Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 1.1(1)

CCO Date: February 4, 2004

Text Part Number: OL-4376-01 A0

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 17.

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 On-Line History Change

Revision	Date	Description
A0	06/23/2005	Added DDTS CSCei25319

Contents

This document includes the following section:

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 offer intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. They combine robust and flexible hardware architecture with multiple layers of network and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9000 Family 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 1.1(1) and includes the following topics:

- Hardware Supported, page 32
- Determining the Software Version, page 5
- Feature Set, page 5

Hardware Supported

Table 2 lists the hardware components supported on the Cisco MDS 9000 Family and the minimum software version required. See the "Determining the Software Version" section on page 5.

Table 2 Cisco MDS 9000 Family Supported Hardware Modules and Minimum Software Requirements

Component	Part Number	Description	Applicable Products
Software	M9500-SF1EK9-1.1.1	MDS 9500 Series supervisor/fabric-I, enterprise software	MDS 9509 only
	M9200-EK9-1.1.1	MDS 9216 enterprise software	MDS 9216 only
Chassis	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 sixteen 1 / 2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately)	MDS 9216 only
Supervisor modules	DS-X9530-SF1-K9	MDS 9500 supervisor/fabric-I, module	MDS 9500 Series only

Table 2 Cisco MDS 9000 Family Supported Hardware Modules and Minimum Software Requirements

Component	Part Number	Description	Applicable Products
Switching modules	DS-X9016	MDS 9000 16-port 1/2-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9216
	DS-X9032	MDS 9000 32-port 1/2-Gbps Fibre Channel module (SFPs sold separately)	
Services modules	DS-X9308-SMIP	An eight-port (8) Gigabit Ethernet IP storage services module.	
LC-type fiber-optic SFP[1]	DS-SFP-FC-2G-SW	1/2-Gbps Fibre Channel — short wave SFP	MDS 9500 Series and 9216
	DS-SFP-FC-2G-LW	1/2-Gbps Fibre Channel — long wave SFP	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 1/2-Gbps Fibre Channel—short wave SFP	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 1/2-Gbps Fibre Channel — long wave SFP	
CWDM[2]	CWDM-SFP-xxxx-2G	Gigabit Ethernet and 1/2-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470 nm, 1490 nm, 1510 nm, 1530 nm, 1550 nm, 1570 nm, 1590 nm, 1610 nm	MDS 9500 Series and 9216
	CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths	
	CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths	
	CWDM-CHASSIS-2	Two slot chassis for CWDM add/drop multiplexer(s)	
Power supplies	DS-CAC-845W	845W[3] AC power supply for MDS 9216	MDS 9216 only
	PWR-845-AC	845W AC power supply for MDS 9216	
	DS-CAC-2500W	2500W AC power supply	MDS 9509 only
	DS-CDC-2500W	2500W DC power supply	
	DS-CAC-4000W-US	4000W AC power supply for US (cable attached)	
	DS-CAC-4000W-INT	4000W AC power supply international (cable attached)	
	DS-CAC-1900W	1900W AC power supply for MDS 9506	MDS 9506 only
	DS-CDC-1900W	1900W DC power supply for MDS 9506	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB	MDS 9500 Series only
Port analyzer adapter	DS-PAA	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	MDS 9500 Series and 9216

1. SFP = small form factor pluggable
2. CWDM = coarse wave division multiplexing
3. W = Watt

Determining the Software Version

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

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

Feature Set

This Cisco MDS SAN-OS Release 1.1(1) software is packaged in feature sets (also called software images) depending on the platform. The Cisco MDS SAN-OS software feature sets available for the Cisco MDS 9000 Family include Ethernet, Fibre Channel (1 Gbps and 2 Gbps), SNMP, and IP packets.

Compatibility Matrix

Table 3 lists the compatible matrix for nondisruptive upgrades.

Table 3 Nondisruptive Upgrade Compatibility Matrix

From	To	Supported
Release 1.0(3a)	Release 1.1	Yes
Release 1.0(4)	Release 1.1	Yes
Release 1.0(2a)	Release 1.1	No

New Features in Release 1.1(1)

Caution Release 1.1(1) has been deferred, please use SAN-OS Release 1.1(1a) or later.

SAN-OS Release 1.1(1) is a major release for switches in the Cisco MDS 9000 Family. See the "Caveats" section on page 10 for details on closed and outstanding caveats and limitations. The following new features are introduced in Release 1.1(1):

- MDS 9506 Chassis, page 6
- CWDM/SFPs, page 6
- IP Services Module, page 6
- iSCSI and FCIP, page 6
- iSCSI and FCIP, page 6
- Zoning, page 7
- CDP, page 7

MDS 9506 Chassis

The Cisco MDS 9506 has a 6-slot chassis with the same features as the Cisco MDS 9509. It has space for two supervisor modules, and four switching or services modules. However, the power supplies are located in the back of the chassis, with the Power Entry Modules (PEMS) in the front of the chassis for easy access.

See the *Cisco MDS 9500 Series Hardware Installation Guid*e.

CWDM/SFPs

The Cisco MDS 9000 Family supports Cisco Coarse Wavelength-Division Multiplexing (CWDM) Small Form-factor Pluggables (SFPs). Cisco CWDM SFPs allow enterprise companies and service providers to provide scalable and easy-to-deploy Gigabit Ethernet and Fibre Channel services in their networks. The main features of the Cisco CWDM SFP are as follows:

- Supports both Gigabit Ethernet and Fibre Channel (1Gigabit and 2 Gigabit).
- Matches wavelength plan of Cisco CWDM GBICs and Cisco CWDM OADMs.
- Fixed wavelength SFPs—eight different SFPs.
- Hot-swappable input/output device that plugs into a Gigabit Ethernet and Fibre channel SFP ports or slots of a Cisco switch/ router, linking the port with the network.
- Cisco CWDM SFPs can be used and interchanged on a wide variety of Cisco products and can be intermixed in combinations of 1000BASE-SX, 1000BASE-LX/LH, or 1000BASE-ZX on a port-by-port basis.

See the *Cisco MDS 9000 Family Hardware Guides*.

IP Services Module

The IP Storage (IPS) services module (IPS module) allows you to use FCIP and iSCSI features. It integrates seamlessly into the Cisco MDS 9000 Family, and supports the full range of features available on other switching modules, including VSANs, security, and traffic management.

See the *Cisco MDS 9000 Family Hardware Installation Guides* and the *Cisco MDS 9000 Family Configuration Guide.*

iSCSI and FCIP

The Cisco MDS 9000 Family IP services module integrates seamlessly into the Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches. It delivers both Fibre Channel over IP (FCIP) and iSCSI IP storage services and is configurable on a port-by-port basis.

- FCIP highlights

  - Simplifies data protection and business continuance strategies by enabling backup, remote replication, and disaster recovery over WAN distances using open-standard FCIP tunneling.
  - Improves utilization of WAN resources for backup and replication by tunneling up to 3 virtual Inter Switch Links (ISLs) on a single Gigabit Ethernet port.
  - Reduces SAN complexity by eliminating the need to deploy and manage a separate remote connectivity platform.
  - Preserves Cisco MDS 9000 Family enhanced capabilities including VSANs, advanced traffic management, and security across remote connections.
- iSCSI highlights
  - Extends the benefits of Fibre Channel SAN-based storage to IP-enabled servers at a lower cost point than possible using Fibre Channel interconnect alone.
  - Increases storage utilization and availability through consolidation of IP and Fibre Channel block storage.
  - Transparent operation preserves the functionality of legacy storage applications such as zoning tools.
  - Extending the Benefits of Fibre Channel SANs
  - Supports iSCSI drivers listed in this URL: http://www.cisco.com.

See the *Cisco MDS 9000 Family Configuration Guide.*

Zoning

The switch's zoning implementation extends the VSAN and zoning concepts from the Fibre Channel domain to also cover the iSCSI domain. This extension includes both iSCSI and Fibre Channel features and provides a uniform, flexible access control across a SAN.

The iSCSI interface can be configured to identify hosts based on symbolic node name of the iSCSI host.

See the *Cisco MDS 9000 Family Configuration Guide.*

CDP

The Cisco Discovery Protocol (CDP) is an advertisement protocol used by Cisco devices to advertise itself to other Cisco devices in the same network. CDP runs on the data link layer and is independent of layer 3 protocols. Cisco devices that receive the CDP packets cache the information to make it is accessible over CLI and SNMP.

CDP is supported on the management Ethernet interface on the supervisor module and the Gigabit Ethernet interface on the IPS module. CDP is a highly-available component.

See the *Cisco MDS 9000 Family Configuration Guide.*

New CLI Commands

Several new CLI commands introduced to support the IPS module are addressed in the *Cisco MDS 9000 Family Configuration Guide (Chapter 17, "Configuring IP Services").* Other commands introduced or significantly updated in Release 1.1.(1) are addressed in this section.

The do Command

Using the **do** command, you can execute an EXEC mode command from a configuration mode or submode prompt. You can issue this command from any submode within the configuration mode. When in configuration mode (or in any submode), enter the **do** command along with the required EXEC mode command. The entered command is executed at the EXEC level and the prompt resumes its current mode level.

The **do** command applies to all EXEC mode commands other than the **end** and **exit** commands. You can also use the help (?) and command completion (tab) features for EXEC commands when issuing a **do** command along with the EXEC command.

See the *Cisco MDS 9000 Family Configuration Guide (Chapter 2, "Before You Begin").*

The purge module Command

The **purge module** command clears the configuration for any module that previously existed in a slot and has since been removed. While the module was in that slot, some parts of the configuration may have been stored in the running configuration and cannot be reused (for example, IP addresses), unless it is cleared from the running configuration.

To delete the configuration in a specific module, issue the **purge module** *slot* **running-config** command from EXEC mode. Once this command is issued, the running configuration is cleared for the specified slot. This command will not work on supervisor modules or on any slot which currently has a module. This command only works on an empty slot (where the specified module once resided).

See the *Cisco MDS 9000 Family Configuration Guide (Chapter 6, "Managing Modules").*

The discover custom-list Command

The SCSI LUN discovery feature is initiated on demand, through CLI or SNMP. This information is also synchronized with neighboring switches, if those switches belong to the Cisco MDS 9000 Family.

With Release 1.1(1), you can specify a **custom-list** option to initiate this discovery. Customized discovery consists of a list of VSAN and domain pairs that are selectively configured to initiate a discovery.

See the *Cisco MDS 9000 Family Configuration Guide (Chapter 22, "Discovering SCSI Targets").*

Configurable COM 1 Port

The COM 1 port is available in Cisco MDS 9000 Family switches, and enables you to connect to an external serial communication device, such as a modem. You can configure the switch using the **line com1** command in configuration mode.

See the *Cisco MDS 9000 Family Configuration Guide.*

Configuring Kernel Core Dumps

When a module's operating system (OS) crashes, it is sometimes useful to obtain a full copy of the memory image (called a kernel core dump) to identify the cause of the crash. When the module experiences a kernel core dump it triggers the proxy server configured on the supervisor. The supervisor sends the module's OS kernel core dump to a Cisco Netserver application. Similarly, if the supervisor

OS fails the supervisor sends its OS kernel core dump to the Cisco Netserver application. You can configure the external server using the **kernel core target** command and the module using the **kernel core module** command in configuration mode.

See the *Cisco MDS 9000 Family Configuration Guide.*

Limitations and Restrictions

The following limitations and restrictions apply to all switches in the Cisco MDS 9000 Family:

SPAN

The following SPAN features are disabled:

- Source interfaces (physical, port channels, sup-fc) and source VSANs cannot be configured in the same SPAN session.
- Interface level VSAN filters on SPAN sources are not supported.

The following behavior is enforced when a configuration is saved from Release 1.x to Release 1.1(1)

- If a session has both source interfaces and source VSANs configured then all the source vsans are removed from that configuration session.
- The source interfaces that have interface level VSANs filters are removed from the session in all directions in which the filters are configured.

See the *Cisco MDS 9000 Family Configuration Guide.*

IPS Module Backward Compatibility

The IPS module is compatible with SAN-OS Release 1.1.1 and above.

To revert to Release 1.0(4) or earlier from Release 1.1(1), follow these steps:

Step 1 Power down all IPS modules using the **poweroff module** *slot* command.

Step 2 Remove any IPS module related configuration (for example, FCIP links, targets, initiators, or any other FCIP or iSCSI feature). See Chapter 17, “Configuring IP Storage” *Cisco MDS 9000 Family Configuration Guide*.

Step 3 Save the configuration using the **copy running-config startup-config** command to save the new configuration into nonvolatile storage.

Step 4 Continue with the manual downgrade procedure. See Chapter 5, “Software Images” in the *Cisco MDS 9000 Family Configuration Guide*.

The auto-sync Option

The **auto-sync** option is disabled by default. If you are replacing a faulty supervisor module, ensure that the **auto-sync option** is enabled so the software versions on both modules synchronize automatically. Once the supervisor synchronization is complete, ensure to disable this option.

If one supervisor module is functioning and the other is not, boot the functioning supervisor module. Then use the booted supervisor module to bring up the supervisor module that is stuck. Issue the **reload module** *slot* **force-dnld** command (after you log into the switch) where *slot* is the slot number of the stuck supervisor module. If the **auto-sync** option is disabled, the supervisor modules will not synchronize automatically. In this case, enable the **auto-sync** option before issuing the **reload module** *slot* **force-dnld** command. Once the synchronization is complete, ensure to disable this option.

See the *Cisco MDS 9000 Family Configuration Guide*.

IPS Module

FCC is not supported on switches that have an IPS module.

Each IPS module can only have 10 configured pWWNs per initiator, 1600 sessions, and 800 iSCSI hosts. Exceeding these figures may result in unpredictable consequences.

Caveats

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

Table 4 Release Caveats and Caveats Corrected Reference

	Software Release (Resolved or Open)	
DDTS Number	**1.0(4)**	**1.1(1)**
Severity 1		
CSCea53477	O	R
CSCea87033	O	R
Severity 2		
CSCdz49739	R	R
CSCea11544	R	R
CSCdz47813	R	R
CSCdz40286	R	R
CSCdz41824	R	R
CSCdz62706	R	R
CSCdz49589	R	R
CSCea34106	O	R
CSCea62969	O	R
CSCea55971	O	R
CSCeb03026	O	R
CSCea92168	O	R

Table 4 Release Caveats and Caveats Corrected Reference

DDTS Number	Software Release (Resolved or Open)	
	1.0(4)	1.1(1)
CSCdz31332		O
CSCeb01264		O
CSCeb05095		O
CSCeb18262		O
CSCeb16270		O
CSCei25319	O	O
Severity 3		
CSCdz40837	R	R
CSCdz39137	R	R
CSCdz38419	R	R
CSCdz25873	R	R
CSCdz42206	R	R
CSCdz39924	R	R
CSCdz40770	R	R
CSCdz34906	R	R
CSCdz16649	R	R
CSCdz80310	R	R
CSCdz30806	R	R
CSCdz36297	R	R
CSCdz41227	R	R
CSCdz73481	R	R
CSCdz73186	R	R
CSCdz62711	R	R
CSCdz81955	R	R
CSCdz76025	R	R
CSCdz38248	R	R
CSCdy77777	R	R
CSCdz40221	R	R
CSCdz29899	R	R
CSCdz80007	R	R
CSCea04957	R	R
CSCea43130	R	R
CSCdy71186	R	R
CSCdz41155	R	R
CSCdz42325	R	R

Table 4 Release Caveats and Caveats Corrected Reference

DDTS Number	Software Release (Resolved or Open)	
	1.0(4)	1.1(1)
CSCea46162	R	R
CSCdz52654	R	R
CSCdz55244	R	R
CSCdz81142	R	R
CSCea40555	O	R
CSCea47778	O	R
CSCdz67484	O	R
CSCea51806	O	R
CSCeb13441	O	R
CSCea89378	O	R
CSCea46162	O	R
CSCea88972	O	R
CSCea89199	O	R
CSCdz43707	O	O
CSCdz12179	O	O
CSCdz43106	O	O
CSCea45726		O
CSCea82028		O
CSCeb07573		O
CSCeb17094		O
CSCeb01112		O
CSCeb18066		O
CSCea60652		O
CSCea80896		O
CSCeb10797		O
CSCeb19609		O
CSCeb19588		O
CSCeg61535	O	O

Resolved Caveats

- CSCea53477

  Symptom: Disabling or enabling the beacon mode on a interface may cause modules to reboot.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea53477

- CSCea87033

Symptom: A Call Home process might restart after approximately 200-300 Call Home events are generated on the system. The configuration is left intact.

Please use the following URL for further information:
http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea87033

- CSCea34106

  Symptom: If you clear a kickstart boot variable that doesn't exist and if a kickstart boot variable with the same name size as the specified variable is stored in the system, the bootvar process crashes.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCe34106

- CSCea62969

  Symptom: Some private initiators (for example, SUN) are not properly registered with FLOGI. This results in the disks not being visible to the initiators.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea62969

- CSCeb03026

  Symptom: The IP address of the Gigabit Ethernet goes to the management interface after a downgrade.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb03026

- CSCea92168

  Symptom: Fabric Manager may report fewer devices in the fabric than those that are actually present.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea92168

- CSCea51806

  Symptom: The counters for the Fibre Channel PortChannel are not shown correctly. The correct value should be sum of counters of all member interfaces.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea51806

- CSCeb13441

  Symptom: After doing a hitless downgrade to 1.0(3) or 1.0(4) release, if a new module is inserted, it doesn't come-up properly

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb13441

- CSCea89378

  Symptom: On downgrading to 1.0(4) release, the modules which are supported in later releases, but not in 1.0(4) release remain powered up. The correct behavior is for unsupported modules to be automatically powered down.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea89378

- CSCea46162

Symptom: Traceroute fails with a `no route to host` error from the Fabric Manager. The same destination succeeds from the CLI.

Please use the following URL for further information:
http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea46162

- CSCea88972

  Symptom: During a nondisruptive upgrade if a name server query is pending, some Emulex HBA drivers do not respond to ELS commands issued on the switch. This results in the link going offline resulting in data traffic interruption.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea88972

- CSCea89199

  Symptom: Under certain circumstances access to the switch may be denied and the switch may be stuck because of an error in the kernel tty driver.This may happen when you have multiple VSH sessions running simultaneously.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea89199

- CSCea40555

  Symptom: During an install procedure, entering **Ctrl-c** returns a message saying that the install procedure cannot be interrupted, while **Ctrl-z** returns the prompt without any message. In either case, the install procedure continues.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea40555

- CSCea47778

  Symptom: If the switch time zone is not UTC (default), the **expire** option for the **username** command returns an error. If the **expire** option is not specified, the **username** command does not have this issue.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea47778

- CSCea55971

  Symptom: The SNMP traceroute process fails to complete on certain trips when issued from the Fabric Manager application.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCea55971

- CSCdz67484

  Symptom: The Ethereal decoder incorrectly decodes the A bit in the Common Service Parameters set as *Normal*, instead of *Alternate* BB_Credit Management.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdx67484

Open Caveats

- CSCdz31332

  Symptom: If automatic image synchronization is enabled, and the standby supervisor module is synchronizing the image from the active supervisor, the switch won't stop the user from issuing the **reload** command on the active or standby supervisor modules. This may result in a failure to synchronize the images.

  Workaround: Be sure to allow sufficient time for the images to be synchronized before reloading a supervisor module.

- CSCdz12179

  Symptom: When the Fabric Manager or Device Manager is run through VPN or any NAT scheme, a generic error occurs while adding duplicate zone members from a VPN connection.

  Workaround: None. If an error occurs while running through VPN/NAT, all errors will show up as generic errors without a detailed message describing the error.

- CSCdz43707

  Symptom: The Fabric Manager or Device Manager reports an error for all operations if the switch is multihomed (both IPFC based in-band management and the out-of-band management interface are up) and the Fabric or Device Manager was started using the IP-FC address. Typically, you will see a `notInTime window` error in the Device Manager and all sets fail.

  Workaround: If the switch is multihomed, then start the Fabric or Device Manager on the switch using the out-of-band address.

- CSCdz43106

  Symptom: The counter values freeze if the Device Manager port monitor window has been up and running for a long time (overnight or a few days).

  Workaround: Close the frozen Device Manager window and open a new session.

- CSCea45726

  Symptom: The Device Manager shows a port in the down state (red square) when the operational status of the port is up. This rare occurrence is due to the failure cause of the port not being empty (for example it reflects the “initializing” state).

  Workaround: None.

- CSCea82028

  Symptom: When the Device Manager has been running for a long time and the switch has been upgraded during this time, a Java error of class cast exception starts occurring at some point. When this error occurs, some Device Manager menu items are unusable while other menu items remain in this error state.

  Workaround: Reopen the switch in the Device Manager from the open dialog to prevent this error.

- CSCeb07573

  Symptom: The Fabric Manager map shows incorrect links between switches. This may be caused by duplicate domain IDs in two or more VSAN islands.

  Workaround: Either reconnect the VSAN islands or force one of the duplicate domains to pick a different domain ID.

- CSCeb01264

  Symptom: When you issue the **copy startup-config running-config** command on a switch which is already up and running, the trunking ports may flap. This happens due to the reapplication of allowed VSANs for trunking ports in the startup configuration.

  Workaround: Ensure that the startup configuration does not contain any allowed VSAN configuration for trunking ports (trunking ports default to the allowed VSAN configuration).

- CSCeb05095

  Symptom: If a **copy running-config startup-config** command is issued when a switching module is temporarily down, the configuration for that module will be deleted from the system. This is visible if the command is issued at boot time before all the modules are online.

  Workaround: First issue the **show module** command to ensure that all modules are online before issuing a **copy running-config startup-config** command.

- CSCeb17094

  Symptom: The following configurations are not allowed:

  - If a member port has subinterfaces, then the member port cannot be added to any PortChannel.
  - If a member port is part of a PortChannel, then you cannot create subinterfaces in this member port.
  - If a Gigabit Ethernet port is part of a PortChannel, then you cannot create a different PortChannel on its adjacent port.

  Workaround: Do not perform these PortChannel related configurations. If you do have one of these configurations, remove it to avoid unexpected results.

- CSCeb18262

  Symptom: After issuing the **fcdomain manager restart disruptive** command, the IBM tape 3590 port on switch displayed a `not connected` status.

  Workaround: Bring up the port by issuing the **shut** command followed by the **noshut** command on that port. For example:

  ```
  switch# config t
  switch(config)# int fc1/1
  switch(config)# shut
  switch(config)# no shut
  ```

- CSCeb16270

  Symptom: Avoid using the same TCP port number for iSCSI and FCIP protocols on a port. Doing so can cause unexpected behavior.

  Workaround: None.

- CSCeb01112

  Symptom: Importing the ASCII configuration multiple times in the same switch can cause the FCIP interface to go into `error disabled` state.

  Workaround: None.

- CSCeb18066

  Symptom: If you change the iSCSI switchport identification from name to IP address, the sessions do not go down

  Workaround: None.

- CSCea60652

Symptom: Both **no pwwn** *hh:hh:hh:hh:hh:hh:hh:hh* and **no pwwn auto** *number* delete all the pWWNs for a given target.

Workaround: None.

- CSCea80896

  Symptom: The Device Manager does not support iSCSI TCP parameters configuration and display.

  Workaround: None.

- CSCeb10797

  Symptom: When you delete a pWWN for an auto-created iSCSI initiator using the Device Manager, the pWWN disappears from DM (removed from snmp fcAddress table), but still shows in the CLI (the initiator is still auto-created).

  Workaround: None.

- CSCeb19609

  Symptom: After pulling out or plugging in a Gigabit Ethernet cable multiple times the PortChannel gets isolated and issues a `remote domain manager not responding` error.

  Workaround: None.

- CSCeb19588

  Symptom: Sometimes, the **zone merge import** command results in isolation.

  Workaround: Reissue the command to resolve the isolation.

- CSCeg61535

  Symptom:The Telnet server may not be disabled even if you disable it through setup. A telnet session will still work in the switch.

  Workaround: Issue the **no telnet server enable** command in configuration mode to disable telnet after you login to the switch.

- CSCei25319

  Sympton: An error message in the log file occurs because the platform manager component passes the wrong parameter while responding to a SNMP query. In some cases, this results in the query not being responded to.

  Workaround: Perform a refresh on Device Manager to clear the problem.

Related Documentation

Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family

Quick Start Guide for the Cisco MDS 9000 Family

Cisco MDS 9200 Series Hardware Installation Guide

Cisco MDS 9500 Series Hardware Installation Guide

Cisco MDS 9000 Family Command Reference

Cisco MDS 9000 Family Fabric Manager User Guide

Cisco MDS 9000 Family Troubleshooting Guide

Cisco MDS 9000 Family System Messages Guide

Cisco MDS 9000 Family MIB Reference Guide

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

Send documentation comments to mdsfeedback-doc@cisco.com

You can e-mail your comments to 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.

Obtaining Technical Assistance

Note If you purchased this product through a Cisco reseller, contact the reseller directly for technical support. If you purchased this product directly from Cisco, contact Cisco Technical Support at this URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

- Priority level 1 (P1)—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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html