Cisco MDS 9000 NX-OS Software Release 7.3

Product Overview

Cisco® MDS 9000 NX-OS Software powers the award-winning Cisco MDS 9000 Family of multilayer switches. It enables data center switches to create a strategic platform with superior reliability, performance, and scalability. Cisco has expanded its unified fabric storage portfolio with enhanced Fibre Channel over Ethernet (FCoE) and Fibre Channel options, unified management, and new fabric services for MDS 9000 Family products and Cisco Nexus® Family switches. These new capabilities enable convergence, scalability, and intelligence across LAN and SAN environments in large, virtualized data centers.

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

Note: This document discusses the features and capabilities supported by Cisco MDS 9000 NX-OS Software Release 7.3 across all Cisco MDS 9000 Family platforms, but not all features may be available on every hardware platform. To determine the features supported on a particular MDS 9000 Family platform, please refer to the data sheet for that specific hardware platform.

Flexibility and Scalability

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

Common Software across All Platforms

MDS 9000 NX-OS runs on all MDS 9000 Family switches, including multilayer fabric switches and multilayer directors. Using the same base system software across the entire product line helps provide an extensive, consistent, and compatible feature set across the MDS 9000 Family. NX-OS also runs on Cisco Nexus Family switches, providing a common software infrastructure for evolving a unified fabric.

Multiprotocol Support

In addition to Fibre Channel Protocol (FCP), MDS 9000 NX-OS supports IBM Fibre Connection (FICON), Small Computer System Interface over IP (iSCSI), FCoE, and Fibre Channel over IP (FCIP). Native iSCSI support in the MDS 9000 Family lets you consolidate storage for a wide range of servers into a common pool on the SAN. FCoE allows an evolutionary approach to I/O consolidation by preserving all Fibre Channel constructs and maintaining the latency, security, and traffic management attributes of Fibre Channel, while preserving investment in Fibre Channel tools, training, and SANs.

FCoE recognizes Fibre Channel as the dominant storage protocol in the data center while offering customers a viable I/O consolidation solution. It simplifies customer environments by using Ethernet and allowing the industry to avoid creation of another, separate protocol for I/O consolidation. Native FCIP support lets you use existing investments in IP networks for cost-effective business-continuity solutions in both Fibre Channel and FICON environments. With MDS 9000 NX-OS multiprotocol support, customers can use their enterprise resources better, thereby lowering costs and reducing business risk.

Virtual SANs

Virtual SAN (VSAN) technology partitions a single physical SAN into multiple VSANs. MDS 9000 Family switches lead the market with VSAN support built into the switch hardware, and they have the most mature and comprehensive support for the industry's virtual fabric standard. VSAN capabilities allow 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 improves network stability considerably by containing fabric reconfiguration settings and error conditions within an individual VSAN. 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, scalability, and resilience. VSANs also help reduce costs by facilitating the consolidation of isolated SAN islands into a common infrastructure without compromising availability, security, or scalability. Users can create SAN administrator roles that are limited in scope to certain VSANs. For example, a SAN 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 within specific VSANs only. This approach improves the manageability of large SANs and reduces disruptions resulting from human errors by isolating the effect of a SAN administrator's action to a specific VSAN whose membership can be isolated based on the switch ports or World Wide Names (WWNs) of attached devices.

VSANs are supported across FCIP links between SANs, extending VSANs to include devices at remote locations. The 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 can also be used in conjunction with FCIP to create more efficient business-continuity and disaster-recovery solutions.

Intelligent Fabric Applications

MDS 9000 NX-OS provides a solid foundation for delivery of network-based storage applications and services such as virtualization, snapshots, continuous data protection, data acceleration, data migration, and replication on MDS 9000 Family switches. MDS 9000 Family intelligent fabric applications use all Fibre Channel features and services offered by MDS 9000 NX-OS, simplifying security, diagnostics, and management.

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

Network-Assisted Applications

MDS 9000 Family network-assisted storage applications offer deployment flexibility and investment protection by allowing the deployment of appliance-based storage applications for any server or storage device in the SAN without the need to rewire SAN switches or end devices. Easy insertion and provisioning of appliance-based storage applications is achieved by eliminating the need to insert the appliance into the primary I/O path between servers and storage devices.

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 operation while data migration is in progress. Advanced capabilities such as data verification, unequal-size logical unit number (LUN) migration, and multipath support provide flexibility and meet the high-availability requirements of enterprise data centers. DMM is transparent to host applications and storage devices, and it can be introduced without the need to rewire or reconfigure the SAN. Cisco Data Center Network Manager (DCNM) for SAN is used to administer Data Mobility Manager; no additional management software is required.

For more information, see http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/product_data_sheet0900aecd80692d6d_ps10729_Products_Data_Sheet.html.

I/O Accelerator

The Cisco MDS 9000 I/O Accelerator (IOA) is a SAN-based intelligent fabric application that provides SCSI acceleration to significantly improve the number of SCSI I/O operations per second (IOPS) over long distances in a Fibre Channel or 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). I/O Accelerator can be deployed in conjunction with disk data-replication solutions such as EMC Symmetrix Remote Data Facility (SRDF), EMC MirrorView, and HDS TrueCopy to extend the distance between data centers or reduce the effects of latency. I/O Accelerator can also be used to enable remote tape backup and restore operations without significant throughput degradation.

I/O Accelerator (IOA) includes the following features:

- Transport independence: 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 independence: IOA can accelerate 1/2/4/8/10/16-Gbps links and consolidate traffic over 8/10/16-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. Integration of 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 port channels 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 Data Center Network Manager for SAN.

For more information, see http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/ps10531/data_sheet_c78-538860.html.

Extended Remote Copy Acceleration

IBM Extended Remote Copy (XRC), which is now officially renamed IBM z/OS Global Mirror, is a mainframe-based software replication solution widely used in financial institutions worldwide. In the past, Cisco has supported XRC over FCIP at distances of up to 124 miles (200 km). 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 MDS 9000 Family 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.

For more information, see http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/ps10526/data_sheet_c78-538834.html.

Network Security

Cisco takes a comprehensive approach to network security with MDS 9000 NX-OS. In addition to VSANs, which provide true isolation of SAN-attached devices, MDS 9000 NX-OS offers other significant security features such as role-based access control (RBAC) and Cisco TrustSec® Fibre Channel Link Encryption and supports the industry-standard security protocol for authentication, authorization, and accounting (AAA). MDS 9000 Family management is 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 MDS 9000 NX-OS provide switch-to-switch and host-to-switch authentication for enterprise wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) is used to perform authentication locally in the MDS 9000 Family director 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 MDS 9000 NX-OS offer secure authentication, data encryption for privacy, and data integrity for both FCIP and iSCSI connections on MDS 9000 Family switches. 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. It is an extension of the FC-SP feature and uses the existing FC-SP architecture. Starting with MDS 9000 NX-OS 4.2(1), Fibre Channel data between E-ports of MDS 9000 8-Gbps Fibre Channel switching modules can be encrypted. Starting with Cisco 9000 NX-OS 6.2(9), the link encryption capability extends to E-ports of MDS 9000 16-Gbps Fibre Channel switching modules. The encryption algorithm is 128-bit Advanced Encryption Standard (AES) and enables either AES-Galois/Counter Mode (AES-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 would want to help ensure the privacy and integrity of any data that leaves the secure confines of their data center through 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, because the encryption is at full line rate with no performance penalty.

Forward Error Correction

Forward error correction (FEC) improves the reliability of links by automatically detecting and recovering from bit errors that occur in high-speed networks. FEC helps reduce or avoid data stream errors that can lead to application performance degradation. Lossy media such as loose transceivers (SFPs), dirty cables, etc. can result in corrupted packets on Inter-Switch Links (ISLs). FEC facilitates recovery from some of these errors, helping improve the reliability of links. All MDS 9000 Family switches can detect and drop corrupt frames at the switch input, but FEC adds another layer of resiliency to help correct errors wherever feasible and reduce the number of packet drops.

Starting with MDS 9000 NX-OS 6.2(7), support for FEC is available for 16-Gbps ISLs on Cisco MDS 9700 Series Multilayer Directors.

Role-Based Access Control

MDS 9000 NX-OS provides RBAC for management access to the MDS 9000 Family command-line interface (CLI) and Simple Network Management Protocol (SNMP). In addition to two default roles on the switch, up to 64 user-defined roles can be configured. Applications using SNMP Version 3 (SNMPv3), such as Data Center Network Manager for SAN, 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 are shared, and only one administrative account is required for each user.

Port Security and Fabric Binding

Port security locks the mapping of an entity to a switch port. The entities can be hosts, targets, or switches, identified by their WWNs. This locking mechanism helps ensure that unauthorized devices connecting to the switch port do not disrupt the SAN fabric. Fabric binding extends port security to allow ISLs between only specified switches.

Zoning

Zoning provides access control for devices within a SAN. In addition, the software provides support for smart zoning, which dramatically reduces operation complexity while consuming fewer resources on the switch. As an alternative to creating multiple two-member zones, smart zoning enables customers to intuitively create fewer multimember zones at an application level, a physical cluster level, or a virtualized cluster level with optimal consumption of switch resources such as memory (ternary content-addressable memory [TCAM]).

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

For strict network security, zoning is always enforced per frame using access control lists (ACLs) 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:

- Fabric-wide role-based AAA services using RADIUS, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory (AD), and TACACS+
- Secure Shell (SSH) Protocol Version 2 and SNMPv3 for authentication, data integrity, and confidentiality of management traffic
- Secure FTP (SFTP) to protect 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 MDS 9000 Family switches and RADIUS servers
- Digital certificates using public key infrastructure (PKI) for IPsec.

Availability

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

Nondisruptive Software Upgrades

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

Stateful Process Failover

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 Port Channels

Port channels 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.

MDS 9000 NX-OS uses a protocol to exchange PortChannel configuration information between adjacent switches. This feature simplifies 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 the availability of MDS 9000 Family management traffic routed over both Ethernet and Fibre Channel networks. VRRP dynamically manages redundant paths for external MDS 9000 Family management applications, making control-traffic path failures transparent to applications.

VRRP also 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 MDS 9000 Family switch.

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

Port Tracking for Resilient SAN Extension

The port-tracking feature enhances SAN extension resiliency. If an MDS 9000 Family switch detects a WAN or MAN link failure, it takes down the associated disk-array link if 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.

Manageability

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 MDS 9000 NX-OS include:

- 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 an OOB management port and in-band IPFC
- Starting with MDS 9000 NX-OS 7.3, the MDS 9000 Family supports Cisco NX-API, a Representational State Transfer (REST) API framework providing programmatic access to the MDS 9000 Family over HTTP and HTTPS using an OOB management port
- 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

More information about MDS 9000 Family SAN management is available at http://www.cisco.com/go/dcnm.

Cisco Data Center Network Manager (DCNM) for SAN and Cisco Device Manager

Cisco Data Center Network Manager for SAN and Cisco Device Manager are responsive, easy-to-use Java applications with GUIs that provide an integrated approach to switch and fabric administration. DCNM offers storage administrators fabricwide management capabilities such as discovery, multiple switch configurations, real-time network monitoring, historical performance monitoring for network traffic hotspot analysis, and troubleshooting. The DCNM interactive summary dashboard provides intuitive views into the top fabric users with the capability to see detailed information to analyze key, or main, performance indicators (KPIs).

DCNM simplifies management of virtual infrastructure by managing the entire path: from the physical to the virtual network across the whole data center environment. The virtual machine–aware views increase service availability by identifying bottlenecks in virtual machine and VMware ESX performance and extending the visibility to the physical fabric. The virtual machine–aware topology view shows all the dependencies from the virtual machine to the physical host, to the switch, and to storage, with quick access to a detailed view of their attributes. The virtual machine–aware dashboard displays all the information needed to manage the virtual environment, including performance charts, inventory information, events, and virtual machine and VMware ESX use information. This powerful approach greatly reduces switch setup times, increases overall fabric reliability, and provides extensive diagnostics for resolving configuration inconsistencies.

Cisco IOS Software CLI Similarity

MDS 9000 NX-OS presents a consistent, logical CLI. Adhering to the syntax of the widely known Cisco IOS® Software CLI, the MDS 9000 NX-OS CLI is easy to learn and delivers broad management capabilities. The 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 MDS 9000 Family using standard scripting languages.

Programmability and Open APIs

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

Starting with MDS 9000 NX-OS 7.3, Cisco supports NX-API, a REST API framework that allows programmatic access to the MDS 9000 Family over HTTP and HTTPS. NX-API provides the configuration and management capabilities of the MDS 9000 NX-OS CLI with web-based APIs, letting users control the MDS 9000 Family switch using a web browser. The switch can be set to publish the output of the API calls in XML or JavaScript Object Notation (JSON) format, simplifying scripting and supporting more effective programmability to enable a broad range of use cases. NX-API offers nearly a 10-fold improvement over SNMP queries and can be used for automation of network functions, troubleshooting, and custom use cases.

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

The Data Center Network Manager for SAN Storage Management Initiative Specification (SMI-S) server provides an XML interface with an embedded agent that complies with the Web-Based Enterprise Management (WBEM) and SMI-S standards, including switch, fabric, server, and zoning profiles.

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 MDS 9000 NX-OS open API allows the CiscoWorks Resource Manager Essentials (RME) application to provide centralized 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 MDS 9000 Family device health, such as supervisor memory and processor utilization. The Device Fault Manager can also monitor the health of important components such as fans, power supplies, and temperature.

N-Port Virtualization

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. 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 MDS 9000 Family blade switches and Cisco MDS 9100 Series Multilayer Fabric Switches.

Autolearn for Network Security Configuration

The autolearn feature lets the MDS 9000 Family 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.

FlexAttach

One of the main problems faced today in SAN environments 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 have to be changed when a new server is installed or an existing server is replaced. FlexAttach addresses these problems, reducing the number of configuration changes and the time and coordination required by SAN and server administrators when installing and replacing servers. MDS 9000 NX-OS supports the FlexAttach feature on MDS 9100 Series Multilayer Fabric Switches deployed in NPV mode.

PowerOn Auto Provisioning

PowerOn Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on MDS 9000 Family switches that are being deployed in the network for the first time, enabling touchless bootup and automated provisioning.

When a MDS 9000 Family fabric switch with the POAP feature boots and does not find the startup configuration, the switch enters POAP mode, locates a Dynamic Host Configuration Protocol (DHCP) server, and bootstraps itself with its interface IP address, gateway, and Domain Name System (DNS) server IP addresses. It also obtains the IP address of a Trivial FTP (TFTP) server or the URL of an HTTP server and downloads a configuration script, which runs on the switch. This script then downloads and installs the appropriate software image and configuration file.

Starting with MDS 9000 NX-OS 6.2(9), the POAP capability is available on Cisco MDS 9148 and MDS 9148S 16G Multilayer Fabric Switches, and starting with MDS 9000 NX-OS 7.3, the POAP capability is available on MDS 9700 Series Multilayer Directors.

Host Provisioning Wizard

The Data Center Network 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 Data Center Network Manager Server Federation

Data Center Network Manager server federation improves management availability and scalability by load balancing fabric-discovery, performance-monitoring, and event-handling processes. Cisco DCNM 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 DCNM instance and view all reports, inventory, statistics, and

logs from a single web browser. Up to 10 Cisco DCNM instances can form a federation (or cluster) that can manage more than 75,000 end devices.

Network Boot for iSCSI Hosts

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

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 times that back-end tasks such as Fibre Channel zoning and storage-device configuration must be performed.

iSCSI Server Load Balancing

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, promoting high availability.

IPv6

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 MDS 9000 Family switches running previous software revisions. This dual-stack approach allows the 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, MDS 9000 NX-OS enhances the architecture of the 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.

Extended Credits

Full line-rate Fibre Channel ports provide at least 255 buffer credits as 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 of 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 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 available bandwidth under high-use 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 Port-Channel Traffic

Port Channels load balance Fibre Channel traffic using a hash of the 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. 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. Compression and write acceleration further enhance FCIP performance for SAN extension.

For WAN performance optimization, MDS 9000 NX-OS includes a SAN extension tuner, which directs SCSI I/O commands to a specific virtual target and reports IOPS and I/O latency results, helping determine the number of concurrent I/O operations needed to increase FCIP throughput.

FCIP Compression

FCIP compression in MDS 9000 NX-OS increases effective WAN bandwidth without the need for costly infrastructure upgrades. By integrating data compression into the 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. 10/1 Gigabit Ethernet ports on the Cisco MDS 9250i Multiservice Switch and 1 Gigabit Ethernet ports on the Cisco MDS 9222i Multiservice Modular Switch (MMS), MDS 9000 18/4-Port Multiservice Module (MSM), and MDS 9000 16-Port Storage Services Node (SSN) achieve up to a 43:1 compression ratio, with typical ratios of 4:1 over a wide variety of data sources.

FCIP Tape Acceleration

Centralization of 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 for restore operations for open systems.

Serviceability, Troubleshooting, and Diagnostics

MDS 9000 NX-OS is among the first storage network operating systems to provide a broad 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. MDS 9000 NX-OS can shut down malfunctioning ports if errors exceed user-defined thresholds. This capability helps isolate problems and reduce risks by preventing errors from spreading to the whole fabric.

Cisco 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 Cisco 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 MDS 9000 Family switch to save Fibre Channel control traffic within 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 MDS 9000 Family storage service modules.

Fibre Channel Ping, Traceroute, and Pathtrace

MDS 9000 NX-OS brings to storage networks features such as Fibre Channel ping and traceroute. With Fibre Channel ping, administrators can check the connectivity of an N-port and determine its round-trip latency. 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. Starting with MDS 9000 NX-OS 6.2(5), the new pathtrace feature builds on the Fibre Channel traceroute feature to provide more statistics about each hop in the path, such as ingress and egress ports, number of transmitted and received frames, and errors.

Cisco Call Home

MDS 9000 NX-OS offers Cisco Call Home feature for proactive fault management. Call Home provides a notification system triggered by software and hardware events. It 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, an in-house server or a server at a service provider’s facility, and the Cisco Technical Assistance Center (TAC).

System Log

The MDS 9000 Family syslog capabilities greatly enhance debugging and management. Syslog severity levels can be set individually for all 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:

- 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. Cisco MDS 9000 NX-OS 6.2 introduces support for the Cisco Generic Online Diagnostics (GOLD) framework on the Cisco MDS 9700 Series Multilayer Directors in lieu of the Cisco Online Health Management System (OHMS) diagnostic framework used on the other MDS platforms. Generic Online Diagnostics is a suite of diagnostic facilities for verifying that hardware and internal data paths are operating as designed. Boot-time diagnostics, continuous monitoring, standby fabric loopback tests, and on-demand and scheduled tests are part of the diagnostics feature set. This industry-leading diagnostics subsystem allows rapid fault isolation and continuous system monitoring, critical features in today's continuously operating environments.
- Cisco Embedded Event Manager (EEM): Embedded Event Manager is a powerful device and system management technology integrated into MDS 9000 NX-OS. It provides a policy framework that can be used to define the actions to be taken when a configurable event or condition occurs. Starting with MDS 9000 NX-OS 6.2(11), the MDS 9000 Family includes an Embedded Event Manager based scale-limit monitoring capability. This feature lets you send syslog alerts to users whenever the default or configured scale threshold is exceeded.
- Loopback testing: The 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.
- ISL Diagnostics: Starting with MDS 9000 NX-OS 7.3, Inter-Switch-Link (ISL) Diagnostics capability is available to help check health and performance of ISLs, before activating the links for production traffic. These tests are expected to measure traffic loss rate, link latency and cable length among other parameters.
- IPFC: The 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 an 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: 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 comprehensive supplemental source of information for managing 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 MDS 9000 Family software features are included in the standard package: the base configuration of the switch. 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, Data Center Network Manager Package, Data Mobility Manager Package, I/O Accelerator Package, and XRC Acceleration Package. On-demand port activation licenses are also available for the MDS 9000 Family blade switches and the MDS 9100 Series Multilayer Fabric Switches.

Enterprise Package

The standard software package bundled at no charge with the MDS 9000 Family switches includes the base set of features that Cisco believes are required by most customers for building a SAN. The MDS 9000 Family also has a set of advanced features that are recommended for all enterprise SANs. These features are bundled together in the MDS 9000 Enterprise Package. Refer to the MDS 9000 Enterprise Package data sheet for more information, at http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6029/product_data_sheet09186a00801ca6ac.html.

SAN Extension over IP Package

The MDS 9000 SAN Extension over IP Package allows the customer to use FCIP to extend SANs over long distances on IP networks using the MDS 9000 Family IP storage services. Refer to the MDS 9000 SAN Extension over IP Package data sheet for more information, at http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps4358/product_data_sheet09186a00801cc917.html.

Mainframe Package

The 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. This package also includes FICON Tape Write/Read Acceleration. Refer to the MDS 9000 Mainframe Package data sheet for more information, at http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps4358/product_data_sheet09186a00801d721c_ps6029_Products_Data_Sheet.html.

Data Center Network Manager Packages

Data Center Network Manager for SAN Essentials Edition and Device Manager applications bundled at no charge with the MDS 9000 Family switches provide basic configuration and troubleshooting capabilities. Data Center Network Manager for SAN Advanced Edition extends these capabilities by providing historical performance monitoring for network traffic hotspot analysis, centralized management services, and advanced application integration for greater management efficiency. Refer to the Data Center Network Manager data sheet for more information, at http://www.cisco.com/go/dcnm.

On-Demand Port Activation License

On-demand ports allow customers to benefit from MDS 9000 NX-OS features while initially purchasing only a small number of activated ports on MDS 9100 Series, MDS 9250i and MDS 9396s switches. Customers can expand switch connectivity as needed by licensing additional ports.

Data Mobility Manager Package

The MDS 9000 Data Mobility Manager Package enables data migration between heterogeneous disk arrays without introducing a virtualization layer or the need to rewire or reconfigure SANs. Data Mobility Manager allows concurrent migration between multiple LUNs of unequal size. Rate-adjusted migration, data verification, dual Fibre Channel fabric support, and management using Data Mobility Manager provide a complete solution that greatly simplifies and eliminates most downtime associated with data migration. Refer to the MDS 9000 Data Mobility Manager Package data sheet for more information, at http://cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/ps8507/data_sheet_c78-491879.html.

I/O Accelerator Package

The MDS 9000 I/O Accelerator Package provides SCSI acceleration to significantly 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 MDS 9000 I/O Accelerator Package data sheet for more information, at http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/ps10531/data_sheet_c78-538860.html.

XRC Acceleration Package

The 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 MDS 9000 Family module that is local to the SDM, reducing or eliminating 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 MDS 9000 XRC Acceleration Package data sheet for more information, at http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/ps10526/data_sheet_c78-538834.html.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

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 platform 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 C78-736345-00 12/15