

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)*

# Cisco MDS 9020 Fabric Switch Release Notes for Cisco MDS 9020 FabricWare Release 2.1(2)

---

**Release Date:** August 24, 2005

**Text Part Number:** OL-6990-01 D0

This document describes the caveats and limitations for the Cisco MDS 9020 Fabric Switch. Use this document in conjunction with the documents listed in the “[Related Documentation](#)” section on [page 6](#).

## Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Image Upgrade, page 3](#)
- [Limitations and Restrictions, page 3](#)
- [Caveats, page 3](#)
- [Related Documentation, page 6](#)
- [Obtaining Documentation, page 7](#)
- [Documentation Feedback, page 8](#)
- [Cisco Product Security Overview, page 9](#)
- [Obtaining Technical Assistance, page 10](#)
- [Obtaining Additional Publications and Information, page 11](#)

[Table 1](#) shows the on-line change history for this document.



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Table 1 On-Line History Change**

Revision	Date	Description
A0	08/24/2005	Created release notes
B0	11/10/2005	Added interoperability information (note).
C0	12/20/2005	Corrected SFP part number.
D0	03/02/2006	Added limitation.

## Introduction

The Cisco MDS 9020 Fabric Switch offers Fibre Channel fabric-switching services that enable maximum performance and ensure high reliability. This switch combines robust and flexible hardware architecture and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features. The Cisco MDS 9020 Fabric Switch provides essential storage networking features that include advanced security, debug tools, and unified SAN management.



**Note**

No configuration is needed on the Cisco MDS 9020 Fabric Switch for interoperability with Brocade and McData switches. For information about configuring these third party switches, refer to the *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*.

## System Requirements

This section describes the system requirements for Cisco MDS 9000 FabricWare Release 2.1(2) and includes the following topics:

- [Software and Hardware Supported, page 2](#)
- [Determining the Software Version, page 3](#)

## Software and Hardware Supported

[Table 2](#) lists the software and hardware components supported by the Cisco MDS 9020 Fabric Switch.

**Table 2 Cisco MDS 9020 Fabric Switch Software and Hardware Components**

Component	Part Number	Description	Applicable Products
Software	M90S1K9-2.1.2	MDS 9020 Supervisor/Fabric-I, FabricWare Release 2.1.2	MDS 9020 switch
Chassis	DS-C9020-20K9	MDS 9020 20-Port 4 Gbps Fibre Channel Fabric Switch	MDS 9020 switch
LC-type fiber-optic SFP <sup>1</sup>	DS-SFP-FC4G-SW	1-, 2- or 4-Gbps Fibre Channel — short wavelength SFP	MDS 9000 Family
CD-ROM	M90FM-CD-212=	MDS 9000 Management Software and Documentation CD-ROM, spare	MDS 9000 Family

1. SFP = small form-factor pluggable

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

## Determining the Software Version



### Note

We strongly recommend that you use the latest available software release supported by your vendor for the Cisco MDS 9020 Fabric Switch.

To determine the version of the Cisco MDS 9000 FabricWare software currently running on a Cisco MDS 9020 Fabric Switch using the CLI, log into the switch and enter the **show version EXEC** command.

To determine the version of the Cisco MDS 9000 FabricWare software currently running on a Cisco MDS 9020 Fabric Switch using the Fabric Manager, from the Switches tab in the information pane, locate the switch using its IP address, logical name, or WWN, and then check its version in the Release column.

## Image Upgrade

The Cisco MDS 9000 FabricWare software is designed for high availability environments. As new software releases become available, you can nondisruptively upgrade the switch.

## Limitations and Restrictions

This section lists the limitations and restrictions for this release.

## Merging Fabrics

You must only configure pWWN-type zoning on an MDS switch running Cisco SAN-OS if there is a Cisco MDS 9020 switch running FabricWare in the same fabric to avoid Inter-Switch Link (ISL) isolation. It is important to remove all non-pWWN-type zone entries prior to merging fabrics.

For additional information on zoning, refer to the *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*.

## Caveats

This section lists the open and resolved caveats for this release. Use [Table 3](#) to determine the status of a particular caveat. In the table, “R” indicates a resolved caveat, “O” indicates an open caveat, and “C” indicates a closed caveat.

**Table 3** Caveats for Cisco MDS 9020 Fabricware Release 2.1.2

DDTS Number	State
<b>Severity 2</b>	
• <a href="#">CSCei30894</a>	C
• <a href="#">CSCei52587</a>	O

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

**Table 3** *Caveats for Cisco MDS 9020 Fabricware Release 2.1.2 (continued)*

DDTS Number	State
<b>Severity 2</b>	
<b>Severity 3</b>	
• <a href="#">CSCsc77866</a>	O

## Closed FabricWare Caveats

- CSCei30894

**Symptom:** When Cisco VPN client version 3.6.3 is installed but not used, some of the ISLs might be missing from the Fabric Manager map if an MDS 9020 switch is used as a seed switch for the discovery of the fabric. An SNMP GET-BULK timeout occurs because of an incompatibility between the TCP/IP stack on the MDS 9020 switch and the client stack being configured or tuned during installation of the Cisco VPN client on the client itself.

**Workaround:** If you connect through Cisco VPN client 3.6.3 and then open Fabric Manager, it will discover properly.

## Open FabricWare Caveats

- CSCei52587

**Symptom:** If a Cisco MDS 9020 switch is used as the seed switch for Fabric Manager discovery in a mixed fabric of Cisco MDS 9000 Series switches, some ISL links might be missing.

**Workaround:** Use a Cisco MDS 9100, Cisco MDS 9200, or Cisco MDS 9500 series switch as the seed switch or rediscover the network if it is not possible to have them as seed switches.

- CSCsc77866

**Symptom:** When a fabric including a Cisco MDS 9020 Fabric Switch and third party devices is discovered using Fabric Manager, where the Cisco MDS 9020 Fabric Switch is used as a seed for the discovery, the map might not display some of the end devices (hosts and disks) connected to the third party switches. When the zone with these devices is highlighted on the Fabric Manager map display, the devices on the third party switches are shown as 'not in fabric'. CLI displays for FCNS and zone information are correct.

**Workaround:** None.

## Related Cisco SAN-OS Caveats

Cisco MDS 9000 Family switches must be running Cisco MDS SAN-OS Release 2.1(2) to work properly with a Cisco MDS 9020 switch. This section lists the Cisco SAN-OS caveats related to Cisco FabricWare.

The following caveats are resolved in Cisco SAN-OS Release 2.1(2):

- CSCei39900

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

**Symptom:** If the Cisco MDS 9020 switch is loaded with more devices than recommended, timeouts may occur on a Cisco MDS 9000 Family switch running Cisco MDS SAN-OS Release 2.1(1a) or earlier, when Name Server queries are issued to the loaded Cisco MDS 9020 switch. The queries are retried to the point where the Cisco MDS 9000 Family switch can crash. In Cisco MDS FabricWare Release 2.1(2), the retries are limited to mitigate this effect.

**Workaround:** Upgrade the Cisco MDS 9000 Family switches to Cisco MDS SAN-OS Release 2.1(2).

- CSCei15625

**Symptom:** If a device registers symbolic port names on the Cisco MDS 9020 switch, the same symbolic port names cannot be properly propagated across VSANs through an IVR fabric where the Cisco MDS 9020 switch is an edge switch in the IVR topology.

**Workaround:** None.

- CSCei52222

**Symptom:** When devices with specific FC4-type log-in to a Cisco MDS 9000 Series switch and the Cisco MDS 9020 switch issues a GE\_FT query to a Cisco MDS 9000 Series switch running Cisco MDS SAN-OS Release 2.1(1a) or earlier, the query might be rejected. This will result in that name server entry on the Cisco MDS 9020 switch not having FC4 type information of the device logged into the Cisco MDS 9000 Series switch. The affected FC4 type is 255.

**Workaround:** Upgrade the Cisco MDS 9000 Family switches to Cisco MDS SAN-OS Release 2.1(2).

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at:

[http://www.cisco.com/en/US/products/ps5989/products\\_documentation\\_roadmap09186a00804500c1.html](http://www.cisco.com/en/US/products/ps5989/products_documentation_roadmap09186a00804500c1.html).

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website:

<http://www.ibm.com/storage/support/2062-2300/>

## Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS SVC Releases*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

## Compatibility Information

- *Cisco MDS 9000 SAN-OS Hardware and Software Compatibility Information*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS SAN-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*

## Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

## Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*

**[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Fabric Manager Online Help*
- *Cisco MDS 9000 Fabric Manager Web Services Online Help*

## Command-Line Interface

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family CLI Quick Configuration Guide*
- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Quick Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*

## Troubleshooting and Reference

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9020 Fabric Switch MIB Quick Reference*
- *Cisco MDS 9000 Family SMI-S Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9020 Fabric Switch System Messages Reference*

## Installation and Configuration Note

- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

---

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

---

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access *iQ Magazine* at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

Copyright © 2006 Cisco Systems, Inc. All rights reserved.