

Cisco MDS 9000 Family Enterprise Package

Package Description

The Cisco® MDS 9000 Family Enterprise Package enables a set of advanced traffic-engineering and security features that are useful for large or complex SANs. It is well suited for enterprise customers who have more sophisticated requirements beyond the standard SAN features that are included at no charge with Cisco MDS 9000 Series Multilayer Switches.

Advanced Traffic-Engineering Features

The Cisco MDS 9000 Family Enterprise Package includes the following advanced traffic-engineering features:

- **Inter-VSAN Routing (IVR):** Fibre Channel control traffic does not flow between VSANs. IVR allows selective transfer of data traffic between specific initiators and targets on different virtual SANs (VSANs). It eliminates the need to merge VSANs into a single logical fabric. It also facilitates resource sharing across VSANs without compromising the VSAN benefits of scalability, reliability, availability, or network security.

IVR also works across WANs using Fibre Channel Interface Protocol (FCIP). IVR can be used with FCIP to create more efficient business-continuity and disaster-recovery solutions. With the introduction of IVR, Cisco has become the first vendor to provide routing capability for Fibre Channel networks in SAN switches.
- **Quality of service (QoS):** The QoS feature in Cisco MDS 9000 NX-OS Software already allows traffic to be classified into four distinct levels for service differentiation. In the Cisco MDS 9000 Family Enterprise Package, zone-based QoS complements the standard QoS and simplifies configuration and administration. It classifies data traffic by VSAN ID, N-port worldwide name (WWN), and Fibre Channel identifier (FC-ID). You can also configure QoS per VSAN, policy, or class.
- **Extended credits:** The extended credits feature allows up to 4095 buffer credits from a pool of more than 6000 buffer credits for a module to be allocated to ports as needed. Adding credits increases distance for Fibre Channel SAN extension.

Enhanced Network Security Features

The Cisco MDS 9000 Family Enterprise Package includes the following enhanced network security features:

- **Switch-switch and host-switch authentication:** Fibre Channel Security Protocol (FC-SP) capabilities in Cisco MDS 9000 NX-OS Software provide switch-switch and host-switch authentication. This feature helps eliminate disruptions that may occur when unauthorized devices connect to a large enterprise fabric.
- **Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP):** This protocol performs authentication locally in a Cisco MDS 9000 Family switch or remotely through RADIUS or TACACS+. If authentication fails, a switch or host cannot join the fabric.
- **Port security:** This feature locks mappings of entities to switch ports. The entity can be a host, target, or switch and is identified by its WWN. Port security helps ensure that SAN security is not compromised if unauthorized devices connect to a switch port.
- **VSAN-based access control:** This feature limits roles to certain VSANs. For example, a network administrator role can be established to allow configuration of all platform-specific capabilities. VSAN-

administrator roles can be created to allow configuration and management of specific VSANs. VSAN-based access control reduces SAN disruptions by localizing the effects of user errors to the VSANs for which the user has administrative privileges.

- **IP Security (IPsec):** IPsec is available for FCIP and SCSI over IP (iSCSI) over Gigabit Ethernet ports on the Cisco MDS 9000 18/4-Port Multiservice Module (MSM), MDS 9000 16-Port Storage Services Node (SSN), MDS 9222i Multiservice Modular Switch (MMS), and MDS 9250i Multilayer Fabric Switch. Proven IETF-standard IPsec capabilities offer secure authentication, data encryption, and data integrity. Internet Key Exchange Version 1 (IKEv1) and IKEv2 protocols are deployed to dynamically establish security associations for IPsec using preshared keys for remote-side authentication.
- **Digital certificates:** A trusted third party issues digital certificates as electronic passports to prove the identity of certificate owners. After the owner's identity is verified, the certificate uses the owner's public encryption key to protect identity data contained in the certificate. On the Cisco MDS 9000 Family platform, digital certificates apply to IKE as well as to Secure Shell (SSH).
- **Fabric binding for open systems:** Fabric binding helps ensure that Inter-Switch Links (ISLs) are enabled only between switches that have been authorized in the fabric-binding configuration. This feature helps prevent unauthorized switches from joining the fabric or disrupting current fabric operations.
- **Cisco TrustSec[®] Fibre Channel Link Encryption:** Cisco TrustSec Fibre Channel Link Encryption uses the existing FC-SP architecture to help ensure data integrity and privacy. Starting with Cisco MDS 9000 NX-OS Software Release 4.2(1), Fibre Channel data between E-ports of 8-Gbps modules can be encrypted. Starting with Cisco MDS 9000 NX-OS Software Release 6.2(9), Fibre Channel data between E-ports of Cisco MDS 9000 16-Gbps Fibre Channel switching modules can also be encrypted. The encryption algorithm is 128-bit Advanced Encryption Standard (AES) and enables either AES Galois Counter Mode (GCM) or AES Galois Message Authentication Mode (GMAC) interfaces. AES-GCM mode encrypts and authenticates the frames. AES-GMAC only authenticates the frames passing between two E-ports. Line-rate encryption encapsulates frames at egress with encryption using GCM and AES 128-bit encryption. At ingress, frames are decrypted and authenticated for integrity. There are two primary use cases: one for connecting outside the data center over native Fibre Channel (for example, using dark fiber, coarse wavelength-division multiplexing [CWDM] or dense wavelength-division multiplexing [DWDM]), and one for encryption within the data center.

Software Release

To use Cisco MDS 9000 Family Enterprise Package features, Cisco MDS 9000 NX-OS 4.1(1) or later must be installed on a Cisco MDS 9000 Family switch.

License Information

The Cisco MDS 9000 Family Enterprise Package is licensed per switch for all the ports on the switch. Some package features can be used only if all the switches in the fabric have licenses for this package. Please refer to the data sheets for the respective switches for information about features with limited or no support listed in this document.

Limitations on Cisco MDS 9100 Series Switches

The following features of the Cisco MDS 9000 Family Enterprise License are not supported on Cisco MDS 9100 Series Multilayer Fabric Switches:

- IPsec
- Extended credits
- Cisco TrustSec Fibre Channel Link Encryption

Ordering Information

Table 1 lists the part numbers associated with this package.

Table 1. Ordering Information

Part Number	Description
M97ENTK9	• Enterprise Package for one Cisco MDS 9700 Series Multilayer Director
M97ENTK9=	• Spare
L-M97ENTK9=	• Spare-Electronic Delivery
M9500ENT1K9	• Enterprise Package for one Cisco MDS 9500 Series Multilayer Director
M9500ENT1K9=	• Spare
L-M95ENT1K9=	• Enterprise Package for one Cisco MDS 9500 Series Multilayer Director, spare-Electronic Delivery
M9200ENT1K9	• Enterprise Package for one Cisco MDS 9200 Series Multilayer Fabric Switch
M9200ENT1K9=	• Spare
L-M92ENT1K9=	• Enterprise Package for one Cisco MDS 9200 Series Multilayer Fabric Switch, spare-Electronic Delivery
M9100ENT1K9	• Enterprise Package for one Cisco MDS 9100 Fabric Switch
M9100ENT1K9=	• Spare
L-M9100ENT1K9=	• Enterprise Package for one Cisco MDS 9100 Fabric Switch, spare-Electronic Delivery

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 about Cisco MDS 9000 NX-OS, view the data sheet at http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps5989/data_sheet_c78-708102.html.




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

 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: 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)