CISCO MDS 9000 FAMILY SAN OS 2.0(X)

The Cisco® MDS 9000 Family SAN-OS is the underlying system software that powers the award-winning Cisco MDS 9000 Family Multilayer Switches. SAN-OS is designed for storage area networks (SANs) in the best traditions of Cisco IOS® Software to create a strategic SAN platform of superior reliability, performance, scalability, and features.

In addition to providing all the features that the market expects of a storage network switch, the SAN-OS provides many unique features that help the Cisco MDS 9000 Family to deliver low total cost of ownership (TCO) and a quick return on investment (ROI).

FLEXIBILITY AND SCALABILITY

The following features help characterize SAN-OS as a highly flexible and scalable platform for enterprise SANs.

Common Software Across All Platforms

The SAN-OS runs on all Cisco MDS 9000 Family switches, from multilayer fabric switches to multilayer directors. Using the same base system software across the entire product line enables Cisco Systems® to provide an extensive, consistent, and compatible feature set on the Cisco MDS 9000 Family.
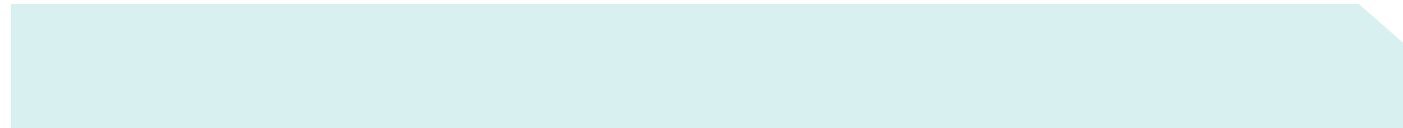
Multiprotocol Support

In addition to supporting Fibre Channel Protocol (FCP), the SAN-OS also supports IBM Fibre Connection (FICON), Small Computer System Interface over IP (iSCSI), and Fibre Channel over IP (FCIP) in a single platform. Native iSCSI support in the Cisco MDS 9000 Family helps customers to consolidate storage for a wider range of servers into a common pool on the SAN. Native FCIP support allows customers to take advantage of their existing investment in IP networks for cost-effective business-continuance solutions for both Fibre Channel and FICON environments. With SAN-OS multiprotocol support, customers can better use their enterprise resources, thereby lowering costs.

Virtual SANs

Virtual SAN (VSAN) technology partitions a single physical SAN into multiple VSANs. The Cisco MDS 9000 Family switches are the first SAN switches on the market with VSAN support built into the switch hardware. VSAN capabilities allow the SAN-OS to logically divide a large physical fabric into separate isolated environments to improve Fibre Channel SAN scalability, availability, manageability, and network security. For FICON, VSANs help ensure that there is true hardware-based separation of FICON and open systems.

Each VSAN is a logically and functionally separate SAN with its own set of Fibre Channel fabric services. This partitioning of fabric services greatly reduces network instability by containing fabric reconfigurations and error conditions within an individual VSAN. The strict traffic segregation provided by VSANs helps ensure that the control and data traffic of a given VSAN is confined within its own domain, increasing SAN security. VSANs help reduce costs by facilitating consolidation of isolated SAN islands into a common infrastructure without compromising availability.

Users can create administrator roles that are limited in scope to certain VSANs. For example, a network administrator role can be set up to allow configuration of all platform-specific capabilities, while other roles can be set up to only allow configuration and management within specific VSANs. This improves the manageability of large SANs and reduces disruptions due to human error by isolating the effect of a user's action to a specific VSAN whose membership may be assigned based on switch ports or the worldwide name (WWN) of attached devices.

VSANs are supported across FCIP links between SANs, extending VSANs to include devices at a remote location. The Cisco MDS 9000 Family also implements trunking for VSANs. Trunking allows Inter-Switch Links (ISLs) to carry traffic for multiple VSANs on the same physical link.

Inter-VSAN Routing

Data traffic can be transported between specific initiators and targets on different VSANs using Inter-VSAN Routing without merging VSANs into a single logical fabric. Fibre Channel control traffic does not flow between VSANs, nor can initiators access any resources aside from the ones designated with Inter-VSAN Routing. Valuable resources like tape libraries can be easily shared without compromise. Inter-VSAN Routing can also be used in conjunction with FCIP to create more efficient business-continuity and disaster-recovery solutions.

Intelligent Fabric Services

The SAN-OS supports intelligent storage services. It forms a solid basis for delivering storage applications such as virtualization, snapshots, and replication on Cisco MDS 9000 Family switches in the network. Thus, the flexibility of SAN-OS provides future investment protection.

NETWORK SECURITY

Cisco takes a comprehensive approach to network security with SAN-OS. In addition to VSANs, which provide true isolation of SAN-attached devices, SAN-OS offers numerous additional security features.

Switch and Host Authentication

Fibre Channel Security Protocol (FC-SP) capabilities in the SAN-OS provide Switch-Switch and Host-Switch authentication for enterprise wide fabrics. Diffie-Hellman extensions with Challenge Handshake Authentication Protocol (DH-CHAP) are used to perform authentication locally in the Cisco MDS 9000 Family or remotely through RADIUS or TACACS+. If authentication fails, a switch or host cannot join the fabric.

IP Security for FCIP and iSCSI

Traffic flowing outside the data center must be protected. The proven IETF standard IP Security (IPsec) capabilities in the SAN-OS offer secure authentication, data encryption for privacy, and data integrity for both FCIP and iSCSI connections on the Cisco MDS 9000 Family Multiprotocol Services Module and Cisco MDS 9216i Multilayer Fabric Switch. SAN-OS uses Internet Key Exchange Version 1 (IKEv1) and IKEv2 protocols to dynamically set up security associations for IPsec using preshared keys for remote-side authentication.

Roles-Based Access Control

The SAN-OS provides roles-based access control (RBAC) for management access of the Cisco MDS 9000 Family command-line interface (CLI) and Simple Network Management Protocol (SNMP). In addition to the two default roles in the switch, up to 64 user-defined roles can be configured. Applications using SNMP Version 3 (SNMPv3), such as Cisco Fabric Manager, have full RBAC for switch features managed using this protocol. The roles describe the access-control policies for various feature-specific commands on one or more VSANs. CLI and SNMP users and passwords are also shared; only a single administrative account is required for each user.

Port Security and Fabric Binding

Port security locks down the mapping of an entity to a switch port. The entities can be hosts, targets, or switches that are identified through worldwide name. This helps ensure unauthorized devices connecting to the switch port do not disrupt the SAN fabric. Fabric binding extends port security to enable ISLs only between specified switches.

Zoning

Zoning provides access control for devices within a SAN. SAN-OS supports the following types of zoning:

- N_Port zoning—Defines zone members based on the end-device (hosts and storage) port
  – Worldwide Name
  – Fibre Channel Identifier (FC-ID)

- Fx_Port zoning—Defines zone members based on the switch port
  – Worldwide Name
  – Worldwide Name + Interface Index, or Domain ID + Interface index
  – Domain ID + port number (for Brocade interoperability)

- iSCSI zoning—Defines zone members based on the host's zone
  – iSCSI name
  – IP address

- Logical unit number (LUN) zoning—When combined with N-Port zoning, LUN zoning helps ensure LUNs are accessible only by specific hosts, providing a single point of control for managing heterogeneous storage-subsystem access.
- Read-only zones—An attribute can be set to restrict I/O operations in any zone type to SCSI read-only commands. This feature is especially useful for sharing volumes across servers for backup, data warehousing, etc.
- Broadcast zones—An attribute can also be set for any zone type to restrict broadcast frames to members of the specific zone.

To provide strict network security, zoning is always enforced per frame using access control lists (ACLs) that are applied at the ingress switch. All zoning polices are enforced in hardware and do not cause performance degradation. Enhanced zoning session-management capabilities further enhance security by allowing only one user to modify zones at a time.

Additional Network Security Features

Additional network security features include the following:

- Fabric wide, role-based authentication, authorization, and accounting (AAA) services using RADIUS and TACACS+
- Secure Shell (SSH) Protocol Version 2 and SNMPv3 for authentication, data integrity, and confidentiality of management traffic
- Secure FTP (SFTP) for protecting file transfers
- Advanced Encryption Standard (AES), Message Digest 5 (MD5), and Secure Hash Algorithm (SHA 1) for secure authentication and management
- IP ACLs for management access

AVAILABILITY

The SAN-OS provides resilient software architecture for mission-critical hardware deployments.

Nondisruptive Software Upgrades

SAN-OS provides nondisruptive software upgrades for director-class products with redundant hardware and minimally disruptive upgrades for the fabric switches that do not have redundant supervisor engine hardware.

Stateful Process Failover

The SAN-OS automatically restarts failed software processes and provides stateful supervisor engine failover to help ensure that any hardware or software failures on the control plane do not disrupt traffic flow in the fabric.

Inter-Switch Link Resiliency Using PortChannels

PortChannels aggregate multiple physical Inter-Switch Links (ISLs) into one logical link with higher bandwidth and port resiliency for both Fibre Channel and FICON traffic. With this feature, up to 16 expansion ports (E_Ports) or trunking E_Ports (TE_Ports) can be bundled into a PortChannel to achieve a maximum of 32 Gbps of aggregate bandwidth. ISL ports can reside on any switching module and do not need a designated master port. Thus, in the event of the failure of a port or a switching module, the PortChannel continues to function properly without causing a fabric reconfiguration.

The SAN-OS uses a protocol to exchange PortChannel configuration information between adjacent switches to simplify PortChannel management, including misconfiguration detection and autocreation of PortChannels among compatible ISLs. In the autoconfigure mode, ISLs with compatible parameters automatically form channel groups; no manual intervention is required.

iSCSI, FCIP, and Management Interface High Availability

Virtual Routing Redundancy Protocol (VRRP) increases availability of Cisco MDS 9000 Family management traffic routed over both Ethernet and Fibre Channel networks. VRRP dynamically manages redundant paths for the external Cisco MDS 9000 Family management applications, making control-traffic path failures transparent to applications.

Similarly, VRRP increases IP network availability for iSCSI and FCIP connections by allowing failover of connections from one port to another. This facilitates the failover of an iSCSI volume from one IP services port to any other IP services port, either locally or on another Cisco MDS 9000 Family switch.

The Auto-Trespass feature allows high-availability iSCSI connections to RAID subsystems, independent of host software. Trespass commands can be issued automatically when the SAN-OS detects failures on active paths.

Port Tracking for Resilient SAN Extension

SAN extension resiliency is enhanced by the SAN-OS Port Tracking feature. If a Cisco MDS 9000 Family Switch detects a WAN or metropolitan-area network (MAN) link failure, it brings down the associated disk-array link when Port Tracking is configured, so the array can redirect a failed I/O to another link without waiting for an I/O timeout. Otherwise, disk arrays must wait seconds for an I/O timeout to recover from a network link failure.

MANAGEABILITY

SAN-OS incorporates many management features that help growing storage environments to be managed effectively with existing resources. Cisco Fabric Services (CFS) simplify SAN provisioning by automatically distributing configuration information to all switches in a fabric. Distributed Device Alias Services provide fabric wide alias names for host bus adapters (HBAs), storage devices, and switch ports, which eliminates reentering names when devices are moved.

Management interfaces supported by SAN-OS include:

- CLI through a serial port, out-of-band (OOB) Ethernet management port, and in-band IP over Fibre Channel
- SNMPv1, v2, and v3 over OOB management port and in-band IP over Fibre Channel
- FICON control unit port (CUP) for in-band management from IBM S/390 or z/900 processors

Fabric Manager and Device Manager

Cisco Fabric Manager and Device Manager are responsive, easy-to-use Java applications with GUIs that provide an integrated approach to switch and fabric administration. Cisco Fabric Manager offers storage administrators fabric wide management capabilities, including discovery, multiple switch configurations, real-time network monitoring, historical performance monitoring for network traffic hot-spot analysis, and troubleshooting. This powerful approach greatly reduces switch setup times, increases overall fabric reliability, and provides extensive diagnostics for resolving configuration inconsistencies.

CLI Similar to Cisco IOS Software

The SAN-OS presents the user with a consistent, logical CLI. Adhering to the syntax of the widely known Cisco IOS Software CLI, it is easy to learn and delivers broad management capability. The Cisco MDS 9000 Family CLI is an extremely efficient and direct interface designed to provide optimal capability to administrators in enterprise environments. Administrators can write CLI scripts to manage the Cisco MDS 9000 Family using standard scripting languages.

Open APIs

SAN-OS provides a truly open API for the Cisco MDS 9000 Family based on the industry-standard SNMP. Commands performed on the switches by Cisco Fabric Manager use this open API extensively. Also, all major storage and network management software vendors are using the SAN-OS management API.

Fabric-Device Management Interface (FDMI) capabilities provided by the SAN-OS simplify management of devices such as Fibre Channel HBAs though in-band communications. With FDMI, management applications can gather HBA and host operating-system information without installing proprietary host agents.

The SAN-OS provides an Extensible Markup Language (XML) interface with an embedded agent that complies with the Web-Based Enterprise Management (WBEM), Common Information Model (CIM), and Storage Management Initiative-Specification (SMI-S) standards, including switch, fabric, server, and zoning profiles.

Auto-Learn for Network Security Configuration

The Auto-Learn feature allows the Cisco MDS 9000 Family to automatically learn about devices and switches that connect to it. The administrator can use this feature to configure and activate network security features such as Port Security without having to manually configure the security for each port.

Network Boot for iSCSI Hosts

The SAN-OS also simplifies iSCSI-attached host management by providing network-boot capability.

Configuration and Software Image Management

CiscoWorks is a commonly used suite of tools for a wide range of Cisco devices such as IP switches, routers, and wireless devices. The SAN-OS open API allows the CiscoWorks Resource Manager Essentials (RME) application to provide centralized Cisco MDS 9000 Family configuration management, software-image management, intelligent system message logging (syslog) management, and inventory management. The open APIs also help CiscoWorks Device Fault Manager (DFM) to monitor Cisco MDS device health, such as supervisor memory and processor usage. The health of important components like fans, power supplies, and temperature also can be monitored by CiscoWorks DFM.

Internet Storage Name Service

The Internet Storage Name Service (iSNS) helps existing TCP/IP networks to function more effectively as SANs by automating discovery, management, and configuration of iSCSI devices. iSCSI targets presented by IP Storage Services and Fibre Channel device-state-change notifications are registered by the SAN-OS, either with the highly available, distributed iSNS services built into the SAN-OS, or with external iSNS servers.

Proxy iSCSI Initiator

The Proxy iSCSI Initiator feature simplifies configuration procedures when multiple iSCSI initiators (hosts) are assigned to the same iSCSI target ports. Proxy mode reduces the number of separate times that "back-end" tasks such as Fibre Channel zoning and storage-device configuration must be performed.

TRAFFIC MANAGEMENT

In addition to implementing Fibre Channel Shortest Path First (FSPF) Protocol to calculate the best path between two switches and providing in-order delivery features, SAN-OS enhances the architecture of the Cisco MDS 9000 Family with several advanced traffic-management features that help ensure consistent performance of the SAN during varying load conditions.

Quality of Service

Four distinct quality of service (QoS) priority levels are available: three for Fibre Channel data traffic and one for Fibre Channel control traffic. Fibre Channel data traffic for latency-sensitive applications can be configured to receive higher priority than throughput-intensive applications using data QoS priority levels. Control traffic is assigned the highest QoS priority automatically, to accelerate convergence of fabric wide protocols such as FSPF, zone merges, and principal switch selection.

Data traffic can be classified for QoS by the VSAN identifier, zones, N-Port worldwide name, or FC-ID. Zone-based QoS helps simplify configuration and administration by using the familiar zoning concept.

Fibre Channel Congestion Control

Fibre Channel Congestion Control provides an innovative, end-to-end congestion control mechanism that augments the standard Fibre Channel Buffer-to-Buffer credit mechanism. A switch experiencing congestion explicitly signals this condition to the ingress switch (the entry point for traffic into the fabric that is causing congestion). Upon receiving an explicit notification, the ingress switch throttles the N_Port/NL_Port traffic by reducing the buffer-to-buffer credits.

Extended Credits

Cisco MDS 9000 Family full line-rate ports provide 256 buffer credits standard. With Extended Credits, up to 3500 credits can be assigned to a single Fibre Channel port within a group of 4 Fibre Channel ports on the Multiprotocol Services Module and Cisco MDS 9216i. Adding credits extends distances for Fibre Channel SAN Extension.

Virtual Output Queuing

Virtual output queuing (VOQ) buffers Fibre Channel traffic at the ingress port to eliminate head-of-line blocking. The switch is designed such that the presence of a slow N_Port on the SAN does not affect the performance of any other port in the SAN.

Fibre Channel Port Rate Limiting

The Fibre Channel Port Rate Limiting feature for Cisco MDS 9100 Series Multilayer Fabric Switches controls the amount of bandwidth available to individual Fibre Channel ports within groups of 4 host-optimized ports. By limiting bandwidth on one or more Fibre Channel ports, the other ports in the group receive a greater share of the available bandwidth under maximum utilization conditions. Port Rate Limiting is also beneficial for throttling WAN traffic at the source to help eliminate excessive buffering in Fibre Channel or IP ∫data network devices.

Load Balancing of PortChannel Traffic

PortChannels load balance Fibre Channel traffic using a hash of source FC-ID and destination FC-ID, and optionally the exchange ID. Load balancing using PortChannels is performed over both Fibre Channel and FCIP links. The SAN-OS can also be configured to load balance across multiple same-cost FSPF routes.

Fibre Channel Write Acceleration

Fibre Channel Write Acceleration reduces I/O latency and extends the distance for disaster-recovery and business-continuity applications over MANs. This feature is only available on the Cisco MDS 9000 Family Storage Services Module (SSM) and Cisco MDS 9000 Family Advanced Services Module (ASM).

iSCSI and SAN Extension Performance Enhancements

iSCSI and FCIP enhancements address out-of-order delivery issues, optimize transfer sizes for the IP network topology, and reduce latencies by eliminating TCP connection setup for most data transfers. FCIP performance is further enhanced for SAN extension by compression and write acceleration.

For WAN performance optimization, the SAN-OS includes a SAN Extension Tuner. It directs SCSI I/O commands to a specific virtual target and reports I/Os per second and I/O latency results, which helps determine the number of concurrent I/Os needed to maximize FCIP throughput.

FCIP Compression

FCIP compression in the SAN-OS increases the effective WAN bandwidth without costly infrastructure upgrades. By integrating data compression in the Cisco MDS 9000 Family, more efficient FCIP-based business-continuity and disaster-recovery solutions can be implemented without needing to add and manage a separate device. Gigabit Ethernet ports for IP Storage Services achieve up to a 30:1 compression ratio, with typical ratios of 2:1 over a wide variety of data sources.

FCIP Tape Acceleration

Centralizing tape-backup and archive operations provides significant cost saving by allowing expensive robotic tape libraries and high-speed drives to be shared. This poses a challenge for remote backup media servers that need to transfer data across a WAN. High-performance streaming tape drives require a continuous flow of data to avoid write data underruns dramatically reduces write throughput.
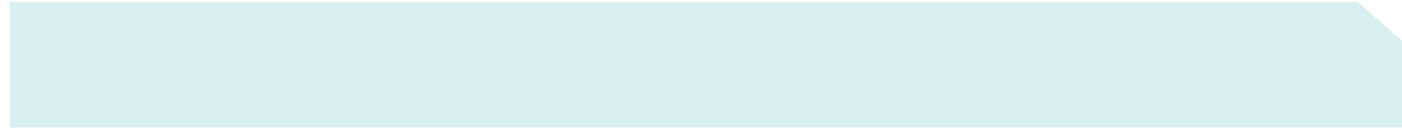
Without FCIP Tape Acceleration, the effective WAN throughput for remote tape backup decreases exponentially as the WAN latency increase. FCIP Tape Acceleration helps achieve near full throughput over WAN links for remote tape-backup operations.

SERVICEABILITY—TROUBLESHOOTING AND DIAGNOSTICS

The SAN-OS is the first storage network OS to provide a wide set of serviceability features that simplify the process of building, expanding, and maintaining SANs. These features also increase availability by minimizing SAN disruptions for maintenance and reducing recovery time from critical problems.

Switched Port Analyzer and Cisco Fabric Analyzer

Typically, debugging errors in a Fibre Channel SAN requires the use of a Fibre Channel analyzer. This causes significant disruption of traffic in the SAN. The Switched Port Analyzer (SPAN) feature allows an administrator to analyze all traffic between ports (called the SPAN source ports) by nonintrusively directing the SPAN session traffic to a SPAN destination port that has an external analyzer attached to it. The SPAN destination port does not have to be on the same switch as the SPAN source ports; any Fibre Channel port in the fabric can be a source. SPAN sources may include Fibre Channel ports and FCIP and iSCSI virtual ports for IP services.

The embedded Cisco Fabric Analyzer feature allows the Cisco MDS 9000 Family to save Fibre Channel control traffic inside the switch for text-based analysis, or send IP-encapsulated Fibre Channel control traffic to a remote PC for decoding and display using the open-source Ethereal network analyzer application. It is therefore possible to capture and analyze Fibre Channel control traffic without an expensive Fibre Channel analyzer.

SCSI Flow Statistics

LUN-level SCSI Flow Statistics can be collected for any combination of initiator and target. The scope of these statistics includes read, write, control commands, and error statistics. This feature is only available on the SSM and ASM.

Fibre Channel Ping and Fibre Channel Traceroute Features

SAN-OS brings to storage networks features such as Fibre Channel Ping and Fibre Channel Traceroute that are essential for IP network troubleshooting. With Fibre Channel Ping, administrators can check the connectivity of an N-Port and determine its round-trip latency, while Fibre Channel Traceroute enables them to check the reachability of a switch by tracing the path followed by frames and determining hop-by-hop latency.

Call Home

The SAN-OS offers a Call Home feature for proactive fault management. Call Home provides a notification system triggered by software and hardware events. The Call Home feature forwards the alarms and events packaged with other relevant information in a standard format to external entities. Alert grouping capabilities and customizable destination profiles offer the flexibility needed to notify specific individuals or support organizations only when necessary. These notification messages can be used to automatically open technical assistance tickets and resolve problems before they become critical. External entities can include, but are not restricted to, an administrator's e-mail account or pager, a server in-house or at a service provider's facility, or the Cisco Technical Assistance Center (TAC).

System Log

The Cisco MDS 9000 Family system log (syslog) capabilities greatly enhance debugging and management. Syslog severity levels can be set individually for all SAN-OS facilities, facilitating logging and display of messages ranging from brief summaries to very detailed information for debugging. Messages can be selectively routed to a console and log files. Messages are logged internally and they can be sent to external syslog servers.

Other Serviceability Features

Additional serviceability features include the following:

- Online diagnostics—Advanced online diagnostics capabilities are provided by the SAN-OS. Periodically tests are run to verify that supervisor engines, switching modules, and interconnections are functioning properly. These online diagnostics do not adversely affect normal Fibre Channel operations, allowing them to be run in production SAN environments.
- Loopback testing—The Cisco MDS 9000 Family uses offline port loopback testing to check port capability. During testing, a port is isolated from the external connection and traffic is looped internally from the transmit path back to the receive path.
- IP-over-Fibre Channel—The Cisco MDS 9000 Family provides the capability to carry IP packets over a Fibre Channel network. With this feature, an external management station attached through an OOB management port to a Cisco MDS 9000 Family switch in the fabric has the ability to manage all other switches in the fabric using the in-band IP-over-Fibre Channel Protocol.
- Network Time Protocol (NTP) support—The NTP synchronizes system clocks in the fabric, providing a precise time base for all switches. An NTP server must be accessible from the fabric through the OOB Ethernet port. Within the fabric, NTP messages are transported using IP-over-Fibre Channel.

- Enhanced event logging and reporting using SNMP traps and syslog—Cisco MDS 9000 Family events filtering and Remote Monitoring (RMON) provide complete and exceptionally flexible control over SNMP traps. Traps can be generated based on a threshold value, switch counters, or time stamps. Syslog provides a rich, supplemental source of information for managing Cisco MDS 9000 Family switches. Messages ranging from only high-severity events to detailed debugging messages can be logged if desired.

APPENDIX A—LICENSED SAN-OS SOFTWARE PACKAGES

Most Cisco MDS 9000 Family software features are included in the base configuration of the switch, the "Standard package." However, some features are logically grouped into add-on packages that must be licensed separately, such as the Cisco MDS 9000 Family Enterprise package, Cisco MDS 9000 Family SAN Extension Over IP package, Cisco MDS 9000 Family Mainframe package, Cisco MDS 9000 Family Fabric Manager Server package, and Cisco MDS 9000 Family Storage Services Enabler package.

Enterprise Package

The Standard software package that is bundled at no charge with the Cisco MDS 9000 Family switches includes the base set of features that Cisco believes are required by most customers for building a SAN. The Cisco MDS 9000 Family also has a set of advanced features, which are recommended for all enterprise SANs. These features are bundled together in the Cisco MDS 9000 Enterprise package. Please see the Cisco MDS 9000 Family Enterprise package fact sheet.

SAN Extension over IP Package

The SAN Extension package facilitates FCIP for IP Storage Services and allows the customer to use the IP Storage Services to extend SANs over wide distances on IP networks. Please see the Cisco MDS 9000 SAN Extension over IP package fact sheet.

Mainframe Package

The Mainframe package uses the FICON protocol and allows control unit port (CUP) management for in-band management from IBM S/390 or z/900 processors. FICON VSAN support is provided to help ensure that there is true hardware-based separation of FICON and open systems. Switch cascading, fabric binding, and intermixing are also included in this package. Please see the Cisco MDS 9000 Family Mainframe package fact sheet.

Fabric Manager Server Package

The Standard Cisco Fabric Manager and Devices Manager applications bundled at no charge with the Cisco MDS 9000 Family provide basic configuration and troubleshooting capabilities. The Fabric Manager Server package extends Cisco Fabric Manager by providing historical performance monitoring for network traffic hotspot analysis, centralized management services, and advanced application integration for greater management efficiency. Please see the Cisco MDS 9000 Family Fabric Manager Server package fact sheet.

Storage Services Enabler Package

The Storage Services Enabler package enables network-hosted storage applications to run on the Cisco MDS 9000 Family Advanced Services Module (ASM). Network-hosted storage applications such as VERITAS Storage Foundation for Networks allow companies to simplify complex IT storage environments and gain control of capital and operating costs by providing consistent and automated management of storage. A Storage Services Enabler package must be installed on each ASM in order for a licensed version of VERITAS Storage Foundations for Networks to run on the module. Please see the Cisco MDS 9000 Family Storage Services Enabler package fact sheet.

The SAN-OS Software package fact sheets are available at:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/products_data_sheets_list.html

CISCO SYSTEMS