Cisco Video Management and Storage System SRE CLI Administrator Guide

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Video Management and Storage System SRE CLI Administrator Guide
© 2010 Cisco Systems, Inc. All rights reserved.

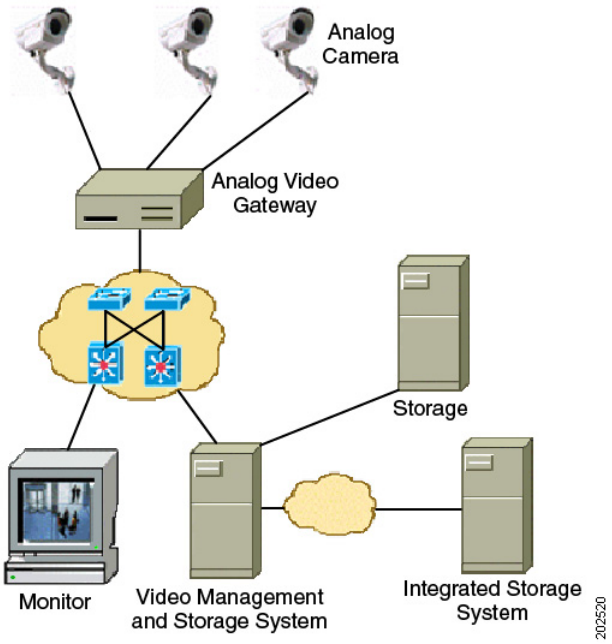
CONTENTS

Cisco Video Management and Storage System Overview

Last Updated: April 22, 2010

The Cisco Video Management and Storage System application runs on the Cisco Service Module-Service Ready Engine (Cisco SM-SRE) module, which is the service module hardware component of the Cisco Video Management and Storage System. The Cisco SM-SRE module can reside either in Cisco 2900 Series or 3900 Series Integrated Service Routers Generation 2 (ISR G2). The application uses IP network infrastructure to manage live video, archived video, and video sample retrieval. It also monitors inputs for event triggering and serves as the focal point for live monitoring of video data streams (see Figure 1).

Figure 1 Cisco Video Management and Storage System System Overview



The Cisco SM-SRE-700 and SM-SRE-900 modules are designed to fit into the modular slots of the next generation Cisco 2900 Series or 3900 Series Integrated Services Routers, which is optimized for the secure, wire-speed delivery of concurrent data, voice, video, and wireless services.

The capabilities of the Cisco Video Management and Storage System application include:

- Management of all of your video sources through a single converged interface
  - Support for Cisco IP Video Surveillance Integrated Analog Video Gateway
  - Support for most major third-party IP cameras and encoders and decoders
- Viewing of live and archived video through the same Internet Explorer “thin client” interface
- Storage of archival video on local hard drives, external Network File System (NFS):
  - Cisco SM-SRE-900—Up to 1 TB of local hard disk drive storage on the Cisco SM-SRE module and the ability to expand storage capacity to an external NFS storage for long-term archival
  - Cisco SM-SRE-700—Up to 500 GB of local hard disk drive storage on the Cisco SM-SRE located in the same Integrated Services Router (ISR).
- Intelligent management of your video store through event-based up-speeding of video stream recording
- Notification sent to relevant security personnel through the use of e-mail messages, pages, and Short Message Service (SMS)
- Control over system access with highly configurable user privileges

This guide supports features for version 6.2.1 and later versions of the Cisco Video Management and Storage System. To view the product feature history, see *Release Notes for the Cisco Video Management and Storage System*, which lists feature support history for Cisco Video Management and Storage System software versions.

The Cisco Video Management and Storage System can be used in conjunction with the Cisco Analog Video Gateway, which converts analog camera signals into IP-accessible endpoints. For more information about configuring the Cisco Analog Video Gateway, see the *Cisco Analog Video Gateway CLI Administrator Guide*.

The Cisco Video Management and Storage System is one of four components that make up the overarching Cisco IP Video Surveillance solution. Other components are:

- Cisco 2900 Series or 3900 Series ISR
- Cisco IP Video Surveillance 16-Port Analog Video Gateway Network Module
- Cisco Video Surveillance Manager product line, consisting of the Cisco Video Surveillance Operations Manager Software and the Cisco Video Surveillance Media Server Software

Security operations personnel can access live video and review archived surveillance video recorded at remote sites from terminals in their local facility.

You use the command-line interface (CLI) to configure the Cisco Video Management and Storage System software. This guide describes how to use the CLI to configure the software options of the Cisco Video Management and Storage System.

System Application

The Cisco Video Management and Storage System application runs on a Linux-based operating system (see *Open Source License Notice*) that resides on a Cisco SM-SRE, which fits into a host Cisco ISR that runs Cisco IOS software. The Cisco Video Management and Storage System is a network video management and storage engine with its own startup and run-time configurations and its own CLI, all of which are independent of the Cisco IOS configuration on the ISR. The Linux-based software of the module does not have its own console on the front panel but uses internal virtual console sessions accessed from the host router.

After the Cisco Video Management and Storage System is configured using the CLI, the module runs a GUI-based video distribution and management system application, called the Cisco Video Surveillance Operations Manager, based on next-generation video encoding standards.

This arrangement—host router plus Cisco SM-SREs—provide a router-integrated application platform for accelerating data-intensive applications.

Applications typically involve:

- Video management and storage
- Application-oriented networking
- Contact centers and interactive-voice-response applications
- Content caching and delivery
- Network analysis
- Voice-mail and auto-attendant applications
- Application Extension Platform (AXP)

Configuring Host Router and Cisco SM-SRE Module Interfaces

Last Updated: April 22, 2010

To configure the Cisco SM-SRE module interfaces to run the Cisco Video Management and Storage System application after the module hardware is installed in your host router, you need to configure the following:

- 2900 Series of 3900 Series ISR G2 external interface to an external network link, using the Cisco IOS CLI for setting standard router settings
- ISR G2 internal interface to the Cisco SM-SRE module, using the Cisco IOS CLI for setting the network module IP address and default gateway router
- Cisco SM-SRE module internal interface to the host router

The following sections describe the tasks required to configure the host router and Cisco SM-SRE interfaces:

Before Configuring the Cisco Video Management and Storage Interfaces

Make sure that the following prerequisites for the ISR G2, the Cisco SM-SRE, and file server are met before you attempt to configure the module:

Cisco ISR G2 Prerequisites

- Check the latest release notes (see the *Release Notes for the Cisco Video Management and Storage System*) to ensure that your Cisco router is running the appropriate Cisco IOS software release and recognizes the Cisco SM-SRE module.

Note After minimum release requirements are met, you can change the image either on the host router or on the Cisco SM-SRE module, without affecting the other image.

Cisco SM-SRE Module Prerequisites

Note In most cases, the Cisco SM-SRE module is shipped from the factory installed in the 2900 Series or 3900 Series ISR G2.

- If the Cisco SM-SRE module was not already installed at the factory, install it in the host router that has sufficient physical memory, depending on the model number, to accommodate the Cisco Video Management and Storage application. For detailed information on physical memory and hardware installation, see *Installing Cisco Network Modules and Service Modules in Cisco Access Routers*.
- If you need to swap out an active Cisco SM-SRE module:
  - Before swapping out a module in an existing router, perform a full backup of all data.
  - After the swap, restore the data.

Note For more information, see the "Backing Up and Restoring Configurations on the Cisco Video Management and Storage System" section on page 16.

  - Follow the instructions in the *Installing Cisco Network Modules and Service Modules in Cisco Access Routers* guide for removing the older module and installing the newer module.
- Note the Cisco SM-SRE module slot location in the host router:
  - *slot*: Number of the host router chassis slot for the module. After you install the module, you can obtain this information by using the Cisco IOS software command-line interface (CLI) **show running-config** command.
  - *port*: Number of the daughter card on the module. This value should be 0.

Note You must have this information to later configure the Cisco SM-SRE module.

File Server Prerequisites

- If you need to download a new image or to perform a configuration backup and restore, you will need to access a File Transfer Protocol (FTP)/Secure FTP (SFTP) and Trivial File Transfer Protocol (TFTP) server. To verify that your download FTP/SFTP and TFTP file servers are accessible, see the *Cisco Video Management and Storage System Installation and Upgrade Guide*.
- Verify that the Cisco Video Management and Storage application is accessible by first accessing Cisco IOS CLI commands.

Configuring the Cisco SM-SRE Module Interfaces

The host router and the Cisco SM-SRE module uses several interfaces for internal and external communication. Each interface is configurable from the router by using Cisco IOS CLI commands.

The following information is required for entering the Cisco SM-SRE module command environment before configuring the interfaces:

- IP address of the Cisco ISR G2 that contains the Cisco SM-SRE module
- Username and password for logging in to the router
- Slot and unit number of the Cisco SM-SRE module

To configure the host router to Cisco SM-SRE module interfaces, see the *Cisco SRE Service Module Configuration and Installation Guide*. After the module interfaces have been successfully configured, continue to the Administering the Cisco Video Management and Storage System Module chapter to configure appropriate parameters of the Cisco Video Management and Storage System application.

Administering the Cisco Video Management and Storage System Module

Last Updated: April 22, 2010

This chapter contains the following information for administering the Cisco Video Management and Storage System application:

Note

- The tables in these sections list only common router commands and network module commands.
  - To view a complete list of the available commands, enter **?** at the prompt.

    Example: `Router(config-if)# ?`
  - To view a complete list of command keyword options, enter **?** at the end of the command.

    Example: `Router# service-module sm ?`
- The commands are grouped in the tables by the configuration mode in which they are available. If the same command is available in more than one mode, it can act differently in each mode.

Establishing a Session

After you have configured the Cisco SM-SRE module interfaces (see Configuring Host Router and Cisco SM-SRE Module Interfaces), establish a session with the module to configure the Cisco Video Management and Storage System. This section describes how to enter and exit the command environment and open a session with the module.

Entering and Exiting the Command Environment

The Cisco Video Management and Storage System user EXEC, privileged EXEC, and configuration command modes are similar to those used by Cisco IOS CLI commands. The description for each command in this section indicates the command mode.

This section provides the procedures for entering and exiting the command environment, It also provides procedures for establishing a session with the Cisco Video Management and Storage System that is running on the Cisco SM-SRE module, where configuration commands are executed.

Entering the Command Environment

Use the following procedure to enter the Cisco Video Management and Storage System command environment using the Telnet network protocol. In the configuration mode, you can configure the Cisco Video Management and Storage System application.

SUMMARY STEPS

1. Open a Telnet or console session.
2. **telnet** *ip-address*
3. Enter the user ID and password of the router.
4. **service-module sm** *slot*/*port* **session**
5. (Optional) **enable**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Open a Telnet or console session.	To open a Telnet or console session, use a Microsoft Windows command prompt window, a software emulation tool such as WRQ Reflection, or connect to the console port of the host router. The following examples use a Telnet session.
Step 2	**telnet** *ip-address* or Connect to the router console port and start a session **Example:** `C:\>telnet 172.16.231.195`	Specifies the IP address of the router at the Telnet prompt Connects the router to a PC or other Data Terminal Equipment device and start a session
Step 3	`Enter the Username: userid and Password: password.`	Enters your user ID and password for the router.

Step 4	**service-module sm** *slot/port* **session**
	
	Example:
	`Router> service-module sm 1/0 session`
	`cvmss-10-0-0-0>`
		Enter the Cisco SM-SRE module command environment from the host router, using the module *slot* and *port* numbers. The router prompt changes to the service module prompt.
		Note If the message `"Trying ip-address slot/port ..." Connection refused by remote host` appears, enter the command **service-module sm** *slot/port* **session clear** and repeat Step 4.

Step 5	**enable**
	
	Example:
	`cvmss-10-0-0-0> enable`
	`cvmss-10-0-0-0#`
		(Optional) Enters Cisco Video Management and Storage System application's privileged EXEC mode. You can now begin configuring the Cisco Video Management and Storage System.

Exiting the Command Environment

To leave the Cisco Video Management and Storage System command environment and return to the Cisco IOS router command environment, enter the **exit** command twice, or enter **Alt-Ctrl-6** and **x**.

The following example shows the exit procedure:

```
cvmss-10-0-0-0# exit
cvmss-10-0-0-0> exit
Router#
```

or

```
cvmss-10-0-0-0# Alt-Ctrl-6, x
```

Opening and Closing a Cisco SM-SRE Module Session

This section describes how to open and close a session on the Cisco SM-SRE module, on which the Cisco Video Management and Storage System is running. To configure the Cisco Video Management and Storage System using configuration commands, you must first open a session with the module, use the appropriate configuration commands, and then close the session. For a summary and description of the Cisco Video Management and Storage System configuration commands, see Administering the Cisco Video Management and Storage System Module.

The boot helper is a small subset of the system software that runs on the module. It is used in the following example. It boots the module from the network and assists in software installation and upgrades, disaster recovery, and other operations when the module cannot access its software.

Note

- You can conduct only one module session at any one time.
- Steps 1 and 2 open the host-router CLI and access the Cisco SM-SRE module. The remaining steps open a session with the module, configure the boot helper example, and clears the module session, returning you to the host-router Cisco IOS software CLI.

SUMMARY STEPS

From the Host-Router CLI

1. **enable**
2. **service-module sm** *slot*/**0 status**
3. **service-module sm** *slot*/**0 session**

From the Service-Module Interface

4. Use Cisco SR-SME module configuration commands. In this example, the boot loader.
5. **Control-Shift-6 x**
   or
   exit

From the Host-Router CLI

6. **service-module sm** *slot*/**0 session clear**

DETAILED STEPS

	Command or Action	Purpose
	From the Host-Router CLI	
Step 1	**enable** <password> **Example:** Router> enable Router> <password> Router#	Enters privileged EXEC mode on the host router. If prompted, enter your password.

	Command or Action	Purpose
Step 2	**service-module sm** *slot*/**0 status** **Example:** `Router# service-module sm 2/0 status`	Displays the status of the module, so that you can ensure that the module is running (that is, the module is in a steady state). **Note** If the module is not running, start it with one of the startup commands listed in the "Common Cisco IOS Software and Cisco SM-SRE Commands" section on page 14.

Step 3	**service-module sm** *slot*/**0 session**
	
	Example:
	`Router# service-module sm 1/0 session`
	
	`Trying 10.10.10.1, 2065 ... Open`
		Begins a module session on the specified module. Do one of the following:
		
		• To interrupt the auto-boot sequence and access the boot loader, quickly type ***.
		
		• To start a configuration session, press **Enter**.

	From the Service-Module Interface (boot loader prompt or configuration prompt)	

Step 4	.
	.
	.
	
	Example (boot loader):
	`cvmss-module boot loader> config`
	
	or
	
	Example (configuration):
	`cvmss-module> configure terminal`
	`cvmss-module(config)>`
	.
	.
	.
	`cvmss-module(config)> exit`
	`cvmss-module> write`
		Enters boot loader or configuration commands on the module as needed.
		
		• Boot loader command choices include **boot**, **config**, **exit**, **help**, **ping**, **reboot**, **show**, and **verify**.
		
		or
		
		• Configuration command choices are similar to the Cisco IOS commands that are available on the host router. To access global configuration mode, use the **configure terminal** command. Enter the appropriate configuration commands to set application parameters. Then exit global configuration mode by using the **exit** command. Save your new configuration by using the **write** command.
		
		Note You do not need to use the **enable** command and the prompt does not change from **>**.

Step 5	**Example (boot loader):**
	Press **Control-Shift-6 x**
	
	or
	
	exit
	
	Example (Configuration):
	`cvmss-module(config)> exit`
	`cvmss-module> exit`
		Closes the module session and returns to the router's Cisco IOS CLI.
		
		Note The module session stays up until you clear it in Step 6. While the session remains operational, you can return to it from the router's Cisco IOS CLI by pressing **Enter**.

	From the Host-Router CLI	
Step 6	**service-module sm** *slot*/**0 session clear** **Example:** `Router# service-module sm 1/0 session clear`	Clears the module session for the specified module. When prompted to confirm this command, press **Enter**.

Common Cisco IOS Software and Cisco SM-SRE Commands

Table 1 summarizes and briefly describes commonly used Cisco IOS software and Cisco SM-SRE commands. For a more complete description of the Cisco SM-SRE commands on which the Cisco Video Management and Storage System runs, see "Common Cisco Video Management and Storage System Module Commands" section on page 39. For a more complete description of the Cisco IOS software commands, see "Cisco IOS Commands" section on page 69.

To start up or shut down the Cisco SR-SRE module, use the **shutdown** and **startup** commands as necessary from Table 1.

Note

- Some shutdown commands can potentially disrupt service. If command output for such a command displays a confirmation prompt, confirm by pressing **Enter** or cancel by typing **n** and pressing **Enter**. Alternatively, prevent the prompt from displaying by using the **no-confirm** keyword.
- Some commands shut down the module or application and then immediately restart it.

Table 1 Common Cisco IOS Software and Cisco SM-SRE Module Commands

Configuration Mode	Command	Purpose
`Router#`	**service-module sm** *slot/port* **default-boot**	Configures the Cisco SM-SRE module to use the default BIOS and bootloader.
`Router#`	**service-module sm** *slot/port* **heartbeat-reset** {**disable** | **enable**}	Prevents Cisco IOS software from rebooting the Cisco SM-SRE service module when the heartbeat is lost.
`Router#`	**service-module sm** *slot/port* **install url** *url* [**script** *filename*] [**argument "***string***"**] [**force**]	Installs an application on a Cisco SM-SRE module.
`Router#`	**service-module sm** *slot/port* **install abort** [**force**]	Aborts the application install process on a Cisco SM-SRE.
`Router#`	**service-module sm** *slot/port* **reload**	Gracefully shuts down and reboots the Cisco SM-SRE module operating system.
`Router#`	**service-module sm** *slot*/**0 reset**	Resets the hardware on a module. Used only to recover from shutdown or a failed state. **Caution** Use this command with caution. It does *not* provide an orderly software shutdown, and it can affect file operations in progress.
`Router#`	**service-module sm** *slot*/**0 session**	Begins a configuration session for a Cisco SM-SRE module through a console connection.

Table 1 Common Cisco IOS Software and Cisco SM-SRE Module Commands (continued)

Configuration Mode	Command	Purpose
`Router#`	**service-module sm** *slot*/**0 shutdown**	Gracefully shuts down the Cisco SM-SRE module operating system. Use this command when removing or replacing a hot-swappable module during online insertion and removal.
`Router#`	**service-module sm** *slot*/*port* **statistics**	Displays reset and reload information for the Cisco SM-SRE module and its Cisco IOS software.
`Router#`	**service-module sm** *slot*/**0 status**	Displays configuration information related to the hardware and software on a Cisco SM-SRE module.
`Router#`	**service-module sm** *slot*/*port* **uninstall** [**force**]	Uninstalls an application on the Cisco SM-SRE.
`Router(config)#` `Router(config-if)#`	**interface** *slot*/**0** **shutdown**	Shuts down the module gracefully.
`cvmss-module boothelper>`	**boot**	Starts the boot helper or application.
`cvmss-module>`	**disk remove** {**0** | **1**}	Allows the local disk drive to be physically removed from the Cisco SM-SRE module after a disk drive failure; the disk drive can now be hot swapped with a new disk drive. **Note** The CLI keeps track of which drive has failed. If the selected drive (0 or 1) is not the failed drive, the CLI does not allow the command to take effect and an error appears.
`cvmss-module>`	**disk add** {**0** | **1**}	Adds new local disk drive after a new drive is swapped for the failed drive and physically plugged into the Cisco SM-SRE module. **Note** The CLI keeps track of which drive has been replaced. If the selected drive (0 or 1) is not the newly swapped drive, the CLI does not allow the command to take effect and an error appears.
`cvmss-module(config)`	**event poll-interval** *seconds*	Sets the HTTP trigger event polling interval in seconds.
`cvmss-module(offline)>`	**reload**	Performs a graceful halt and reboot of the module operating system.
`cvmss-module>`	**reload**	Shuts down the module application gracefully and then reboots the module from the boot loader.
`cvmss-module>`	**shutdown**	Shuts down the module application gracefully and then shuts down the module.

Backing Up and Restoring Configurations on the Cisco Video Management and Storage System

To back up or restore configuration settings or to manage previous backups, use the commands listed in Table 2.

Note The backup server can be configured using either the configuration mode or the offline mode.

Table 2 Common Backup and Restore Commands

Configuration Mode	Command	Purpose
`cvmss-module(config)>`	**backup revisions**	Specifies the number of previous backups to keep on the server. A value of zero removes all previous backups and saves only the current backup.
`cvmss-module(config)>`	**backup server**	Configures an external FTP backup server for storage.
`cvmss-module(offline)>`	**backup category** {**all** | **configuration** | **data** | **VSMS** | **VSOM**}	Performs a backup of the configuration files to a backup server. **VSMS**[1] backs up the Video Surveillance Management System data files. **VSOM**[2] backs up the Video Surveillance Operations Management data files. See also Appendix A: Backing Up Files in the *Cisco Video Management and Storage System Installation and Upgrade Guide*
`cvmss-module(offline)>`	**backup revisions**	Specifies the number of previous backups to keep on the server. A value of zero removes all previous backups and saves only the current backup.
`cvmss-module(offline)>`	**backup server**	Configures an external FTP backup server for storage.
`cvmss-module(offline)>`	**restore**	Restores the system to its factory default configuration or to the specified backup. See also Appendix B: Restoring Files in the *Cisco Video Management and Storage System Installation and Upgrade Guide*
`cvmss-module>`	**show backup**	Displays information about previous backups and about the configured backup server.

1. VSMS = Video Surveillance Management System
2. VSOM = Video Surveillance Operations Management

Verifying System Status

To verify the status of an installation, upgrade or downgrade, or to troubleshoot problems, use verification and troubleshooting commands as necessary from Table 3.

Note

- Among keyword options for many **show** commands is the provision to display diagnostic output on your screen or to "pipe" it to a file or a URL (that is, to read the output from one command and write it to the file or URL).
- In Table 3 through Table 5, the *Router#* prompt indicates that the command is a host-router Cisco IOS privileged EXEC command prompt; the *cvmss-module*> prompt indicates the command is a Cisco Video Management and Storage System application command prompt.

Table 3 Common Verification and Troubleshooting Commands

Configuration Mode	Command	Purpose
`Router#`	**ping**	Pings a specified IP address to check network connectivity (does not accept a hostname as destination).
`Router#`	**show arp**	Displays the current ARP[1] table.
`Router#`	**show clock**	Displays the current date and time.
`Router#`	**show configuration**	Displays the current configuration as entered by means of the **configure** command.
`Router#`	**show controllers integrated-service-engine**	Displays interface debug information.
`Router#`	**show diag**	Displays standard Cisco IOS diagnostics information, including information about the Cisco Video Management and Storage System module.
`Router#`	**show hardware**	Displays information about network module and host router hardware.
`Router#`	**show hosts**	Displays the default domain name, style of name lookup, list of name-server hosts, and cached list of hostnames and addresses.
`Router#`	**show interfaces**	Displays information about all hardware interfaces, including network and disk.
`Router#`	**show interfaces sm**	Displays information about the module side of the router-module interface.
`Router#`	**show ntp status**	Displays information about NTP[2].
`Router#`	**show processes**	Displays a list of the application processes that are running.
`Router#`	**show running-config**	Displays the configuration commands that are in effect.

Table 3 Common Verification and Troubleshooting Commands (continued)

Configuration Mode	Command	Purpose
Router#	**show startup-config**	Displays the startup configuration.
Router#	**show tech-support**	Displays general information about the host router that is useful to Cisco technical support for problem diagnostics.
Router#	**show version**	Displays information about the router software or network module hardware.
Router#	**test scp ping**	Pings the network module to check network connectivity.
cvmss-module>	**ping**	Pings a specified IP address to check network connectivity (does not accept a hostname as destination).
cvmss-module>	**show arp**	Displays the current ARP table.
cvmss-module>	**show disk stats**	Displays the statistics of the local disk drives.
cvmss-module>	**show clock**	Displays the current date and time.
cvmss-module>	**show config**	Displays the current boot loader configuration as entered by the **configure** command.
cvmss-module>	**show hosts**	Displays the default IP domain name, lookup style, name servers, and host table.
cvmss-module>	**show interfaces**	Displays information about the network-module interfaces.
cvmss-module>	**show ntp status**	Displays information about NTP.
cvmss-module>	**show processes**	Displays a list of the application processes that are running.
cvmss-module>	**show running-config**	Displays the configuration commands that are in effect.
cvmss-module>	**show snmp**	Displays the SNMP[3] statistics are stored in system counters.
cvmss-module>	**show software directory download**	Displays the contents of the downgrade or download directory on the download FTP file server.
cvmss-module>	**show software download server**	Displays the name and IP address of the configured download FTP file server.
cvmss-module>	**show software licenses**	Displays license information for installed packages.
cvmss-module>	**show software packages**	Displays version information for installed packages.
cvmss-module>	**show software versions**	Displays version information for installed software.

Table 3 Common Verification and Troubleshooting Commands (continued)

Configuration Mode	Command	Purpose
`cvmss-module>`	**show startup-config**	Displays the startup configuration.
`cvmss-module>`	**show tech-support**	Displays general information about the network module that is useful for problem diagnosis to Cisco technical support. **Note** Other **tech-support** commands should only be used under the guidance of Cisco TAC[4].
`cvmss-module>`	**show trace**	Displays the contents of the trace buffer.
`cvmss-module>`	**show version**	Displays information about the hardware and devices.
`cvmss-module>`	**show video-surveillance**	Displays video surveillance configurations, logs, reports, and tasks.
`cvmss-module>`	**software remove**	Removes downloaded files (all files, downloaded package and payloads, or stored downgrade files created during an upgrade).

1. ARP = Address Resolution Protocol
2. NTP = Network Time Protocol
3. SNMP = Simple Network Management Protocol
4. Cisco TAC = Cisco Technical Assistance Center

Diagnostics and Logging Options

To configure logging options for Cisco Video Management and Storage System, use logging commands listed in Table 4.

Note Among the keyword options for many **log** and **trace** commands is the provision to display diagnostic output on your screen or to save it to a file or a URL.

Table 4 Common Logging Commands

Configuration Mode	Command	Purpose
`cvmss-module>`	**log console monitor**	Configures error logging by means of console logging (logged messages are displayed on the console).
`cvmss-module>`	**log console**	Configures error logging by means of console logging (logged messages are displayed on the console).
`cvmss-module>`	**log server**	Configures error logging by means of a system-log (syslog) server (syslog is an industry-standard protocol for capturing log information for devices on a network).

Diagnostics are of two types:

- System log (syslog)—Syslog is an industry-standard protocol for capturing the following events:
  - Fatal exceptions that cause an application or system crash, during which normal error-handling paths are typically nonfunctional
  - Application run-time errors that cause unusual conditions and configuration changes

  The syslog file size is fixed at 10 MB. Syslog configurations survive a power failure.
- Traces—Trace logs capture events related to the progress of a request through the system.

  Trace logs survive a CPU reset; trace configurations survive a power failure. Log and display these configurations with the **trace** commands.

To generate and display syslog and trace diagnostics, use trace commands from Table 5.

Table 5 Common Trace Commands

Configuration Mode	Command	Purpose
`cvmss-module>`	**clear trace**	Clears logged trace events for specified modules.
`cvmss-module>`	**log trace**	Logs configured traces to the network module (can be done locally or remotely).
`cvmss-module>`	**no trace**	Disables tracing for specified modules, entities, or activities.
`cvmss-module>`	**show errors**	Displays error statistics by module, entity, or activity.

Table 5 Common Trace Commands (continued)

Configuration Mode	Command	Purpose
`cvmss-module>`	**show trace**	Displays trace settings.
`cvmss-module>`	**show trace buffer**	Displays the contents of the trace buffer.
`cvmss-module>`	**show trace store**	Displays the contents of the stored trace messages.
`cvmss-module>`	**trace**	Enables tracing (that is, generates error reports) for specified modules, entities, or activities.

SNMP CLI Commands

Table 6 lists and describes the **snmp-server** SNMP command-line interface commands.

Table 6 SNMP CLI Commands

Configuration Mode	Command	Purpose
`cvmss-module(config)#`	**snmp-server community** *community-string* [**RO** | **RW**] **no snmp-server community** *community-string* [**RO** | **RW**] Example: `cvmss-module(config)# snmp-server community cisco-snmp RO`	Enables the SNMP agent with the configured case sensitive community string. The password and the mode of access can be set to read-only or read-write. Up to five community strings that can be set for each read-only or read-write category. *community-string*—case sensitive character string with a maximum length of 15 characters. RO—Read-Only access mode. RW—Read-Write access mode. Use the **no** form of this command to remove the configuration associated with the community string. **Note** Even after all community string configurations are removed, you can still have read-only access of MIB variables using the *default* community strings. The default read-only community string is *broadware-snmp*.
`cvmss-module(config)#`	**snmp-server contact** *contact-name* **no snmp-server contact** *contact-name* Example: `cvmss-module(config)# snmp-server contact "John Doe"`	Sets or clears the contact name. *contact-name*—character string with a maximum length of 31 characters. Use the **no** form of this command to clear the contact name.

Table 6 SNMP CLI Commands (continued)

Configuration Mode	Command	Purpose
`cvmss-module(config)#`	**snmp-server enable traps** **no snmp-server enable traps** Example: `cvmss-module(config)# snmp-server enable traps`	Enables SNMP traps to be sent to the SNMP trap destination. **Note** This command is effective only for certain types of notifications. Not all types of notifications are controlled by this command. The notifications generated as a result of archive creation or deletion are not configured by this CLI, but are configured in the Video Surveillance Management Console web page with the "SNMP Trap Destination" link. Also, this CLI does not control the traps generated from exceeding the system resource thresholds. The only form of notifications enabled (or disabled) by this CLI are the traps generated from syslog messages with severity level greater than or equal to that of warning level. Use the **no** form of this command to disable trap notifications to be sent to the trap destination.
`cvmss-module(config)#`	**snmp-server host** *ip-address community-string* **no snmp-server host** *ip-address community-string* Example: `cvmss-module(config)# snmp-server host 1.100.10.219 cisco-snmp`	Configures the IP address of the host that is to receive the trap notifications. The community string must also be specified. Up to a maximum of 5 hosts that can be configured. **Note** The **snmp-server enable traps** command must be executed for the hosts to receive the trap notifications. *ip-address*—IP address (IPv4 only is supported) in dotted decimal notation of the host that is to receive the trap notifications. *community-string*—character string with a maximum length of 15 characters. Use the **no** form of this command to clear the host configuration.

Table 6 SNMP CLI Commands (continued)

Configuration Mode	Command	Purpose
`cvmss-module(config)#`	**snmp-server location** *location-name* **no snmp-server location** *location-name* Example: `cvmss-module(config)# snmp-server contact "San Jose"`	Sets or clears the location name. *location-name*—character string with a maximum length of 31 characters. Use the **no** form of this command to clear the location name.
`cvmss-module(config)#`	**snmp-server monitor disk** *percentage* **no snmp-server monitor disk** *percentage* Example: `cvmss-module(config)# snmp-server monitor disk 20`	Sets the threshold for monitoring the disk usage for all the disks, including local and NFS servers. *percentage*—Integer variable in the range of 1 to 30 that represents the percentage of free space within each disk partition. If the free disk space percentage falls below this threshold, the system will generate a trap. Use the **no** form of this command to disable disk monitoring.
`cvmss-module(config)#`	**snmp-server monitor cpu** *percentage* **no snmp-server monitor cpu** *percentage* Example: `cvmss-module(config)# snmp-server monitor cpu 10`	Sets the threshold for monitoring the CPU utilization. *percentage*—Number in the range of 0 to 20 that represents the percentage of idle CPU time. This number includes *wait* states. Use the **no** form of this command to disable CPU monitoring
`cvmss-module(config)#`	**snmp-server monitor swap** *percentage* **no snmp-server monitor swap** *percentage* Example: `cvmss-module(config)# snmp-server monitor swap 25`	Sets the threshold for monitoring the utilization of swap space. *percentage*—Number from 1 to 50 that represents the percentage of available free swap space. Use the **no** form for this command to disable swap space monitoring.

Table 6 SNMP CLI Commands (continued)

Configuration Mode	Command	Purpose
cvmss-module>	**show snmp configuration**	Displays the configuration of all SNMP commands. It also lists all the resource monitoring threshold configurations.

	Example:
	`cvmss-module> show snmp configuration`
	`Contact: 1234`
	`Location: SAN JOSE`
	`Community 1 RO: test1`
	`Community 2 RO: test2`
	`Community 3 RO: test3`
	`Community 4 RO: test4`
	`Community 5 RO: test5`
	`Traps: disabled`
	`Host Community 1: 1.100.10.219 cisco-snmp`
	`Host Community 2: 1.100.10.218 cisco-snmp`
	`Host Community 3: 1.100.10.217 cisco-snmp`
	`Host Community 4: 1.100.10.216 cisco-snmp`
	`Host Community 5: 1.100.10.215 cisco-snmp`
	`monitor disk limit: 8`
	`monitor memory limit: 10`
	`monitor cpu limit: 15`
	`cvmss-module>`	

Adding a DNS Server (Optional)

Cisco Video Management and Storage System uses a cache-only Domain Name System (DNS) server that listens on port 53 for both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) packets. A typical use for such a server is to enable the application to continue operation in a branch office when the WAN is down and the server is on the other side of the WAN in an enterprise or service-provider data center.

The DNS server cache policy is to automatically revaluate a cached entry when its time to live (TTL) expires and to discard an entry only when the parent DNS server is accessible and no longer contains the name. This differs from most DNS caches, which simply discard an entry when the TTL expires.

Note

- Step 1 opens a session to the Cisco SRE module from the host router Cisco IOS CLI. The remaining steps configure the Cisco SRE module and return to the host router Cisco IOS CLI.

SUMMARY STEPS

From the Host-Router CLI

1. **service-module sm** *slot*/**0 session**

From the Service-Module Interface

2. **configure terminal**
3. **hostname** *hostname*
4. **ip domain-name** *domain*

5. **ip name-server** <*ip-address*> [<*ip-address*> …]
6. **exit**
7. **show hosts**
8. **write**
9. **Control-Shift-6 x**

From the Host-Router CLI

10. **service-module sm** *slot*/**0 session clear**

DETAILED STEPS

	Command or Action	Purpose
	From the Host-Router CLI	
Step 1	**service-module sm** *slot*/**0 session** **Example:** `Router# service-module sm 2/0 session`	Opens a Cisco SM-SRE module session.
	From the Service-Module Interface	
Step 2	**configure terminal** **Example:** `cvmss-module> configure terminal`	Enters global configuration mode on the module.
Step 3	**hostname** *hostname* **Example:** `cvmss-module(config)> hostname hostname1`	Specifies the hostname of the Cisco Video Management and Storage System that appear in the prompt.
Step 4	**ip domain-name** *domain* **Example:** `cvmss-module(config)> ip domain-name domain1.com`	Defines a default domain name for use in completing unqualified hostnames (names without a dotted-decimal domain name).
Step 5	**ip name-server** *ip-address* [<*ip-address*> …] **Example:** `cvmss-module(config)> ip name-server 10.0.0.0`	Specifies the IP address for one or more DNS servers. The argument is as follows: *ip-address*—Server IP address
Step 6	**exit** **Example:** `cvmss-module(config)> exit`	Exits global configuration mode on the module.
Step 7	**show hosts** **Example:** `cvmss-module> show hosts`	Displays the default domain name, style of name lookup, list of name-server hosts, and cached list of hostnames and addresses.

	Command or Action	Purpose
Step 8	**write** **Example:** `cvmss-module> write`	Saves the new running configuration of the module.
Step 9	Press **Control-Shift-6 x**.	Closes the session.
	From the Host-Router CLI	
Step 10	**service-module sm** *slot*/**0 session clear** **Example:** `Router# service-module integrated-service-engine 1/0 session clear`	Clears the session for the specified module. When prompted to confirm this command, press **Enter**.

Additional References

The following sections provide references related to the Cisco Video Management and Storage System application.

Related Documents

Related Topic	Document Title
Cisco Video Management and Storage System and the Cisco Video Surveillance Solution	• *Release Notes for the Cisco Video Management and Storage System SRE* • *Installing Cisco Network Modules and Service Modules in Cisco Access Routers* • *Cisco Video Management and Storage System SRE Installation and Upgrade Guide* • *Cisco Integrated Storage System Installation and Upgrade Guide* • *Cisco Integrated Storage System CLI Administrator Guide* • *Cisco Analog Video Gateway Installation and Upgrade Guide* • *Cisco Analog Video Gateway CLI Administrator Guide* • *Cisco Analog Video Gateway XML API Guide* • *Open Source License Notice*
Cisco IOS software	*Cisco IOS Software*
Technical documentation, including feedback and assistance	*What's New in Cisco Product Documentation* (including monthly listings of new and revised documents)

Technical Assistance

Description	Link
For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at: Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.	http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html
Cisco Feature Navigator website	http://www.cisco.com/go/cfn Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. An account on Cisco.com is not required.
Cisco Software Center website	http://www.cisco.com/public/sw-center/

Configuring Local and Remote Storage

Last Updated: April 22, 2010

This section describes how to configure the Cisco Video Management and Storage System to store archive files on local redundant array of inexpensive disks (RAID) and external NFS storage servers. Use the Cisco Video Management and Storage System CLI commands to add or modify NFS server configurations.

This chapter describes the following:

Configuring Local Storage Devices

The following section describes the configuration of local storage devices:

Local Disk Drive RAID Array Options

RAID 1, Linear RAID, and RAID 0 are all supported by the Cisco Video Management and Storage System application version 6.2.1 and later on the Cisco SM-SRE-900 module.

Note The Cisco SM-SRE-700 module only contains one disk drive, so RAID is not an option.

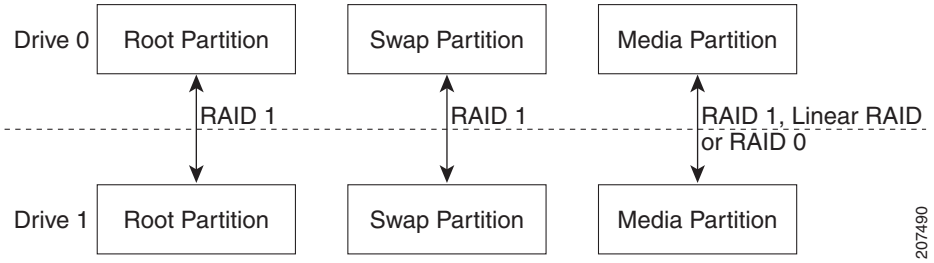
During the installation of the Cisco Video Management and Storage System application on the Cisco SM-SRE-900, you can choose the type of RAID support as RAID 1, Linear RAID, or RAID 0.

The following sections describe the Cisco Video Management and Storage System RAID options and the CLI commands required to remove a faulty drive and add an new drive.

RAID 1 Option

With the RAID 1 option, the two-disk drive RAID 1 mirrors the root partition, swap drive, and media partitions (see Figure 2) of the two disk drives of the Cisco SM-SRE module, creating a one-for-one ratio real-time backup. It provides fault tolerance from disk errors and failure of one of the two drives. The contents of each disk in the array are identical to that of the other disk in the array. The array continues to operate as long as one of the two disk drives is functional.

Figure 2 RAID 1, Linear RAID, and RAID 0 Disk Drive Partition Mirroring



The RAID 1 option provides complete high availability and fault tolerance to the Cisco Video Management and Storage System; if one of the disk drives fails, the VSOM and VSMS configurations and archives are preserved, and the Cisco Video Management and Storage System remains operational. The cost for this high availability and fault tolerance, however, is that only half of the total potential disk storage space is available.

If the RAID 1 disk drive fails and is hot swapped with a new drive, the new drive is automatically reformatted to match the working drive and the RAID arrays are reassembled.

Hot Swapping the Faulty RAID 1 Drive

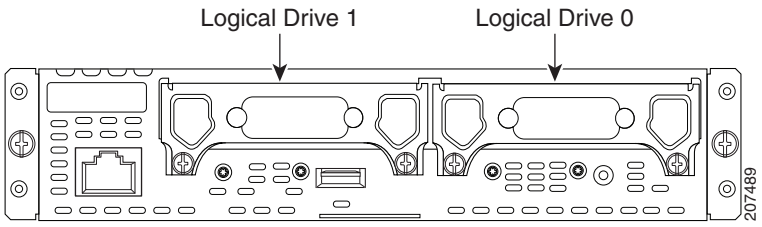
You can remove a failed disk drive when the RAID 1 option is chosen at the time of software installation. Figure 2 shows the typical partitions in the RAID 1 disk drive array.

Before you can remove the faulty drive, you must first enter the CLI command **disk remove <0 | 1>** for drive 0 or drive 1, whichever is the faulty drive.

Note

- Determine which drive number is logical drive 0 and which drive 1 (see Figure 3).
- You can only remove one drive.

Figure 3 Location of Drive 0 and Drive 1 on the Cisco SRE Module



If you do not know which of the two drives is faulty, the CLI can identify which of the drives is faulty and does not allow the **disk remove** command to complete unless the faulty drive number is correctly entered; entering the incorrect drive number results in an error message, notifying you that the incorrect drive option has been entered in the command. If this occurs, enter the other drive number in the **disk remove** command.

After identifying the faulty drive, physically remove the faulty drive and replace it with a new drive on the Cisco SM-SRE module (see the "Replacing Hard Drives on Service Modules" section of the *Installing Cisco Network Modules and Service Modules in Cisco Access Routers*).

When the new disk drive is inserted in the Cisco SRE module to replace the faulty drive, the new drive is automatically reformatted to match the working drive and the RAID arrays are reassembled as the drive recovers.

The following is an example of a successful CLI **disk remove 0** command.

```
cvmss-module# disk remove 0
You are about to remove disk 0 (sda) from the RAID array and SCSI
Do you wish to continue [y/n]? y
raid1: Disk failure on sda2, disabling device.
Feb  2 16:30:25 localhost kernel: raid1: Disk failure on sda2, disabling device.
mdadm: set /dev/sda1 faulty in /dev/md0
mdadm: set /dev/sda2 faulty in /dev/md1
mdadm: hot removed /dev/sda1
mdadm: hot removed /dev/sda2
/dev/md2 /media0 ext3 ro,data=ordered 0 0
Buffer I/O error on device md2, logical block 1116
mdadm: stopped /dev/md2
```

After the failed local disk drive 0 on the Cisco SM-SRE module is physically removed, a new replacement disk drive is swapped and plugged into the module. The following example shows the Linear RAID disk drive hot swap **disk add 0** command and the **show disk stats** command to display the drive's recovery progress. If the **disk add 0** command is successful, the following is displayed.

```
cvmss-module# disk add 0
You are about to add disk 0 (sda) back to the RAID array and SCSI
Do you wish to continue [y/n]? y
!!!WARNING!!!
!!!WARNING!!!  You are about to start a serious operation on the
!!!WARNING!!!  local media.  Adding a new drive requires the
!!!WARNING!!!  linear storage partition to be rebuilt and formatted.
!!!WARNING!!!
!!!WARNING!!!  During this operation, your console is locked and
!!!WARNING!!!  unavailable for use.
!!!WARNING!!!
!!!WARNING!!!  If you are not sure what to do, answer no to the
!!!WARNING!!!  following question and then exit.
!!!WARNING!!!
Do you wish to proceed [y/n]? : y
Checking that no-one is using this disk right now ...
OK

Disk /dev/sda: 60801 cylinders, 255 heads, 63 sectors/track
Old situation:
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

   Device Boot Start     End   #cyls    #blocks   Id  System
/dev/sda1          0+    365     366-   2939863+  fd  Linux raid autodetect
/dev/sda2        366     609     244    1959930   fd  Linux raid autodetect
/dev/sda3        610    1826    1217    9775552+  fd  Linux raid autodetect
/dev/sda4          0       -       0          0    0  Empty
New situation:
No partitions found
```

```
sfdisk: no partition table present.
Checking that no-one is using this disk right now ...
OK

Disk /dev/sda: 60801 cylinders, 255 heads, 63 sectors/track
Old situation:
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

   Device Boot Start     End   #cyls    #blocks   Id  System
/dev/sda1          0+    365     366-   2939863+  fd  Linux raid autodetect
/dev/sda2        366     609     244    1959930   fd  Linux raid autodetect
/dev/sda3        610    1826    1217    9775552+  fd  Linux raid autodetect
/dev/sda4          0       -       0          0    0  Empty
New situation:
Units = sectors of 512 bytes, counting from 0

   Device Boot    Start       End   #sectors  Id  System
/dev/sda1            63   5879789    5879727  fd  Linux raid autodetect
/dev/sda2       5879790   9799649    3919860  fd  Linux raid autodetect
/dev/sda3       9799650  29350754   19551105  fd  Linux raid autodetect
/dev/sda4             0         -          0   0  Empty
Warning: no primary partition is marked bootable (active)
This does not matter for LILO, but the DOS MBR will not boot this disk.
Successfully wrote the new partition table

Re-reading the partition table ...

If you created or changed a DOS partition, /dev/foo7, say, then use dd(1)
to zero the first 512 bytes:  dd if=/dev/zero of=/dev/foo7 bs=512 count=1
(See fdisk(8).)
mdadm: added /dev/sda1
mdadm: added /dev/sda2
mke2fs 1.35 (28-Feb-2004)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
1224000 inodes, 2443888 blocks
122194 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2503999488
75 block groups
32768 blocks per group, 32768 fragments per group
16320 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 29 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
mdadm: chunk size defaults to 64K
mdadm: /dev/sda3 appears to contain an ext2fs file system
    size=9775552K  mtime=Wed Dec 31 16:00:00 1969
mdadm: /dev/sdb3 appears to contain an ext2fs file system
    size=9775552K  mtime=Tue Feb  2 10:57:14 2010
mdadm: /dev/sdb3 appears to be part of a raid array:
    level=linear devices=2 ctime=Tue Feb  2 15:19:04 2010
Continue creating array? mdadm: array /dev/md2 started.
vmss-25-210-30# lin sh
Saving session script in: linux_session.log
```

```
cvmss-module# cat /proc/mdstat
Personalities : [linear] [raid1]
md1 : active raid1 sda2[0] sdb2[1]
      1959808 blocks [2/2] [UU]

md2 : active linear sdb3[1] sda3[0]
      19550976 blocks 64k rounding

md0 : active raid1 sda1[0] sdb1[1]
      2939776 blocks [2/2] [UU]

unused devices: <none>
```

As the new RAID 1 drive recovers, use the **show disk stats** command to display the recovery as the new disk drive recovers. The **show disk stats** command can be repeated periodically to display the recovery as an incremental progress bar that indicates the percentage completion of disk recovery, as shown in the following example:

```
cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[2] sda2[0]
      1959808 blocks [2/1] [U_]
        resync=DELAYED

md2 : active raid1 sdb3[2] sda3[0]
      9775488 blocks [2/1] [U_]
        resync=DELAYED

md0 : active raid1 sdb1[2] sda1[0]
      2939776 blocks [2/1] [U_]
      [==>..................]  recovery = 13.4% (396288/2939776) finish=0.8min
speed=49536K/sec

unused devices: <none>

cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[2] sda2[0]
      1959808 blocks [2/1] [U_]
        resync=DELAYED

md2 : active raid1 sdb3[2] sda3[0]
      9775488 blocks [2/1] [U_]
      [================>.....]  recovery = 77.6% (7589248/9775488) finish=0.7min
speed=50901K/sec

md0 : active raid1 sdb1[1] sda1[0]
      2939776 blocks [2/2] [UU]

unused devices: <none>

cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      1959808 blocks [2/2] [UU]

md2 : active raid1 sdb3[1] sda3[0]
      9775488 blocks [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
      2939776 blocks [2/2] [UU]

unused devices: <none>
```

If the incorrect disk drive has been entered in the **disk remove** command, in this case disk drive 1, it results in the following example output. Note the error message, shown here in **bold** type for emphasis, explaining that he drive is active and cannot be removed.

```
cvmss-module# disk remove 1
You are about to remove disk 1 (sdb) from the RAID array and SCSI
Do you wish to continue [y/n]? y
sdb is the only active drive, can't be removed
```

Linear RAID Option

With the Linear RAID option, only the root partition and swap drive are mirrored, giving up only a fraction of the disk storage capacity (see Figure 2). The remainder of the available storage space is contained in a Linear RAID array used as the storage partition. Even with a drive failure with this option, the Cisco Video Management and Storage System can still be used to view live video streams from the VSOM and VSMS, and the CLI of the application is still accessible. The cost for higher disk capacity with the Linear RAID option, however, is that all archive data on the local drive is lost when there is a disk drive failure.

If the Linear RAID drive fails and is replaced with a new drive, the Cisco Video Management and Storage System reformats the media partition and provides a fresh media mount; the root partition and swap partitions are restored.

The following example shows the disk removed and Linear RAID remounted.

```
cvmss-module# ext3_abort called.
EXT3-fs error (device md2): ext3_journal_start_sb: Feb  2 16:27:03 Detected aborted
journal
localhost kernelRemounting filesystem read-only
: ext3_abort called.
Feb  2 16:27:03 localhost kernel: EXT3-fs error (device md2): ext3_journal_start_sb:
Detected aborted journal
Feb  2 16:27:03 localhost kernel: Remounting filesystem read-only
Buffer I/O error on device md2, logical block 1

cvmss-module# cat /proc/mdstat
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      1959808 blocks [2/2] [UU]

md2 : active linear sdb3[1] sda3[0]
      19550976 blocks 64k rounding

md0 : active raid1 sdb1[1] sda1[2](F)
      2939776 blocks [2/1] [_U]

unused devices: <none>

cvmss-module# cat /proc/mounts | grep md2
/dev/md2 /media0 ext3 ro,data=ordered 0 0
cvmss-module# exit
exit
```

Raid 0 Option

With the RAID 0 option, disk drive performance is enhanced but there is no data redundancy. RAID 0 data are evenly divided across two or more disks (striped) without redundancy.

If a drive fails, it wipes out the whole array. It is destroyed because, when data is written to a RAID 0 drive, the data is broken into fragments. With these fragments, smaller portions of the entire data can be read off the drive in parallel, increasing bandwidth and overall drive performance. However, there is no error checking with a RAID 0 array, which makes the array susceptible to unrecoverable errors. With two disks in the array there is higher bandwidth but greater risk of data loss.

The RAID 0 configuration examples are the same as those presented in the "Linear RAID Option" section on page 34, except that the output is for RAID 0.

Formatting the Local Drive

The **format storages local** command formats the local storage device with the media tag of *media0*. Use the **show storages all filesystem** command to get information about the current state of *media0*. The **local** command option is also available.

As shown in Examples, a data loss warning message appears immediately after this command is entered. Local storage device formatting proceeds only after a **y(es)** confirmation is entered.

Note If the Cisco Video Management and Storage System application is in the process of storing or reviewing an archive from *media0*, formatting of *media0* will not proceed and a device busy message will appear.

SUMMARY STEPS

1. **format storages local** *media-tag*

Caution The format command erases all data from the disk drive. Make sure that any data you want to preserve is backed up.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**format storages local** *media-tag* **Example:** `cvmss-module# format storages local media0`	Formats the local storage device. *media-tag:* For the local storage device, the media tag sets the unique string identifier for the local storage device *media0*.

Examples

The following example shows the command to format the local storage device, media0:

```
cvmss-module> format storages local media0

!!!WARNING!!!
!!!WARNING!!!  You are about to start a destructive sequence of
!!!WARNING!!!  operations. All data on the storage device media0
!!!WARNING!!!  will be lost and unrecoverable.
!!!WARNING!!!  The device formatting can take up to a few minutes.
!!!WARNING!!!  During formatting, your console is locked and
!!!WARNING!!!  unavailable for use. Before you proceed further, back
!!!WARNING!!!  up the contents of the storage device media0.
```

```
!!!WARNING!!!
!!!WARNING!!!  If you are not sure what to do, answer "no" to the
!!!WARNING!!!  following question and then exit.
!!!WARNING!!!

Do you wish to proceed [y/n]? :
```

Configuring NFS Mounts from NFS Servers

NFS allows data to be stored on central servers and easily accessed from client devices in a client/server network configuration through a process called mounting. It allows a system to share directories and files with others over a network. Files stored on external remote systems can be accessed almost as if they were local files. The Cisco Video Management and Storage System supports the CLI configuration of NFS for remote video archiving.

NFS supports multiple mounts. However, the Cisco Video Management and Storage System supports a one-to-one relationship between NFS exports and mount configurations. For example, if you had an NFS server with four exports and you wanted to configure three of those mounts for video archive storage, you need to configure three separate media enclosures.

NFS supports the **target-ip** command differently. You no longer need to disable an export to mount a new export. You can simply issue a **target-ip** *ip-address* **exportName** *export-name* command to mount a new export. If you want to change the media's IP address, simply issue **target-ip** *ip-address* command, which automatically unmounts the old IP address and export name and adds the new IP address.

SUMMARY STEPS

1. **configure terminal**
2. **storages nfs** *media-tag*
3. **end**
4. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`cvmss-module> configure terminal`
	
	Example:
	
	`cvmss-module> configure terminal`
	`cvmss-module (config)#`
		Enter global configuration mode.

Step 2	`cvmss-module (config)# storages nfs media-tag`
	
	Example:
	
	`cvmss-module (config)# storages nfs media1`
	`Modifying existing nfs`
	`cvmss-module (config-nfs)#`
		Enter the NFS configuration mode for the NFS mount identified by *media-tag.*
		
		media-tag:
		
		For NFS mount, the media tag sets the unique string identifier for the NFS mount from an NFS server in the range of *media1* to *media9*.

	Command or Action	Purpose

Step 3	[**default** | **state** | **switch-on-fail** | **target-ip**]
	
	Example:
	`cvmss-module(config-nfs)> storages nfs media1`
	`Adding new nfs`
	`cvmss-module(config-nfs)> default`
	`cvmss-module(config-nfs)> state disabled`
	`cvmss-module(config-nfs)>`
	`cvmss-module(config-nfs)> target-ip 10.10.10.60`
	`Connecting 10.10.10.60... succeeded.`
	`cvmss-module(config-nfs)> target-ip 10.10.10.60`
	`Connecting 10.10.10.60... failed.`
	`ERROR: The target could not be connected because multiple exports exist on this storage server`
	`/var/nfs`
	`/source/nfs`
	`cvmss-module(config-nfs)> target-ip 10.10.10.60 exportname /var/nfs`
	`Connecting 10.10.10.60... succeeded.`
	`cvmss-module(config-nfs)> state enabled`
	`cvmss-module(config-nfs)> end`
	`cvmss-module(config)> exit`
	`cvmss-module>`
		Configures NFS mount configuration parameters.
		
		default: NFS mount default values.
		
		state: Enables or disables the operational state of the NFS mount:
		• **disabled**: The NFS export is not mounted.
		• **enabled**: The NFS export is mounted.
		
		Default: Disabled.
		
		switch-on-fail [**on** | **off**]: Configures whether the archives can be switched to the local hard drive in the case where the NFS media device is not available. When **on**, the switchover of the archives process to the local drive occurs in the event the NFS media is not available.
		
		Note This feature is only available to the NFS device on the ISS module. It checks whether the configured device is the NFS media from the ISS module.
		
		Default: Off—The application waits for the configured NFS media device to become available before starting the archive.
		
		target-ip: Sets the NFS target IP address in dotted decimal format or name of the export server.
		• *ip-address*: Selects the IP address of a single export.
		• **exportname** *server-export*: Selects the server export directories.

Step 4	**end** **Example:** `cvmss-module (config-nfs)# end`	Exits NFS mount format configuration mode.
Step 5	**end** **Example:** `cvmss-module (config)# end`	Exits global configuration mode.

Cisco Video Management and Storage System Command Reference

Last Updated: April 22, 2010

This section documents commands for the Cisco Video Management and Storage System application and commands for Cisco IOS software:

Common Cisco Video Management and Storage System Module Commands

disk add

To add a replacement RAID 1, Linear RAID, or RAID 0 local disk drive, use the **disk add** command in global configuration mode.

disk add {**0** | **1**}

Syntax Description

0	Local disk drive 0.
1	Local disk drive 1.

Command Modes

Global configuration mode

Command History

Version	Modification
6.2.1	This command was introduced.

Usage Guidelines

The CLI keeps track of which drive has failed. If the selected drive (0 or 1) is not the failed drive, the CLI does not allow the command to take effect and an error appears.

If a local disk drive fails and the incorrect disk drive is selected in the CLI, the CLI displays error messages as shown in the following example:

```
cvmss-module# disk add 1
You are about to add disk 1 (sdb) back to the RAID array and SCSI
Do you wish to continue [y/n]? y
sdb is already active, can't add it back again.

cvmss-module# disk add 0
You are about to add disk 0 (sda) back to the RAID array and SCSI
Do you wish to continue [y/n]? y
sda still exists in the RAID array.  Please issue a "disk remove" first.
```

Examples

Linear Disk Drive Swap and Recovery

After the failed local disk drive 0 on the Cisco SM-SRE module is physically removed, a new replacement disk drive is swapped and plugged into the module. The following example shows the Linear RAID disk drive hot swap **disk add 0** command and the **show disk stats** command to display the drive's recovery progress. If the **disk add 0** command succeeds, the following is displayed:

```
cvmss-module# disk add 0
You are about to add disk 0 (sda) back to the RAID array and SCSI
Do you wish to continue [y/n]? y
!!!WARNING!!!
!!!WARNING!!!  You are about to start a serious operation on the
!!!WARNING!!!  local media.  Adding a new drive requires the
!!!WARNING!!!  linear storage partition to be rebuilt and formatted.
!!!WARNING!!!
!!!WARNING!!!  During this operation, your console is locked and
!!!WARNING!!!  unavailable for use.
!!!WARNING!!!
!!!WARNING!!!  If you are not sure what to do, answer no to the
```

```
!!!WARNING!!!  following question and then exit.
!!!WARNING!!!
Do you wish to proceed [y/n]? : y
Checking that no-one is using this disk right now ...
OK

Disk /dev/sda: 60801 cylinders, 255 heads, 63 sectors/track
Old situation:
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

   Device Boot Start     End   #cyls    #blocks   Id  System
/dev/sda1          0+    365     366-   2939863+  fd  Linux raid autodetect
/dev/sda2        366     609     244    1959930   fd  Linux raid autodetect
/dev/sda3        610    1826    1217    9775552+  fd  Linux raid autodetect
/dev/sda4          0       -       0          0    0  Empty
New situation:
No partitions found

sfdisk: no partition table present.
Checking that no-one is using this disk right now ...
OK

Disk /dev/sda: 60801 cylinders, 255 heads, 63 sectors/track
Old situation:
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

   Device Boot Start     End   #cyls    #blocks   Id  System
/dev/sda1          0+    365     366-   2939863+  fd  Linux raid autodetect
/dev/sda2        366     609     244    1959930   fd  Linux raid autodetect
/dev/sda3        610    1826    1217    9775552+  fd  Linux raid autodetect
/dev/sda4          0       -       0          0    0  Empty
New situation:
Units = sectors of 512 bytes, counting from 0

   Device Boot    Start       End   #sectors  Id  System
/dev/sda1            63   5879789    5879727  fd  Linux raid autodetect
/dev/sda2       5879790   9799649    3919860  fd  Linux raid autodetect
/dev/sda3       9799650  29350754   19551105  fd  Linux raid autodetect
/dev/sda4             0         -          0   0  Empty
Warning: no primary partition is marked bootable (active)
This does not matter for LILO, but the DOS MBR will not boot this disk.
Successfully wrote the new partition table

Re-reading the partition table ...

If you created or changed a DOS partition, /dev/foo7, say, then use dd(1)
to zero the first 512 bytes:  dd if=/dev/zero of=/dev/foo7 bs=512 count=1
(See fdisk(8).)
mdadm: added /dev/sda1
mdadm: added /dev/sda2
mke2fs 1.35 (28-Feb-2004)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
1224000 inodes, 2443888 blocks
122194 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2503999488
75 block groups
32768 blocks per group, 32768 fragments per group
16320 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
```

```
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 29 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
mdadm: chunk size defaults to 64K
mdadm: /dev/sda3 appears to contain an ext2fs file system
    size=9775552K  mtime=Wed Dec 31 16:00:00 1969
mdadm: /dev/sdb3 appears to contain an ext2fs file system
    size=9775552K  mtime=Tue Feb  2 10:57:14 2010
mdadm: /dev/sdb3 appears to be part of a raid array:
    level=linear devices=2 ctime=Tue Feb  2 15:19:04 2010
Continue creating array? mdadm: array /dev/md2 started.
vmss-25-210-30# lin sh
Saving session script in: linux_session.log

cvmss-module# cat /proc/mdstat
Personalities : [linear] [raid1]
md1 : active raid1 sda2[0] sdb2[1]
      1959808 blocks [2/2] [UU]

md2 : active linear sdb3[1] sda3[0]
      19550976 blocks 64k rounding

md0 : active raid1 sda1[0] sdb1[1]
      2939776 blocks [2/2] [UU]

unused devices: <none>
```

As the new Linear RAID drive recovers, use the **show disk stats** command to display the recovery as a progress bar and percentage recovered. The **show disk stats** command can be repeated to monitor the drive recover.

```
cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[2] sda2[0]
      1959808 blocks [2/1] [U_]
        resync=DELAYED

md2 : active raid1 sdb3[2] sda3[0]
      9775488 blocks [2/1] [U_]
        resync=DELAYED

md0 : active raid1 sdb1[2] sda1[0]
      2939776 blocks [2/1] [U_]
      [==>..................]  recovery = 13.4% (396288/2939776) finish=0.8min
speed=49536K/sec

unused devices: <none>

cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[2] sda2[0]
      1959808 blocks [2/1] [U_]
        resync=DELAYED

md2 : active raid1 sdb3[2] sda3[0]
      9775488 blocks [2/1] [U_]
      [===============>.....]  recovery = 77.6% (7589248/9775488) finish=0.7min
speed=50901K/sec

md0 : active raid1 sdb1[1] sda1[0]
```

```
      2939776 blocks [2/2] [UU]

unused devices: <none>

cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      1959808 blocks [2/2] [UU]

md2 : active raid1 sdb3[1] sda3[0]
      9775488 blocks [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
      2939776 blocks [2/2] [UU]

unused devices: <none>

cvmss-module# ext3_abort called.
EXT3-fs error (device md2): ext3_journal_start_sb: Feb  2 16:27:03 Detected aborted
journal
localhost kernelRemounting filesystem read-only
: ext3_abort called.
Feb  2 16:27:03 localhost kernel: EXT3-fs error (device md2): ext3_journal_start_sb:
Detected aborted journal
Feb  2 16:27:03 localhost kernel: Remounting filesystem read-only
Buffer I/O error on device md2, logical block 1

cvmss-module# cat /proc/mdstat
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      1959808 blocks [2/2] [UU]

md2 : active linear sdb3[1] sda3[0]
      19550976 blocks 64k rounding

md0 : active raid1 sdb1[1] sda1[2](F)
      2939776 blocks [2/1] [_U]

unused devices: <none>

cvmss-module# cat /proc/mounts | grep md2
/dev/md2 /media0 ext3 ro,data=ordered 0 0
cvmss-module# exit
exit
```

Related Commands

Command	Description
disk remove	Removes a failed RAID 1 local disk drive device.

disk remove

To remove a failed RAID 1, Linear RAID, or RAID 0 local disk drive device, use the **disk remove** command in global configuration mode.

disk remove {**0** | **1**}

Syntax Description

0	Local disk drive 0.
1	Local disk drive 1.

Command Modes

Global configuration mode

Command History

Version	Modification
6.2.1	This command was introduced.

Usage Guidelines

The CLI keeps track of which drive has failed. If the selected drive (0 or 1) is not the failed drive, the CLI does not allow the command to take effect and an error appears.

If a local disk drive fails and the incorrect disk drive is selected in the CLI, the CLI displays error messages as shown in the following example:

```
cvmss-module# disk remove 1
You are about to remove disk 1 (sdb) from the RAID array and SCSI
Do you wish to continue [y/n]? y
sdb is the only active drive, can't be removed
```

Examples

Linear Raid Disk Drive Removal

The following example shows the Linear RAID disk drive hot swap **disk remove 0** command. If the **disk remove 0** command succeeds, the following CLI output is displayed:

```
cvmss-module# disk remove 0
You are about to remove disk 0 (sda) from the RAID array and SCSI
Do you wish to continue [y/n]? y
raid1: Disk failure on sda2, disabling device.
Feb  2 16:30:25 localhost kernel: raid1: Disk failure on sda2, disabling device.
mdadm: set /dev/sda1 faulty in /dev/md0
mdadm: set /dev/sda2 faulty in /dev/md1
mdadm: hot removed /dev/sda1
mdadm: hot removed /dev/sda2
/dev/md2 /media0 ext3 ro,data=ordered 0 0
Buffer I/O error on device md2, logical block 1116
mdadm: stopped /dev/md2

cvmss-module# lin sh
Saving session script in: linux_session.log
bash-2.05b# cat /proc/mdstat
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[1]
      1959808 blocks [2/1] [_U]
```

```
md0 : active raid1 sdb1[1]
      2939776 blocks [2/1] [_U]
```

The failed local disk drive 1 on the Cisco SM-SRE module is physically removed and a new replacement disk drive swapped. The following example shows the Linear RAID disk drive hot swap **disk add 1** command:

```
cvmss-module# disk add 1
You are about to add disk 1 (sdb) back to the RAID array and SCSI
Do you wish to continue [y/n]? y

Disk /dev/sdb: 60801 cylinders, 255 heads, 63 sectors/track
Old situation:
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

   Device Boot Start     End   #cyls    #blocks   Id  System
/dev/sdb1          0+    365     366-   2939863+  fd  Linux raid autodetect
/dev/sdb2        366     609     244    1959930   fd  Linux raid autodetect
/dev/sdb3        610    1826    1217    9775552+  fd  Linux raid autodetect
/dev/sdb4          0       -       0          0    0  Empty
New situation:
Units = sectors of 512 bytes, counting from 0

   Device Boot    Start       End   #sectors  Id  System
/dev/sdb1            63   5879789    5879727  fd  Linux raid autodetect
/dev/sdb2       5879790   9799649    3919860  fd  Linux raid autodetect
/dev/sdb3       9799650  29350754   19551105  fd  Linux raid autodetect
/dev/sdb4             0         -          0   0  Empty
Successfully wrote the new partition table

Re-reading the partition table ...

mdadm: added /dev/sdb1
mdadm: added /dev/sdb2
mdadm: added /dev/sdb3
```

As the new Linear RAID disk drive recovers, the **show disk stats** command can be repeated periodically to display the recovery as an incremental progress bar that indicates the percentage completion of disk recovery, as shown in the following example:

```
cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[2] sda2[0]
      1959808 blocks [2/1] [U_]
        resync=DELAYED

md2 : active raid1 sdb3[2] sda3[0]
      9775488 blocks [2/1] [U_]
        resync=DELAYED

md0 : active raid1 sdb1[2] sda1[0]
      2939776 blocks [2/1] [U_]
      [==>..................]  recovery = 13.4% (396288/2939776) finish=0.8min
speed=49536K/sec

unused devices: <none>

cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[2] sda2[0]
      1959808 blocks [2/1] [U_]
        resync=DELAYED
```

```
md2 : active raid1 sdb3[2] sda3[0]
      9775488 blocks [2/1] [U_]
      [===============>.....]  recovery = 77.6% (7589248/9775488) finish=0.7min
speed=50901K/sec

md0 : active raid1 sdb1[1] sda1[0]
      2939776 blocks [2/2] [UU]

unused devices: <none>

cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      1959808 blocks [2/2] [UU]

md2 : active raid1 sdb3[1] sda3[0]
      9775488 blocks [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
      2939776 blocks [2/2] [UU]

unused devices: <none>
```

Related Commands

Command	Description
disk add	Adds a replacement RAID 1 or Linear RAID local disk drive.

event poll-interval

To set the HTTP trigger event polling interval in seconds, use the **event poll-interval** command in global configuration mode.

Note The event polling interval configures the sensitivity of the system for event detection. However, it does not specify the exact amount of time it takes until an event is detected.

Use the **no** form of the command to return the event polling interval to its default value.

event poll-interval *seconds*

no event poll-interval

Syntax Description

seconds	Number of seconds to set the event polling interval. **Note** Event polling interval can only be within the range of 2 to 30 seconds.

Command Default

2 seconds

Command Modes

Global configuration

Command History

Version	Modification
6.2.1	This command was introduced.

Usage Guidelines

The default HTTP trigger event polling interval (2 seconds) optimizes performance as well as triggered event responses.

However, if performance issues arise because the event polling is too frequent, then you can increase the polling interval at the expense of delayed event detection.

Examples

If the times of the polling interval are not within the valid 2 to 30 second range, the CLI returns “Event polling interval can only be 2-30 sec,” and does not accept any interval that is not within this range:

```
cvmss-module(config)# event poll-interval 32
Event polling interval can only be 2-30 sec.
```

In the next example, the poll interval of 11 seconds is accepted:

```
cvmss-module(config)# event poll-interval 11
Event polling interval changed. New value will take effect after restarting video
application.
```

To verify that the CLI has accepted the new event polling interval, use the **show event poll-interval** command, as shown in the following example:

```
cvmss-module(config)# end
cvmss-module# show event poll-interval
Event polling interval is 11 seconds.
```

For the new HTTP trigger event polling interval to take effect, you must restart the video using the **video-surveillance task restart** command. This command restarts all Cisco video services, as shown in the following example:

```
cvmss-module# video-surveillance task restart
Restarting all Cisco Video Surveillance services, please wait ...
snmpd:/usr/BWhttpd/sbin/snmpd:status...Running
snmptrapd:/usr/BWhttpd/sbin/snmptrapd:status...Running
Checking for vsrecorder
    Checking for xvcrmanMonitor... Running.
    Checking for xvcrman... Running.
    Checking for xvcrconfig... Running.
Checking for vsms daemons... running.
Checking for mediaout... Running.
Checking for httpd... running.
Checking for service MRTG mrtg:/usr/BWhttpd/bin/mrtg:status...Running
Checking for backup server... Running.
Checking for sys config agent... Running.
```

To verify that the video services are now running, use the **show video-surveillance task status** command.

Related Commands

Command	Description
show event poll-interval	Displays the HTTP trigger event polling interval.

format storages local

Note Use the following command for version 2.0 and later of the Cisco Video Management and Storage System.

To format a local storage device, use the **format storages local** command in format storages local configuration mode.

Note For the changes to take effect, the media must first be disabled and then reenabled.

format storages local *media-tag*

Syntax Description

media-tag	Unique string identifier for the LOCAL mass storage device in the range of media1 to media9.

Command Default

The local storage device contains software applications.

Command Modes

Format storages local configuration

Command History

Version	Modification
2.0	This command was introduced.

Usage Guidelines

The media tag for the local storage device is media0.

Examples

The following example shows the command to format the local storage device media0:

```
cvmss-module> format storages local media0

!!!WARNING!!!
!!!WARNING!!!  You are about to start a destructive sequence of
!!!WARNING!!!  operations. All data on the storage device media0
!!!WARNING!!!  will be lost and unrecoverable.
!!!WARNING!!!  The device formatting can take up to a few minutes.
!!!WARNING!!!  During formatting, your console is locked and
!!!WARNING!!!  unavailable for use. Before you proceed further, back
!!!WARNING!!!  up the contents of the storage device media0.
!!!WARNING!!!
!!!WARNING!!!  If you are not sure what to do, answer "no" to the
!!!WARNING!!!  following question and then exit.
!!!WARNING!!!

Do you wish to proceed [y/n]? :
```

Related Commands

Command	Description
show storages all filesystem	Displays the configuration parameter summary for all storage file systems.

show event poll-interval

To display the HTTP trigger event polling interval, use the **show even poll-interval** command user EXEC configuration mode.

show event poll-interval

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Version	Modification
6.2.1	This command was introduced.

Examples

The following example shows the display output for the **show event poll-interval** command:

```
cvmss-module# show event poll-interval
Event polling interval is 11 seconds.
```

Related Commands

Command	Description
event poll-interval	Sets the HTTP trigger event polling interval in seconds.

show disk stats

To display the statistics of the active disk drives, use the **show disk stats** command user EXEC configuration mode.

show disk stats

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Version	Modification
6.2.1	This command was introduced.

Examples

The following example shows the statistics display output for the **show disk stats** command:

```
cvmss-module# show disk stats
Personalities : [linear] [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      1959808 blocks [2/2] [UU]

md2 : active raid1 sdb3[1] sda3[0]
      9775488 blocks [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
      9775424 blocks [2/2] [UU]

unused devices: <none>
```

The **show disk stats** command can be entered repeatedly to monitor disk recovery after a disk drive swap.

Related Commands

Command	Description
disk add	Adds a replacement RAID 1 or Linear RAID local disk drive.
disk remove	Removes a failed RAID 1 local disk drive device.

show storages all filesystem

To display a configuration parameter summary for all storage file systems, use the **show storage all filesystem** command in user EXEC configuration mode.

show storages all filesystem

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Version	Modification
1.0	This command was introduced.

Examples

To view a summary of all configured file systems, use the **show storages all filesystem** command. For example:

```
cvmss-module# show storages all filesystem
Filesystem            1K-blocks      Used  Available Use% Mounted on
==================== ===========  ======= ========== ==== ==========
rootfs                 9775184   1081480   8693704    12% /
/dev/root              9775184   1081480   8693704    12% /
none                   1036520         0   1036520     0% /dev/shm
/dev/sda3            142284500     32828 135024032     1% /media0
/dev/sdb            2307162084 1172169844 1017795172 54% /media1_0
/dev/sdc             576789800    106560 547384004     1% /media1_1
```

Table 7 lists and describes the output fields of the **show storages all filesystem** command.

Table 7 show storages all filesystem Field Descriptions

Field	Description
Filesystem	Lists the file system and devices.
1K-blocks	Displays the available number of 1-kilobyte blocks for each of the target devices.
Used	Displays the used number of 1-kilobyte blocks for each of the target devices.
Available	Displays the available remaining number of 1-kilobyte blocks for each of the target devices.
Use%	Displays the used percentage of 1-kilobyte blocks for each of the target devices.
Mounted on	Displays the target device name on which the file system is mounted.

Related Commands

Command	Description
show storages nfs filesystem	Displays the parameter summary for currently configured NFS file systems.

show storages nfs

To display the summary of the current NFS mount details, use the **show storages nfs** command in user EXEC configuration mode.

show storages nfs

Note This command might not reflect the actual state of the NFS mount because the configuration only occurs at mount time. You must unmount and then mount the device again for the configuration to take effect. To confirm the current mount values, use the show storages nfs status command.

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Version	Modification
2.2	This command was introduced.

Examples

To view the values of the current NFS configuration, use the **show storages nfs** command. For example:

```
cvmss-module# show storages nfs
Tag     Target IP     Mount Name   IO Error Handling
======= ===========   ==========   =================
Media1  10.10.10.60   /var/nfs     hard
```

Table 8 lists and describes the output fields of the **show storages nfs** command.

Table 8 show storages nfs Field Descriptions

Field	Description
Tag	Displays the unique string identifier for the NFS mount from an NFS server in the range of media1 to media9.
Target IP	Displays the NFS device IP address.
Mount Name	Displays the NFS device mount directory name.
IO Error Handling	Displays the type of input/output error handling of the NFS mount.

Related Commands

Command	Description
state (storages nfs)	Mounts or unmounts an NFS export.
switch-on-fail (storages nfs)	Configures whether the archives can be switched to the local hard drive when the NFS media device is not available.
target-ip (storages nfs)	Configures the IP address and name of an NFS export target.

show storages nfs filesystem

To display the parameter summary for currently configured NFS file systems, use the **show storage nfs filesystem** command in user EXEC configuration mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Version	Modification
2.2	This command was introduced.

Examples

To view a summary of the currently configured NFS file systems, use the **show storages nfs filesystem** command. For example:

```
cvmss-module# show storages nfs filesystem
Filesystem            1K-blocks   Used    Available  Use% Mounted on
==================== ===========  ======= ========== ==== ==========
10.10.10.60/var/nfs  206424760    3999716 191939284  3%   /media1
```

Table 9 lists and describes the output fields of the **show storages nfs filesystem** command.

Table 9 show storages nfs filesystem Field Descriptions

Field	Description
Filesystem	Lists the file system and devices.
1K-blocks	Displays the available number of 1-kilobyte blocks for each of the corresponding NFS mounts.
Used	Displays the used number of 1-kilobyte blocks for each of the NFS mounts.
Available	Displays the available remaining number of 1-kilobyte blocks for each of the NFS mounts.
Use%	Displays the used percentage of 1-kilobyte blocks for each of the NFS mounts.
Mounted on	Displays the NFS mount name on which the file system is mounted.

Related Commands

Command	Description
storages nfs	Configures NFS file system parameters.

show storages nfs status

To display the status of the settings of the specified NFS mount, use the **show storages nfs status** command in user EXEC configuration mode.

show storages nfs status {summary | detail}

Syntax Description

summary	Displays a general summary of the status of configured NFS mount.
detail	Displays a detailed summary of the status of configured NFS mount.

Command Modes

User EXEC

Command History

Version	Modification
2.2	This command was introduced.

Examples

To view the status summary of the NFS mount settings of the specified NFS mount, use the **show storages nfs status** command. For example:

```
cvmss-module# show storages nfs status summary
Tag    Filesystem            Mounts   Port       Receive-  Write- Version  Proto  IO Error
                                      Reachable  Buffer-   Buffer-               Handling
                                                 Size      Size
====== ====================== ======  ========== ========= ====== ========  ====  ========
Media1 10.10.10.60:/var/mfs  /media1  Yes        65536     65536  3         UDP    hard
```

Table 10 lists and describes the output fields of the **show storages nfs status** command.

Table 10 show storages nfs status summary Field Descriptions

Field	Description
Tag	Displays the unique string identifier for the NFS mount from an NFS server in the range of media1 to media9.
Filesystem	Displays the NFS file system device IP address and directory.
Mounts	Displays the NFS mounts.
Port Reachable	Displays whether or not the NFS mount port is reachable.
Receive Buffer Size	Displays the NFS device receive buffer size.
Write Buffer Size	Displays the NFS device write buffer size.
Version	Displays the version number of the NFS protocol currently being used.
Proto	Displays the transport protocol currently being used.
IO Error Handling	Displays the type of input/output error handling of the NFS mount.

Related Commands

Command	Description
state (storages nfs)	Mounts or unmounts an NFS export.
switch-on-fail (storages nfs)	Configures whether the archives can be switched to the local hard drive when the NFS media device is not available.
target-ip (storages nfs)	Configures the IP address and name of an NFS export target.

show video-surveillance

To display video surveillance configurations, logs, reports, and tasks, use the **show video-surveillance** command in user EXEC configuration mode.

show video-surveillance [**archive** | **config** | **configs** | **log** | **logs** | **reports** | **tasks**]

Note The **show video-surveillance tasks** command removed in version 2.0 and later versions.

Syntax Description

archive	Displays a list of the running archives and their corresponding destinations along with the IP address and export point.
config	Displays the content of a configuration file.
configs	Displays all the configuration file names.
log	Displays the content of a log file.
logs	Displays all log file names.
reports	Displays all report file names.
tasks	Displays predefined tasks.

Command Modes

User EXEC

Command History

Version	Modification
1.0	This command was introduced.
2.0	This command was modified. The **tasks** command option is removed in version 2.0 and later versions.

Examples

To view predefined tasks, use the **show video surveillance tasks** command. For example:

```
cvmss-module# show video-surveillance tasks
TASK                 DESCRIPTION
restart          Restarting all Cisco Video Surveillance services, please wait
start            Starting all Cisco Video Surveillance services, please wait
status           Report on status of Cisco Video Surveillance services
stop             Stops all running Cisco Video Surveillance services
support-report   Generate the system support report
vsom_db_restore Restore VSOM database from local disk
cron-restart     Restart cron daemon after timezone changes
cert-gen         Generate a ssl server key and certificate
```

To view the archive summary, use the **show video surveillance archive summary** command. For example:

```
cvmss-module# show video-surveillance archive summary
Archive Name            Archive Location (IP Address)   Type      Export Directory
a_p_lab_cam1_-_a_ar1    —                               local
a_p_lab_cam2_-_a_ar2    1.100.30.220                    nfs       /media0
```

Related Commands

Command	Description
video-surveillance	Sets video surveillance configurations, logs, reports, and tasks.

state (storages nfs)

To mount or unmount an NFS export, use the **state** sub-command in the Storages NFS configuration mode.

state [**disabled** | **enabled**]

Syntax Description

disabled	NFS export unmounted.
enabled	NFS export mounted.

Command Default

Disabled

Command Modes

Storages NFS configuration

Command History

Version	Modification
2.2	This command was introduced.

Usage Guidelines

Configure the NFS export state to enabled (mounted) or disabled (unmounted).

Examples

The following example shows the NFS **state** command to mount the NFS export:

```
cvmss-module# configure terminal
cvmss-module(config)# storages nfs media1
cvmss-module(config-nfs)# state enabled
Media successfully enabled!
```

Related Commands

Command	Description
switch-on-fail (storages nfs)	Configures whether the archives can be switched to the local hard drive when the NFS media device is not available.
target-ip (storages nfs)	Configures the IP address and name of an NFS export target.

storages nfs

To configure the media tag for an NFS mount, use the **storages nfs** command in global configure mode.

storages nfs *media-tag*

Syntax Description

media-tag	Unique string identifier for the NFS mount from an NFS server in the range of media1 to media9.

Command Default

NFS mount is not configured.

Command Modes

G1obal Configuration

Command History

Version	Modification
2.2	This command was introduced.

Usage Guidelines

For the NFS mount configuration, nine media tags, *media1* through *media9*, are configurable.

Examples

The following example shows configuring the NFS mount media1 tag for *media1* using the **storages nfs** command:

```
cvmss-module# configure terminal
cvmss-module(config)# storages nfs media1
Adding new nfs
cvmss-module(config-nfs)#
```

Related Commands

Command	Description
state (storages nfs)	Mounts or unmounts an NFS export.
switch-on-fail (storages nfs)	Configures whether the archives can be switched to the local hard drive when the NFS media device is not available.
target-ip (storages nfs)	Configures the IP address and name of an NFS export target.

switch-on-fail (storages nfs)

To configure whether the archives can be switched to the local hard drive in the case where the NFS media device is not available, use the **switch-on-fail** sub-command in Storages NFS configuration mode.

switch-on-fail [**on** | **off**]

Syntax Description

switch-on-fail	Set to whether the archives can be switched to the local hard drive in the case where the NFS media device is not available.
on	Switchover of the archives processing to the local drive occurs in the event the NFS media is not available.
off	The application waits for the configured NFS media device to become available before starting the archive.

Command Default

Off

Command Modes

Storages NFS configuration

Command History

Version	Modification
2.2	This command was introduced.

Usage Guidelines

The **switch-on-fail** sub-command activates a standby repository and provides automatic failover from one repository to the other. The local repository (*media0*) is the standby repository and an external storage server (*media1*, *media2*, *media3*... or *media9*) is the active repository in the initial setup. When there is a disconnect from the external storage server, the local repository, media0, automatically becomes the active repository. The failover process is as follows:

1. When an external storage server is configured for archiving, the system automatically enables media0 as the standby repository location.
2. In the event of a disconnect to the external server (determined through a *portal reachability* test), the archive automatically uses media0 as the active repository.
3. When the external server is reconnected, all archives must be moved from media0 back to the external server.
4. Archives accumulated on media0 during the failover process are removed.

Note This failover archive feature is only available to the NFS device on the Cisco Integrated Storage System module. The software checks whether or not the configured device is the NFS media from the Cisco Integrated Storage System module.

Examples

The following example shows the NFS **state** command to mount the NFS export:

```
cvmss-module# configure terminal
cvmss-module(config)# storages nfs media1
cvmss-module(config-nfs)# switch-on-fail on
Media successfully enabled!
```

Related Commands

Command	Description
state (storages nfs)	Mounts or unmounts an NFS export.
target-ip (storages nfs)	Configures the IP address and name of an NFS export target.

target-ip (storages nfs)

To configure the IP address and export name of an NFS export target, use the **target-ip** sub-command in Storages NFS configuration mode. To remove the IP address and export name of an NFS storage target device, use the **no** form of this command.

target-ip *ip-address* **exportname** *name*

no target-ip *ip-address* **exportname** *name*

Syntax Description

ip-address	IP address in dotted decimal notation.
exportname	Configures the NFS export directory name.
name	Directory name.

Command Default

No NFS target IP address is configured.

Command Modes

Storages NFS configuration

Command History

Version	Modification
2.2	This command was introduced.

Usage Guidelines

For the NFS configuration, nine media tags are configurable (for example, media1, media2, and so on) for up to nine NFS target devices.

Examples

The following example shows the **target-ip** command assumes only one export:

```
cvmss-module# configure terminal
cvmss-module(config)# storages nfs media1
cvmss-module(config-nfs)# target-ip 10.10.10.60
Connecting 10.10.10.60... succeeded.
```

The following example shows the **target-ip** command assumes multiple exports, causing the following failed connection error message to appear:

```
cvmss-module# configure terminal
cvmss-module(config)# storages nfs media1
cvmss-module(config-nfs)# target-ip 10.10.10.60
Connecting 10.10.10.60... failed.

ERROR: The target could not be connected because multiple exports exist on this storage
server. The following exports exist on this storage server:
/var/nfs
/source/nfs
```

The following example shows the **target-ip** command and the resulting error message when the target IP address fails to connect:

```
cvmss-module# configure terminal
cvmss-module(config)# storages nfs media1
cvmss-module(config-nfs)# target-ip 10.10.10.60
Connecting 10.10.10.60... failed.
10.10.10.60--target connection failed.
Please reissue "target-ip" to retry connection.
```

The following example shows the target-ip command with the export parameter:

```
cvmss-module# configure terminal
vmss-module(config)# storages nfs media1
cvmss-module(config-nfs)# target-ip 10.10.10.60 exportname /nfs/export
Connecting 172.107.146.207 export /nfs/export... succeeded.
```

Related Commands

Command	Description
state (storages nfs)	Mounts or unmounts an NFS export.
switch-on-fail (storages nfs)	Configures whether the archives can be switched to the local hard drive when the NFS media device is not available.

video-surveillance

To set video surveillance configurations, logs, reports, and tasks, use the **video-surveillance** command in user EXEC configuration mode.

video-surveillance {**httpd** {**set** *attribute* [*value*] | **unset** *attribute* [*value*]} | **logging** {**set** ***attribute*** [*value*] | **unset** *attribute* [*value*]} | **task** {**archive-restart** *string* | **archive-stop** *string* | **cert-gen** | **cron-restart** | **restart** | **start** | **status** | **stop** | **support-report** | **vsom_db_restore**}}

Syntax Description

httpd	Sets and unsets HTTP-related tasks.
set	Sets the attribute value name of a shell **httpd**-related or **logging**-related variable.
unset	Unsets a shell **httpd**-related or **logging**-related attribute value name, removing it from memory.
attribute	Attribute related to shell **httpd** or **logging** to set or unset.
value	Optional. Value of related to shell **httpd** or **logging** to set or unset.
logging	Sets and unsets shell **log**-related tasks.
task	Starts predefined tasks.
archive-restart	Restarts the NFS archiving process.
string	Configures NFS media tag in the range of *media1* to *media9*.
archive-stop	Stops archive processes running on NFS storage media.
cert-gen	Generates a secure SSL server key and certificate.
cron-restart	Restarts the cron daemon after time changes are made in time zones.
restart	Restarts Cisco Video Surveillance services.
start	Starts Cisco Video Surveillance services.
status	Displays the status of Cisco Video Surveillance services.
stop	Stops Cisco Video Surveillance services.
support-report	Generates the system report for tech support.
vsom_db_restore	Restores the VSOM database from the local disk drive.

Command Modes

User EXEC

Command History

Version	Modification
1.0	This command was introduced.
6.5.1	This command was modified.

Examples

To view predefined tasks, use the **show video surveillance tasks** command. For example:

```
cvmss-module# video-surveillance task status
Report on status of Cisco Video Surveillance services ...
Checking for vsms daemons... running.
Checking for httpd... running.
```

```
snmpd:/usr/BWhttpd/sbin/snmpd:status...Running
snmptrapd:/usr/BWhttpd/sbin/snmptrapd:status...Running
Checking for service MRTG mrtg:/usr/BWhttpd/bin/mrtg:status...Running
```

Related Commands

Command	Description
show video-surveillance	Displays video surveillance configurations, logs, reports, and tasks.

Cisco IOS Commands

This section documents new Cisco IOS commands used for accessing the Cisco Video Management and Storage System module from the host router.

Use the following commands to access and configure the Cisco Video Management and Storage System module from the host router:

- **service-module sm default-boot**
- **service-module sm heartbeat-reset**
- **service-module sm install**
- **service-module sm install abort**
- **service-module sm reload**
- **service-module sm reset**
- **service-module sm session**
- **service-module sm shutdown**
- **service-module sm statistics**
- **service-module sm status**
- **service-module sm uninstall**
- **show controllers sm**
- **show interfaces sm**

service-module sm default-boot

To configure the Cisco SM-SRE service module to use the default BIOS and bootloader, use the **service-module sm default-boot** command in privileged EXEC mode.

service-module sm *slot/port* **default-boot**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/port	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

After a downtime event or failed upgrade, use this command to configure the service module to use the primary BIOS and primary bootloader to perform startup routines.

Examples

The following is sample output for a service module:

```
Router# service-module sm 1/0 default-boot
clear  Clear Default Boot
set    Set Default Boot

Router# service-module sm 1/0 default-boot clear
Router# service-module sm 1/0 default-boot set
```

service-module sm heartbeat-reset

To prevent Cisco IOS software from rebooting the Cisco SM-SRE service module when the heartbeat is lost, use the **service-module sm heartbeat-reset** command in privileged EXEC mode.

service-module sm *slot*/*port* **heartbeat-reset** {**disable** | **enable**}

Syntax Description

slot	Number of the router slot in which the service module is installed. Range: 1 to 4.
/*port*	Port number of the module interface. Always use 0. The slash mark (/) is required.
disable	Disables reset of the service module if the heartbeat is lost.
enable	Enables reset of the service module if the heartbeat is lost.

Command Default

Service module is reset when heartbeat is lost.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

When the service module is booted in fail-safe mode or is undergoing an upgrade, this command prevents a reboot during the process.

When the service module heartbeat is lost, the router applies a fail-open or fail-close configuration option to the module, stops sending traffic to the module, and sets the module to error state. The router performs a hardware reset on the service module and monitors it until the heartbeat is reestablished.

Examples

The following example shows how to disable the service module from being reset if the heartbeat is lost:

```
Router# service-module sm 1/0 heartbeat-reset disable
```

You can display the status of the heartbeat reset feature with the **service-module sm status** command:

```
Router# service-module sm 1/0 status

Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled <=====
```

Related Commands

Command	Description
interface sm	Configures an interface for a service module and enters interface configuration mode.
service-module sm reload	Performs a graceful shutdown and reboot of the service module.
service-module sm reset	Resets the service module hardware.
service-module sm shutdown	Performs a graceful shutdown of the service module.
service-module sm status	Displays configuration information related to the hardware and software on a service module.

service-module sm install

To use Cisco SRE to install an application on a service module (Cisco SM-SRE), use the **service-module sm install** command in privileged EXEC configuration mode.

service-module sm *slot/port* **install url** *url* [**script** *filename*] [**argument "***string***"**] [**force**]

Syntax Description

slot/port	Location of the services engine module in the router. For service modules, the slot number is 1 to 4 and the port number must be 0.
url *url*	Address of FTP or HTTP server, as defined in RFC 2396, on which application packages and Tcl scripts are located.
script	(Optional) Changes name of Tcl script to be run from default value to script specified by *filename* argument.
filename	Name of Tcl script.
argument	(Optional) Installer will not present options for the variable specified in the *string* argument.
string	Alphanumeric characters of variable to be passed directly to the Tcl script via the command line. Variable must be enclosed in quotation marks (" ").
force	(Optional) Tcl script automatically proceeds with install without prompting for user input.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command uses a common module-dependent bootloader on Cisco SRE to install a Linux-based application on a service module (Cisco SM-SRE).

The slash mark (**/**) is required between the *slot* argument and the *port* argument.

You can only issue one instance of this command at a time on a router. You cannot use this command to install an application on two or more services engine modules in the same router at a time.

The Tcl script to be run must reside in the same FTP or HTTP server and directory as the application packages to be installed. If a credential is required, the user name and password must be imbedded in the url as shown in the following example:

```
Router# service-module sm 1/0 install url
ftp://username:passwd@server.com/vmss-k9.sme.version.pkg
```

If two or more of the optional keyword/argument combinations are used with this command, they must be issued in the order presented in the command syntax. For example, you cannot use the **force** keyword before the **script** or **argument** keywords nor the **argument** keyword before the **script** keyword when you issue this command.

Use the **script** *filename* keyword/argument combination with this command to specify that the Cisco IOS software use some Tcl script other than the default installer during the installation.

Use the **argument "***string***"** keyword/argument combination with this command to manually provide variables during installation process and bypass the user interaction feature of the installer. The variable must include the left and right quotation marks (" ").

Use the **force** keyword with this command to install an application without prompting for user input. If you use this keyword and if the application requires you to provide certain variables during the installation, you should also use the **argument "***string***"** keyword/argument combination to manually provide the required variables because the **force** keyword will direct the installer to bypass all user interaction during the installation.

To stop the install while the Tcl script is being downloaded, use the **service-module sm install abort** command. This command cannot be used once the actual installation begins.

Examples

The following example shows how to use the install menu on the Cisco Video Management and Storage System application, choose the first choice, **Install software**:

```
        Welcome to Cisco Systems Service Engine Helper Software
Please select from the following
1       Install software
2       Reload module
3       Disk cleanup
4       Install License(s)
5       Linux shell
(Type '?' at any time for help)
Choice: 1
Package name: vmss-k9.sme.eng_bld.pkg

cvmss-module#$mss-k9.sme.eng_bld.pkg script vmss-k9.sme.eng_bld.pkg.install.s$
Delete the installed Cisco Foundation Software and proceed with new installation? [no]:
yes
Loading pub/VMSS-RAID0/vmss-k9.sme.eng_bld.pkg.install.sre !
[OK - 7918/4096 bytes]
Please select RAID mode for storage partition (1 = RAID-1, 2 = Linear RAID, 3 = RAID-0): 3
If you are installing on a system which already has VMSS installed your media partition
may contain archives.
Would you like for the install to preserve this partition if it exists? Please note that
if you are changing
your RAID option from the previous install, the media partition will not be preserved.
Preserve? [n]:
```

Related Commands

Command	Description
service-module sm install abort	Stops the install and returns to the boot-loader prompt.
service-module sm uninstall	Uses Cisco SRE to uninstall an SRE-supported application on an SRE-enabled services engine module.

service-module sm install abort

To abort the install process on a Cisco SM-SRE, use the **service-module sm install abort** command in privileged EXEC configuration mode.

service-module sm *slot/port* **install abort** [**force**]

Syntax Description

slot/port	Location of the services engine module in the router. For service modules, the slot number is 1 to 4 and the port number must be 0.
force	(Optional) Tcl script automatically stops the installation without prompting for confirmation.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command stops the installation during the downloading portion of the process only and returns the console to the boot-loader prompt.

Note You cannot use this command to stop the process once the actual installation has begun.

Use the **force** keyword with this command to stop the process without first prompting for confirmation.

Examples

The following example shows how to use this command to stop an application installation without first prompting for confirmation:

```
Router# service-module sm 4/0 install abort force
.
.
.
boot-loader>
```

Related Commands

Command	Description
service-module sm install	Uses Cisco SRE to install an SRE-supported application on an SRE-enabled services engine module.

service-module sm reload

To perform a graceful shutdown and reboot of the Cisco SM-SRE service module operating system, use the **service-module sm reload** command in privileged EXEC mode.

service-module sm *slot*/*port* **reload**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/port	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example shows how to gracefully shut down the module and reboot the operating system:

```
Router# service-module sm 1/0 reload

Do you want to proceed with reload?[confirm]
```

Related Commands

Command	Description
interface sm	Configures an interface for a service module and enters interface configuration mode.
service-module sm reset	Resets the service module hardware.
service-module sm shutdown	Gracefully shuts down the service module.
show diag	Displays controller information for service modules.
show interfaces sm	Displays basic interface configuration information for service modules.

service-module sm reset

To reset the Cisco SM-SRE service module hardware, use the **service-module sm reset** command in privileged EXEC mode.

service-module sm *slot*/*port* **reset**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/*port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Caution Because you may lose data, use the **service-module sm reset** command only to recover from a shutdown or failed state.

Examples

The following example shows how to reset the service module hardware:

```
Router# service-module sm 1/0 reset

Use reset only to recover from shutdown or failed state
Warning: May lose data on the NVRAM, nonvolatile file system or unsaved configuration!
Do you want to reset?[confirm]
```

Related Commands

Command	Description
interface sm	Configures an interface for a service module and enters interface configuration mode.
service-module sm reload	Performs a graceful shutdown and reboot of the service module operating system.
service-module sm shutdown	Gracefully shuts down the service module.
show diag	Displays controller information for service modules.
show interfaces sm	Displays basic interface configuration information for service modules.

service-module sm session

To begin a configuration session for an Cisco SM-SRE service module through a console connection, use the **service-module sm session** command in privileged EXEC mode.

service-module sm *slot*/*port* **session** [**clear**]

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/*port*	Port number of the module interface. Always use 0. The slash mark (/) is required.
clear	(Optional) Clears the service module configuration session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Only one session at a time is allowed into the service module from the service module interface.

After starting a session, you can perform any service module configuration task. You first access the service module console in a user-level shell. To access the privileged EXEC command shell, where most commands are available, use the **enable** command.

After you finish configuration tasks and exit the service module console session, use this command with the **clear** keyword to clear the session. At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Examples

The following example shows a session being opened for a Cisco SM-SRE:

```
Router# service-module sm 1/0 session

Trying 10.10.10.1, 2129 ... Open

SE-Module con now available
Press RETURN to get started!

SE-Module> enable
```

The following example clears the session that had been used to configure the Cisco SM-SRE in slot 1:

```
Router# service-module sm 1/0 session clear
[confirm]
 [OK]
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
interface	Configures an interface and enters interface configuration mode.
show diag	Displays controller information for a service module.
show interface sm	Displays basic interface configuration information for service modules.

service-module sm shutdown

To gracefully shut down a Cisco SM-SRE service module, use the **service-module sm shutdown** command in privileged EXEC mode.

service-module sm *slot*/*port* **shutdown**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/port	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

This command brings down the operating system of the specified service module in an orderly fashion to protect the hard drive. When the system is shut down, the module can be removed from the router.

Examples

The following example shows how to gracefully shut down the service module:

```
Router# service-module sm 1/0 shutdown

Do you want to proceed with shutdown?[confirm]
Use service module reset command to recover from shutdown.

WARNING: Confirm that the service-module status shows 'is Shutdown' before removing the
module or powering off the system !
```

Related Commands

Command	Description
interface sm	Configures an interface for a Cisco SM-SRE and enters interface configuration mode.
service-module sm reload	Performs a graceful shut down and reboot of the Cisco SM-SRE operating system.
service-module sm reset	Resets the hardware on the Cisco SM-SRE.
show diag	Displays controller information for service modules.
show interfaces sm	Displays basic interface configuration information for the Cisco SM-SREs.

service-module sm statistics

To display reset and reload information for a Cisco SM-SRE service module and its Cisco IOS software, use the **service-module sm statistics** command in EXEC mode.

service-module sm *slot*/*port* **statistics**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/*port*	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

The following example displays information for a service module in slot 1:

```
Router# service-module sm 1/0 statistics

Module Reset Statistics:
 CLI reset count = 0
 CLI reload count = 0
 Registration request timeout reset count = 1
 Error recovery timeout reset count = 1
 Module registration count = 1
```

Related Commands

Command	Description
interface sm	Configures an interface for a Cisco SM-SRE and enters interface configuration mode.
service-module sm reload	Performs a graceful shutdown and reboot of the Cisco SM-SRE operating system.
service-module sm reset	Resets the Cisco SM-SRE hardware.
service-module sm shutdown	Gracefully shuts down the Cisco SM-SRE.
show interfaces sm	Displays basic interface configuration information for the Cisco SM-SREs.

service-module sm status

To display configuration information related to the hardware and software on a Cisco SM-SRE service module, use the **service-module sm status** command in privileged EXEC mode.

service-module sm *slot*/*port* **status**

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/port	Port number of the module interface. Always use 0. The slash mark (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to:

- Display the Cisco SM-SREs software release version
- Check the Cisco SM-SRE status (steady or down)
- Display hardware information for the Cisco SM-SRE, including CPU, memory, and interface information

Examples

The following example displays information for a Cisco SM-SRE:

```
Router# service-module sm 1/0 status

Service Module is Cisco SM1/0
Service Module supports session via TTY line 67
Service Module is in Steady state
Service Module heartbeat-reset is enabled
Getting status from the Service Module, please wait..
Cisco Foundation Software 1.0
FNDN Running on SM
No install/uninstall in progress
```

Related Commands

Command	Description
interface sm	Configures an interface for a Cisco SM-SRE and enters interface configuration mode.
show diag	Displays controller information for service modules.
show interfaces sm	Displays basic interface configuration information for the Cisco SM-SREs.

service-module sm uninstall

To use Cisco SRE to uninstall an application on a service module (Cisco SM-SRE), use the **service-module sm uninstall** command in privileged EXEC configuration mode.

service-module sm *slot/port* **uninstall** [**force**]

Syntax Description

slot/port	Location of the services engine module in the router. For service modules, the slot number is 1 to 4 and port number must be 0.
force	(Optional) Tcl script automatically proceeds with uninstall without prompting for confirmation.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

This command completely erases the disk or compact flash of the SRE-enabled services engine module and removes the application keys. It does not remove application licenses.

The slash mark (**/**) is required between the *slot* argument and the *port* argument.

You can only issue one instance of this command at a time on a router. You cannot use this command to uninstall an application on two or more services engine modules in a router at a time.

Use the **force** keyword with this command to uninstall an application without first prompting for confirmation.

Examples

The following example shows how to use this command to uninstall an application without first prompting for confirmation:

```
Router# service-module sm uninstall 1/0 force
Router#
```

Related Commands

Command	Description
service-module sm install	Uses Cisco SRE to install an SRE-supported application on an SRE-enabled services engine module.

show controllers sm

To display controller information for the service module interface, use the **show controllers sm** command in user EXEC or privileged EXEC mode.

show controllers sm *slot/unit*

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
unit	Port number of the module interface. Always use 0. The slash mark (/) is required between the slot argument and the unit argument.

Command Default

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Version	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The output from this command is generally useful for diagnostic tasks performed by technical support only. You can, however, use the displayed hardware statistics to obtain the receive and transmit packet statistics that are collected by the hardware controller during packet processing.

Examples

The following example shows how to display information for the Cisco SM-SRE installed in the router:

```
Router# show controllers sm 1/0

Interface SM1/0
Hardware is PSE2
HWIDB: 0x11E3C8C8 INSTANCE: 0x01323100, FASTSEND: 0x040D6C44
Init flags: 0x23

FPGA registers
----------------
  Base address:   0xE4000000    Revision:       0x09030416
  FPGA type:      0x316B6278    FPGA_error_val: 0x00000000
  Cfg MSI mask:   0x00000008    Rx_buffer_size: 0x00000600

Frame statistics: (polling enabled)
-----------------------------------
  tx_frame_cnt: 177                     rx_frame_cnt: 28
  tx_byte_cnt: 45154                    rx_byte_cnt: 2113
  tx_pause_frame_cnt: 0                 rx_pause_frame_cnt: 0
  rx_unicast_filtered_cnt: 0            rx_multicast_filtered_cnt: 8
  rx_undersize_pkts: 0                  rx_oversize_pkts: 0
  tx_64_byte_pkts: 38                   rx_64_byte_pkts: 17
  tx_65_to_127_byte_pkts: 17            rx_65_to_127_byte_pkts: 8
```

```
  tx_128_to_255_byte_pkts: 6            rx_128_to_255_byte_pkts: 3
  tx_256_to_511_byte_pkts: 116          rx_256_to_511_byte_pkts: 0
  tx_512_to_1023_byte_pkts: 0           rx_512_to_1023_byte_pkts: 0
  tx_1024_to_1518_byte_pkts: 0          rx_1024_to_1518_byte_pkts: 0
  rx_congestion_drop_cnt: 0             rx_mtusize_drop_cnt: 0
  rx_bad_cnt: 0

Interrupt statistics
--------------------
  ge_tx_interrupt: 171                  ge_rx_interrupt: 20
  txbd_seq_err: 0                       txbd_done_err: 0
  rxbd_done_err: 0                      isl_inner_crc_err: 0
  pcie_busmstr_dsbld_err: 0             pcie_tgt_abort_err: 0
  pcie_mst_abort_err: 0                 spi_done_event: 0
  rx_empty_pak: 0                       rx_sw_usage_err: 0
  ing_buf_adrs_err: 0                   pcie_null_ptr_err: 0
  uart_tx_intr: 13                      uart_rx_intr: 27169
  uart_break_detected: 1                uart_framing_err: 0
  uart_bad_egr_adrs: 0                  uart_egr_overflow: 0
  i2c_errs: misc/nack/tmo: 0/0/0

TX ring
-------
  Tx Ring txr_head/txr_tail:  178/178
  Tx Shadow txs_head/txs_tail/txs_free: 178/178/256
  Tx Ring(txr): 0x3C631800 Tx Shadow (malloc): 0x01323380
  Tx Limited: 0 Tx Count: 0 hold_pak 0x00000000

RX rings
--------
  size: 256      max_spin_size 32       head: 20
  Rx Ring(rxr):   0x3C631000  rxr_malloc: 0x3C631000
  Rx Shadow(rxs): 0x11E3D6CC   rxs_malloc: 0x11E3D6CC

Software MAC Address Filter (hash:length/addr/mask/hits)
--------------------------------------------------------
   000:  0  ffff.ffff.ffff  0000.0000.0000         3
   007:  0  001e.4a97.644d  0000.0000.0000         0
   192:  0  0180.c200.0002  0000.0000.0000         0
   192:  1  0100.0ccc.cccc  0000.0000.0000         0
   197:  0  0180.c200.0007  0000.0000.0000         0

   Software filtered frames: 0
   Unicast overflow mode:   0
   Multicast overflow mode: 1
   Promiscuous mode:        0

  HW MAC Address Filter
  ---------------------
   Unicast Addr0: 001E.4A97.644D
   Unicast Addr1: 0000.0000.0100
   Unicast Addr2: 0000.0000.0100
   Unicast Addr3: 0000.0000.0100
   Unicast Addr4: 0000.0000.0100
   Unicast HW Filter Count   : 1

   Multicast Hash b63_32: 0x2000001
   Multicast Hash b32_00: 0x00
   HW unicast filter enabled: Yes
   HW multicast filter enabled: Yes

FPGA upgrade info
-----------------
  Golden area fpga version:  00000000
```

```
Upgrade area fpga version: 09030416
IOS bundled fpga version:  09030416
```

Table 11 describes the significant fields shown in the display.

Table 11 show controllers analysis-module Field Descriptions

Field	Description
Hardware	Description of the chip being used.
IDB, FASTSEND	Address in router memory of the IDB[1] and the fastsend routine.
INSTANCE	Device-specific data stored in router memory that lists the memory locations and current indexes of receive (Rx) and transmit (Tx) rings in router I/O memory.
CONTROL AND STATUS REGISTERS (CSR)	Control and status registers that are physically located on the chip itself and that are accessed by the CPU over the Peripheral Component Interconnect (PCI) bus.
PHY REGISTERS	Contents of the PHY registers. PHY is a device that interfaces the physical Ethernet line and that is located between the chip and the physical line.
HARDWARE STATISTICS	Receive (Rx) and transmit (Tx) traffic statistics collected by the chip.
INTERRUPT STATISTICS	Transmit (Tx), Receive (Rx), control, software, and flow control interrupt statistics collected by the chip.

1. IBD = Interface Descriptor Block

Related Commands

Command	Description
service-module sm status	Displays hardware and software status information about the Cisco SM-SRE.
show interfaces sm	Displays status, traffic data, and configuration information about the Cisco SM-SRE interface.

show interfaces sm

To display status, traffic data, and configuration information about the Cisco SM-SRE service module interface, use the **show interfaces sm** command in user EXEC or privileged EXEC mode.

show interfaces sm *slot/port*

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
port	Port number of the module interface. The slash mark (/) is required.

Defaults

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Version	Modification
115.0(1)M	This command was introduced.

Usage Guidelines

The service module interface is the Gigabit Ethernet interface on the router that connects to the Cisco SM-SRE.

Examples

The following example shows output from the **show interfaces sm 1/0** command:

```
Router# show interfaces sm 1/0
SM1/0 is up, line protocol is up
  Hardware is PSE2, address is 001e.4a97.644d (bia 001e.4a97.644d)
  Internet address is 30.0.0.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is internal
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:13, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/60 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     22 packets input, 1398 bytes, 0 no buffer
     Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     134 packets output, 42720 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
```

Table 12 describes the significant fields shown in the display.

Table 12 show interfaces sm Field Descriptions

Field	Description
Hardware, address	Hardware type and address.
MTU	MTU[1] of the service module interface.
BW	Bandwidth of the interface, in kbps.
DLY	Delay of the interface, in microseconds.
reliability	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
txload	Transmit load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
rxload	Receive load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to the interface.
loopback	Indicates whether or not loopback is set.
Keepalive	Indicates whether or not keepalives are set and the interval between keepalives if they have been set.
ARP type...ARP Timeout	Type of ARP[2] assigned and length of timeout.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by the interface and processed locally on the router. This field is useful for detecting when a dead interface failed. **Note** This field is not updated by fast-switched traffic.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. This field is useful for detecting when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because a transmission took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Table 12 show interfaces sm Field Descriptions (continued)

Field	Description
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Asterisks (***) indicate that the elapsed time is too large to be displayed.
Input queue	Number of packets in the input queue. Each number is followed by a slash, the maximum size of the queue, the number of packets dropped because of a full queue, and the number of times that queued packets have been discarded.
Total output drops	Number of packets in the output queue that have been dropped because of a full queue.
Queueing strategy	Queueing strategy applied to the interface, which is configurable under the interface. The default is FIFO[3].
Output queue	Number of packets in the output queue, and the maximum size of the queue. Each number is followed by a slash.
5 minute input rate, 5 minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (rather than all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period. **Note** The 5-minute period referenced in this output is a load interval that is configurable under the interface. The default value is 5 minutes.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC[4] encapsulation, in the error-free packets received by the system.

Table 12 show interfaces sm Field Descriptions (continued)

Field	Description
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
Received...broadcasts	Number of broadcasts received.
runts	Number of packets that are discarded because they are smaller than the minimum packet size of the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
throttles	Number of times that the interface requested another interface within the router to slow down.
input errors	Errors that include runts, giants, no buffer, CRC[5], frame, overrun, and ignored counts. Other input-related errors can also cause the input errors count to be increased, and some datagrams may have more than one error; therefore, this sum may not balance with the sum of enumerated input error counts.
CRC	Errors created when the CRC generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station that is transmitting bad data.
frame	Number of packets received incorrectly that have a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times that the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets that were ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from system buffer space described. Broadcast storms and bursts of noise can cause the ignored count to increase.

Table 12 show interfaces sm Field Descriptions (continued)

Field	Description
input packets with dribble condition detected	Number of packets with dribble condition. Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages that have been transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted by the system.
underruns	Number of times that the transmitter has run faster than the router could handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages that have been retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets that were queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
babbles	Count of frames greater than 1518 bytes that have been transmitted, indicating that the transmitter has been on the interface longer than the time necessary to transmit the largest frame.
late collision	Number of late collisions. A collision becomes a late collision when it occurs after the preamble has been transmitted.

Table 12 show interfaces sm Field Descriptions (continued)

Field	Description
deferred	Deferred indicates that the chip, while ready to transmit a frame, had to defer because the carrier was asserted.
lost carrier	Number of times that the carrier was lost during transmission.
no carrier	Number of times that the carrier was not present during the transmission.
output buffer failures, output buffers swapped out	Number of failed buffers and number of buffers swapped out.

1. MTU = Maximum transmission unit
2. ARP = Address Resolution Protocol
3. FIFO = first-in, first-out
4. MAC = Media Access Control
5. CRC = cyclic redundancy checksum

Related Commands

Command	Description
show controllers sm	Displays controller information for the service module interface.

INDEX