Send documentation comments to mdsfeedback-doc@cisco.com.

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 2.1(2b)

Release Date: September 28, 2005

Text Part Number: OL-7411-04 S0

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 30.

Note

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	09/28/2005	Created release notes
B0	09/30/2005	Added NASB information to the Limitations and Restrictions section.
C0	11/03/2005	Added DDTS CSCeh69186
D0	11/17/2005	Added DDTS CSCsc53604
E0	12/07/2005	Added DDTS CSCsc31424, CSCsc46451, and CSCsc28722
F0	12/13/2005	Added DDTS CSCsc72994
G0	12/30/2005	Added DDTS CSCei91968
H0	2/17/2006	Added DDTS CSCeh51924, CSCsb90192, CSCsc16506, CSCsc23435, CSCsc24966, CSCsc57865, CSCsc68084, CSCsc97070, and CSCsc98796 Added limitation for iSCSI proxy initiators

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

J0	06/06/2006	Removed DDTS CSCed16845
K0	08/07/2006	Removed DDTS CSCeg33121, CSCeg12962, CSCeg84871, CSCeg90336, CSCeh04183, CSCeh30951, CSCeh52973, CSCeh70232, CSCeh93109, CSCei10774, CSCei36082, CSCei55208, CSCei55341, CSCec31365, CSCeg12383, CSCeg53114, CSCeg55238, CSCeh34828, CSCei48889, CSCei83322, CSCei91676, CSCej08751, CSCin92870, CSCin95789, CSCsd71701. Added DDTS CSCse84811
L0	08/18/2006	Added DDTS CSCse89151
M0	09/05/2006	Added DDTS CSCsd78967 and CSCse88606.
N0	09/13/2006	Added DDTS CSCsf21970
O0	11/08/2006	Added DDTS CSCin95789, CSCsd81137, CSCse70275, CSCse71420, CSCsf96043, CSCsg12020, and CSCsg15392.
P0	02/23/2007	Added DDTS CSCse99087, CSCsg03171, CSCsg62359, and CSCsh27840.
Q0	03/26/2007	Added DDTS CSCsd41578 and added a Workaround for DDTS CSCsd58774.
R0	04/04/2007	Added the section "Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch".
S0	08/24/2007	Added DDTS CSCsd83775.

Contents

Introduction

fabric-switching services that realize maximum performance while ensuring high reliability levels. These switches 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

-
-

Components Supported

Note

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
	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 ASM or SSM
	M9200SSE1K9	Storage Services Enabler package.	MDS 9200 Series with ASM or SSM

		slots for supervisor modules—SFPs[1] 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-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 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
Supervisor modules	DS-X9530-SF1-K9	MDS 9500 Supervisor/Fabric-I, module.	MDS 9500 Series only
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).	
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP Storage Services module.	
	DS-X9304-SMIP	4-port Gigabit Ethernet IP Storage Services module.	
	DS-X9032-SMV	32-port Fibre Channel Advanced Services Module (ASM).	
	DS-X9032-SSM	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM).	
	DS-X9560-SMC	Caching Services Module (CSM).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	

[2]	CWDM-SFP-xxxx-2G	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
	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-300W	300-W[3] AC power supply.	MDS 9100 Series only
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC 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.	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB.	MDS 9500 Series only
Port analyzer adapter	DS-PAA-2	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. CWDM = coarse wavelength division multiplexing
3. W = Watt

Determining the Software Version

Note

show version

Image Upgrade

You can nondisruptively upgrade to Cisco MDS SAN-OS Release 2.1(2b) from any SAN-OS software release beginning with Release 1.3(x). If you are running an older version of the SAN-OS, upgrade to Release 1.3(x) and then Release 2.1(2b).

When downgrading from Cisco MDS SAN-OS Release 2.1(2b) to Release 1.3(x), you might need to disable new features in Release 2.1(2b) for a nondisruptive downgrade. Issuing the command from the CLI, or using Fabric Manager to perform the downgrade enables the compatibility check. The check indicates that the downgrade is disruptive and the reason is "current running-config is not supported by new image."

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
      2       yes      disruptive         reset  Current running-config is not
supported by new image
      3       yes      disruptive         reset  Current running-config is not
supported by new image
      5       yes      disruptive         reset  Current running-config is not
supported by new image
      6       yes      disruptive         reset  Current running-config is not
supported by new image
```

no device-alias distribute **show incompatibility system bootflash:1.3(x)_filename**

Configuration Guide

Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch

-
-
-

New Features in Cisco MDS SAN-OS Release 2.1(2b)

Notes for Cisco MDS SAN-OS Release 2.1(2)

Limitations and Restrictions

VSFN Compatibility

IVR

NASB

14/2-Port Multiprotocol Services Module

iSCSI Proxy Initiators

Caveats

Table 3 Open Caveats and Resolved Caveats Reference

	Software Release (Open or Resolved)	
DDTS Number	2.1(2)	2.1(2b)

	O‘	O‘
CSCsd12831		O
CSCsd30165	O	O
CSCsd34882	O	O
CSCsd53429		O
CSCsd58774		O
CSCsd60578		O
CSCsd72822	O	O
CSCsd73494		O
CSCsd76429	O	O
CSCsd81137		O
CSCsd81725		O
CSCsd82449		O
CSCsd83775	O	O
CSCsd89872		O
CSCsd94718	O	O
CSCse70275	O	O
CSCse71420		O
CSCse84811	O	O
CSCse88606	O	O
CSCse99087	O	O
CSCsf21970	O	O
CSCsf96043		O
CSCsg03171	O	O

CSCsg12020		O
CSCsg15392	O	O
CSCsg62359		O

CSCei18449

: When upgrading from Cisco MDS SAN-OS Releases 2.1(1x) to 2.1(2x), in some circumstances, the SSM or ASM modules might not boot properly after the install all command is issued.

Workaround

Symptom

Workaround

Symptom

Workaround

Symptoms

Workaround

Symptom

Workaround

If you are unable to upgrade to SAN-OS 2.1.2b at this time, then work with your OSM's service organization to obtain and install a software fix.

CSCei82417

Symptom: When multiple roles are configured on the switch, the SNMP process may consume more memory if the user logs in using the GUI with some VSAN restrictions.

Workaround: Use the network-admin role only, the CLI only, or two well defined roles, network-admin and network-operator.

CSCei88345

Symptom: 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:

–

–

–

1.

2.

a.

Issue the fcdomain domain {id} static vsan {vsan id} command to configure the static domains.

Complete Step 2a for all switches before moving to Step 2b.

b.

Note

c.

```
Example Syslog Error Messages
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 assigment failure)
```

d.

```
switch(config)# vsan database
                        vsan {vsan ID} suspend
                        no vsan        suspend
```

f.

3.

4.

Note

-
-
-
-
-

Open Caveats

Note

-
-
-
-
-

a. **show ivr vsan-topology**

b. **ivr copy auto user**

Note **ivr copy auto user**

c. **ivr vsan-topology activate**

ivr commit

no ivr distribute
show cfs merge status na ivr

ivr distribute
show cfs merge status na ivr

ivr vsan-topo auto **ivr commit**

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

show interface mgmt 0

ivr distribute

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

Workaround

Symptom

```
source IP - Host IP, dest IP - MDS IP,
source port - any, dest port - 3260 (iSCSI), protocol - 6 (TCP).
```

qos

qos

Workaround

Symptom: A TACACS+ key that includes the less than (<) and greater than (>) characters fails when copied to an FTP server, and then copied back to the MDS switch.

: None.

CSCei91968

: In a fabric with more than one switch, there is a possibility of CFS or syslog crashing because of a PSS-FULL condition. This happens because of leakage in the PSS records stored by the CFS module.

CFS internal distributions cause a PSS leakage during one of the following:

An application registration/de-registration. (This is at the rate of 1 PSS records or 60 bytes per event.)

-An ISL Link flap. (This is at the rate of 2 PSS records per CFS registered application. For 10 CFS registered applications, a 1000 flaps would cause a leak of about 1M.)

Application and Regular CFS distributions in a stable fabric do not result in PSS leakages.

: None. A switchover will help in cleaning up these records but the usage of the partition remains same (dev/shm partition). However, CFS will reuse the freed space for further PSS storage.

CSCin95686

: The RRD graph in the Performance Manager does not refresh on a web client opened in Mozilla or Netscape.

: Do not use a proxy server or use the browser's Refresh button.

CSCin95789

: 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.

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

CSCsb89732

: After an upgrade from SAN-OS Release 1.3(2a) to any release lower than SAN-OS Release 3.0(1), you may see errors like the following in the syslog file:

```
2005 Sep 15 17:36:55 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:36:56 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:36:59 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
2005 Sep 15 17:37:43 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:37:44 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:37:47 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
2005 Sep 15 17:38:31 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:38:32 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:38:35 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
```

before

rscn suppress interface fc x/y

show rscn scr-table

show flogi database

Issue the (config #) command to suppress on all required interfaces.

Begin the upgrade progress as you normally would.

Issue the (config #) command.

Issue the command.

CSCsc31424

: Issuing a command on an interface causes the following message to display:

```
fc1/1: (error) port channel config in progress - config not allowed
```

```
switch# config t
                interface fc slot/port
                   no channel-group group-number
```

system switchover

```
config t
        interface fc     /
           channel-group

              group-number


           exit
        no interface port-channel
```

```
interface fc     /
   no shutdown
```

```
Unable to send exit to installer. Return code -1
```

If you upgrade from 1.3(x) to 2.1 or from 2.0(x) to 2.1 and the upgrade fails, and if after the upgrade failure the supervisor modules are running the new software version, but some modules are running the older software version, then the next attempt to execute the **install all**

Workaround

install module **image**

reload module **force-dnld**

Symptom

Workaround

Symptom

Workaround

ssm-module-number **loopback failure-action**

```
%KERN-1-SYSTEM_MSG: eepro100: wait_for_cmd_done timeout 0x801249d2 0xf0!
```

```
java.util.AbstractList$Itr.remove(Unknown Source)
```

```
%LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature FM_SERVER_PKG.
Application(s) shutdown in 119 days.
```

```
switch# copy running-config volatile:
switch# copy volatile: tftp:
```

command; even so, it cannot be added or deleted.

In this situation, you might see the following error message:

```
username <username>  password 0 <passwd>
Internal CLI error: Success error in messaging
Authentication token manipulation error
could not change password for user:<username>
no username <username>
user not present
{could not delete user <username>}
```

```
kernel uptime is 137 days 3 hours 49 minute(s) 32 second(s)
 Last reset at -447213060 usecs after Sun Mar 18 05:59:15 2018
   Reason: Not defined
   System version:    Service: §"H
```

ivr zone name

```
        config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name abc

switch(config-ivr-zone)#



switch#
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#
fabric is now locked for configuration. Please 'commit' configuration when done.
switch(config-ivr-zone)#
```

Management port configuration – Speed:100 Mbps, Duplex: Full
Switch port configuration – Speed: 100 Mbps, Duplex: Full

Resulting mode on management port – Speed: 100 Mbps, Duplex: Half
Resulting mode on switch port – Speed: 100 Mbps, Duplex: Full

: Because an MDS switch always autonegotiates the duplex mode and defaults to half duplex if the autonegotiation fails, you should configure the ports as follows:

Management port configuration – Speed: 100 Mbps, Duplex: Auto
Switchport configuration – Speed: Auto, Duplex: Auto

Resulting mode on management port – Speed: 100 Mbps, Duplex: Full
Resulting mode on switchport – Speed 100 Mbps, Duplex: Full

CSCsd60578

: The problem in FC Write Acceleration on the Storage Services module exhibited itself as a 10% to 15% performance drop once SCSI-Flows are established in both directions in relation to a {SCSI-Initiator, SCSI-Target} pair.

A bidirectional flow configuration may impact performance in a configuration where SCSI Flow is established for a given SCSI initiator SCSI target pair. For a SCSI flow in one direction, a given node in a SCSI initiator SCSI target pair acts as a SCSI initiator, and for the SCSI flow in the other direction, the same node as a SCSI target.

This problem applied only to Fibre Channel Write Acceleration on the Storage Services Module (SSM), and has been resolved in SAN-OS Release 3.0(1).

: None.

CSCsd72822

: If a switch has multiple SSMs with the SCSI flow feature enabled, an SSM may fail to come up when you perform an upgrade or reload.

: Before attempting to upgrade or reload an SSM, remove SCSI flow provisioning. Once the SSM comes back up, enable SCSI flow provisioning again.

Follow these steps:

Issue the following command to remove the provisioning:

Issue the following command to upgrade the SSM:

```
install all system bootflash:m9500-sf1ek9-mz.2.1.2d.bin kickstart
bootflash:m9500-sf1ek9-kickstart-mz.2.1.2d.bin ssi
bootflash:m9000-ek9-ssi-mz.2.1.2j.bin
```

```
switch(config)# ssm enable feature scsi-flow module
```

```
show module
```

5.

```
reload module
```

6.

Note

-
-
-
-

-

-

vsan-id

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

```
SNMP: Unknown username
```

: Close and reopen Fabric Manager with the "Accelerate Discovery" option unchecked. This reflects the latest change, but might need to be done after every change.

CSCsg15392

: If a Generation 1 module has any port that is administratively up, but operationally down when you upgrade from SAN-OS Release 2.x to either Release 3.0(1) or Release 3.0(2x), you might experience traffic disruption on that module.

: Use the command to shut all the ports operationally down and administratively up on all the Generation 1 modules before upgrading from SAN-OS Release 2.x to Release SAN-OS 3.0(x) or Release 3.0(2x). After the upgrade is complete, the ports can be brought to an administratively up state using the command.

CSCsg62359

: If a user attempts to log in using TACACS+ authentication to an MDS switch or an SSH server configured on the switch, the login might fail if password-authentication is the first login method the user tries.

: Use the keyboard-interactive method as the first login method for SSH.

The documentation set for the Cisco MDS 9000 Family includes the following documents:

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 VERITAS Storage Foundation for Networks Software

Cisco MDS SAN-OS Compatibility Matrix for Storage Service Interface Images

Cisco MDS 9000 Family SSM Configuration Note

Cisco MDS 9000 Family ASM Configuration Note

Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family

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 MDS 9000 Family Software Upgrade and Downgrade Guide

Cisco MDS 9000 Family Configuration Guide

Cisco MDS 9000 Family Command Reference

Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference

Cisco MDS 9000 Family Fabric Manager Configuration Guide

Cisco MDS 9000 Family Fabric and Device Manager Online Help

Cisco MDS 9000 Family SAN Volume Controller Configuration Guide

Cisco MDS 9000 Family Quick Configuration Guide

Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide

Cisco MDS 9000 Family MIB Quick Reference

Cisco MDS 9020 Fabric Switch MIB Quick Reference

Cisco MDS 9000 Family CIM Programming Reference

Cisco MDS 9000 Family System Messages Reference

Cisco MDS 9020 Fabric Switch System Messages Reference

Cisco MDS 9000 Family Troubleshooting Guide

Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note

Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note

For information on VERITAS Storage Foundation™ for Networks for the Cisco MDS 9000 Family, refer to the VERITAS website: http://support.veritas.com/

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/

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

Product Documentation DVD

Ordering Documentation

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

Cisco Product Security Overview

Reporting Security Problems in Cisco Products

Tip

Obtaining Documentation

Cisco.com

Product Documentation DVD

Ordering Documentation

Documentation Feedback

Cisco Product Security Overview

-
-
-

Reporting Security Problems in Cisco Products

-
-
-
-

Tip

Obtaining Technical Assistance

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

Note

Tools & Resources
Cisco Product Identification Tool **Cisco Product Identification Tool**
show

Submitting a Service Request

Definitions of Service Request Severity

Obtaining Additional Publications and Information

- *Internet Protocol Journal*

-
-
-

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.