small form-factor pluggable (SFP) ports can be configured with either short or long wavelength SFPs for connectivity up to 500 m and 10 km, respectively.
- The Cisco MDS 9500 Series switches support the IP Storage Services (IPS) module and the 14/2-port Multiprotocol Services (MPS-14/2) module. Both modules are configurable for both FCIP and iSCSI operation on a port-by-port basis. Ports configured for FCIP operation can be further configured to support up to three virtual ISL connections. FICON is supported on the MPS-14/2 module and functions with all the IPS features on this module, including IPsec and hardware compression.
- The Cisco MDS 9500 Series switches support the 32-port Fibre Channel Storage Services Module (SSM). The SSM enables pooling of heterogeneous storage for increased storage utilization, simplified storage management, and reduced total cost of storage ownership.

Refer to the *Cisco MDS 9500 Series Hardware Installation Guide*.

Software Features

This section provides an overview of the major software features of the Cisco MDS 9000 Family of multilayer directors and fabric switches.

Licensing

The licensing functionality is available in all switches in the Cisco MDS 9000 Family. This functionality allows you to access specified premium features on the switch after you install the appropriate license for that feature.

See Chapter 3, “Obtaining and Installing Licenses.”

High Availability

The Cisco MDS 9500 Series supports application restartability and nondisruptive supervisor switchability. The switches are protected from system failure by redundant hardware components and a high availability software framework. The high availability (HA) software framework includes the following:

- Provides stateful redundancy for supervisor module failure by using dual supervisor modules.
- Ensures nondisruptive software upgrade capability.

- Protects against link failure using the PortChannel (port aggregation) feature. This feature is also available in Cisco MDS 9200 Series and in the Cisco MDS 9100 Series.
- Provides management redundancy using the Virtual Router Redundancy Protocol (VRRP). This feature is also available in Cisco MDS 9200 Series and in the Cisco MDS 9100 Series.
- Performs nondisruptive restarts of a failed process on the same supervisor module. A service running on the supervisor modules and on the switching or services module tracks the HA policy defined in the configuration and takes action based on this policy. This feature is also available in the Cisco MDS 9200 Series and in the Cisco MDS 9100 Series.

See Chapter 8, "Configuring High Availability," Chapter 6, "Software Images," Chapter 13, "Configuring PortChannels," and the "The Virtual Router Redundancy Protocol" section on page 36-16.

Switch Reliability

Switches in the Cisco MDS 9000 Family maintain internally controlled reliability services that ensure continued service with no degradation. This reliability service includes the following:

- Provides power-on self testing (POST)
- Detects errors, isolates faults, performs parity checking, and checks illegal addresses
- Enables remote diagnostics using Call Home troubleshooting features
- Displays LEDs that summarize the status of each switching or services module, supervisor module, power supply, and fan assembly

Graceful Shut Down

The Cisco SAN-OS software implicitly performs a graceful shut down in response to either of the following actions:

- If you shut down an interface operating in the E port mode
- If a Cisco SAN-OS software application executes a port shut down as part of its function

A graceful shut down ensures that no frames are lost when the interface is shutting down. When a shut down is triggered either by you or the Cisco SAN-OS software, the switches connected to the shut down link coordinate with each other to ensure that all frames in the ports are safely sent through the link before shutting down. This enhancement reduces the chance of frame loss.

Cisco Fabric Services

The Cisco SAN-OS software uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database distribution and to foster device flexibility. It simplifies SAN provisioning by automatically distributing configuration information to all switches in a fabric. The following Cisco SAN-OS features use the CFS infrastructure:

- NTP (see "NTP Configuration Distribution" section on page 4-20).
- Dynamic Port VSAN Membership (see Chapter 17, "Creating Dynamic VSANs").
- Distributed Device Alias Services (see Chapter 20, "Distributing Device Alias Services").
- IVR topology (see "Database Merge Guidelines" section on page 18-29).
- TACACS and RADIUS (see the "Distributing AAA Server Configuration" section on page 28-15).

- User and administrator roles (see the "Role-Based Authorization" section on page 26-1).
- Port security (see the "Port Security Configuration Distribution" section on page 32-9).
- iSNS (see the "About iSCSI Storage Name Services" section on page 35-58).
- Call Home (see the "Call Home Configuration Distribution" section on page 45-12).
- Syslog (see the "System Message Logging Configuration Distribution" section on page 44-8).
- Fctimer (see the "fctimer Distribution" section on page 25-3).
- SCSI Flow Services (see the "Configuring SCSI Flow Services" section on page 38-3).
- Saving the configuration (see the "Saving the Configuration" section on page 7-4).

Virtual SANs

VSANs (virtual SANs) enable higher security and greater scalability in Fibre Channel fabrics. VSANs provide isolation among devices that are physically connected to the same fabric. VSANs allow multiple logical SANs over a common physical infrastructure. VSANs offer the following:

- Traffic isolation—Traffic is contained within VSAN boundaries and devices reside only in one VSAN thus ensuring absolute separation between user groups, if desired.
- Scalability—VSANs are overlaid on top of a single physical SAN. The ability to create several logical VSAN layers increases the scalability of the SAN.
- Per VSAN fabric services—Replication of fabric services on a per VSAN basis provides increased scalability and availability.
- Redundancy—Several VSANs created on the same physical SAN ensure redundancy. If one VSAN fails, there is a configured backup path between the host and the switch.
- Ease of configuration—Devices can be added, moved, or changed between VSANs without changing the physical structure of a SAN. Moving a device from one VSAN to another only requires configuration at the port level, not at a physical level.

See Chapter 16, "Configuring and Managing VSANs."

Dynamic VSANs

Port VSAN membership on the switch is assigned on a port-by-port basis. By default each port belongs to the default VSAN.

You can dynamically assign VSAN membership to ports by assigning VSANs based on the device WWN. This method is referred to as the Dynamic Port VSAN Membership (DPVM) feature. DPVM offers flexibility and eliminates the need to reconfigure the VSAN to maintain fabric topology when a host or storage device connection is moved between two Cisco MDS switches. It retains the configured VSAN regardless of where a device is connected or moved.

See Chapter 17, "Creating Dynamic VSANs."

Intelligent Zoning

Zoning controls access between devices in a VSAN. Zoning accomplishes the following:

- Partitions devices that use different operating systems. In a heterogeneous environment, it is often necessary to separate servers and storage devices to avoid accidental transfer of information between devices with different operating systems. Such transfers could result in corruption or deletion of data.
- Creates logical subsets of closed user groups. Closed user groups are needed to enforce security or to separate functional areas across the fabric.
- Configures groups of devices that are separate from the rest of the fabric. Based on the assigned zone membership, devices outside the zone cannot access devices internal to the zone.
- Provides temporary access between devices (zone sets). Zone restrictions can be imposed temporarily, and then restored to revert to normal operation, if desired.
- Restricts access to specific logical unit numbers (LUNs) associated with a device.
- Allows members to have only read-only access to the media within a read-only Fibre Channel zone.

See Chapter 19, “Configuring and Managing Zones.”

Enhanced Zoning

The zoning feature is compliant with FC-GS-4 and FC-SW-3. Both standards support the basic zoning features explained in the Intelligent Zoning section and the enhanced zoning features described the “About Enhanced Zoning” section on page 19-27.

Device Alias Distribution

All switches in the Cisco MDS 9000 Family offer a new alias distribution feature called Distributed Device Alias Services (device alias). You now have the option to distribute device alias names on a fabric-wide basis.

See Chapter 20, “Distributing Device Alias Services.”

Inter-VSAN Routing

Using Inter-VSAN Routing (IVR), resources across VSANs can be accessed without compromising other VSAN benefits. Valuable resources such as tape libraries are easily shared across VSANs without compromise. Routes that traverse one or more VSANs across multiple switches can be established, if necessary, to establish proper interconnections. IVR used in conjunction with FCIP provides more efficient business continuity or disaster recovery solutions.

See Chapter 18, “Configuring Inter-VSAN Routing.”

Trunking

Trunking is the term used to refer to an ISL link that carries one or more VSANs. Trunking ports receive and transmit Enhanced ISL (EISL) frames. EISL frames carry an EISL header containing VSAN information. Once EISL is enabled on an E port, that port becomes a TE port. The trunking configuration is saved along with the interface information.

See Chapter 11, "Configuring Interfaces" and Chapter 12, "Configuring Trunking."

PortChannels

PortChannel refers to the aggregation of multiple physical Fibre Channel ports into one logical port to provide high aggregated bandwidth, load balancing, and link redundancy. Up to 16 physical ports can be aggregated into a PortChannel. PortChannels can connect to ports across switching or services modules. The failure of a port in one module does not bring down the logical PortChannel link. Specifically, a PortChannel does the following:

- Increases the aggregated bandwidth on an ISL or EISL by distributing traffic among all functional links in the channel.
- Load balances across multiple links and maintains optimum bandwidth utilization. Load balancing is based on a source ID (SID), a destination ID (DID), and optionally an originator exchange ID (OX ID) which identify the flow of the frame.
- Provides high availability on an ISL. If one link fails, traffic previously carried on this link is switched to the remaining links. If a link goes down in a PortChannel, the upper protocol is not aware of it. To the upper protocol, the link is still there, although the bandwidth is diminished. The routing tables are not affected by link failure. PortChannels can contain up to 16 physical links and can span multiple modules for added high availability.
- A protocol to exchange PortChannel configurations is available in all Cisco MDS switches. This feature simplifies PortChannel management with incompatible ISLs. Autocreation mode enables ISLs with compatible parameters to automatically form channel groups without manual intervention.

See Chapter 13, "Configuring PortChannels."

IP Services

Switches in the Cisco MDS 9000 Family support the following IP services:

- IP over Ethernet —These services are limited to management traffic.
- IP over Fibre Channel (IPFC)—IPFC (RFC 2625) specifies how IP packets are transported using encapsulation schemes. By encapsulating IP frames into Fibre Channel frames, management information is exchanged among switches without requiring a separate Ethernet connection to each switch. Each switch includes:
  - Encapsulation for IP and the Address Resolution Protocol (ARP) over Fibre Channel.
  - Address resolution uses the ARP server.
- IP routing services—These services include:
  - Ethernet or TCP/IP connection.
  - Static IP routing services to enable management traffic between VSANs.

  - DNS client support.
  - The Network Time Protocol (NTP) server to synchronize the system clocks of network devices.
- You can apply IP-ACLs to VSAN interfaces, the management interface, Gigabit Ethernet interfaces on IPS modules, and Ethernet PortChannel interfaces.

See Chapter 36, "Configuring IP Services."

FICON

Fibre Connection (FICON) interface capabilities enhance the Cisco MDS 9000 Family by supporting both open systems and mainframe storage network environments. Inclusion of Control Unit Port (CUP) support further enhances the MDS offering by allowing in-band management of the switch from FICON processors.

See the Chapter 24, "Configuring FICON."

Fabric Binding

The fabric binding feature helps prevent unauthorized switches from joining the fabric or disrupting current fabric operations.

See the "Fabric Binding Configuration" section on page 24-37.

RLIR

The Registered Link Incident Report ((RLIR) application provides a method for a switchport to send a LIR to a registered Nx-port.

See the "Displaying RLIR Information" section on page 24-45.

IP Storage

The Cisco MDS 9000 Family IP services module, the 14/2-port Multiprotocol Service module, and the Cisco MDS 9216i Switch integrate seamlessly into the Cisco MDS 9000 Family of multilayer directors and fabric switches. Traffic can be routed between any IP storage port and any other port on a Cisco MDS 9000 Family switch. These products support the full range of services available on other Cisco MDS 9000 Family switching modules including VSANs, security, and traffic management. It uses widely known IP to cost-effectively connect to more servers and more locations over greater distances than previously possible. It delivers both Fibre Channel over IP (FCIP) and iSCSI IP storage services and is configurable on a port-by-port basis.

- FCIP highlights
  - Simplifies data protection and business continuance strategies by enabling backup, remote replication, and disaster recovery over WAN distances using open-standard FCIP tunneling.
  - Improves utilization of WAN resources for backup and replication by tunneling up to three virtual Inter-Switch Links (ISLs) on a single Gigabit Ethernet port.
  - Reduces SAN complexity by eliminating the need to deploy and manage a separate remote connectivity platform.

  - Preserves Cisco MDS 9000 Family enhanced capabilities including VSANs, advanced traffic management, and security across remote connections.
  - Improves application performance using one or more of the following options for the FCIP interface: FCIP write acceleration, FCIP tape acceleration, and FCIP compression.
- iSCSI highlights
  - Extends the benefits of Fibre Channel SAN-based storage to IP-enabled servers at a lower cost point than possible using Fibre Channel interconnect alone.
  - Increases storage utilization and availability through consolidation of IP and Fibre Channel block storage.
  - Preserves through a transparent operation the functionality of legacy storage applications such as zoning tools.
  - Allows your existing TCP/IP networks to function more effectively as storage area networks by automating the discovery, management, and configuration of iSCSI devices.

See Chapter 37, "Configuring IP Storage."

Call Home

The Call Home feature detects switch failures and sends alerts along with relevant failure information. These alerts are sent through e-mail to a user-specified customer center. The Call Home feature also provides message throttling capabilities, periodic inventory messages, port syslog messages, and RMON alert messages.

See Chapter 45, "Configuring Call Home."

QoS and Congestion Control

Switches in the Cisco MDS 9000 Family provide priority queuing and flow control services.

- The Quality of Service (QoS) feature has the following advantages:
  - Guarantees relative bandwidth to application traffic.
  - Controls latency experienced by application traffic.
  - Prioritizes one application over another (for example, prioritizing transactional traffic over bulk traffic) through bandwidth and latency differentiation.
- Fibre Channel Congestion Control (FCC)—FCC is a flow control mechanism that alleviates congestion on Fibre Channel networks. Any switch in the network can detect congestion for an output port. The switches sample frames from the congested queue and generate messages about the congestion level upstream toward the source of the congestion. The switch closest to the source, with FCC enabled, can perform one of two actions:
  - Forwards the frames as other vendor switches do.
  - Limits the flow of frames from the port causing the congestion.

See Chapter 47, "Configuring Fabric Congestion Control and QoS."

SPAN and RSPAN

The Switched Port Analyzer (SPAN) feature is specific to switches in the Cisco MDS 9000 Family. It monitors network traffic though a Fibre Channel interface. Traffic through any Fibre Channel interface can be replicated to a special port called the SPAN destination port (SD port). Any Fibre Channel port in a switch can be configured as an SD port. Once an interface is in SD-port mode, it cannot be used for normal data traffic. You can attach a Fibre Channel Analyzer to the SD port to monitor SPAN traffic.

The Remote SPAN (RSPAN) feature enables you 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 (SD) port is used for remote monitoring in a destination switch. A destination switch may be different from the source switch(es) provided that it is attached to the same Fibre Channel fabric. You can replicate and monitor traffic in any remote Cisco MDS 9000 Family switch or director, just as you would monitor traffic in an MDS source switch. This feature is nonintrusive and does not affect network traffic switching for any SPAN source ports.

See Chapter 43, "Monitoring Network Traffic Using SPAN."

Switch Management Features

Besides the software features already listed, there are additional management features that fall into the following categories: redundant supervisor module management, fabric management, and security management.

Redundant Supervisor Module Management

The Cisco MDS 9500 Series of multilayer directors support two redundant supervisor modules. These supervisor modules are required to provide high availability (see Table 1-1).

Table 1-1 Supervisor Module Options in Cisco MDS 9000 Switches

Product	No. of Supervisor Modules	Supervisor Module Slot No.	Switching/Services Module Features
Cisco MDS 9100 Series	Not applicable		
Cisco MDS 9200 Series	One module (includes 16 additional ports)	1	2-slot chassis allows one optional switching or services module in the other slot.
Cisco MDS 9506	Two modules	5 and 6	6-slot chassis allows any switching or services module in the other four slots.
Cisco MDS 9509	Two modules	5 and 6	9-slot chassis allows any switching or services module in the other seven slots.

When a switch powers up and both supervisor modules are present, the module in slot 5 enters active mode and the second module in slot 6 enters standby mode. All storage management functions occur on the active supervisor module. The standby module constantly monitors the active module. If the active module fails, the standby module takes over without any impact to user traffic.

Refer to the *Cisco MDS 9500 Series Hardware Installation Guide*.

Fabric Management

Cisco MDS 9000 Family switches offer fabric management and control through the command-line interface (CLI) by using Telnet, SSH, or a serial console and through the Cisco MDS 9000 Fabric Manager tool by using the Simple Network Management Protocol (SNMP) services:

- SNMP versions 1, 2c, and 3 are supported. See Chapter 27, "Configuring SNMP."
- Remote Monitoring (RMON) allows you to specify thresholds and monitor alarms on SNMP variables. Extended RMON alarms are available for supported Management Information Base (MIB) objects (refer to the *Cisco MDS 9000 Family MIB Reference*). See Chapter 42, "Configuring RMON."
- System log (syslog) messages are viewed through a console or Telnet session for asynchronous events such as an interface transition. System messages are directed to an internal log and optionally to an external server (refer to the *Cisco MDS 9000 Family System Messages Reference)*. See Chapter 44, "Configuring System Message Logging."

Security Management

The Cisco MDS 9000 Family of switches offer strict and secure switch management options through switch access security, port security, user authentication, and role-based access control.

Network Security

IP Security Protocol (IPsec) is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. It is developed by the Internet Engineering Task Force (IETF). IPsec provides these security services at the IP layer. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IPsec uses the Internet Key Exchange (IKE) protocol to handle protocol and algorithm negotiation and to generate the encryption and authentication keys to be used by IPsec. While IKE can be used with other protocols, its initial implementation is with the IPsec protocol. IKE provides authentication of the IPsec peers, negotiates IPsec security associations, and establishes IPsec keys.

See Chapter 30, "Configuring IPsec Network Security."

Fabric Security

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. It consists of the CHAP protocol combined with the Diffie-Hellman exchange.

See Chapter 31, "Configuring FC-SP and DHCHAP."

Switch Access Security

Each switch can be accessed through the CLI or SNMP:

- Secure switch access—Available when you explicitly enable Secure Shell Protocol (SSH) access to the switch. SSH access provides additional controlled security by encrypting data, user IDs, and passwords. By default, Telnet access is enabled on each switch.
- SNMP access—SNMPv3 provides built-in security for secure user authentication and data encryption.
- IP access control lists (IP-ACLs)—IP-ACLs provide basic network security to all switches in the Cisco MDS 9000 Family. IP-ACLs restrict IP-related inband and out-of-band management traffic based on IP addresses (Layer 3 and Layer 4 information). You can use IP-ACLs to control transmissions on an interface.

See Chapter 29, "Configuring IP Access Control Lists."

Port Security

The following port security features prevent unauthorized access to a switch port in the Cisco MDS 9000 Family:

- Login requests from unauthorized Fibre Channel devices (Nx ports) and switches (xE ports) are rejected.
- All intrusion attempts are reported to the SAN administrator through system messages.

See Chapter 32, "Configuring Port Security."

User Authentication

Authentication, authorization, and accounting (AAA) can be used to verify the identity of, grant access for, and track the actions of remote users. The Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) provide AAA solutions.

Based on the user ID and password combination provided, switches perform local authentication using a local database or remote authentication using AAA server(s). A global, preshared, secret key authenticates communication between the AAA servers. This secret key can be configured for all AAA server groups or for only a specific AAA server. This kind of authentication provides a central configuration management capability.

See Chapter 26, "Configuring Users and Common Roles" and Chapter 28, "Configuring RADIUS and TACACS+."

Role-Based Access

Role-based access control assigns roles or groups (locally through the switch or remotely using AAA servers) to users and limits access to the switch. Access is assigned based on the permission level associated with each user ID. Your administrator can provide complete access to each user or restrict access to specific read and write levels for each command.

Cisco MDS SAN-OS software synchronizes the CLI and SNMP roles. You can use SNMP to modify a role that was created using CLI and vice versa. Each role in SNMP is the same as a role created or modified through the CLI.

Each role is restricted to one or more VSAN as required.

See Chapter 27, "Configuring SNMP."

Port Tracking

The Port Tracking feature is unique to the Cisco MDS 9000 Family of switches. This feature uses information about the operational state of the link to initiate a failure in the link that connects the edge device. This process of converting the indirect failure to a direct failure triggers a faster recovery process towards redundant links. When enabled, the port tracking feature brings down the configured links based on the failed link and forces the traffic to be redirected to another redundant link.

See Chapter 48, "Configuring Port Tracking."

SAN Extension Tuner

The SAN extension tuner (SET) feature is unique to the Cisco MDS 9000 Family of switches. This feature helps you optimize FCIP performance by generating SCSI I/O commands and directing such traffic to a specific virtual target. You can specify the size of the test I/O transfers and how many concurrent I/Os to generate while testing. The SET reports the resulting I/Os per second (IOPS) and I/O latency, which helps you determine the number of concurrent I/Os needed to maximize FCIP throughput.

See Chapter 34, "Configuring the SAN Extension Tuner."

Command Scheduler

The Cisco MDS command scheduler feature helps you schedule configuration and maintenance jobs in any switch in the Cisco MDS 9000 Family. You can use this feature to schedule jobs on a one-time basis or periodically.

See Chapter 15, "Scheduling Maintenance Jobs."

Intelligent Storage Services

The Advanced Services Modules (ASMs) and Storage Services Modules (SSMs) support Intelligent Storage Services Intelligent Storage Services include the following:

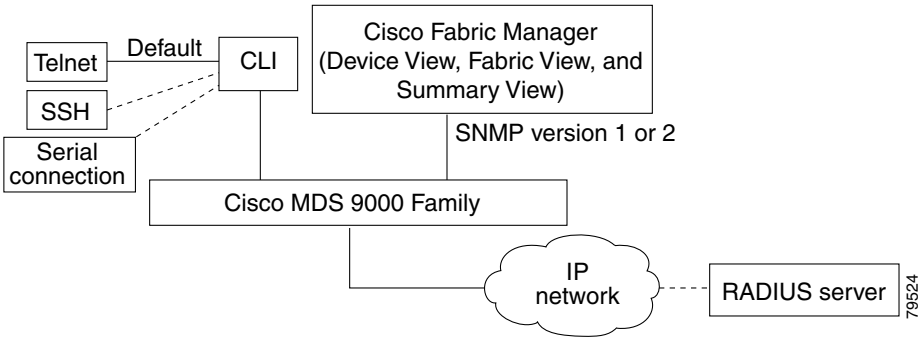
- Fibre Channel write acceleration
- SCSI flow statistics
- SANTap
- Network Accelerated Serverless Backup (NASB)

See Chapter 39, "Configuring Fibre Channel Write Acceleration", Chapter 38, "Configuring SCSI Flow Services and Statistics,", Chapter 40, "Configuring SANTap," and Chapter 41, "Configuring NASB."

Tools for Software Configuration

You can use one of two configuration management tools to configure your SANs: the CLI and the Cisco MDS 9000 Fabric Manager graphical user interface (see Figure 1-1).

Figure 1-1 Tools for Configuring Software



CLI

With the CLI, you can type commands at the switch prompt, and the commands are executed when you press the Enter key. The CLI parser provides command help, command completion, and keyboard sequences that allow you to access previously executed commands from the buffer history.

Continue reading this guide for more information on configuring the Cisco MDS switch using the CLI.

Cisco MDS 9000 Fabric Manager

The Cisco Fabric Manager is a set of network management tools that supports Secure Simple Network Management Protocol version 3 (SNMPv3) and legacy versions. It provides a graphical user interface (GUI) that displays real-time views of your network fabric, and lets you manage the configuration of Cisco MDS 9000 Family devices and third-party switches. The Cisco Fabric Manager applications include the following:

- Fabric Manager Server—performs advanced monitoring, troubleshooting, and configuration for multiple fabrics. It must be started before running the Fabric Manager. It can be accessed by up to 16 Fabric Manager clients at a time.
- Device Manager—presents two views of a switch:
  - Device View displays a continuously updated physical representation of the switch configuration, and provides access to statistics and configuration information for a single switch.
  - Summary View presents real-time performance statistics of all active interfaces and channels on the switch for Fibre Channel and IP connections.
- Fabric Manager Web Client—allows operators to monitor MDS events, performance, and inventory from a remote location using a web browser.
- Performance Manager— provides detailed traffic analysis by capturing data with SNMP. This data is compiled into various graphs and charts which can be viewed with any web browser.

The Cisco Fabric Manager applications are an alternative to the CLI for most switch configuration commands.

Note Resource Manager Essentials (RME) versions 3.4 and 3.5 provide support for switches in the Cisco MDS 9000 Family. Device Updates (DU) are available on Cisco.com (http://www.cisco.com/).

Refer to the *Cisco MDS 9000 Fabric Manager Configuration Guide*.