Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.0(2a)

Release Date: July 18, 2006

Text Part Number: OL-8795-03 D0

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the "Related Documentation" section on page 19.

Note Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*: http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_release_notes_list.html

Table 1 shows the on-line change history for this document.

Table 1 Online History Change

Revision	Date	Description
A0	7/18/2006	Created release notes
B0	7/24/2006	Modified DDTS CSCse33080. Modified the Upgrading with IVR Enabled section.
C0	8/2/2006	Fixed the status of DDTS CSCsd89872
D0	8/7/2006	Clarified DDTS CSCsd89872 description.

Contents

This document includes the following sections:

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

Introduction

The Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches provides industry-leading availability, scalability, security, and management, allowing you to deploy high performance storage-area networks with lowest total cost of ownership. Layering a rich set of intelligent features onto a high performance, protocol agnostic switch fabric, the Cisco MDS 9000 Family addresses the stringent requirements of large data center storage environments: uncompromising high availability, security, scalability, ease of management, and seamless integration of new technologies.

The Cisco MDS 9000 Family SAN-OS is the underlying system software that powers the Cisco MDS 9500 series, 9200 series, and 9100 series multilayer switches. The Cisco SAN-OS provides intelligent networking features, such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 3.0(2a) and includes the following topics:

Components Supported

Table 2 lists the software and hardware components supported by the Cisco MDS 9000 Family.

Note To use the Cisco Storage Services Enabler package, Cisco MDS SAN-OS Release 1.3(5) or later must be installed on the MDS switch.

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
Software	M95S2K9-3.0.2a	MDS 9500 Supervisor/Fabric-2, SAN-OS software.	MDS 9500 Series only
	M95S1K9-3.0.2a	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S1K9-3.0.2a	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S1K9-3.0.2a	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only
License	M9500ENT1K9	Enterprise package.	MDS 9500 Series
	M9200ENT1K9	Enterprise package.	MDS 9200 Series
	M9100ENT1K9	Enterprise package.	MDS 9100 Series
	M9500FIC1K9	Mainframe package.	MDS 9500 Series
	M9200FIC1K9	Mainframe package.	MDS 9200 Series
	M9100FIC1K9	Mainframe package.	MDS 9100 Series
	M9500FMS1K9	Fabric Manager Server package.	MDS 9500 Series
	M9200FMS1K9	Fabric Manager Server package.	MDS 9200 Series
	M9100FMS1K9	Fabric Manager Server package.	MDS 9100 Series
	M9500EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9500 Series
	M9200EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9200 Series
	M9500EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9500 Series
	M9200EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9200 Series
	M9500EXT12K9	SAN Extension over IP package for MPS 14+2 module.	MDS 9500 Series
	M9200EXT12K9	SAN Extension over IP package for MPS 14+2 module.	MDS 9200 Series
	M9500SSE1K9	Storage Services Enabler package.	MDS 9500 Series with SSM
	M9200SSE1K9	Storage Services Enabler package.	MDS 9200 Series with SSM

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Chassis	DS-C9513	MDS 9513 director (13-slot modular chassis with 11 slots for switching modules, and 2 slots reserved for Supervisor 2 modules only—SFPs[1] sold separately).	MDS 9513 only
	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9509 only
	DS-C9506	MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9506 only
	DS-C9216-K9	MDS 9216 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216 only
	DS-C9216A-K9	MDS 9216A 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216A only
	DS-C9216i-K9	MDS 9216i 16-port semi-modular fabric switch (includes 14 1-Gbps/2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216i only
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports).	MDS 9140 only
	DS-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 only
Supervisor modules	DS-X9530-SF2-K9	MDS 9500 Supervisor-2, module.	MDS 9500 Series only
	DS-X9530-SF1-K9	MDS 9500 Supervisor/Fabric-I module.	
Switching modules	DS-X9016	MDS 9000 16-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series
	DS-X9032	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	
	DS-X9112	MDS 9000 12-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216
	DS-X9124	MDS 9000 24-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216
	DS-X9148	MDS 9000 48-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216
	DS-X9704	MDS 9000 4-port 10-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9200 Series, except for the MDS 9216

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP Storage services module.	MDS 9500 Series and 9200 Series
	DS-X9304-SMIP	4-port Gigabit Ethernet IP Storage services module.	
	DS-X9032-SSM	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	
Optics	DS-X2-FC10G-SR	X2/SC optics, 10-Gbps Fibre Channel for short wavelength mode.	MDS 9500 Series and 9200 Series, except for the MDS 9216
	DS-X2-FC10G-LR	X2/SC optics, 10-Gbps Fibre Channel for long wavelength mode.	
LC-type fiber-optic SFP	DS-SFP-FC-2G-SW[2]	2-Gbps/1-Gbps Fibre Channel—short wavelength SFP.	MDS 9000 Family
	DS-SFP-FC-2G-LW[2]	2-Gbps/1-Gbps Fibre Channel—long wavelength SFP.	
	DS-SFP-FCGE-SW[2]	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—short wavelength SFP.	
	DS-SFP-FCGE-LW[2]	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—long wavelength SFP.	
	DS-SFP-GE-T[2]	1-Gbps Ethernet SFP.	
	DS-SFP-FC4G-SW[3]	4-Gbps/2-Gbps/1-Gbps Fibre Channel—short wavelength SFP for DS-X91xx switching modules.	
	DS-SFP-FC4G-MR[3]	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 4 km.	
	DS-SFP-FC4G-LW[3]	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 10 km.	
CWDM[4]	DS-CWDM-xxxx	Gigabit Ethernet and 1-Gbps/2-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm.	MDS 9000 Family
	DS-CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths.	
	DS-CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths.	
	DS-CWDMCHASSIS	Two slot chassis for CWDM add/drop multiplexers.	

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Power supplies	DS-CAC-6000W	6000-W AC power supply.	MDS 9513 only
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC power supply.	
	DS-CAC-3000W	3000-W AC power supply.	
	DS-CAC-4000W-US	4000-W AC power supply for US (cable attached).	
	DS-CAC-4000W-INT	4000-W AC power supply international (cable attached).	
	DS-CAC-1900W	1900-W AC power supply.	MDS 9506 only
	DS-CDC-1900W	1900-W DC power supply.	
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-300W	300-W[5] AC power supply.	MDS 9100 Series only
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512 MB.	MDS 9500 Series only
Port analyzer adapter	DS-PAA-2, DS-PAA	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	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
2. Supported on the DS-X9530-SF1-K9, MDS 9500 Series Supervisor module only
3. Supported on the DS-X9530-SF2-K9, MDS 9500 Series Supervisor-2 module only
4. CWDM = coarse wavelength division multiplexing
5. W = Watt

Determining the Software Version

Note We strongly recommend that you use the latest available software release supported by your vendor for all Cisco MDS 9000 Family products.

To determine the version of Cisco MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the CLI, log in to the switch and enter the **show version** EXEC command.

To determine the version of Cisco MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the Fabric Manager, view the Switches tab in the Information pane, locate the switch using the IP address, logical name, or WWN, and check its version in the Release column.

Downloading Software

To download the latest Cisco MDS SAN-OS software, access the Software Center at this URL:

http://www.cisco.com/public/sw-center

Upgrading Your Cisco MDS SAN-OS Software Image

The Cisco MDS SAN-OS software is designed for mission-critical, high-availability environments. To realize the benefits of nondisruptive upgrades on the Cisco MDS 9500 Directors, we highly recommend that you install dual supervisor modules.

Note If you would like to request a copy of the source code under the terms of either GPL or LGPL, please send an e-mail to mds-software-disclosure@cisco.com.

Use the following guidelines to nondisruptively upgrade your Cisco MDS SAN-OS Release 3.0(2a):

- Install and configure dual supervisor modules.
- Upgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*.
- On a system with at least one SSM installed, the **install all** command might fail on an SSM when you downgrade from Cisco SAN-OS Release 3.0(1) to any SAN-OS 2.x release earlier than SAN-OS Release 2.1(2e). Power down the SSM and perform the downgrade. Bring up the SSM with the new bootvar set to the 2.x SSI image.
- Follow this upgrade path for your current release:
  - Upgrading from Cisco SAN-OS Release 1.x to Release 3.x requires that you upgrade first to Release 1.3(4a), then upgrade to Release 2.1(2b), and then upgrade to Release 3.0(2a) .
  - Upgrading from Cisco SAN-OS Release 2.0(2b), 2.0(2c), 2.0(3), 2.1(2b), 2.1(2c), 2.1(2d), 2.1(2e), or 3.0(1) allows you to nondisruptively upgrade directly to Release 3.0(2a). If you do not have one of these releases installed, you must upgrade first to Cisco SAN-OS Release 2.1(2b) and then upgrade to Release 3.0(2a).
  - Upgrading from other Cisco SAN-OS Release 2.x releases to Release 3.x requires that you upgrade first to Release 2.1(2b), and then upgrade to Release 3.0(2a).
  - If you have IVR enabled and you are upgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a), then there are additional steps you should follow before upgrading. See "Upgrading with IVR Enabled" section on page 8.
  - If you have FICON enabled and you are upgrading from Cisco SAN-OS Release 1.x to Release 3.x then first upgrade to Release 1.3(4a), then upgrade to Release 2.0(2b), and then upgrade to Release 3.0(2a).
- The traffic on all Gigabit Ethernet ports is disrupted during an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module. This impacts those nodes that are members of VSANs traversing an FCIP ISL and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the upgrade is in progress.
- Layer 3 switching on SSM ports is disrupted during upgrades or downgrades. Layer 2 switching is not disrupted under the following conditions:
  - Upgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*.
  - All SSM applications are disabled. Use the **show ssm provisioning** CLI command to determine what applications are configured. Use the **no ssm enable feature** CLI command to disable these applications.

  - No SSM ports are in auto mode. See the "Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.0(2a)" section on page 10.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module** *slot* **epld** CLI command to determine your EPLD version. Refer to the *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images* to upgrade your EPLD image.
  - Refer to the *Cisco MDS Storage Services Module Interoperability Support Matrix* and the "Managing Modules" chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x*, for information on upgrading your SSM.

- Use the **show install all impact** *upgrade-image* CLI command to determine if your upgrade will be nondisruptive.

Caution Upgrading to Cisco MDS SAN-OS Release 2.1(2) or later from any release can disrupt traffic on any SSM installed on your MDS switch.

Note Upgrading from Cisco MDS SAN-OS Release 1.x directly to Cisco SAN-OS Release 3.x is disruptive to all Fibre Channel and Gigabit Ethernet ports.

Note For more information on determining software compatibility, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

Upgrading with IVR Enabled

An Inter-Switch Link (ISL) flap resulting in fabric segmentation or a merge during or after an upgrade from Cisco MDS SAN-OS Release 2.0(x) to a later image where IVR is running might be disruptive. Some possible scenarios include:

- FCIP connection flapping during the upgrade process resulting in fabric segmentation or merge.
- ISL flap results in fabric segmentation or merge because of hardware issues or a software bug.
- ISL port becomes part of PCP results in fabric segmentation or merge because of a port flap.

If this problem occurs, syslogs indicate RDI failure and the flapped ISL could remain in a down state because of a domain overlap. This is caused by conflicts between the allowed domains list and the virtual domain requested through RDI.

This issue was resolved in an earlier release, however upgrades from Cisco SAN-OS Release 2.1(1a), 2.1(1b), or 2.1(2a) to Release 3.0(2a) when IVR is enabled requires that you use the following workaround.

For VSANS in interop mode 2 or 3, issue an IVR refresh, and then follow the upgrade guidelines listed in "Upgrading Your Cisco MDS SAN-OS Software Image" section on page 7.

To upgrade from Cisco SAN-OS Release 2.1(1a), 2.1(1b), or 2.1(2a) to Release 3.0(2a) for all other VSANs with IVR enabled, follow these steps:

Step 1 Configure static domains for all switches in all VSANs where IVR is enabled. Configure the static domain the same as the running domain so that there is no change in domain IDs. Make sure that all domains are unique across all of the IVR VSANs. We recommend this step as a best practice for IVR-non-NAT mode. Issue the **fcdomain domain** *id* **static vsan** *vsan id* command to configure the static domains.

Note Complete Step 1 for all switches before moving to Step 2.

Step 2 Issue the **no ivr virtual-fcdomain-add vsan-ranges** *vsan-range* command to disable RDI mode on all IVR enabled switches. The range of values for a VSAN ID is 1 to 4093. This can cause traffic disruption.

Note Complete Step 2 for all IVR enabled switches before moving to Step 3.

Step 3 Check the syslogs for any ISL that was isolated.

```
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED:
%$VSAN 2005%$ Isolation of interface
port-channel 52 (reason: unknown failure)
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED: %$VSAN 2005%$
Isolation of interface port-channel 51
(reason: domain ID assignment failure)
```

Step 4 Issue the following commands for the isolated switches in Step 3:

```
switch(config)# vsan database
switch(config-vsan-db)# vsan vsan-id suspend
switch(config-vsan-db)# no vsan vsan-id suspend
```

Step 5 Issue the **ivr refresh** command to perform an IVR refresh on all the IVR enabled switches.

Step 6 Issue the **copy running-config startup-config** command to save the RDI mode in the startup configuration on all of the switches.

Step 7 Follow the normal upgrade guidelines for Release 3.0(2a) in the "Upgrading Your Cisco MDS SAN-OS Software Image" section on page 7.

If you are adding new switches running Cisco MDS SAN-OS Release 3.0(x), upgrade all your existing switches to Release 3.0(2a) as described in this procedure. Then add new switches.

Note RDI mode should not be disabled for VSANs running in interop mode 2 or interop mode 3.

Selecting the Correct Software Image for an MDS 9500 Series Switch

The system and kickstart image that you use for an MDS 9500 Series switch depends on whether the switch is based on a Supervisor-1 module or a Supervisor-2 module, as shown in Table 3.

Table 3 Software Image for Supervisor Type

Supervisor Type	Switch	Image
Supervisor-1 module	MDS 9506 and 9509	Filename begins with m9500-sf1ek9
Supervisor-2 module	MDS 9506, 9509, and 9513	Filename begins with m9500-sf2ek9

Use the **show module** command to display the type of supervisor module in the switch.

For a Supervisor-1 module, the output might look like this:

```
switch# show module
```

```
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
...
...
5    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active*
6    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    ha-standby
```

For a Supervisor-2 module, the output might look like this:

```
switch# show module
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
...
...
7    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    active *
8    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    ha-standby
```

Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.0(2a)

Starting with Cisco MDS SAN-OS Release 3.0(1), the SSM front panel ports can no longer be configured in auto mode. Because auto mode is the default for releases prior to Release 3.0(1), you should modify the configuration of the ports before upgrading a SAN-OS software image prior to Release 3.0(1) to Release 3.0(2a) to avoid any traffic disruption.

For more information on upgrading SAN-OS software, see the "Upgrading Your Cisco MDS SAN-OS Software Image" section on page 7.

If the configuration is not updated before the upgrade, the installation process for the new image will automatically convert all ports configured in auto mode to Fx mode. This might cause a disruption if the port is currently operating in E mode.

To make the configuration change without any traffic disruption, follow these steps:

Step 1 Verify the operational mode for each port on the SSM using the **show interface** command:

```
switch# show interface fc 2/1 - 32
fc2/1 is up
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:4b:00:0d:ec:09:3c:00
    Admin port mode is auto             <-------- shows port is configured in auto mode
    snmp traps are enabled
    Port mode is F, FCID is 0xef0300   <-------- shows current port operational mode is F
    Port vsan is 1
    Speed is 2 Gbps
    Transmit B2B Credit is 3
```

Step 2 Change the configuration for the first port of the quad when the admin port mode is auto. (A quad is a group of four ports, supported by a data path processor (DPP). The groups are 1 to 4, 5 to 8, 9 to 12, and so on.) Do not leave the port mode set to auto.

a. Set the port admin mode to Fx if the current operational port mode is F or FL.

```
switch# config t
switch(config)# interface fc 2/1
switch(config-if)# switchport mode fx
```

b. Set the port admin mode to E if the current operational port mode is E:

```
switch# config t
switch(config)# interface fc 2/5
```

```
switch(config-if)# switchport mode e
```

Step 3 Change the configuration for ports 2, 3, and 4 of the quad:

a. If the admin port mode of these ports is auto or E, change the admin port mode to Fx.

```
switch# config t
switch(config)# interface fc 2/2
switch(config-if)# switchport mode fx
```

b. If the first port in the port group has admin mode E or if the port is operational in E port mode, change the admin state of ports 2, 3, and 4 to shutdown.

```
switch# config t
switch(config)# interface fc 2/2
switch(config-if)# shutdown
```

Step 4 Save the running configuration to the startup configuration before the upgrade procedure to ensure that the changes are preserved during and after the upgrade. To save the configuration, enter the following command:

```
switch# copy running-config startup-config
```

Migrating from Supervisor-1 Modules to Supervisor-2 Modules

As of Cisco MDS SAN-OS Release 3.0(1), the Cisco MDS 9509 and 9506 Directors support both Supervisor-1 and Supervisor-2 modules. Supervisor-1 and Supervisor-2 modules cannot be installed in the same switch, except during migration. Both the active and standby supervisor modules must be of the same type, either Supervisor-1 or Supervisor-2 modules. For Cisco MDS 9513 Directors, both supervisor modules must be Supervisor-2 modules.

Caution Migrating your supervisor modules is a disruptive operation.

Note Migrating from Supervisor-2 modules to Supervisor-1 modules is not supported.

To migrate from a Supervisor-1 module to a Supervisor-2 module, refer to the step-by-step instructions in the *Cisco MDS 9000 Family CLI Configuration Guide*.

Configuring Generation 2 Switching Modules

The Cisco MDS 9500 Multilayer Directors are designed to operate with any combination of Cisco MDS 9000 Generation 1 and Generation 2 modules. However, there are limitations to consider when combining the various modules and supervisors in the Cisco MDS 9500 Series platform chassis. The references listed in this section provide specific information about configurations that combine different modules and supervisors.

For information on configuring Generation 2 switching modules, refer to:

http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080664c6b.html

For information on port index availability, refer to:

http://www.cisco.com/en/US/products/ps5990/products_installation_guide_chapter09186a0080419599.html

For information on Cisco MDS 9000 hardware and software compatibility, refer to:

http://www.cisco.com/en/US/products/ps5989/products_device_support_table09186a00805037ee.html

New Features in Cisco MDS SAN-OS Release 3.0(2a)

This section describes the new features introduced in this release. For more information about the features listed, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* and the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

Note These release notes are specific to this release. For the complete Release 3.x documentation set, see the "Related Documentation" section on page 19.

There are no new features available for this release.

Limitations and Restrictions

This section lists the limitations and restrictions for this release.

Downgrading from Cisco MDS SAN-OS Release 3.0(2a)

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.0(2a):

- Install and configure dual supervisor modules.
- Downgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*.
- Disable all features not supported by the downgrade release. Use the **show incompatibility system** *downgrade-image* CLI command to determine what you need to disable.
- Follow the downgrade path for your current release:
  - Downgrading to Cisco SAN-OS Release 1.x from Release 3.x requires that you downgrade first to Release 2.1(2b), then downgrade to Release 1.3(4a), and then downgrade to your 1.x release.
  - You can downgrade nondisruptively from Release 3.x to the following releases: 2.0(2b), 2.0(2c), 2.0(3), 2.1(2b), 2.1(2c), 2.1(2d), 2.1(2e), or 3.0(1).
  - Downgrading to other Cisco SAN-OS Release 2.x releases from Release 3.x requires that you downgrade first to Release 2.1(2b) and then downgrade to an earlier 2.x release.
  - Downgrading for FICON to Cisco SAN-OS Release 1.x from Release 3.x requires that you downgrade first to Release 2.0(2b), then downgrade to Release 1.3(4a), and then downgrade to your 1.x release.
- Traffic on all Gigabit Ethernet ports is disrupted on an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module. This impacts those nodes that are members of VSANs traversing an FCIP ISL or iSCSI initiators connected to the Gigabit Ethernet ports.
- Layer 3 switching on SSM ports is disrupted on upgrades or downgrades.

- Layer 2 switching on SSM ports is not disrupted under the following conditions:
  - All SSM applications are disabled. Use the **show ssm provisioning** CLI command to determine if any applications are provisioned on the SSM. Use the **no ssm enable feature** configuration mode CLI command to disable these features.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module** *slot* **epld** CLI command to determine your EPLD version. Refer to the *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images* to upgrade your EPLD image.
  - Refer to the *Cisco MDS Storage Services Module Interoperability Support Matrix* and to the "Managing Modules" chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x* for information on downgrading your SSM.
- Layer 2 switching traffic is not disrupted when downgrading to Cisco SAN-OS Release 2.1(2) or later.

Use the **show install all impact** *downgrade-image* CLI command to determine if your downgrade will be nondisruptive.

iSNS

The iSNS client and server are not supported in this release.

Reconfiguring SSM Ports

Starting with Cisco MDS SAN-OS Release 3.0(1), the SSM front panel ports can no longer be configured in auto mode, which is the default for releases prior to Release 3.0(1). For instructions about how to modify the configuration of the ports before upgrading to SAN-OS Release 3.0(2a), see the "Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.0(2a)" section on page 10.

Caveats

This section lists the open and resolved caveats for this release. Use Table 4 to determine the status of a particular caveat. In the table, "O" indicates an open caveat, "C" indicates a closed caveat, and "R" indicates a resolved caveat.

Table 4 Open Caveats and Resolved Caveats Reference

	Software Release (Open or Resolved)	
DDTS Number	**3.0(2)**	**3.0(2a)**
Severity 2		
CSCei82909	O	O
CSCsc45880	O	O
CSCsd47064	O	O
CSCsd95862	O	R
CSCse14087	O	R
CSCse33080	O	R

Table 4 Open Caveats and Resolved Caveats Reference (continued)

	Software Release (Open or Resolved)	
DDTS Number	**3.0(2)**	**3.0(2a)**
CSCse35720	–	O
CSCse56522	O	R
CSCse57269	O	O
CSCse67109	O	O
Severity 3		
CSCeg55238	O	R
CSCin95789	O	O
CSCsc95657	O	O
CSCsd19272	O	O
CSCsd34882	O	R
CSCsd51194	O	O
CSCsd52037	O	O
CSCsd79938	O	O
CSCsd89872	O	O
CSCse12209	O	O
CSCse13769	O	R
CSCse13999	O	R
CSCse14032	O	R
CSCse36768	O	R
CSCse42040	O	O

Resolved Caveats

- CSCsd95862

  Symptom: Cisco MDS 9100 Series switches and the 9216i switch do not handle counter roll-over appropriately and might reset after being up for 497 days. MPS-14/2 modules are also susceptible and could be reset by the supervisor.

  Workaround: None. This issue has been resolved.

- CSCse14087

  Symptom: During a link flap, the FCIP tape acceleration feature could get into a state where if the tape is slow in responding, the backup or restore operation may fail.

  Workaround: None. This issue has been resolved.

- CSCse33080

  Symptom: In some cases, after a nondisruptive upgrade (or downgrade) of 48-port and 24-port 4-Gbps Fibre Channel switching modules from Cisco SAN-OS Release 3.0(1) to Release 3.0(2) (or a downgrade from Release 3.0(2) to Release 3.0(1)), the next port flap could result in oversubscribed ports coming up in error-disabled state.

  Workaround: None. This issue has been resolved.

- CSCse56522

  Symptom: In some cases, when a VSAN is in suspended mode, the switch with the suspended VSAN does not appear in the table on the Information pane of the GUI.

  Workaround: None. This issue has been resolved.

- CSCeg55238

  Symptom: Files created using the **fcanalyzer local** command cannot be copied or viewed. Fibre Channel analyzer runs as root, and it creates files with the owner as root. The correct file creation masks are not set when the file is created, so no user other than root can read or copy the file.

  Workaround: None. This issue has been resolved.

- CSCsd34882

  Symptom: The Cisco SAN-OS software creates a syslog message after a configuration change through the command-line interface The syslog message looks like this:

  ```
  switch# 2006 Feb 8 09:00:33 switch %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
  from pts/1 (dhcp-peg3-vl30-144-254-7-182.cisco.com)
  ```

  Using the Fabric Manager to make the same configuration change generates a different syslog message:

  ```
  switch# 2006 Feb 8 09:00:56 switch %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Interface
  fc1/5 is down (Administratively down)
  ```

  Workaround: None. This issue has been resolved.

- CSCse13769

  Symptom: In some cases of link flapping (a link down or up due to removal or insertion of cables or transceivers) on 10-Gbps ISLs, an early LR might arrive before the ELP exchange is complete and would trigger a transmit credit update to the port. This causes the switch port transmit credit to program to the default value of one (1) instead of the actual number configured. This might cause an impact to performance.

  Workaround: None. This issue has been resolved.

- CSCse13999

  Symptom 1: SNMP events are not visible in Fabric Manager because Fabric Manager is unable to register to receive SNMP notifications, even though Device Manager is registered to receive SNMP notifications from the MDS switch.

  Symptom 2: Cisco EMC Call Home does not send call home messages. Cisco EMC Call Home is a new feature for Cisco SAN-OS Release 3.0(1). This does not affect the other Cisco Call Home features.

  Workaround: None. This issue has been resolved.

- CSCse14032

  Symptom: The iSNS server process terminates when ISNS-SERVER is enabled on a switch that has more than 100 iSCSI initiators.

  Workaround: None. This issue has been resolved.

- CSCse36768

  Symptom: The Cisco MDS 9100 and 9200 Series switches might see excessive debugging messages sent to the CompactFlash causing a rare condition where the CompactFlash could lock up. If this occurs, you might experience an inability to save a new configuration to the Flash and a reboot of the switch is required to recover from this failure. If a successful administrative function requires a write to CompactFlash or there is an update within the fabric, then unexpected behavior might occur.

  Workaround: None. This issue has been resolved.

Open Caveats

- CSCed16845

  Symptom: Occasionally, the Common Information Model (CIM) server may be automatically restarted because of an internal error. In this case, the connected CIM client is disconnected.

  Workaround: You must explicitly reconnect the CIM client to the CIM server.

- CSCeg12383

  Symptom: On rare occasions, the PortChannels with FCIP interface members fail to come up when the switch reboots. This occurrence happens when the startup configuration has a default switch port trunk mode setting that does not match the configured trunk mode for PortChannel members (FCIP interfaces). Also, the startup configuration shows any explicit switch port trunk mode setting for the PortChannel.

  Workaround: Reconfigure the switch port trunk mode on the PortChannel.

- CSCeg37598

  Symptom: The iSNS server might crash when iSCSI is disabled and iSNS is enabled using Fabric Manager.

  Workaround: None.

- CSCse35720

  Symptom: If you have a Port Channel with multiple FCIP tunnels, and Write Acceleration is enabled on the the FCIP tunnels, the end device might reboot with an error after the Port Channel comes up or if fcping is issue to that device.

  Workaround: Disable FCIP Write Acceleration on all FCIP tunnels in the Port Channel or configure only a single FCIP tunnel in the Port channel.

- CSCse57269

  Symptom: You cannot bind more than one FCIP interface on Gigabit Ethernet port 2 on an MPS-14/2 module in Cisco SAN-OS Release 3.0(1) and Release 3.0(2).

  Workaround: None.

- CSCse67109

  Symptom: On a 24- or 48-port Fibre Channel switching module, if all ports in a port group are switching traffic at the ports group's full bandwidth, and there is a mix of over-ubscribed and full rate ports, the first four ports in the group might exhibit a transmit credit underrun condition.

  Workaround: Reset the 24- or 48-port FC switching module, or upgrade to Cisco SAN-OS Release 3.0(2a).

- CSCin95789

  Symptom: When you configure Cisco Traffic Analyzer to capture traffic on one or more interfaces on a Windows platform, the configuration web page might not show that the interface has been selected for traffic capture even though traffic capture on that interface is enabled.

  Workaround: Check the logs to clarify that the correct interface has been selected.

- CSCei82909

  Symptom: The implementation of the Internet Key Exchange (IKE) version 2 in MDS switches may not be interoperable with other IKE version 2 implementations. Our IKE version 2 implementation is used whenever an encrypted FCIP tunnel is established between two MDS switches.

  Workaround: If an MDS switch tries to establish an IKE version 2 tunnel with a non-MDS switch running IKE version 2, or vice versa, the gateway or the MDS switch should be configured to use IKE version 1 for that tunnel.

- CSCsc45880

  Symptom: When suspending or deleting VSANs with no delay between those actions, some Fibre Channel interfaces and member ports in a PortChannel are suspended or error-disabled.

  Workaround: Make sure that you suspend and unsuspend one VSAN at a time, and that you wait a minimum of 60 seconds after you issue the **vsan suspend** command before you issue any other configuration command.

- CSCsd47064

  Symptom: The Forwarding Information Base (FIB) process may fail if an IVR zone set push from the Fabric Manager fails because of an SNMP timeout and various switches send conflicting active IVR zone sets.

  Workaround: There are two ways to address the problem:

  - Examine the output of the **show interface mgmt 0** command to see if there is a duplex mismatch that may cause an SNMP timeout.
  - Use the **ivr distribute** command to enable Cisco Fabric Services (CFS) distribution for IVR zone or zone sets and the topology through Inter-Switch Links (ISLs).

- CSCsc95657

  Symptom: When an administrator configures a serverless backup with CommVault QiNetix 5.9, the backup fails the first time (or each time the disks are reconfigured using Volume Explorer on CommVault) a Reservation Conflict error on the disk.

  Workaround: Reset the disk and retry the configured serverless backup.

- CSCsd19272

  Symptom: The Cisco MDS 9216i switch and MPS-14/2 module do not support an MTU size greater than 8000 bytes. An attempt to set the MTU size greater than 8000 bytes will result in an error.

  Workaround: Reset the value of the MTU size (576 to 8000 bytes) and issue the **no shutdown** command on the interface for normal operation.

- CSCsd51194

  Symptom: When a switchover occurs on a switch that is the master for Virtual Router Redundancy Protocol (VRRP) interfaces, the switchover may cause a minor delay. As a result, the VRRP backup (occurring elsewhere) may assume the role of the VRRP master.

  Workaround: Increase the VRRP advertisement interval for these interfaces.

- CSCsd52037

  Symptom: A serverless backup of a volume spanning multiple tapes does not work with CommVault QiNetix 5.9 because CommVault QiNetix 5.9 is not able to determine the end of tape.

  Workaround: None.

- CSCsd79938

  Symptom: After using the **ip access-group** command to configure an access list for the mgmt0 interface and saving the running configuration to the startup configuration, the **ip access-group** command is not present following a reboot of the running configuration. However, the command is in the startup configuration, and the access list is still in the configuration, but the access list is not applied to the mgmt0 interface.

  Workaround: Reissue the **ip access-group** command or issue a **copy startup-config running-config** command to replace the **ip access-group** command.

- CSCsd89872

  Symptom: When using Cisco MDS SAN-OS Release 2.1(2e) or earlier to configure PortChannels, the following message may be displayed:

  ```
  Last membership update failed: port-channel: required service is not responding
  (err_id 0x402B No port
  ```

  If this issue occurs, any attempt to delete the PortChannel will fail and no additional operations can be performed on that specific PortChannel that gave the error.

  Workaround: Upgrade from Cisco SAN-OS Release 2.1(2e) or earlier to Release 3.0(2a) to prevent the problem from occurring. If the problem has already occurred, an upgrade to Release 3.0(2a) will not correct the problem. Issue the **write erase** command and reboot the system to correct this problem.

- CSCse12209

  Symptom: When using Fabric Manager and SNMP, a login does not occur when a user ID contains a backslash "\".

  Workaround: None.

- CSCse42040

  Symptom: If you try to create a user with a weak password, it fails. Subsequent attempts to create the same user with a strong password also fail because of an inConsistentValue error. This is because when the creation failed in the first set, the undo is not handled completely.

  Workaround: Issue the **no snmp-server** *username* command in the CLI before the user creation is attempted a second time.

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. 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*

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.

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML 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= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

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 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.

You can submit comments about Cisco documentation 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

From this site, you will find information about how to:

- 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, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

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 have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—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.

- For Nonemergencies—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 (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*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 at this URL:

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.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

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

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)—An existing 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 operations 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 the network is impaired, while 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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- 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

- *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.