Cisco MDS 9000 NX-OS Software 4.1(1)

Product Overview

Cisco® NX-OS Software is the underlying system software that powers the award-winning Cisco MDS 9000 family multilayer switches. Cisco NX-OS Software 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 storage area network (SAN) switch, Cisco NX-OS Software 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 NX-OS Software is a highly flexible and scalable platform for enterprise SANs.

Common Software Across All Platforms

Cisco NX-OS Software 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.

Multiprotocol Support

In addition to supporting Fibre Channel Protocol (FCP), Cisco NX-OS Software 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 to take advantage of their existing investment in IP networks for cost-effective business-continuance solutions for both Fibre Channel and FICON environments. With Cisco NX-OS Software multiprotocol support, customers can better use their enterprise resources, thereby lowering costs.

Virtual SANs

Virtual SAN (VSAN) technology partitions a single physical SAN into multiple VSANs. The Cisco MDS 9000 family switches are the first SAN switches on the market with VSAN support built into the switch hardware. VSAN capabilities allow Cisco NX-OS Software to logically divide a large physical fabric into separate, isolated environments to improve Fibre Channel SAN scalability, availability, manageability, and network security. For FICON, VSANs 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, while 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 due to human error by isolating the effect of a user's action to a specific VSAN whose membership can be assigned based on switch ports or the worldwide name (WWN) of attached devices.

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

Inter-VSAN Routing

Data traffic can be transported between specific initiators and targets on different VSANs using inter-VSAN routing (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 NX-OS Software 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 accommodates numerous partner applications. The Cisco MDS 9000 family intelligent fabric applications take advantage of all Fibre Channel features and services offered by Cisco NX-OS Software, 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 source-and-target combinations.

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 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

Cisco MDS 9000 family Secure Erase 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 Application Program Interface (ISAPI) platform, and the write operations are performed by the virtual initiators created for this purpose. The host 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.

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 rewiring or reconfiguring the SAN. Cisco Fabric Manager is used to administer Cisco DMM; no additional management software is required. When used with the SAN device virtualization feature, Cisco DMM eliminates most application downtime and dramatically reduces the overall time required for data migration.

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 NX-OS Software. In addition to VSANs, which provide true isolation of SAN-attached devices, Cisco NX-OS Software offers numerous security features. The 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 NX-OS Software 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 NX-OS Software offer secure authentication, data encryption for privacy, and data integrity for both FCIP and iSCSI connections on the Cisco MDS 9000 family. Cisco NX-OS Software 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.

Role-Based Access Control

Cisco NX-OS Software 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 WWN. 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 NX-OS Software 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, LUN 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:** An attribute can be set to restrict I/O operations in any zone type to SCSI read-only commands. This feature is especially useful for sharing volumes across servers for backup, data warehousing, etc.
- **Broadcast zones:** An attribute can be set for any zone type to restrict broadcast frames to members of the specific zone.

To provide strict network security, zoning is always enforced per frame using access control lists (ACLs) that are applied at the ingress switch. All zoning polices are enforced in hardware, and 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:

- Fabricwide 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
- Advanced Encryption Standard (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 NX-OS Software provides resilient software architecture for mission-critical hardware deployments.

Nondisruptive Software Upgrades

Cisco NX-OS Software 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 NX-OS Software 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) 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 NX-OS Software 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 NX-OS Software detects failures on active paths.

Port Tracking for Resilient SAN Extension

SAN extension resiliency is enhanced by the Cisco NX-OS Software port-tracking feature. If a Cisco MDS 9000 family switch detects a WAN or metropolitan-area network (MAN) link failure, it brings down the associated disk-array link when port tracking is configured, so the array can redirect a failed I/O 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 NX-OS Software 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 HBAs,

storage devices, and switch ports, eliminating the need to reenter names when devices are moved.

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

Open APIs

Cisco NX-OS Software 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 NX-OS Software management API.

Fabric-Device Management Interface (FDMI) capabilities provided by Cisco NX-OS Software 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 NX-OS Software provides an Extensible Markup Language (XML) interface with an embedded agent that complies with the Web-Based Enterprise Management (WBEM), Common Information Model (CIM), and Storage Management Initiative Specification (SMI-S) standards, including switch, fabric, server, and zoning profiles.

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 NX-OS Software 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 APIs also help 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 NX-OS Software 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 zoning and port security to be configured 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.

N-port virtualizer (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 Blade Switch Series, the Cisco MDS 9124 Multilayer Fabric Switch, and the Cisco MDS 9134 Multilayer Fabric Switch.

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 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 problem, 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 Blade Switch Series, the Cisco MDS 9124, and the Cisco MDS 9134 when NPV mode is enabled.

Network Boot for iSCSI Hosts

Cisco NX-OS Software 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 NX-OS Software, either through the highly available, distributed iSNS built into Cisco NX-OS Software 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 NX-OS Software 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 NX-OS Software 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 NX-OS Software enhances the architecture of the Cisco MDS 9000 family with several advanced traffic-management features that help ensure consistent performance of the SAN during varying load conditions.

Quality of Service

Four distinct quality-of-service (QoS) priority levels are available: three for Fibre Channel data traffic and one for Fibre Channel control traffic. Fibre Channel data traffic for latency-sensitive applications can be configured to receive higher priority than throughput-intensive applications using data QoS priority levels. Control traffic is assigned the highest QoS priority automatically, to accelerate convergence of 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 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 NX-OS Software also can be configured to load balance across multiple same-cost FSPF routes.

Disk Write Acceleration

Write acceleration for disk arrays reduces I/O latency and extends the distance for disaster-recovery and business-continuity applications over WANs and MANs. Fibre Channel write acceleration is available only on the Cisco MDS 9000 family SSMs. FCIP write acceleration is available on all Cisco MDS 9000 family switches and modules that provide FCIP capabilities.

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 NX-OS Software 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 NX-OS Software 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 and Cisco MDS 9000 18/4-Port Multiservice Module 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 NX-OS Software 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 send IP-encapsulated Fibre Channel control traffic to a remote PC for decoding and display using the open-source Ethereal network-analyzer application. It is, therefore, possible to capture and analyze Fibre Channel control traffic without an expensive Fibre Channel analyzer.

SCSI Flow Statistics

LUN-level SCSI flow statistics can be collected for any combination of initiator and target. The scope of these statistics includes read, write, and control commands and error statistics. This feature is available only on the Cisco MDS 9000 family SSMs.

Fibre Channel Ping and Fibre Channel Traceroute Features

Cisco NX-OS Software 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 NX-OS Software 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 NX-OS Software 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 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 NX-OS Software 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 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 (FMS) package, Storage Services Enabler (SSE) package, Storage Media Encryption package, and Data Mobility Manager package. On-demand ports activation licenses are also available for the Cisco MDS Blade Switch Series, 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 wide distances on IP networks using the Cisco MDS 9000 family IP storage services. Refer to the Cisco MDS 9000 SAN Extension over IP package fact sheet for more information.

Mainframe Package

The Cisco MDS 9000 Mainframe package uses the FICON protocol and allows control unit port 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 fact 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 MDS 9000 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 MDS 9000 FMS package fact 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 SSMs, Cisco MDS 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 fact sheet for more information.

On-Demand Port Activation License

On-demand ports allow customers to benefit from Cisco NX-OS Software features while initially purchasing only a small number of activated ports on 4-Gbps Cisco MDS 9100 Series Multilayer Fabric Switches. As needed, customers can expand switch connectivity by licensing additional ports.

Storage Media Encryption Package

The Cisco MDS 9000 Storage Media Encryption package enables encryption of data at rest on heterogeneous tape devices and virtual tape libraries as a transparent fabric service. Cisco SME is completely integrated with Cisco MDS 9000 family switches and the Cisco Fabric Manager application, enabling highly available encryption services to be deployed without rewiring or reconfiguring SANs, and allowing them to be managed easily without installing additional management software. Refer to the Cisco MDS 9000 Storage Media Encryption package fact sheet for more information.

Data Mobility Manager Package

The Cisco MDS 9000 Data Mobility 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 Data Mobility Manager package fact sheet for more information.

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

For More Information

http://www.cisco.com/go/nxos

http://www.cisco.com/go/storage

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 C78-490861-01 09/08