Cisco MDS 9000 NX-OS Software Release 8.1

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 32-Gbps Fibre Channel and enhanced Fibre Channel over Ethernet (FCoE) capabilities, programmable SAN, and new fabric services for the MDS 9000 Family and Cisco Nexus® Family of SAN switches. These new capabilities enable convergence, scalability, and intelligence across LAN and SAN environments in 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 faster Return On Investment (ROI).

Note: This document discusses the features and capabilities supported by Cisco MDS 9000 NX-OS Software Release 8.1(1) across current-generation 16-Gbps and 32-Gbps platforms in the Cisco MDS 9000 Family. However, 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

Previous versions of NX-OS support Fibre Channel Protocol (FCP), IBM Fibre Connection (FICON), Small Computer System Interface over IP (iSCSI), Fibre Channel over Ethernet (FCoE), and Fibre Channel over IP (FCIP). Starting with MDS 9000 NX-OS Software Release 8.1(1), Non-Volatile Memory Express over Fibre Channel (FC-NVMe) is supported on all Cisco MDS 9000 Series Switches for 16-Gbps and 32-Gbps port speeds. FC-NVMe-ready MDS 9000 Family switches can seamlessly transport NVMe workloads originating from FC-NVMe-capable Host Bus Adapters (HBAs) and terminating on FC-NVMe-capable storage arrays whenever they are introduced to the existing SAN. This feature facilitates outstanding returns on your existing investments in 16-Gbps MDS 9000 Series Switches and exceptional investment protection on currently shipping Cisco MDS 9700 Series Multilayer Directors through seamless insertion of a 32-Gbps module. With this capability, NX-OS 8.1(1) continues its tradition of allowing hosts using multiple storage protocols to co-exist in the same SAN, and it enables the same host to run both SCSI and NVMe protocols on the same switch port.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

FCoE recognizes Fibre Channel as the dominant storage protocol in the data center while offering customers a viable I/O consolidation solution at 10-Gbps and 40-Gbps speeds. It simplifies customer environments by using Ethernet, allowing the industry to avoid creation of another, separate protocol for I/O consolidation. Starting with NX-OS 8.1(1), 40-Gbps FCoE will allow you to extend I/O consolidation to distances up to 25 miles (40 km) using Cisco branded 40-Gbps extended-reach optics modules.

Native FCIP support lets you use existing investments in IP networks for cost-effective business-continuity solutions on your existing MDS 9700 Series Multilayer Directors, using the recently launched Cisco MDS 9000 24/10-Port SAN Extension Module. The new module offers 10-Gbps ports (and 40-Gbps ports, through a future firmware upgrade). It interoperates with earlier-generation SAN extension solutions such as the fixed Cisco MDS 9250i Multiservice Fabric Switch. With MDS 9000 NX-OS multiprotocol support, customers can use their enterprise resources better, thereby lowering costs and reducing business risk.

Optimized Device Scalability

Today's SAN administrators face an ever-increasing demand to reduce Operating Expenses (OpEx) by reducing the costs of space, power, cabling, and management. Hence, SAN administrators are seeking greater consolidation and scale. Pervasive virtualization of computing resources has allowed the data center to scale the number of virtual server instances to a denser physical blade chassis hosting up to five times more virtual machines than before. Similarly, with storage virtualization, storage ports are now being consolidated into fewer Logical Unit Numbers (LUNs) striped across multiple physical storage arrays, thereby significantly reducing the number of LUNs that need to be managed.

The MDS 9000 Family keeps up with such hyper-consolidation in the SAN as well. Smart zoning in NX-OS facilitates zoning optimization and consolidation by reducing the number of initiator-and-target pairs that need to be zoned on a switch. On the basis of their World Wide Port Names (WWPNs), this number is reduced significantly using the name-server profile as target or initiator or both. In addition, starting with NX-OS 8.1(1), MDS 9700 Series directors will support up to 768 line-rate 32-Gbps ports, which will allow far greater consolidation of Fibre Channel bandwidth on a single switch, reducing the need for cables by half compared to the previous generation. Similarly, the number of managed switches can be consolidated to a single switch instead of at least four switches in a non-oversubscribed topology. Commensurate with such high consolidation, Cisco MDS 9718 Multilayer Directors now allow two times the number of device logins for each module and switch to facilitate greater consolidation of end devices on a single switch.

Even with higher number of devices logging into a single switch, optimizations in NX-OS help ensure that fabric convergence doesn't take longer. The MDS 9000 Family powered with port-pacer technology, which was introduced in NX-OS 6.2, facilitates the even spread of device login processing across a given set of Fabric ports (F-ports) as part of the port activation process, thereby helping ensure that the optimal number of logins are processed without the system sending out rejections. Starting with NX-OS 8.1(1), device login optimization has been further enhanced to alleviate the burden on the system caused by unsteady hosts initiating a sequence of login-logout-login operations spaced very close to each other. This frees critical resources to serve a flood of host logins more efficiently in situations in which a downstream server or a Node-port (N-port) Virtualization (NPV) device reloads.

For more information about MDS 9000 Family scale limits, see https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_1/config/config_limits/cisco_mds9000_config_limits_8x.html.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 offer 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.

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 the number of 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. VSAN 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 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

NX-OS 8.1(1) provides a solid foundation for delivery of network-based storage applications and services such as data acceleration 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 https://www.cisco.com/en/US/products/ps6028/index.html.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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). You can deploy IOA 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. You can also use IOA to enable remote tape backup and restore operations without significant throughput degradation.

IOA offers 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 1/2/4/8/10/16/32-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 Cisco Data Center Network Manager (DCNM) for SAN.

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

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Extended Remote Copy Acceleration

IBM Extended Remote Copy (XRC), 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 https://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 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 enterprisewide 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, which now include the recently launched MDS 9000 24/10-Port SAN Extension Module with support for the 256-bit Advanced Encryption Standard (AES) cipher for the strongest encryption of data securely between primary and remote sites. In addition, 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 Expansion ports (E-ports) of MDS 9000 Family 8-Gbps Fibre Channel switching modules can be encrypted. Starting with MDS 9000 NX-OS 6.2(9), the link encryption capability extends to the E-ports of MDS 9000 Family 16-Gbps switching modules, and with NX-OS 8.1(1) it extends to the E-ports of MDS 9000 Family 32-Gbps Fibre Channel switching modules. The encryption algorithm is 128-bit 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.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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.

Cisco TrustSec Fibre Channel Link Encryption has two main use cases:

- Many customers want to help ensure the privacy and integrity of any data that leaves the secure confines of their data centers 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, are 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.

Starting with NX-OS 8.1(1), Cisco TrustSec Fibre Channel Link Encryption is supported on the MDS 9000 Family 32-Gbps module. Cisco TrustSec encryption is also allowed between the 32- and 16-Gbps modules to provide exceptional investment protection and backward compatibility.

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 organizations reduce or avoid data stream errors that can lead to application performance degradation. Loss-prone media such as loose transceivers (Small Form-Factor Pluggables [SFPs]) and dirty cables can result in corrupted packets on 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.

In compliance with the T11-mandated guideline for FEC support between all 32-Gbps ports in the SAN, with NX-OS 8.1(1), FEC is supported for 16-Gbps and 32-Gbps links not only on ISLs between MDS 9700 Series Multilayer Directors, but also on device-facing links connected to 32-Gbps HBAs, providing a complete end-to-end FEC path.

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.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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:

- Fabricwide 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.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 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 Fibre Channel traffic. With this feature, up to 16 E-ports or Trunking E-ports (TE ports) or F-ports connected to proxy N-ports (NP-ports) can be bundled into a port channel. 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 port channel continues to function properly without requiring fabric reconfiguration.

MDS 9000 NX-OS uses a protocol to exchange port-channel configuration information between adjacent switches. This feature simplifies port-channel management, including misconfiguration detection and autocreation of port channels among compatible ISLs. In the autoconfigure mode, ISLs with compatible parameters automatically form channel groups; no manual intervention is required.

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 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.
- 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 https://www.cisco.com/go/dcnm.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Cisco Data Center Network Manager for SAN and Cisco Device Manager

The enhanced Data Center Network Manager for SAN Release 10.1(1) and later provides an easy-to-use HTML5-based GUI that provides an integrated approach to LAN and SAN switch and fabric administration. Data Center Network Manager 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 comprehensive slow-drain analysis and troubleshooting. The Data Center Network Manager interactive summary dashboard provides intuitive views into the top fabric users with the capability to see detailed information to analyze Key Performance Indicators (KPIs). Data Center Network Manager for SAN can manage all current generation SAN switches up to 32-Gbps.

Data Center Network Manager 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 ESX use information. This powerful approach greatly reduces switch setup times, increases overall fabric reliability, and provides extensive diagnostics for resolving configuration inconsistencies.

For more information, refer to the Data Center Network Manager 10 data sheet at https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-data-center-network-manager/datasheet-c78-736613.html.

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 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(0), 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. To facilitate rapid and agile programming using a DevOps-like model, a sandbox environment can be started natively on the switch using a web browser. This environment gives the programmer an NX-API equivalent for each NX-OS CLI command and provides responses in JSON, XML, and Remote Procedure Call (RPC) formats, which can be quickly incorporated into a script.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

In addition, the sandbox generates Python modules for each API and response, which can be reused by any Python script. 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 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.

On-Switch Automation

Management operations performed on a regular basis typically add a lot of operational overhead for the SAN administrator. To that add the possibility of errors creeping in to tasks that are performed manually or the possibility of a missing action for any event that's critical to the SAN's health. NX-OS traditionally provides mechanisms that allow the SAN administrator to program these regular tasks in scripts that can be invoked through Cisco Embedded Event Manager (EEM) and NX-OS Scheduler. The event manager allows you to set both system-default and user-configurable policies to enable watch points on several switch attributes such as CLI commands, counters, SNMP Object Identifiers (OIDs), syslog entries, offline status of critical components, and environment variables such as component power and temperature. If any of the attributes being watched matches the condition in the policy, one of the several actions invoked by the event manager can be to run a script. NX-OS provides options for hosting scripts written in TCL or Python. For more information about how to use the event manager, see https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/4_1/configuration/guides/cli_4_1/clibook/eem.html.

In addition to running scripts using policies through the event manager, NX-OS provides a mechanism to schedule maintenance tasks that need to be performed at a specific time and repeated periodically, right on the switch. The scheduler can invoke CLI commands, one of which can be a command to invoke a script through which the scheduled task is programmed. Again, the script can be written in either TCL or Python. For more information about NX-OS scheduler, see https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/4_1/configuration/guides/cli_4_1/clibook/maint.html.

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. Instead, 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.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 concerns 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.

Power-On Auto Provisioning

Power-On Auto Provisioning (POAP) automates the process of configuring the MDS 9000 Family switches that are being deployed in the network for the first time, enabling touchless bootup and automated provisioning.

When an 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 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.

USB Based Plug and Play

USB based plug and play capability facilitates the startup of MDS 9000 Family switches using a USB memory stick. It reduces management overhead and simplifies the deployment of new switches in the existing fabric. It also reduces the amount of time needed to rebuild an existing switch from its factory settings whenever this action is required. With the introduction of this feature in MDS 9000 NX-OS 6.2(13), administrators no longer need to travel to provision switches in remote data centers, but instead can just transport a USB memory stick to the data centers. A simple Python-based user interface is now available in the Cisco open-source repository (github.com) that allows users to configure the USB stick with the ease of a single click. The USB stick can store configurations for multiple switches denoted by the serial number of each switch, the desired version of the NX-OS image, and a TCL script that runs automatically whenever the memory stick is plugged in before the switch is reloaded with its factory settings. The switch boots from the NX-OS image in the USB memory stick, and the desired configuration is automatically applied to that switch.

For more information, see https://github.com/Cisco-SAN/PoapConf.

Starting with MDS 9000 NX-OS 7.3, the USB plug-and-play feature extends to all MDS 9000 Family 16-Gbps switches from the existing support for MDS 9700 Series Multilayer Directors and 9396S 16-Gbps Multilayer abric witches.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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. Data Center Network Manager provides a single management pane for viewing and managing all fabrics within a single federation. A storage administrator can discover and move fabrics within a federation for the purposes of load balancing, high availability, and disaster recovery. In addition, users can connect to any Data Center Network Manager instance and view all reports, inventory, statistics, and logs from a single web browser. Up to 10 Data Center Network Manager instances can form a federation (or cluster) that can manage more than 75,000 end devices.

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.

Slow-Drain Device Detection and Isolation

Slow drain is a typical problem that affects most Fibre Channel SAN environments. MDS 9000 NX-OS provides multiple features for monitoring, detecting, and avoiding slow-drain conditions in the SAN. These switch-native capabilities are supplemented by advanced SAN-wide slow-drain monitoring and detection capabilities on Data Center Network Manager 10.1. NX-OS 8.1(1) introduces another solution, in which the penalty for a slow-drain condition on an ISL is significantly reduced.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Slow-drain detection and isolation, in addition to automatically and continuously monitoring and detecting Fibre Channel flows originating from slow devices, isolates the slow devices within the same ISL. As a result, Fibre Channel flows originating from normal devices are not penalized. This process is accomplished by using a standard Fibre Channel primitive called Extended Receiver Ready (ERRDY) that is exchanged between the end ports of an ISL connecting two MDS 9000 Family switches. The isolated slow flows are awarded a lower priority than the high-priority control traffic and the regular flows with normal priority. A dynamic and efficient algorithm distributes the Buffer-to-Buffer (B2B) credits allocated to the ISL port among the different flows based on their priority. This approach not only shields the normal-priority and high-priority flows from the effects of the low-priority isolated flows, but also helps ensure fairness to all flows, including the slow flows, so that they are not starved of credits and dropped. In the event that more slow flows are detected and isolated and contention for credits increases among the slow flows, the extended B2B credits available with the enterprise NX-OS version can be used by the algorithm.

Enhanced Port Monitor

Introduced in NX-OS 5.2, the port monitor has proven to be one of the most effective tools for monitoring events that are recorded on every switch port. Its usefulness is enhanced by the flexibility to dynamically provision port-monitoring policies that can be applied across all ISL ports, all access ports, or all ports on the switch. These policies can be replicated on multiple switches in the fabric using Data Center Network Manager. An extensive number of interface events can be monitored today, and whenever an event exceeds a rising or falling threshold on an interface, the port monitor can alert the SAN administrator and trigger corrective actions on the affected ports using the port monitor's port-guard action. If events occur rapidly and at small intervals, policies can be programmed to check for events more frequently using an aggressive check interval. This feature provides a very effective first line of defense against typical problems such as slow drain and congestion that affect the SAN fabric.

Starting with NX-OS 8.1(1), the port monitor has been enhanced to detect excessive state-change events on the interface, which essentially allows it to monitor for any underlying condition, including both the most commonly monitored ones and those that might otherwise be precluded. Also starting this release, the port monitor automatically differentiates a Trunking F-port (TF-port) connected to a downstream NPV switch from a regular F-port and disables port-monitor actions such as port flap and port error disable that would otherwise affect multiple end devices that are connected to that NPV switch. This differentiation can be optionally activated by marking an access port in TF-mode with a flag. The port monitor also supports a new port-guard isolation action for trunk ports, to help enable slow-drain isolation to take effect on those ISL ports.

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.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Extended Credits

32-Gbps and 16-Gbps full-line-rate Fibre Channel ports provide at least 500 buffer credits as standard. Adding credits allows longer distances for native Fibre Channel SAN extension. Up to 8191 extended buffer credits from a shared pool of 8300 buffer credits for a group of 16 ports for a MDS 9000 Family 32-Gbps Fibre Channel module can be allocated to a single port when needed to extend the distance of Fibre Channel SANs by up to 512 kilometers

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 for 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 port channels 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.

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-Gbps Ethernet ports on the MDS 9250i Multiservice Fabric 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. The latest-generation MDS 9000 24/10-Port SAN Extension Module on NX-OS 8.1(1) consistently delivers these high compression ratios and is backward compatible with earlier-generation platforms.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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. Tape backup server ports can now be consolidated into the same modular MDS 9000 Series Switches and tape traffic accelerated over FCIP using the 24/10-Port SAN Extension Module, which can interoperate with earlier-generation FCIP tape acceleration switches such MDS 9250i that are currently connected to the backup tape libraries at in the remote site.

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.

Fibre Channel Read Diagnostics Parameters

A KPI for a Fibre Channel SAN is its capability to provide predictable and consistent performance for each and every workload initiated by different applications. The MDS 9000 Family helps ensure that the right tools are in place to monitor and troubleshoot all underlying conditions that can potentially degrade application performance. In addition to ISL diagnostics, which can detect error conditions on an active link between two switches, MDS 9000 Family 16-Gbps and 32-Gbps switches now support Read Diagnostics Parameters (RDP), which can be run on device-facing active links connecting the switch ports to the HBAs or storage-array ports. RDP, which is a T11 standards-based feature, extends this diagnostic capability, so that the HBA driver can request the parameters from the connected switch port to detect any of these error conditions. RDP also allows the host to perform regular housekeeping activities on a live link: for instance, the host can monitor port speed, FEC status, B2B credits, and as well as inspect the optical element. This feature was developed and validated in conjunction with leading HBA vendors.

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.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 information about each hop in the path, such as the ingress and egress ports, the number of transmitted and received frames, and errors.

Cisco Call Home

MDS 9000 NX-OS offers the 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 MDS 9700 Series Multilayer Directors instead 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 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.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- 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, ISL diagnostics capability is available to help check the health and performance of ISLs before the links are activated for production traffic. These tests measure traffic loss rate, link latency, and cable length, along with 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 specialized 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.

Cisco Smart Licensing for Cisco MDS 9000 NX-OS Software Packages

NX-OS 8.1(1) marks the introduction of a new philosophy in licensing. Cisco Smart Licensing gives our customers the option of a completely electronic method of fulfilment for their new licensing needs. It also provides a mechanism for converting all existing and new licenses to an electronic account. These license entitlements are no longer restricted to a single physical hardware. They can now be automatically transferred across the same product model, and this transfer is not restricted to a single physical site, but can be implemented across multiple sites worldwide. This model provides exceptional efficiency and investment protection and single-pane monitoring of resource utilization and budgets. This approach is implemented through a native agent running on all switches. This agent registers the switch and licenses activated periodically with the smart account, which resides on the customer's premises or in the cloud. The smart account instance for every site then is periodically synchronized with the central smart account, which manages multiple sites to allow transfer of entitlements and monitoring utilization across these sites. Smart Licensing is available for all the currently shipping license packages listed here.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 to build 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 https://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 https://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps4358/product_data_sheet09186a00801cc917.html.

Data Center Network Manager Packages

Data Center Network Manager for SAN Essentials Edition and Cisco 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 https://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, 9250i, and 9396S switches. Customers can expand switch connectivity as needed by licensing additional ports.

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 https://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 https://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/ps10526/data_sheet_c78-538834.html.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

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 https://www.cisco.com/go/nxos and https://www.cisco.com/go/storage.

The Cisco MDS 9000 NX-OS platform data sheets are available at https://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 **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C78-739224-00 08/17

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.