Cisco MDS 9000 NX-OS Software Release 4.2

Product Overview

Cisco® MDS 9000 NX-OS Software is the underlying system software that powers the award-winning Cisco MDS 9000 Family multilayer switches. Cisco MDS 9000 NX-OS is designed for data center switches to create a strategic platform with superior reliability, performance, scalability, and features.

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

Flexibility and Scalability

Cisco MDS 9000 NX-OS is a highly flexible and scalable platform for enterprise SANs.

Common Software Across All Platforms

Cisco MDS 9000 NX-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 helps Cisco provide an extensive, consistent, and compatible feature set across the Cisco MDS 9000 Family. In addition, Cisco MDS 9000 NX-OS also runs on the entire Cisco Nexus family of Data Center Ethernet switches, providing a common software infrastructure for the evolution of unified fabrics.

Multiprotocol Support

In addition to supporting Fibre Channel Protocol (FCP), Cisco MDS 9000 NX-OS 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 consolidate storage for a wide range of servers into a common pool on the SAN. Native FCIP support allows customers take advantage of their existing investment in IP networks for cost-effective business-continuance solutions for both Fibre Channel and FICON environments. With Cisco MDS 9000 NX-OS multiprotocol support, customers can better use their enterprise resources, thereby lowering costs. Servers using the Fibre Channel over Ethernet (FCoE) standard can connect to Cisco MDS 9000 SANs via the Cisco Nexus 5000 Series Switches.

Virtual SANs

Virtual SAN (VSAN) technology partitions a single physical SAN into multiple VSANs. The Cisco MDS 9000 Family switches led the market with VSAN support built into the switch hardware, and have the most mature and comprehensive support for this implementation of the industry "virtual fabric" standard. VSAN capabilities allow Cisco MDS 9000 NX-OS to logically divide a large physical fabric into separate, isolated environments to improve Fibre Channel SAN scalability, availability, manageability, and security. For mainframe environments, VSANs facilitate 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 are confined within the VSAN's 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, and other roles can be set up to allow configuration and management only within specific VSANs. This approach improves the manageability of large SANs and reduces disruptions resulting from to human error by isolating the effect of a user's action to a specific VSAN whose membership can be assigned based on the switch ports or the worldwide names (WWNs) 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. F-port trunking allows multiple VSANs on a single uplink in N-port virtualization (NPV) mode.

Inter-VSAN Routing

Data traffic can be transported between specific initiators and targets on different VSANs using inter-VSAN routing (IVR) 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 IVR. Valuable resources such as tape libraries can be easily shared without compromise. IVR also can be used in conjunction with FCIP to create more efficient business continuity and disaster recovery solutions.

Intelligent Fabric Applications

Cisco MDS 9000 NX-OS forms a solid foundation for delivering network-based storage applications and services such as virtualization, snapshots, continuous data protection, data migration, and replication on Cisco MDS 9000 Family switches. The Fabric Application Interface Standard (FAIS)–based API and the SANTap protocol accommodate sophisticated partner applications. The Cisco MDS 9000 Family intelligent fabric applications make use of all Fibre Channel features and services offered by Cisco MDS 9000 NX-OS, simplifying security, diagnostics, and management.

Network-Hosted Applications

The Cisco MDS 9000 Family network-hosted storage applications architecture overcomes inherent bottlenecks associated with other virtualization architectures. Performance can be easily scaled to levels required by the largest organizations. Because Cisco MDS 9000 Family network-hosted storage applications are switch based, any host can access any virtual volume in the fabric, independent of the host's attachment point in the SAN. A single point of management, transparent data mobility and migration, improved storage use, and a single set of copy services across heterogeneous storage capabilities are supported for Cisco MDS 9000 Family network-hosted applications.

Network-Assisted Applications

Cisco MDS 9000 Family network-assisted storage applications offer deployment flexibility and investment protection by allowing appliance-based storage applications for any server or storage device in the SAN without rewiring. Easy insertion and provisioning of appliance-based storage applications are achieved by moving the appliance out of the primary I/O between servers and storage. Also, host-side agents are reduced or eliminated, simplifying heterogeneous OS support.

The SANTap protocol allows appliances to get an I/O copy for data replication, continuous data protection, and data migration without affecting the integrity, availability, and performance of the primary I/O between servers and storage. Cisco MDS 9000 Family network-assisted storage applications with SANTap provide highly scalable solutions that allow efficient workload distribution to multiple appliances based on the application and the source and target combination.

Cisco Storage Media Encryption

Cisco Storage Media Encryption (SME) provides a complete, integrated solution for encryption of data at rest on heterogeneous tape drives and virtual tape libraries (VTLs) in SAN environments. Storage in any VSAN can fully utilize Cisco SME capabilities, providing exceptional flexibility for provisioning this transparent fabric service. Cisco SME requires no SAN reconfiguration or rewiring, eliminating downtime for deployment. Cisco SME employs clustering technology to enhance reliability and availability, enable automated load-balancing and failover capabilities, and simplify provisioning. This encryption service is managed as a single, logical feature rather than within individual switches or modules. Secure lifecycle key management is included, with essential features such as key archival, shredding, and export and import for single- and multiple-site environments. Cisco SME provisioning and key management are both integrated into Cisco Fabric Manager; no additional software is required for management.

Secure Erase

The Cisco MDS 9000 Secure Erase feature is a SAN-based intelligent fabric application offering capabilities to erase data on a given target. It erases data in such a way that reconstructing that data is essentially impossible. The Secure Erase process runs over the Internet Server API (ISAPI) platform, and the write operations are performed by the virtual initiators created for this purpose. The hosts or servers connected to the SAN have no role in this process. SAN-based Secure Erase has numerous advantages over traditional data erase mechanisms such as high speed, low cost, ease of execution, and platform independence.

Cisco Data Mobility Manager

Cisco Data Mobility Manger (DMM) is a SAN-based, intelligent fabric application offering data migration between heterogeneous disk arrays. Cisco DMM offers rate-adjusted online migration to enable applications to continue uninterrupted while data migration is in progress. Advanced capabilities such as data verification, unequal size logical unit (LUN) migration, and multipath support provide flexibility and meet the high-availability requirements of enterprise data centers. Cisco DMM is transparent to host applications and storage devices. It can be introduced without the need to rewire or reconfigure the SAN. Cisco Fabric Manager is used to administer Cisco DMM; no additional management software is required.

I/O Accelerator

The Cisco MDS 9000 I/O Accelerator (IOA) feature is a SAN-based intelligent fabric application that provides SCSI acceleration to dramatically improve the number of SCSI I/O operations per second over long distances in a Fibre Channel or Fibre Channel over IP (FCIP) SAN by reducing the effect of transport latency on the processing of each operation. The feature also extends the distance for disaster recovery and business continuity applications over WANs and metropolitan area networks (MANs). IOA can be deployed in conjunction with disk data replication solutions such as EMC Symmetrix Remote Data Facility (SRDF) and MirrorView and HDS TrueCopy to extend the distance between data centers or reduce the effects of latency. IOA can also be used to enable remote tape backup and restore operations without significant throughput degradation. IOA includes the following features:

- **Transport independent:** IOA provides a unified solution to accelerate I/O operations over the MAN and WAN.
- **IOA as a fabric service:** IOA service units (interfaces) can be located anywhere in the fabric and can provide acceleration service to any port.
- **Speed independent:** IOA can accelerate 1/2/4/8/10-Gbps links and consolidate traffic over 8/10-Gbps ISLs.
- **Write acceleration:** IOA provides write acceleration for Fibre Channel and FCIP networks. Write acceleration significantly reduces latency and extends the distance for disk replication.

- **Tape acceleration:** IOA provides tape acceleration for Fibre Channel and FCIP networks. Tape acceleration improves the performance of tape devices and enables remote tape vaulting over extended distances for data backup for disaster recovery purposes.
- **Compression:** Compression in IOA increases the effective MAN and WAN bandwidth without the need for costly infrastructure upgrades. Integrating data compression into IOA enables implementation of more efficient Fibre Channel– and FCIP–based business continuity and disaster recovery solutions without the need to add or manage a separate device.
- **High availability and resiliency:** IOA combines PortChannels and equal-cost multipath (ECMP) routing with disk and tape acceleration for higher availability and resiliency.
- **Service clustering:** IOA delivers redundancy and load balancing for I/O acceleration.
- **Transparent insertion:** IOA requires no fabric reconfiguration or rewiring and can be transparently turned on by enabling the IOA license.
- **Intuitive provisioning:** IOA can be easily provisioned using Cisco MDS 9000 Fabric Manager.

XRC Acceleration

IBM Extended Remote Copy (XRC), which is now officially renamed IBM z/OS Global Mirror, is a mainframe-based software replication solution in widespread use in financial institutions worldwide. In the past, Cisco has supported XRC over FCIP at distances of up to 124 miles (200 km) on the Cisco MDS 9000 18/4-Port Multiservice Module. The new Cisco MDS 9000 XRC Acceleration feature supports essentially unlimited distances. XRC Acceleration accelerates dynamic updates from the primary to the secondary direct-access storage device (DASD) by reading ahead of the remote replication IBM System z, known as the System Data Mover (SDM). This data is buffered within the Cisco MDS 9000 module that is local to the SDM, reducing or eliminating the latency effects that can otherwise reduce performance at distances of 124 miles (200 km) or greater. This process is sometimes referred to as XRC emulation or XRC extension.

More information about the Cisco MDS 9000 Family intelligent fabric applications is available at http://www.cisco.com/en/US/products/ps6028/index.html.

Network Security

Cisco takes a comprehensive approach to network security with Cisco MDS 9000 NX-OS. In addition to VSANs, which provide true isolation of SAN-attached devices, Cisco MDS 9000 NX-OS offers numerous security features. Cisco MDS 9000 Family management has been certified for Federal Information Processing Standards (FIPS) 140-2 Level 2 and validated for Common Criteria (CC) Evaluation Assurance Level 3 (EAL 3).

Switch and Host Authentication

Fibre Channel Security Protocol (FC-SP) capabilities in Cisco MDS 9000 NX-OS provide switch-to-switch and host-to-switch authentication for enterprisewide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) is 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 Cisco MDS 9000 NX-OS offer secure authentication, data encryption for privacy, and data integrity for both FCIP and iSCSI connections on the Cisco MDS 9000 Family. Cisco MDS 9000 NX-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.

Cisco TrustSec Fibre Channel Link Encryption

Cisco TrustSec Fibre Channel Link Encryption addresses customer needs for data integrity and privacy. Cisco TrustSec Fibre Channel Link Encryption is an extension of the FC-SP feature and uses the existing FC-SP architecture. Starting with Cisco MDS 9000 NX-OS 4.2(1), Fibre Channel data between E-ports of Cisco MDS 9000 8-Gbps Fibre Channel Switching modules can be encrypted. The encryption algorithm is 128-bit Advanced Encryption Standard (AES) and enables either AES-Galois/Counter Mode (GCM) or AES-Galois Message Authentication Code (AES-GMAC) for an interface. AES-GCM encrypts and authenticates frames, and AES-GMAC authenticates only the frames that are being passed between the two E-ports. Encryption is performed at line rate by encapsulating frames at egress with encryption using the GCM mode of AES 128-bit encryption. At ingress, frames are decrypted and authenticated with integrity check. There are two primary use cases for Cisco TrustSec Fibre Channel Link Encryption. Many customers will want to ensure the privacy and integrity of any data that leaves the secure confines of their data center via a native Fibre Channel link, such as dark fiber, Coarse Wavelength-Division Multiplexing (CWDM), or Dense Wavelength-Division Multiplexing (DWDM). Other customers, such as those in defense and intelligence services, may be even more security-focused and choose to encrypt all traffic within their data center as well, since the encryption is at full line rate with no performance penalty.

Role-Based Access Control

Cisco MDS 9000 NX-OS provides role-based access control (RBAC) for management access to the Cisco MDS 9000 Family command-line interface (CLI) and Simple Network Management Protocol (SNMP). In addition to the two default roles on the switch, up to 64 user-defined roles can be configured. Applications using SNMP Version 3 (SNMPv3), such as Cisco Fabric Manager, offer 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 also are 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 WWNs. This locking helps ensure that unauthorized devices connecting to the switch port do not disrupt the SAN fabric. Fabric binding extends port security to allow ISLs only between specified switches.

Zoning

Zoning provides access control for devices within a SAN. Cisco MDS 9000 NX-OS supports the following types of zoning:

- **N-port zoning:** Defines zone members based on the end-device (host and storage) port
  - WWN
  - Fibre Channel identifier (FC-ID)
- **Fx-port zoning:** Defines zone members based on the switch port
  - WWN
  - WWN plus interface index, or domain ID plus interface index
  - Domain ID plus port number (for Brocade interoperability)
- **iSCSI zoning:** Defines zone members based on the host zone
  - iSCSI name
  - IP address
- **LUN zoning:** When combined with N-port zoning, helps ensure that LUNs are accessible only by specific hosts, providing a single point of control for managing heterogeneous storage-subsystem access

- **Read-only zones:** When an attribute is set for a zone type, restricts I/O operations in that zone type to SCSI read-only commands; this feature is especially useful for sharing volumes across servers for backup, data warehousing, etc.
- **Broadcast zones:** When an attribute is set for a zone type, restricts broadcast frames to members of that 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 none of them cause performance degradation. Enhanced zoning session-management capabilities further enhance security by allowing only one user at a time to modify zones.

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 protection of file transfers
- AES, Message Digest Algorithm 5 (MD5), and Secure Hash Algorithm 1 (SHA 1) for secure authentication and management
- IP ACLs for management and Gigabit Ethernet ports
- Microsoft CHAP (MS-CHAP) to secure the management interface between Cisco MDS 9000 Family switches and RADIUS servers
- Digital certificates using public key infrastructure (PKI) for IPsec

Availability

Cisco MDS 9000 NX-OS provides resilient software architecture for mission-critical hardware deployments.

Nondisruptive Software Upgrades

Cisco MDS 9000 NX-OS provides nondisruptive software upgrades for director-class products with redundant hardware and 4-Gbps fabric switches. Minimally disruptive upgrades are provided for the other Cisco MDS 9000 Family fabric switches that do not have redundant supervisor engine hardware.

Stateful Process Failover

Cisco MDS 9000 NX-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.

ISL Resiliency Using PortChannels

PortChannels aggregate multiple physical 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) or F-ports connected to NP-ports can be bundled into a PortChannel. ISL ports can reside on any switching module, and they do not need a designated master port. Thus, if a port or a switching module fails, the PortChannel continues to function properly without requiring fabric reconfiguration.

Cisco MDS 9000 NX-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

The 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 feature 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 autotrespass feature enables high-availability iSCSI connections to RAID subsystems, independent of host software. Trespass commands can be sent automatically when Cisco MDS 9000 NX-OS detects failures on active paths.

Port Tracking for Resilient SAN Extension

SAN extension resiliency is enhanced by the Cisco MDS 9000 NX-OS port-tracking feature. If a Cisco MDS 9000 Family switch detects a WAN or MAN link failure, it takes down the associated disk-array link when port tracking is configured, so the array can redirect a failed I/O operation 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.

SAN Device Virtualization

Cisco SAN device virtualization (SDV) allows virtual devices representing physical end-devices to be used for SAN configuration. Virtualization of SAN devices significantly reduces the time needed to swap out hardware. For example, if a storage array were replaced without using SDV, server downtime would be required for SAN zoning changes and host operating system configuration updates. With SDV, only the mapping between virtual and physical devices needs to change after hardware is swapped, insulating the SAN and end devices from extensive configuration changes.

Manageability

Cisco MDS 9000 NX-OS incorporates many management features that facilitate effective management of growing storage environments with existing resources. Cisco fabric services simplify SAN provisioning by automatically distributing configuration information to all switches in a storage network. Distributed device alias services provide fabricwide alias names for host bus adapters (HBAs), storage devices, and switch ports, eliminating the need to reenter names when devices are moved.

Management interfaces supported by Cisco MDS 9000 NX-OS include the following:

- CLI through a serial port or out-of-band (OOB) Ethernet management port, and in-band IP over Fibre Channel (IPFC)
- SNMPv1, v2, and v3 over OOB management port and in-band IPFC
- Cisco FICON Control Unit Port (CUP) for in-band management from IBM S/390 and z/900 processors
- IPv6 support for iSCSI, FCIP, and management traffic routed in band and out of band

Cisco Fabric Manager and Cisco 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 fabricwide management capabilities, including discovery, multiple switch configurations, real-time network

monitoring, historical performance monitoring for network traffic hotspot analysis, and troubleshooting. This powerful approach greatly reduces switch setup times, increases overall fabric reliability, and provides extensive diagnostics for resolving configuration inconsistencies.

More information about Cisco MDS 9000 Family SAN management is available at http://www.cisco.com/en/US/products/ps6030/index.html.

CLI Similar to Cisco IOS Software

Cisco MDS 9000 NX-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 capabilities. 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

Cisco MDS 9000 NX-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 use the Cisco MDS 9000 NX-OS management API.

Fabric Device Management Interface (FDMI) capabilities provided by Cisco MDS 9000 NX-OS simplify management of devices such as Fibre Channel HBAs though in-band communications. With FDMI, management applications can gather HBA and host OS information without installing proprietary host agents.

Cisco MDS 9000 NX-OS provides an 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.

Configuration and Software-Image Management

The CiscoWorks solution is a commonly used suite of tools for a wide range of Cisco devices such as IP switches, routers, and wireless devices. The Cisco MDS 9000 NX-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 log (syslog) management, and inventory management. The open API also helps CiscoWorks Device Fault Manager (DFM) monitor Cisco MDS device health, such as supervisor memory and processor utilization. The health of important components such as fans, power supplies, and temperature also can be monitored by CiscoWorks DFM.

N-Port Virtualization

Cisco MDS 9000 NX-OS supports industry-standard N-port identifier virtualization (NPIV), which allows multiple N-port fabric logins concurrently on a single physical Fibre Channel link. HBAs that support NPIV can help improve SAN security by enabling configuration of zoning and port security independently for each virtual machine (OS partition) on a host. In addition to being useful for server connections, NPIV is beneficial for connectivity between core and edge SAN switches.

NPV is a complementary feature that reduces the number of Fibre Channel domain IDs in core-edge SANs. Cisco MDS 9000 Family fabric switches operating in the NPV mode do not join a fabric; they just pass traffic between core switch links and end devices, which eliminates the domain IDs for these switches. NPIV is used by edge switches in the NPV mode to log in to multiple end devices that share a link to the core switch. This feature is available only for Cisco MDS 9000 Family blade switches and the Cisco MDS 9124 and 9134 Multilayer Fabric Switches.

Autolearn for Network Security Configuration

The autolearn 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.

FlexAttatch

Cisco MDS 9000 NX-OS supports the FlexAttatch feature. One of the main problems faced today in SAN environment is the time and effort required to install and replace servers. The process involves both SAN and server administrators, and the interaction and coordination between them can make the process time consuming. To alleviate the need for interaction between SAN and server administrators, the SAN configuration should not be changed when a new server is installed or an existing server is replaced. FlexAttach addresses these problems, reducing configuration changes and the time and coordination required by SAN and server administrators when installing and replacing servers. This feature is available only for Cisco MDS 9000 Family blade switches and the Cisco MDS 9124 and 9134 when NPV mode is enabled.

Host Provisioning Wizard

The Cisco Fabric Manager Host Provisioning Wizard enables customers to move existing host and storage nodes using a single management tool. The wizard provides the requisite utilities for transparent migration operations.

The wizard allows the administrator to quickly commission or decommission hosts and:

- Create a device alias for the host
- Create a Dynamic Port VSAN Membership (DPVM) entry for the host
- Add the host and storage to a zone and activate the zone
- Create a flow between the host and storage for performance monitoring

Cisco Fabric Manager Server Federation

Cisco Fabric Manager Server (FMS) federation improves management availability and scalability by load balancing fabric discovery, performance monitoring, and event handling processes. Cisco Fabric Manager provides a single management pane for viewing and managing all fabrics within a single federation. A storage administrator can discover and move fabrics within a federation for the purposes of load balancing, high availability, and disaster recovery. In addition, users can connect to any Cisco FMS and view all reports, inventory, statistics, and logs from a single web browser. Up to 10 Cisco FMSs can form a federation (or cluster) that can manage more than 150,000 end devices.

Network Boot for iSCSI Hosts

Cisco MDS 9000 NX-OS simplifies iSCSI-attached host management by providing network-boot capability.

Internet Storage Name Service

The Internet Storage Name Service (iSNS) helps existing TCP/IP networks function more effectively as SANs by automating discovery, management, and configuration of iSCSI devices. iSCSI targets presented by Cisco MDS 9000 Family IP storage services and Fibre Channel device-state-change notifications are registered by Cisco MDS 9000 NX-OS, either through the highly available, distributed iSNS built into Cisco MDS 9000 NX-OS or through external iSNS servers.

Proxy iSCSI Initiator

The proxy iSCSI initiator 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.

iSCSI Server Load Balancing

Cisco MDS 9000 NX-OS helps simplify large-scale deployment and management of iSCSI servers. In addition to allowing fabricwide iSCSI configuration from a single switch, iSCSI server load balancing (iSLB) is available to automatically redirect servers to the next available Gigabit Ethernet port. iSLB greatly simplifies iSCSI configuration and provides automatic, rapid recovery from IP connectivity problems for high availability.

IPv6

Cisco MDS 9000 NX-OS provides IPv6 support for FCIP, iSCSI, and management traffic routed in band and out of band. A complete dual stack has been implemented for IPv4 and IPv6 to remain compatible with the large base of IPv4-compatible hosts, routers, and Cisco MDS 9000 Family switches running previous software revisions. This dual-stack approach allows the Cisco MDS 9000 Family switches to easily connect to older IP networks, transitional networks with a mixture of both versions, and pure IPv6 data networks.

Traffic Management

In addition to implementing the Fabric Shortest Path First (FSPF) protocol to calculate the best path between two switches and providing in-order delivery features, Cisco MDS 9000 NX-OS enhances the architecture of the Cisco MDS 9000 Family with several advanced traffic-management features that help ensure consistent performance of the SAN under 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 fabricwide protocols such as FSPF, zone merges, and principal switch selection.

Data traffic can be classified for QoS by the VSAN identifier, zone, N-port WWN, 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 receipt of an explicit notification, the ingress switch throttles the N-port or NL-port traffic by reducing the buffer-to-buffer credits.

Extended Credits

Full line-rate Fibre Channel ports provide at least 255 buffer credits standard. Adding credits lengthens distances for Fibre Channel SAN extension. Using extended credits, up to 4095 buffer credits from a pool of more than 6000 buffer credits for a module can be allocated to ports as needed to greatly extend the distance for Fibre Channel SANs.

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 so that the presence of a slow N-port on the SAN does not affect the performance of any other port on the SAN.

Fibre Channel Port Rate Limiting

The Fibre Channel port rate-limiting feature for the Cisco MDS 9100 Series Multilayer Fabric Switches controls the amount of bandwidth available to individual Fibre Channel ports within groups of four host-optimized ports. Limiting bandwidth on one or more Fibre Channel ports allows the other ports in the group to receive a greater share of the available bandwidth under high-utilization conditions. Port rate limiting is also beneficial for throttling WAN traffic at the source to help eliminate excessive buffering in Fibre Channel and 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. Cisco MDS 9000 NX-OS also can be configured to load balance across multiple same-cost FSPF routes.

iSCSI and SAN Extension Performance Enhancements

iSCSI and FCIP enhancements address out-of-order delivery problems, optimize transfer sizes for the IP network topology, and reduce latency 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, Cisco MDS 9000 NX-OS includes a SAN extension tuner, which directs SCSI I/O commands to a specific virtual target and reports I/O operations per second and I/O latency results, helping determine the number of concurrent I/O operations needed to increase FCIP throughput.

FCIP Compression

FCIP compression in Cisco MDS 9000 NX-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 the need to add and manage a separate device. Gigabit Ethernet ports for the Cisco MDS 9222i Multiservice Modular Switch, the MDS 9000 18/4-Port Multiservice Module, and the MDS 9000 16-Port Storage Services Node achieve up to a 43:1 compression ratio, with typical ratios of 4:1 over a wide variety of data sources.

FCIP Tape Acceleration

Centralizing tape backup and archive operations provides significant cost savings by allowing expensive robotic tape libraries and high-speed drives to be shared. This centralization 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, which dramatically reduce write throughput.

Without FCIP tape acceleration, the effective WAN throughput for remote tape operations decreases exponentially as the WAN latency increases. FCIP tape acceleration helps achieve nearly full throughput over WAN links for remote tape-backup operations for both open systems and mainframe environments, and restore operations for open systems.

Serviceability, Troubleshooting, and Diagnostics

Cisco MDS 9000 NX-OS is among 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 decreasing SAN disruptions for maintenance and reducing recovery time from problems.

Switched Port Analyzer and Cisco Fabric Analyzer

Typically, debugging errors in a Fibre Channel SAN require the use of a Fibre Channel analyzer, which 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 can include Fibre Channel ports and FCIP and iSCSI virtual ports for IP services.

The embedded Cisco Fabric Analyzer allows the Cisco MDS 9000 Family to save Fibre Channel control traffic inside the switch for text-based analysis, or to send IP-encapsulated Fibre Channel control traffic to a remote PC for decoding and display using the open-source Ethereal network-analyzer application. Fibre Channel control traffic therefore can be captured and analyzed 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, and control commands and error statistics. This feature is available only on the Cisco MDS 9000 Family storage service modules.

Fibre Channel Ping and Fibre Channel Traceroute Features

Cisco MDS 9000 NX-OS brings to storage networks features such as Fibre Channel Ping and Fibre Channel Traceroute, which 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, and with Fibre Channel Traceroute, administrators can check the reachability of a switch by tracing the path followed by frames and determining hop-by-hop latency.

Call Home

Cisco MDS 9000 NX-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 email account or pager, a server in-house or at a service provider’s facility, and the Cisco Technical Assistance Center (TAC).

System Log

The Cisco MDS 9000 Family syslog capabilities greatly enhance debugging and management. Syslog severity levels can be set individually for all Cisco MDS 9000 NX-OS functions, 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 to 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:** Cisco MDS 9000 NX-OS provides advanced online diagnostics capabilities. Periodically tests are run to verify that supervisor engines, switching modules, optics, 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 capabilities. During testing, a port is isolated from the external connection, and traffic is looped internally from the transmit path back to the receive path.
- **IPFC:** 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 can manage all other switches in the fabric using the in-band IPFC protocol.

- **Network Time Protocol (NTP) support:** 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 IPFC.
- **Enhanced event logging and reporting with 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.

Licensed Cisco MDS 9000 NX-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 Enterprise Package, SAN Extension over IP Package, Mainframe Package, Fabric Manager Server Package, Storage Services Enabler Package, Storage Media Encryption Package, Data Mobility Manager Package, I/O Accelerator Package, and the XRC Acceleration Package. On-demand port activation licenses are also available for the Cisco MDS 9000 Family blade switches and 4-Gbps Cisco MDS 9100 Series Multilayer Fabric Switches.

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 that are recommended for all enterprise SANs. These features are bundled together in the Cisco MDS 9000 Enterprise Package. Refer to the Cisco MDS 9000 Enterprise Package fact sheet for more information.

SAN Extension over IP Package

The Cisco MDS 9000 SAN Extension over IP Package allows the customer to use FCIP to extend SANs over long distances on IP networks using the Cisco MDS 9000 Family IP storage services. Refer to the Cisco MDS 9000 SAN Extension over IP Package data sheet for more information.

Mainframe Package

The Cisco MDS 9000 Mainframe Package uses the FICON protocol and allows IBM CUP management for in-band management from IBM S/390 and z/900 processors. FICON VSAN support is provided to help ensure true hardware-based separation of FICON and open systems. Switch cascading, fabric binding, and intermixing also are included in this package. Refer to the Cisco MDS 9000 Mainframe Package data sheet for more information.

Fabric Manager Server Package

The standard Cisco Fabric Manager and Device Manager applications bundled at no charge with the Cisco MDS 9000 Family provide basic configuration and troubleshooting capabilities. The Cisco FMS 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. Refer to the Cisco FMS Package data sheet for more information.

Storage Services Enabler Package

The Cisco MDS 9000 SSE Package allows network-based storage applications and services to run on the Cisco MDS 9000 Family storage services modules, Cisco MDS 9000 18/4-Port Multiservice Module, and Cisco MDS 9222i.

Intelligent fabric applications simplify complex IT storage environments and help organizations gain control of capital and operating costs by providing consistent and automated storage management. Refer to the Cisco MDS 9000 SSE Package data sheet for more information.

On-Demand Port Activation License

On-demand ports allow customers to benefit from Cisco MDS 9000 NX-OS features while initially purchasing only a small number of activated ports on 4-Gbps Cisco MDS 9100 Series switches. Customers can expand switch connectivity as needed by licensing additional ports.

Storage Media Encryption Package

The Cisco MDS 9000 SME Package enables encryption of data at rest on heterogeneous tape devices and VTLs as a transparent fabric service. Cisco SME is completely integrated with Cisco MDS 9000 Family switches and the Cisco Fabric Manager application, enabling deployment of highly available encryption services without the need to rewire or reconfigure SANs, and allowing easy management of these services without the need to install additional management software. Refer to the Cisco MDS 9000 SME Package data sheet for more information.

Data Mobility Manager Package

The Cisco MDS 9000 DMM Package enables data migration between heterogeneous disk arrays without introducing a virtualization layer or rewiring or reconfiguring SANs. Cisco DMM allows concurrent migration between multiple LUNs of unequal size. Rate-adjusted migration, data verification, dual Fibre Channel fabric support, and management using Cisco Fabric Manager provide a complete solution that greatly simplifies and eliminates most downtime associated with data migration. Refer to the Cisco MDS 9000 DMM Package fact sheet for more information.

I/O Accelerator Package

The Cisco MDS 9000 IOA Package provides SCSI acceleration to dramatically improve the number of SCSI I/O operations per second over long distances in a Fibre Channel or FCIP SAN by reducing the effect of transport latency on the processing of each operation. It also extends the distance for disaster recovery and business continuity applications over WANs and MANs. Refer to the Cisco MDS 9000 IOA Package data sheet for more information.

XRC Acceleration Package

The Cisco MDS 9000 XRC Acceleration Package accelerates dynamic updates from the primary to the secondary DASD by reading ahead of the remote replication IBM System z, known as the SDM. This data is buffered within the Cisco MDS 9000 module that is local to the SDM, reducing or eliminating the latency effects, which can otherwise reduce performance at distances of 124 miles (200 km) or greater. This process is sometimes referred to as XRC emulation or XRC extension. Refer to the Cisco MDS 9000 XRC Acceleration Package data sheet for more information.

For More Information

For more information please visit http://www.cisco.com/go/nxos and http://www.cisco.com/go/storage.

The Cisco MDS 9000 NX-OS package data sheets are available at http://www.cisco.com/en/US/products/hw/ps4159/ps4358/products_data_sheets_list.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Printed in USA C78-550303-00 07/09