

Cisco MDS 9000 Family Enterprise Package

Package Description

The standard software package that is bundled at no charge with Cisco® MDS 9000 Series Multilayer Switches includes the base set of features that Cisco believes are required by most customers to build a SAN (Storage Area Network). The Cisco MDS 9000 Family also has a set of advanced traffic-engineering and advanced security features that are recommended for all enterprise SANs. These features are bundled together in the Cisco MDS 9000 Family Enterprise package.

Advanced Traffic-Engineering Features

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

- **Inter-VSAN Routing (IVR):** IVR allows selective transfer of data traffic between specific initiators and targets on different virtual SANs (VSANs) without merging VSANs into a single logical fabric. Fibre Channel control traffic does not flow between VSANs, nor can initiators access resources except the ones designated with IVR. In this way, IVR facilitates resource sharing across VSANs without compromising the VSAN benefits of scalability, reliability, availability, and network security.

IVR also works across WANs over the Fibre Channel Interface Protocol (FCIP). IVR can be used in conjunction 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 allows traffic to be classified into four distinct levels for service differentiation. QoS can be applied to help ensure that Fibre Channel data traffic for latency-sensitive applications receives higher priority over throughput-intensive applications such as data warehousing.

Zone-based QoS is included in the Cisco MDS 9000 Family Enterprise Package and complements the standard QoS data-traffic classification by VSAN ID, N-port worldwide name (WWN), and Fibre Channel identifier (FC-ID). Zone-based QoS helps simplify configuration and administration by using the familiar zoning concept. QoS can also be configured per VSAN or can be policy or class based.

- **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 distances for Fibre Channel SAN extension.
- **Small Computer System Interface (SCSI) flow statistics:** Logical unit number (LUN)-level SCSI flow statistics are collected for any combination of initiator and target. The scope of these statistics includes read, write, and error statistics. This feature is available only on Cisco MDS 9000 Family storage services modules and the Cisco MDS 9000 Advanced Services Module.

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 provide switch-switch and host-switch authentication. This feature helps eliminate disruptions that may occur because of unauthorized devices connecting to a large enterprise fabric.
- Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP): This protocol is used to perform authentication locally in the 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 the mapping of an entity to a switch port. The entity can be a host, target, or switch and is identified by its WWN. This feature helps ensure that SAN security is not compromised by connection of unauthorized devices to a switch port.
- VSAN-based access control: This feature allows customers to define roles in which the scope of a role is limited to certain VSANs. For example, a network administrator role can be set up to allow configuration of all platform-specific capabilities, and VSAN-administrator roles can be set up to allow configuration and management of only 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), and MDS 9222i Multiservice Modular Switch (MMS). In a future MDS 9000 NXOS release, IPsec shall also be available on the Cisco MDS 9250i Multilayer Fabric Switch, the next-generation intelligent services switch. The proven IETF standard IPsec capabilities offer secure authentication, data encryption for privacy, and data integrity. Internet Key Exchange Version 1 (IKEv1) and IKEv2 protocols are used to dynamically set up the security associations for IPsec using preshared keys for remote-side authentication.
- Digital certificates: Digital certificates are issued by a trusted third party and are used as electronic passports to prove the identity of certificate owners. After the owner's identity is verified by the trusted third party, 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 helps ensure data integrity and privacy. Cisco TrustSec Fibre Channel Link Encryption is an extension of the FC-SP feature and uses the existing FC-SP architecture. Starting with Cisco MDS 9000 NX-OS Release 4.2(1), Fibre Channel data between E-ports of 8-Gbps modules can be encrypted, and in a future MDS 9000 NXOS release, 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) for an interface. AES-GCM mode provides encryption and authentication of the frames, and AES-GMAC provides only the authentication of the frames that are being passed between the two E-ports. Encryption is performed at line rate by encapsulating frames at egress, with encryption using GCM and AES 128-bit encryption. At ingress, frames are decrypted and authenticated for integrity.

There are two primary use cases: one for customers 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 the 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.

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:

- IVR
- IPsec
- Extended credits
- SCSI flow statistics
- 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
M9500ENT1K9 M9500ENT1K9=	• Enterprise Package for one Cisco MDS 9500 Series Multilayer Director • Spare
M9200ENT1K9 M9200ENT1K9=	• Enterprise Package for one Cisco MDS 9200 Series Multilayer Fabric Switch • Spare
M9100ENT1K9 M9100ENT1K9=	• Enterprise Package for one Cisco MDS 9100 Fabric Switch • Spare
L-M95ENT1K9=	• Enterprise Package for one Cisco MDS 9500 Series Multilayer Director, spare-Electronic Delivery
L-M92ENT1K9=	• Enterprise Package for one Cisco MDS 9200 Series Multilayer Fabric Switch, spare-Electronic Delivery
L-M9100ENT1K9=	• Enterprise Package for one Cisco MDS 9100 Fabric Switch, spare-Electronic Delivery
M97ENTK9 M97ENTK9= L-M97ENTK9=	• Enterprise Package for one Cisco MDS 9700 Series Multilayer Director • Spare • Spare-Electronic Delivery

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)