



APPENDIX **B**

Supervisor Console Commands



Note

Additional Cisco IOS commands used with this product (those that already exist and have not been modified) are documented in the Cisco IOS Release 12.2 command reference publications.

The following commands, listed in alphabetical order, are introduced or modified in Cisco IOS Release 12.2(33)SRC and later to support the SAMI platform, and are supported at the supervisor engine console:

- [boot device module, page B-3](#)
- [bouncer-program-summit, page B-4](#)
- [clear logging slot, page B-6](#)
- [clear sami module, page B-8](#)
- [copy sami#, page B-10](#)
- [delete sami#, page B-11](#)
- [dir sami#, page B-12](#)
- [encapsulation dot1q, page B-14](#)
- [execute-on, page B-16](#)
- [hw-module boot, page B-19](#)
- [hw-module reset, page B-21](#)
- [hw-module shutdown, page B-22](#)
- [logging listen, page B-26](#)
- [power enable, page B-27](#)
- [sami module, page B-28](#)
- [session slot, page B-30](#)
- [show logging slot, page B-34](#)
- [show logging summary, page B-37](#)
- [show sami module, page B-44](#)
- [show svc module, page B-45](#)
- [show upgrade software progress, page B-47](#)
- [show vlans dot1q, page B-48](#)

- [svclc console](#), page B-52
- [svclc module](#), page B-53
- [svclc multiple-vlan-interfaces](#), page B-54
- [svclc vlan-group](#), page B-56
- [upgrade hw-module](#), page B-57

The following Cisco IOS software commands, listed in alphabetical order, are not new or modified. They are included in this reference section because they are useful for configuring and managing the SAMI.

- [hw-module reset](#), page B-21
- [ip rcmd rcp-enable](#), page B-23
- [ip rcmd remote-host](#), page B-24
- [show inventory](#), page B-31
- [show module](#), page B-41

boot device module

To set the boot variable for the SAMI LCP, use the **boot device module** command in global configuration mode:

```
boot device module slot_num { disk0: | disk1: | sup-: } image_name
```

Syntax Description	
<i>slot_num</i>	Number of the slot in which the module resides.
disk0:	Sets the boot variable to disk0:.
disk1:	Sets the boot variable to disk1:.
sup-bootflash:	Sets the boot variable to sup-bootflash:.
<i>image_name</i>	Name of the SAMI image bundle.

Defaults This command has no default setting.

Command Modes Global configuration

Command History	Release	Modification
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines To set the boot variable for the LCP and the image using the **boot device module** command, the SAMI LCP must be at the ROM-monitor prompt. This command does not work with the supervisor bootflash: file system.

Examples The following example shows how to set the boot variable if the LCP is in slot 3:

```
Router(config)#boot device module 3 disk0:c6ace-t1k9-mz.3.0.0_A1_4.bin
Device BOOT variable = disk0:c6ace-t1k9-mz.3.0.0_A1_4.bin
Warning: Device list is not verified
Router#
```

Related Commands	Command	Description
	boot eobc:	Boots the SAMI from the image on the supervisor engine. (This is a SAMI LCP ROM monitor command.)
	hw-module boot eobc	Boots using an image downloaded through EOBC.

bouncer-program-summit

To program all registers to increase the tolerance band for voltage fluctuations, use the **bouncer-program-summit** privileged EXEC command.

bouncer-program-summit

Syntax Description There are no keywords or arguments for this command.

Defaults There are no default values.

Command Modes Privileged EXEC.

Command History	Release	Modification
	12.4(24)MD, 12.4(24)MDA, 12.4(24)MDB, 12.4(24)YE, 12.4(24)T4A	This command was introduced as a workaround in the listed releases.

Usage Guidelines Use this command only if the SAMI reloads or fails to bootup citing FRU power failure errors.



Caution

You should only execute this command under the supervision of TAC during a maintenance window. Execute the command on processor 0 of the affected SAMI cards .

Examples Here is an example configuration.

Load the image with the fix:

```
ABHV-SUP# upgrade hw-module slot 2 software
tftp://202.153.144.25/abhv/c7svcsami-noapp-mz-3_2
Loading abhv/c7svcsami-csg-mz from 202.153.144.25 (via Vlan75):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 28823127 bytes]
```

```
% Waiting for upgrade to be committed..
% Software upgrade completed.
% Please reset hw-module to load the upgraded software.
```

```
ABHV-SUP#hw-module module 2 reset
```

```
Proceed with reload of module?[confirm]
ABHV-SUP#
```

Session to processor 0 of SAMI (username: admin password: admin):

```
ABHV-SUP#session slot 2 processor 0
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.20 ... Open
```

```
ABHV-LCP-2 login: admin
Password:admin
Bad terminal type: "network". Will assume vt100.
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, by Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available athttp://www.gnu.org/licenses/gpl.html.
```

```
Service and Application Module for IP (SAMI)
Utility Console
```

```
ABHV-LCP-2#
```

Execute the **bouncer-program-summit** command:

```
ABHV-LCP-2# bouncer-program-summit
This must be performed only in a maintenance window with assistance from TAC. Are you sure
you want to continue? [no] yes
ABHV-LCP-2#
```



Note

In rare cases, if the programming or verification of summit registers fails for some reason, a message will be printed asking you to execute the command again. Please retry the same command.

Exit and reload the card:

```
ABHV-LCP-2# exit

Connection to 127.0.0.20 closed by foreign host
ABHV-SUP#hw-module module 2 reset
Proceed with reload of module?[confirm]
ABHV-SUP#
```

clear logging slot

To clear logging status counters from the logging buffer, use the **clear logging slot** command in privileged EXEC mode.

clear logging slot *slot_number* **counts**

Syntax Description

<i>slot_number</i>	Number of the slot in which the SAMI is installed.
counts	Clears the logging status counters.

Defaults

No default behaviors or values exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

Use this command to clear the logging status counters that display when you use the **show logging** command.

Note that the **clear logging slot** command only clears the counters displayed by the **show logging** command. The **clear logging slot** command does not clear the control information displayed in the **show logging** command output, such as send and receive sequence numbers.

Specifically, the **clear logging slot** command clears the following counters displayed by the **show logging** command:

- kpa_missed
- cmd_timeouts
- logger_events
- bad_info
- seq_errors
- reset_count

Examples

The following example illustrates the results of issuing the `clear logging slot counts` command to clear the counters for a module in slot 5:

```
Sup# clear logging slot 5 counts
```

```
Clear logging buffer [confirm]
```

```
Sup#
```

Related Commands

Command	Description
<code>logging buffered</code>	Logs messages to an internal buffer.
<code>show logging</code>	Displays the state of logging (syslog).

clear sami module

To clear the counters displayed by the show interface privileged EXEC command, use the **clear sami module** in privileged EXEC mode.

clear sami module *slot_number* [**port** *port_number*] **traffic**

Syntax Description		
	<i>slot_number</i>	Number of the slot in which the SAMI is installed.
	port <i>port_number</i>	(Optional) Number of the data port on the SAMI.
	traffic	Clears traffic counters.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRC	This command was introduced.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use this command to clear the traffic counters displayed by the **show sami module** privileged EXEC command.

Examples The following example illustrates how to use the **clear sami module** command:

```
Sup#show sami module 2 port 1 traffic
Specified interface is up line protocol is up (connected)
Hardware is c7600 10Gb 802.3, address is 0030.f276.41e4 (bia 0030.f276.41e4)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 10Gb/s
input flow-control is on, output flow-control is unsupported
    202 packets input
    0 input errors,
    0 CRC
    6 packets output
```

```
Sup#clear sami module 2 port 1 traffic
Clear "show interface" counters on this interface [confirm]
Sup#
Sup#show sami module 2 port 1 traffic
Specified interface is up line protocol is up (connected)
Hardware is c7600 10Gb 802.3, address is 0030.f276.41e4 (bia 0030.f276.41e4)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
```

```
Full-duplex, 10Gb/s
input flow-control is on, output flow-control is unsupported
  0 packets input
  0 input errors,
  0 CRC
  0 packets output
```

Related Commands

Command	Description
<code>show sami module</code>	Displays traffic counters on the SAMI.

copy sami#

To copy a SAMI coredump file from the core directory on a SAMI, use the **copy sami#** command in privileged EXEC mode.

```
copy sami#slot_number{-fs:core/file-name dest-file}
```

Syntax Description

<i>slot_number</i>	Number of the slot in which the SAMI is installed.
core / <i>file-name</i>	Name of the file containing crash information in the core directory on the SAMI.
<i>dest-file</i>	Name of the destination file.

Defaults

No default behavior or values exist.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

Use this command to copy the coredump file from the core directory to a destination file.

Examples

The following example illustrates how to use the **copy sami#** command:

```
Sup# copy sami#7-fs:core/crashinfo tftp://64.102.16.25/operatorA/
Address or name of remote host [64.102.16.25]?
Destination filename [operatorA/crashinfo]?
!!!!!!
1048576 bytes copied in 2.568 secs (408324 bytes/sec)
```

Related Commands

Command	Description
delete sami#	Deletes files in the SAMI image: or core directory.
dir sami#	Lists the files in the image: or core: directories on a SAMI.

delete sami#

To delete the files the image: or core: directories on a SAMI, use the **dir sami#** command in privileged EXEC mode.

```
delete sami#slot_number{-fs:image/ | -fs:core/}file-name
```

Syntax Description		
	<i>slot_number</i>	Number of the slot in which the SAMI is installed.
	image/	Specifies the file is located in the image directory.
	core/	Specifies the file is located in the core directory.
	<i>file_name</i>	Name of the file to delete.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB1	This command was introduced.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use this command to delete a file in the image: or core directory of a SAMI.

Examples The following example illustrates how to use the **delete sami#** command:

```
Sup# delete sami#7-fs:image/sb-csg2-mzg.bin
Delete filename [image/sb-csg2-mzg.bin]?
Delete sami#7-fs:image/sb-csg2-mzg.bin? [confirm]
```

```
Sup# delete sami#7-fs:core/crashinfo
Delete filename [core/crashinfo]?
Delete sami#7-fs:core/crashinfo? [confirm]
```

Related Commands	Command	Description
	copy sami#	Copies a SAMI core dump file from the core directory.
	dir sami#	Lists the files in the image: or core: directories on a SAMI.

dir sami#

To list the files in the image: or core: directories on a SAMI, use the **dir sami#** command in privileged EXEC mode.

```
dir sami#slot_number{-fs:image/ | -fs:core/}
```

Syntax Description		
	<i>slot_number</i>	Number of the slot in which the SAMI is installed.
	image/	Lists the SAMI image directory.
	core/	Lists the SAMI core directory.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB1	This command was introduced.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use this command to list the image: or core directory files of a SAMI.

Examples The following example illustrates how to use the **dir sami#-fs:image** command:

```
Sup# dir sami#7-fs:image/
Directory of sami#7-fs:image/
16 ---- 36514563 Jan 1 2000 00:23:56 +00:00 itasca_diag33.mz
17 ---- 27281352 Jan 1 2000 00:25:12 +00:00 c6ace-tlk9-mz.3.0.0_A1_1a.bin
18 ---- 35067659 Nov 10 2006 16:26:52 +00:00 sb-csg2-mzg.shyeh.bin
19 ---- 34592592 Nov 9 2006 21:21:52 +00:00 sb-csg2-mzg.csg2-bundle.061108.nvfix
20 ---- 8230260 Nov 8 2006 17:31:26 +00:00 svcsami-csg-mz.unit_test
21 ---- 393216 Nov 8 2006 18:32:08 +00:00 BOUNCER_RM.bin_061108
22 ---- 1654432 Oct 25 2006 18:11:46 +00:00 sb-csg2_dplug-mzg.bin.061025
102400000 bytes total (496435200 bytes free)
```

```
Sup# dir sami#7-fs:core/
Directory of sami#7-fs:core/
13 ---- 1048576 Nov 4 2006 04:51:25 +00:00 crashinfo
12 ---- 1048576 Nov 4 2006 04:45:33 +00:00 crashinfo.old
14 ---- 27691 Nov 10 2006 16:44:55 +00:00 0x701_ppc_dnld_daemon_log.995.tar.gz
15 ---- 27725 Nov 10 2006 17:54:01 +00:00 0x801_ppc_dnld_daemon_log.995.tar.gz
19 ---- 70793 Oct 25 2006 01:15:37 +00:00 0x901_ppc_dnld_daemon_log.995.tar.gz
21 ---- 71707 Oct 25 2006 16:12:30 +00:00 0x901_ppc_dnld_daemon_log.997.tar.gz
203097088 bytes total (199715840 bytes free)
```

Related Commands	Command	Description
	copy sami#	Copies a SAMI coredump file from the core directory.
	delete sami#	Deletes files in the SAMI image: or core directory.

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN), use the **encapsulation dot1q** command in subinterface configuration modes. To disable IEEE 802.1Q encapsulation, use the **no** form of this command.

```
encapsulation dot1q vlan-id second-dot1q {any | vlan-id | vlan-id |
vlan-id-vlan-id [,vlan-id-vlan-id] }
```

```
no encapsulation dot1q vlan-id second-dot1q {any | vlan-id | vlan-id |
vlan-id-vlan-id [,vlan-id-vlan-id] }
```

Syntax Description

any	Sets the inner VLAN ID value to a number that is not configured on any other subinterface.
<i>vlan-id</i>	Virtual LAN identifier. The allowed range is from 1 to 4094. For the IEEE 802.1Q-in-Q VLAN Tag Termination feature, the first instance of this argument defines the outer VLAN ID, and the second and subsequent instances define the inner VLAN ID.
second-dot1q	Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature by allowing an inner VLAN ID to be configured.
-	Hyphen must be entered to separate inner and outer VLAN ID values that are used to define a range of VLAN IDs.
,	(Optional) Comma must be entered to separate each VLAN ID range from the next range.

Defaults

IEEE 802.1Q encapsulation is disabled.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The native keyword was added.
12.2(2)DD	Support was added for this command in interface range configuration mode.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(7)T	The second-dot1q keyword was added to support the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

Subinterface Configuration Mode

After a subinterface is defined, use the **encapsulation dot1q** command to add outer and inner VLAN ID tags to allow one VLAN to support multiple VLANs. You can assign a specific inner VLAN ID to the subinterface; that subinterface is unambiguous. Or you can assign a range or ranges of inner VLAN IDs to the subinterface; that subinterface is ambiguous.

Use the **second-dot1q** keyword to configure the IEEE 802.1Q-in-Q VLAN Tag Termination feature. 802.1Q in 802.1Q (Q-in-Q) VLAN tag termination adds another layer of 802.1Q tag (called “metro tag” or “PE-VLAN”) to the 802.1Q tagged packets that enter the network. Double tagging expands the VLAN space, allowing service providers to offer certain services such as Internet access on specific VLANs for some customers and other types of services on other VLANs for other customers.

Examples

The following example shows how to terminate a Q-in-Q frame on an unambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID of 200:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)# encapsulation dot1q 100 second-dot1q 200
```

The following example shows how to terminate a Q-in-Q frame on an ambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID in the range from 100 to 199 or from 201 to 600:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600
```

execute-on

To execute a command on a processor remotely when the remote console and logging (RCAL) feature is enabled, use the **execute-on** command in privileged EXEC mode.

```
execute-on { {slot_number [, slot_number] | all-mwams | all-samis } {cpu_number [, cpu_num] | all | all-ppc } remote-command }
```

Syntax Description	
<i>slot_number</i>	Number of the slot in which the module is installed. Optionally, you can specify additional slot numbers, separated by a comma (.).
all-mwams	Specifies all Cisco Multiprocessor WAN Application Modules (MWAMs) in the chassis. ¹
all-samis	Specifies all SAMIs in the chassis.
<i>cpu_number</i>	Number of the processor. Valid values for a SAMI are 0 for the LCP and 3 through 8 for the PPCs. Valid values for an MWAM are 1 for the control CPU and 2 through 7 for the processors.
all	Specifies all processors.
all-ppc	Specifies all PPC processors 3 through 8.
<i>remote-command</i>	The remote command to execute on the processor. The following commands are supported: <ul style="list-style-type: none"> • debug • dir • sami (SAMI only) • show • systat • undebug • ping • log {show systat dir}

1. When using the **all** option, the command is executed on all active processors but is not executed on processors that are inactive. To show the processor state, use the [show logging slot](#) command.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2(14)ZA4	This command was introduced.
	12.3(5a)B	This command was integrated into Cisco IOS Release 12.3(5a)B and RCAL support for processor control commands was added.
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

Use this command to execute a command on one or all processors of one or all SAMIs or MWAMs in a chassis, and to monitor and maintain information. The RCAL feature allows you to issue commands remotely without having to log in to a processor directly.

Table B-1 lists the command sets that you can execute remotely from the supervisor to a SAMI PPC (processor number 3 through 8).

Table B-1 PPC RCAL Command Set

Command	Description
<code>debug</code>	Enables debugging functions
<code>dir</code>	Lists files in a file system
<code>log dir</code>	Logs the <code>dir</code> command to syslog
<code>log show</code>	Logs the <code>show</code> command to syslog
<code>log systat</code>	Logs the <code>systat</code> command to syslog
<code>ping ip_address</code>	Executes a ping on a remote processor
<code>show</code>	Displays running system information
<code>systat</code>	Displays information about terminal lines
<code>undebug</code>	Disables debugging functions

Table B-2 lists the command sets that you can execute remotely from the supervisor to a SAMI LCP (processor number 0).

Table B-2 LCP RCAL Command Set

Command	Description
<code>clear</code>	Clears counters and statistics
<code>console-select</code>	Specifies console selection for front panel consoles DB1 and DB2
<code>reload</code>	Reloads the entire SAMI or SAMIs
<code>command show</code>	Displays SAMI remote commands

When the **execute-on** command is issued with an **all** keyword option specified, the specified command is executed on active processors. Inactive processors are ignored.

To determine if the processor is active, use the **show logging** command.

To determine the escape sequence for your console/vty connection, use the **show line line_number** command.

This command requires that the RCAL feature be enabled.

Examples

The following example illustrates how to use the **execute-on** command:

```
Sup# execute-on all-samis all-ppc show proc cpu | inc CPU
----- Slot 2/CPU 3, show proc cpu | inc CPU-----
----- Slot 2/CPU 3, show processes cpu -----
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
----- Slot 2/CPU 4, show processes cpu -----
CPU utilization for five seconds: 16%/15%; one minute: 15%; five minutes: 15%
----- Slot 2/CPU 5, show processes cpu -----
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
----- Slot 2/CPU 6, show processes cpu -----
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
----- Slot 2/CPU 7, show processes cpu -----
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
----- Slot 2/CPU 8, show processes cpu -----
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

Sup# execute-on 2 3 show version
----- Slot 2/CPU 3, show version-----
Cisco IOS Software, SAMI Software (SAMI-CSG-M), Version 12.4(nightly.CSG2070509) NIGHTLY
BUILD, synced to bouncer BOUNCER_NIGHTLY_061020
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 09-May-07 03:11 by user

ROM: System Bootstrap, Version 12.3(20070509:064827) [BLD-bouncer_csg.nightly 101],
DEVELOPMENT SOFTWARE

SAMI2 uptime is 5 hours, 22 minutes
System returned to ROM by reload at 08:21:10 EDT Wed May 9 2007
System restarted at 08:26:03 EDT Wed May 9 2007
System image file is "c7svcsami-csg-mz.bouncer_csg.070509.plp3"

Cisco Systems SAMI (MPC8500) processor (revision 0.702) with 983040K/65536K bytes of
memory.
Processor board ID SAD1042040X
FS8548H CPU at 1250MHz, Rev 2.0, 512KB L2 Cache
1 Gigabit Ethernet interface
65536K bytes of processor board system flash (AMD S29GL256N)

Configuration register is 0x1

Sup#
```

hw-module boot

To specify the boot options for the module through the power management bus control register, use the **hw-module boot** command in privileged EXEC mode.

```
hw-module module num boot [value] { config-register | eobc | flash image | rom-monitor }
```

Syntax Description	Parameter	Description
	module <i>num</i>	Specifies the number of the module to apply the command.
	boot <i>value</i>	(Optional) Literal value for the module's boot option; valid values are from 0 to 15. See the "Usage Guidelines" section for additional information.
	config-register	Boots using the module's config-register value.
	eobc	Boots using an image downloaded through EOBC.
	flash <i>image</i>	Specifies the image number in the module's internal flash memory for the module's boot option; valid values are 1 and 2.
	rom-monitor	Stays in ROM-monitor mode after the module resets.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.3(22)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

The valid values for the **boot** *value* argument are as follows:

- 0—Specifies the module's config-register value.
- 1—Specifies the first image in the flash memory.
- 2—Specifies the second image in the flash memory.
- 3—Stays in ROM-monitor mode after the module reset.
- 4—Specifies the download image through EOBC.

Examples

This example shows how to reload the module in slot 6 using the module's config-register value:

```
Sup# hw-module module 1 boot config-register
Sup#
```

This example shows how to reload the module in slot 3 using an image downloaded through EOBC:

```
Sup# hw-module module 1 boot eobc
Sup#
```

Related Commands

Command	Description
show module	Displays the module status and information for all modules in the chassis.

hw-module reset

To reset the entire module by turning the power off and then on, use the **hw-module reset** command in privileged EXEC mode.

hw-module module *slot_number* reset

Syntax Description	module <i>num</i>	Number of the slot in which the module that you want to reset is installed. Valid values depend on the chassis that is used. For example, in a 13-slot chassis, valid values for the module number are from 1 to 13.
---------------------------	--------------------------	--

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.3(22)SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines The **hw-module reset** command resets the module by turning the power off and then on. The reset process requires several minutes.

This command is typically used in the upgrade process to switch between Application Partition (AP) and Maintenance Partition (MP) images or to recover from a shutdown.

Examples The following example illustrates how to reset a module in slot 3:

```
Sup# hw-module rmodule 3 reset
```

hw-module shutdown

To shut down the module, use the **hw-module shutdown** command in privileged EXEC mode.

hw-module module slot_number shutdown

Syntax Description	module slot_number	Description
		Number of the slot in which the module that you want to shut down is installed. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.3(22)SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines If you enter the **hw-module shutdown** command to shut down the module, you will have to enter the **no power enable module** command and the **power enable module** command to restart (power off and then power on) the module.

Examples This example shows how to shut down and restart a module in slot 3:

```
Sup# hw-module module 3 shutdown

Sup# no power enable module 3

Sup# power enable module 3
```

ip rcmd rcp-enable

To configure the Cisco IOS software to allow remote users to copy files to and from the router using remote copy protocol (RCP), use the **ip rcmd rcp-enable** command in global configuration mode. To disable RCP on the device, use the **no** form of this command.

ip rcmd rcp-enable

no ip rcmd rcp-enable

Syntax Description This command has no arguments or keywords.

Defaults To ensure security, RCP is not enabled by default.

Command Modes Global configuration

Command History	Release	Modification
	10.1	This command was introduced.

Usage Guidelines

To allow a remote user to execute RCP commands on the router, you must also create an entry for the remote user in the local authentication database using the **ip rcmd remote-host** command.

The **no ip rcmd rcp-enable** command does not prohibit a local user from using RCP to copy system images and configuration files to and from the router.

To protect against unauthorized users copying the system image or configuration files, the router is not enabled for RCP by default.

Examples The following example illustrates how to use the **ip rcmd rcp-enable** command:

```
Sup# ip rcmd rcp-enable
```

Related Commands	Command	Description
	ip rcmd remote-host	Creates an entry for the remote user in a local authentication database so that remote users can execute commands on the router using remote shell protocol (RSH) or remote shell protocol (RCP).

ip rcmd remote-host

To create an entry for the remote user in a local authentication database so that remote users can execute commands on the router using remote shell protocol (rsh) or remote copy protocol (rcp), use the **ip rcmd remote-host** command in global configuration mode. To remove an entry for a remote user from the local authentication database, use the **no** form of this command.

ip rcmd remote-host *local-username* {*ip-address* | *host-name*} *remote-username* [**enable** [*level*]]

no ip rcmd remote-host *local-username* {*ip-address* | *host-name*} *remote-username* [**enable** [*level*]]

Syntax Description

<i>local-user-name</i>	Name of the user on the local router. You can specify the router name as the username. This name must be communicated to the network administrator or to the user on the remote system. To be allowed to remotely execute commands on the router, the remote user must specify this value correctly.
<i>ip-address</i>	IP address of the remote host from which the local router accepts remotely executed commands. Either the IP address or the hostname is required.
<i>host-name</i>	Name of the remote host from which the local router accepts remotely executed commands. Either the hostname or the IP address is required.
<i>remote-username</i>	Name of the user on the remote host from which the router accepts remotely executed commands.
enable [<i>level</i>]	(Optional) Specifies to enable the remote user to execute privileged EXEC commands using rsh or to copy files to the router using rcp. The range is from 1 to 15. The default is 15. For information on the enable level, refer to the privilege level global configuration command in the Release 12.2 Cisco IOS Security Command Reference.

Defaults

No entries are in the local authentication database.

Command Modes

Global configuration

Command History

Release	Modification
10.1	This command was introduced.

Usage Guidelines

A TCP connection to a router is established using an IP address. Using the hostname is valid only when you are initiating an rcp or rsh command from a local router. The hostname is converted to an IP address using DNS or host-name aliasing.

To allow a remote user to execute rcp or rsh commands on a local router, you must create an entry for the remote user in the local authentication database. You must also enable the router to act as an rsh or rcp server.

To enable the router to act as an:

- RSH server—Issue the **ip rcmd rsh-enable** command.
- RCP server—Issue the **ip rcmd rcp-enable** command.

The router cannot act as a server for either of these protocols unless you explicitly enable the capacity.

A local authentication database, which is similar to a UNIX .rhosts file, is used to enforce security on the router through access control. Each entry that you configure in the authentication database identifies the local user, the remote host, and the remote user. To permit a remote user of rsh to execute commands in privileged EXEC mode or to permit a remote user of rcp to copy files to the router, specify the **enable** keyword and level. For information on the enable level, refer to the privilege level global configuration command in the Release 12.2 Cisco IOS Security Command Reference.

An entry that you configure in the authentication database differs from an entry in a UNIX .rhosts file. Because the .rhosts file on a UNIX system resides in the home directory of a local user account, an entry in a UNIX .rhosts file need not include the local username; the local username is determined from the user account. To provide equivalent support on a router, specify the local username along with the remote host and remote username in each authentication database entry that you configure.

For a remote user to be able to execute commands on the router in its capacity as a server, the local username, host address or name, and remote username sent using the remote client request must match values configured in an entry in the local authentication file.

A remote client host should register with DNS. The Cisco IOS software uses DNS to authenticate the remote hostname and address. Because DNS can return several valid IP addresses for a hostname, the Cisco IOS software checks the address of the requesting client against all of the IP addresses for the named host returned by DNS. If the address sent by the requester is considered invalid, that is, it does not match any address listed with DNS for the hostname, the software rejects the remote-command execution request.

If no DNS servers are configured for the router, then that device cannot authenticate the host. In this case, the Cisco IOS software sends a broadcast request to attempt to gain access to DNS services on another server. If DNS services are not available, you must use the **no ip domain-lookup** command to disable the attempt to gain access to a DNS server by sending a broadcast request.

If DNS services are not available and, therefore, you bypass the DNS security check, the software accepts the request to remotely execute a command only if all three values sent with the request match exactly the values configured for an entry in the local authentication file.

Examples

The following example illustrates how to use the **ip rcmd remote-host enable** command:

```
Sup# ip rcmd remote-host * 24 * enable
```

Related Commands

Command	Description
ip rcmd rcp-enable	Configures the Cisco IOS software to allow remote users to copy files to and from the router.

logging listen

To configure the port on which the supervisor receives system messages from SAMI processors when using the remote console and logging (RCAL) feature, use the **logging listen** command in global configuration mode. To remove this configuration, use the **no** form of the command.

logging listen *udp_port*

no logging listen *udp_port*

Syntax Description

<i>udp_port</i>	UDP port on the supervisor on which to listen for system messages from the SAMI processors. The UDP port must match the port specified on the processors using the logging main-cpu command. We recommend that you use port 4000. If a port other than 4000 is used, RCAL to the SAMI LCP (processor 0) will not work.
-----------------	--

Defaults

No default behavior or values exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

The UDP port must be in the range of 4000 to 10000 and be a multiple of 100.

The UDP port must match the port specified on the processors using the **logging main-cpu** command. We recommend that you use port 4000.

If a port other than 4000 is used, RCAL to the SAMI LCP (processor 0) does not work.

Examples

The following example illustrates how to use the **logging listen** command:

```
Sup# logging listen 4000
```

power enable

To power on the modules, use the **power enable** command in global configuration mode. To power off a module, use the **no** form of this command.

power enable module *slot*

Syntax Description	<i>slot</i>	Number of the slot in which the module is installed. Valid values are 1 to 13, depending on the chassis being used.
---------------------------	-------------	---

Defaults	No default behavior or values exist.
-----------------	--------------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33) SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines	<p>When you enter the:</p> <ul style="list-style-type: none"> • no power enable command to power off a module, the module's configuration is not saved. • no power enable to power off an empty slot, the configuration is saved. <p>The <i>slot</i> argument designates the number of the slot in which the module is installed. Valid values for slot depend on the chassis that is used. For example, in a 13-slot chassis, valid values for the module number are from 1 to 13.</p>
-------------------------	---

Examples	This example shows how to power on a module that was previously powered off:
-----------------	--

```
Sup(config)# power enable module 5
Sup(config)#
```

This example shows how to power off a module:

```
Sup(config)# no power enable module 5
Sup(config)#
```

sami module

To define a remote console and logging (RCAL) server (or servers), and to specify the level of messages to receive and display system message, use the **sami module logging** command in global configuration mode. To remove the configuration, use the **no** form of the command.

```
sami module {mod_num | all} {cpu {cpu_num | all}} logging severity
```

```
no sami module {mod_num | all} {cpu {cpu_num | all}} logging severity
```

Syntax Description

<i>mod_num</i>	Number of the slot in which the SAMI is installed.
all	Specifies all SAMIs installed in the chassis.
cpu { <i>cpu-num</i> all }	Defines the RCAL server, where <ul style="list-style-type: none"> <i>cpu-num</i>—Number of the processor (0 for LCP and 3 through 8 for PPCs) all—Specifies all processors.
logging severity	Specifies the severity level for which the supervisor receives and displays messages. Messages of lower severity than the configured level are filtered.

Defaults

By default, the supervisor receives all system messages sent by SAMI processors.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB1	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

Use this command to define RCAL servers and specify the severity level for which messages are received and displayed.

The level of messages sent by a processor to the supervisor is defined on the processor using the **logging main-cpu** global configuration command.

[Table B-3](#) lists and defines the severity levels of the messages.

Table B-3 Message Severity Level Definitions

Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition

Table B-3 *Message Severity Level Definitions (continued)*

Level	Description
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

Examples

The following example illustrates how to use the **sami module cpu logging** command set for debugging:

```
Sup# sami module 5 | cpu 3 logging 7
```

session slot

To establish a session with a processor on the SAMI, use the **session slot** command in privileged EXEC mode.

```
session slot mod_num processor processor_num
```

Syntax Description

<i>mod_num</i>	Number of the slot in which the module is installed.
<i>processor_num</i>	ID of the processor with which you want to establish a session. For the SAMI, valid values are 0 (the LCP), and 3 through 8.

Defaults

No default behavior or values exist.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(9)ZA	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

Use the **session slot** command to establish a console session with a processor (line control processor [LCP] or PowerPC [PPC]) on the SAMI.

To end the session, enter the **exit** command.

Examples

The following example shows how to open a session with PPC3 on a SAMI installed in slot 2 of the chassis:

```
Sup# session slot 2 processor 3
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.23 ... Open

PPC3> enable
Password:
PPC3# exit

[Connection to 127.0.0.23 closed by foreign host]
Sup#
```

show inventory

To display the product inventory list of all Cisco products that are installed in a networking device, use the **show inventory** command in privileged EXEC mode.

show inventory [*entity*]

Syntax Description

<i>entity</i>	(Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot).
---------------	---

Defaults

No default behavior or values exist.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.3(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a Cisco Unique Device Identifier (UDI).

The UDI is a combination of three separate data elements:

- product identifier (PID)—Name by which the product can be ordered. The PID is also called the Product Name or Part Number. You can use this identifier to order a replacement part.
- version identifier (VID)—Version of the product. Each time a product is revised, the VID is incremented.
- serial number (SN)—Vendor-unique serialization of the product.

Each manufactured product has a unique serial number assigned at the factory; this number identifies a specific instance of a product. This number cannot be changed.

The UDI refers to each product as an entity. Some entities, such as a chassis, have subentities, such as slots. Each entity displays on a separate line.

Examples

The following is sample output from the **show inventory** command without any arguments specified.

```
Sup# show inventory

NAME: "CISCO7613", DESCR: "Cisco Systems Cisco 7600 13-slot Chassis System"
PID: CISCO7613          , VID:          , SN: SAL083014CF

NAME: "WS-C6K-VTT 1", DESCR: "VTT FRU 1"
```

```

PID: WS-C6K-VTT          , VID:      , SN: SMT0829G582

NAME: "WS-C6K-VTT 2", DESCR: "VTT FRU 2"
PID: WS-C6K-VTT          , VID:      , SN: SMT0829B510

NAME: "WS-C6K-VTT 3", DESCR: "VTT FRU 3"
PID: WS-C6K-VTT          , VID:      , SN: SMT0829B486

NAME: "WS-C6513-CL 1", DESCR: "CXXXX Clock FRU 1"
PID: WS-C6513-CL        , VID:      , SN: SMT0827B366

NAME: "WS-C6513-CL 2", DESCR: "CXXXX Clock FRU 2"
PID: WS-C6513-CL        , VID:      , SN: SMT0827B234

NAME: "module 1", DESCR: "WS-SVC-CSG-1 4 ports Content Services Gateway Rev. 1.4"
PID: WS-SVC-CSG-1       , VID:      , SN: SAD0846034C

NAME: "module 2", DESCR: "WS-SVC-SAMI-BB 1 ports Service and Application Module for IP
(SAMI) Rev. 0.702"
PID: WS-SVC-SAMI-BB     , VID: VXX, SN: SAD1042040X

NAME: "module 6", DESCR: "Cisco 7600 / Catalyst 6500 Services SPA Carrier Card-400 Rev.
1.0"
PID: 7600-SSC-400       , VID: V01, SN: JAB100900CF

NAME: "SPA subslot 6/1", DESCR: "IPSec Shared Port Adapter with 2 Gbps DES/3DES/AES"
PID: SPA-IPSEC-2G       , VID: V01, SN: JAB100605N7

NAME: "module 7", DESCR: "WS-SUP720-3BXL 2 ports Supervisor Engine 720 Rev. 3.0"
PID: WS-SUP720-3BXL    , VID:      , SN: SAD08320GDX

NAME: "msfc sub-module of 7", DESCR: "WS-SUP720 MSFC3 Daughterboard Rev. 2.1"
PID: WS-SUP720          , VID:      , SN: SAD08270B3S

NAME: "switching engine sub-module of 7", DESCR: "WS-F6K-PFC3BXL Policy Feature Card 3
Rev. 1.3"
PID: WS-F6K-PFC3BXL    , VID:      , SN: SAD0832014M

NAME: "module 8", DESCR: "WS-SUP720-3BXL 2 ports Supervisor Engine 720 Rev. 3.0"
PID: WS-SUP720-3BXL    , VID:      , SN: SAD081402MM

NAME: "msfc sub-module of 8", DESCR: "WS-SUP720 MSFC3 Daughterboard Rev. 2.0"
PID: WS-SUP720          , VID:      , SN: SAD08130CE8

NAME: "switching engine sub-module of 8", DESCR: "WS-F6K-PFC3BXL Policy Feature Card 3
Rev. 1.1"
PID: WS-F6K-PFC3BXL    , VID:      , SN: SAD08130EH1

NAME: "module 10", DESCR: "WS-SVC-MWAM-1 3 ports MWAM Module Rev. 4.0"
PID: WS-SVC-MWAM-1     , VID:      , SN: SAD083904YM

NAME: "module 11", DESCR: "WS-SVC-MWAM-1 3 ports MWAM Module Rev. 4.0"
PID: WS-SVC-MWAM-1     , VID:      , SN: SAD08340BTT

NAME: "module 12", DESCR: "WS-X6748-GE-TX CEF720 48 port 10/100/1000mb Ethernet Rev. 2.0"
PID: WS-X6748-GE-TX    , VID:      , SN: SAL08342NZP

NAME: "switching engine sub-module of 12", DESCR: "WS-F6700-CFC Centralized Forwarding
Card Rev. 2.0"
PID: WS-F6700-CFC      , VID:      , SN: SAL08280AK9

```

```
NAME: "module 13", DESCR: "WS-X6408A-GBIC 8 port 1000mb GBIC Enhanced QoS Rev. 3.1"
PID: WS-X6408A-GBIC , VID: , SN: SAL08342N59
```

```
NAME: "PS 1 WS-CAC-3000W", DESCR: "AC power supply, 3000 watt 1"
PID: WS-CAC-3000W , VID: , SN: SNI0812AL43
```

```
NAME: "PS 2 WS-CAC-3000W", DESCR: "AC power supply, 3000 watt 2"
PID: WS-CAC-3000W , VID: , SN: AZS09250H6G
```

Sup#

[Table 4](#) describes the fields shown in the show inventory command output.

Table 4 *show inventory Field Descriptions*

Field	Description
Name	Name of the component
Description	Description of the component
PID	Product identifier
VID	Version identifier
SN	Serial number

show logging slot

To display logging status and counters for all processors on a SAMI using the remote command and logging (RCAL) feature, use the **show logging slot** command in privileged EXEC mode.

show logging slot *slot_number*

Syntax Description	<i>slot_number</i>	Number of the slot in which the SAMI is installed. A valid value is a number between 3 and 8.
--------------------	--------------------	---

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(14)ZA4	This command was introduced.
	12.2(14)ZA5	This command was integrated into Cisco IOS 12.2(14)ZA5.
	12.2(33)SRB1	This command was integrated into Cisco IOS 12.3(33)SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use the **show logging slot** command to collect logging status and counters for all PPCs on a SAMI using the RCAL feature (without having to establish a session with a PPC).

Examples The following example shows how to collect status and counters for the processors on a SAMI installed in slot 2 of a chassis:

```
Sup# show logging slot 2

CPU: 02/0      State: ACTIVE      Command Active: No
  ttynum: -1      Logging Level: emergencies
  timeouts:          0 logevents:          0
  sequence errors:  0 reset count:          7 KPA_missed:          0
  send seq:         226 tty recv seq:      0 log recv seq:          0
  Current queue count:  0 IP addr: 127.0.0.20

CPU: 02/1      State: INIT        Command Active: No
  ttynum: -1      Logging Level: emergencies
  timeouts:          0 logevents:          0
  sequence errors:  0 reset count:          0 KPA_missed:          0
  send seq:         0 tty recv seq:      0 log recv seq:          0
  Current queue count:  0 IP addr: 0.0.0.0

CPU: 02/2      State: INIT        Command Active: No
  ttynum: -1      Logging Level: emergencies
  timeouts:          0 logevents:          0
```

```

sequence errors:          0 reset count:          0 KPA_missed:          0
send seq:                 0 tty rcv seq:          0 log rcv seq:          0
Current queue count:      0 IP addr: 0.0.0.0

CPU: 02/3      State: ACTIVE      Command Active: No
ttynum: -1     Logging Level: emergencies
timeouts:      0 logevents:          0
sequence errors: 0 reset count:          8 KPA_missed:          20
send seq:      221 tty rcv seq:          0 log rcv seq:          0
Current queue count: 0 IP addr: 127.0.0.23

CPU: 02/4      State: INIT        Command Active: No
ttynum: -1     Logging Level: emergencies
timeouts:      0 logevents:          0
sequence errors: 0 reset count:          0 KPA_missed:          0
send seq:      0 tty rcv seq:          0 log rcv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/5      State: INIT        Command Active: No
ttynum: -1     Logging Level: emergencies
timeouts:      0 logevents:          0
sequence errors: 0 reset count:          0 KPA_missed:          0
send seq:      0 tty rcv seq:          0 log rcv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/6      State: INIT        Command Active: No
ttynum: -1     Logging Level: emergencies
timeouts:      0 logevents:          0
sequence errors: 0 reset count:          0 KPA_missed:          0
send seq:      0 tty rcv seq:          0 log rcv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/7      State: INIT        Command Active: No
ttynum: -1     Logging Level: emergencies
timeouts:      0 logevents:          0
sequence errors: 0 reset count:          0 KPA_missed:          0
send seq:      0 tty rcv seq:          0 log rcv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/8      State: INIT        Command Active: No
ttynum: -1     Logging Level: emergencies
timeouts:      0 logevents:          0
sequence errors: 0 reset count:          0 KPA_missed:          0
send seq:      0 tty rcv seq:          0 log rcv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

```

Table 5 describes the fields that display in the show logging slot command output.

Table 5 *show logging slot* Field Descriptions

Field	Description
CPU	Number of the processor on the SAMI. Valid values are 0 through 8, where 0 is the LCP, 1 and 2 are IXP1 and IXP2, and 3 through 8 are the six PPCs.
State	Current state of the processor. Valid values are: <ul style="list-style-type: none"> ACTIVE INIT
Command Active	RCAL is active.

Table 5 *show logging slot Field Descriptions (continued)*

Field	Description
ttynum	Line number of the user with an active command on the processor. A value of -1 indicates no user.
Logging Level	Indicates the maximum severity level at which the supervisor displays logger messages from an SAMI.
timeouts	Number of occurrences of remote command execution time-out.
logevents	Serial number.
sequence errors	Protocol sequence errors caused by an overrun or a time-out.
reset count	
KPA_missed	
send seq	
tty recv seq	
log recv seq	
Current queue count	Number of messages received at the supervisor and queued to be processed (logged/displayed).
IP addr	IP address of the SAMI processor.

show logging summary

To display logging status and counters for all processors on all SAMIs in a chassis using the remote console and logging (RCAL) feature, use the **show logging summary** command in privileged EXEC mode.

show logging summary

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Release	Modification
12.2(14)ZA4	This command was introduced.
12.2(14)ZA5	This command was integrated into Cisco IOS 12.2(14)ZA5.
12.2(33)SRB1	This command was integrated into Cisco IOS 12.3(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use this command to collect logging status and counters for all PPCs on all SAMIs in a chassis using the RCAL feature (without establishing a session).

Examples The following example shows how to collect status and counters for the processors on all SAMIs installed in a chassis:

```
Sup# show logging summary
CPU: 02/0      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:      7 KPA_missed:      0
send seq:      232 tty rcv seq:    0 log rcv seq:      0
Current queue count: 0 IP addr: 127.0.0.20

CPU: 02/1      State: INIT      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:      0 KPA_missed:      0
send seq:      0 tty rcv seq:    0 log rcv seq:      0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/2      State: INIT      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:      0 KPA_missed:      0
```

show logging summary

```

send seq:                0 tty recv seq:          0 log recv seq:          0
Current queue count:    0 IP addr: 0.0.0.0

CPU: 02/3      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      8 KPA_missed:          20
send seq:      227 tty recv seq:    0 log recv seq:          0
Current queue count: 0 IP addr: 127.0.0.23

CPU: 02/4      State: INIT        Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      0 KPA_missed:          0
send seq:      0 tty recv seq:      0 log recv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/5      State: INIT        Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      0 KPA_missed:          0
send seq:      0 tty recv seq:      0 log recv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/6      State: INIT        Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      0 KPA_missed:          0
send seq:      0 tty recv seq:      0 log recv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/7      State: INIT        Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      0 KPA_missed:          0
send seq:      0 tty recv seq:      0 log recv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 02/8      State: INIT        Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      0 KPA_missed:          0
send seq:      0 tty recv seq:      0 log recv seq:          0
Current queue count: 0 IP addr: 0.0.0.0

CPU: 10/1     State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      4 KPA_missed:          0
send seq:      232 tty recv seq:    0 log recv seq:          0
Current queue count: 0 IP addr: 127.0.0.101

CPU: 10/2     State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      4 KPA_missed:          0
send seq:      226 tty recv seq:    0 log recv seq:          0
Current queue count: 0 IP addr: 127.0.0.102

CPU: 10/3     State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:        0
sequence errors: 0 reset count:      4 KPA_missed:          0
send seq:      227 tty recv seq:    0 log recv seq:          0

```

```

Current queue count:      0 IP addr: 127.0.0.103

CPU: 10/4      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:    4 KPA_missed:      0
send seq:      226 tty rcv seq:    0 log rcv seq:    0
Current queue count:      0 IP addr: 127.0.0.104

CPU: 10/5      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:    4 KPA_missed:      0
send seq:      227 tty rcv seq:    0 log rcv seq:    0
Current queue count:      0 IP addr: 127.0.0.105

CPU: 10/6      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      1
sequence errors: 0 reset count:    4 KPA_missed:      0
send seq:      226 tty rcv seq:    0 log rcv seq:    0
Current queue count:      0 IP addr: 127.0.0.106

CPU: 10/7      State: INIT        Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:    0 KPA_missed:      0
send seq:      0 tty rcv seq:      0 log rcv seq:    0
Current queue count:      0 IP addr: 0.0.0.0

CPU: 11/1      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:    4 KPA_missed:      0
send seq:      231 tty rcv seq:    0 log rcv seq:    0
Current queue count:      0 IP addr: 127.0.0.111

CPU: 11/2      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:    4 KPA_missed:      0
send seq:      226 tty rcv seq:    0 log rcv seq:    0
Current queue count:      0 IP addr: 127.0.0.112

CPU: 11/3      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:    4 KPA_missed:      0
send seq:      227 tty rcv seq:    0 log rcv seq:    0
Current queue count:      0 IP addr: 127.0.0.113

CPU: 11/4      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:    4 KPA_missed:      0
send seq:      226 tty rcv seq:    0 log rcv seq:    0
Current queue count:      0 IP addr: 127.0.0.114

CPU: 11/5      State: ACTIVE      Command Active: No
ttynum: -1      Logging Level: emergencies
timeouts:      0 logevents:      0
sequence errors: 0 reset count:    4 KPA_missed:      0
send seq:      227 tty rcv seq:    0 log rcv seq:    0
Current queue count:      0 IP addr: 127.0.0.115

```

```

CPU: 11/6      State: ACTIVE      Command Active: No
  ttynum: -1      Logging Level: emergencies
  timeouts:      0 logevents:      1
  sequence errors: 0 reset count:      4 KPA_missed:      0
  send seq:      227 tty recv seq: 0 log recv seq:      0
  Current queue count: 0 IP addr: 127.0.0.116

CPU: 11/7      State: INIT       Command Active: No
  ttynum: -1      Logging Level: emergencies
  timeouts:      0 logevents:      0
  sequence errors: 0 reset count:      0 KPA_missed:      0
  send seq:      0 tty recv seq: 0 log recv seq:      0
  Current queue count: 0 IP addr: 0.0.0.0

```

Sup#

Table 6 describes the fields shown in the **show logging slot** command display.

Table 6 *show logging slot Field Descriptions*

Field	Description
CPU	Number of the processor on the SAMI. Valid values are 0 through 8, where 0 is the LCP, 1 and 2 are IXP1 and IXP2 (future), and 3 through 8 are the six PPCs.
State:	Current state of the processor. Valid values are: <ul style="list-style-type: none"> ACTIVE INIT
Command Active	Whether remote console and logging (RCAL) is enabled. Possible values are Active or No.
ttynum	Line number of the user with an active command on the processor. A value of -1 indicates no user.
Logging Level	Indicates the maximum severity level at which the supervisor displays logger messages from an SAMI.
timeouts	Number of occurrences of remote command execution time-out.
logevents	Serial number.
sequence errors	Protocol sequence errors caused by an overrun or a time-out.
reset count	
KPA_missed	
send seq	
tty recv seq	
log recv seq	
Current queue count	Number of messages received at the supervisor and queued to be processed (logged/displayed).
IP addr	IP address of the SAMI processor.

show module

To display module status and information, use the **show module** command in privileged EXEC mode.

show module [*mod-num* | **all** | **power** | **provision** | **version**]

Syntax Description		
	<i>mod-num</i>	(Optional) Number of the module.
	all	(Optional) Displays information for all modules.
	power	(Optional) Displays administration and operating status.
	provision	(Optional) Displays status about the module processing.
	version	(Optional) Displays version information.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Cisco Supervisor Engine 720.
	12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB.
	12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5 and the power keyword was added.
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines In the Mod Sub-Module fields, the **show module** command displays the supervisor engine number, with the uplink daughter card's module type and information appended.

If a SAMI is installed in the router chassis, the slot number in which the SAMI is installed will also display in the Mod Sub-Module fields, with the SAMI daughter cards' model type and information appended.



Note

When the SAMI status and the sub-module status for both daughter cards display as "Ok," the SAMI module is online.

Entering the **show module** command with no arguments is the same as entering the **show module all** command.

Examples

This example shows how to display information for all modules on a router that is configured with a Cisco Supervisor Engine 720:

```
Sup# show module
```

Mod	Ports	Card Type	Model	Serial No.
4	1	SAMI Module (CSG2)	WS-SVC-SAMI-BB-K9	SAD1140096M
6	2	Supervisor Engine 720 (Active)	WS-SUP720-3BXL	SAD083400U3
7	48	SFM-capable 48-port 10/100 Mbps RJ45	WS-X6548-RJ-45	SAD0611007M
9	1	SAMI Module (GENERIC)	WS-SVC-SAMI-BB-K9	SAD095003X1

Mod	MAC addresses	Hw	Fw	Sw	Status
4	001d.45f9.0922 to 001d.45f9.0929	2.2	8.7(0.5-Eng)	3.0(0)W1(0.0	Ok
6	0011.21b9.ac20 to 0011.21b9.ac23	4.0	8.1(3)	12.2(2007052	Ok
7	0002.7ee1.f010 to 0002.7ee1.f03f	4.2	6.3(1)	8.7(0.22)FW6	Ok
9	0001.0002.0003 to 0001.0002.000a	1.0	8.7(0.5-Eng)	3.0(0)W1(0.0	Ok

Mod	Sub-Module	Model	Serial	Hw	Status
4	SAMI Daughterboard 1	SAMI-DC-BB	SAD113909PZ	1.1	Ok
4	SAMI Daughterboard 2	SAMI-DC-BB	SAD113909U5	1.1	Ok
6	Policy Feature Card 3	WS-F6K-PFC3BXL	SAD083903ML	1.3	Ok
6	MSFC3 Daughterboard	WS-SUP720	SAD083606TK	2.1	Ok
9	SAMI Daughterboard 1	SAMI-DC-BB	SAD110709TS	0.701	Ok
9	SAMI Daughterboard 2	SAMI-DC-BB	SAD110709SF	0.701	Ok

```
Mod Online Diag Status
```

```
-----
4 Pass
6 Pass
7 Pass
9 Pass
```

```
Sup#
```

This example shows how to display information for a specific module:

```
Sup# show module 2
```

Mod	Ports	Card Type	Model	Serial No.
5	2	Supervisor Engine 720 (Active)	WS-SUP720-BASE	SAD0644030K

Mod	MAC addresses	Hw	Fw	Sw	Status
5	00e0.aabb.cc00 to 00e0.aabb.cc3f	1.0	12.2(2003012	12.2(2003012	Ok

Mod	Sub-Module	Model	Serial	Hw	Status
5	Policy Feature Card 3	WS-F6K-PFC3	SAD0644031P	0.302	Ok
5	MSFC3 Daughtercard	WS-SUP720	SAD06460172	0.701	

```
Mod Online Diag Status
```

```
-----
5 Not Available
```

```
Sup#
```

This example shows how to display module version information:

```
Sup# show module version
```

```
Mod Port Model                Serial #      Versions
-----
 2  0   WS-X6182-2PA                Hw : 1.0
                               Fw : 12.2(20030125:231135)
                               Sw : 12.2(20030125:231135)

 4 16   WS-X6816-GBIC              SAD04400CEE Hw : 0.205
                               WS-F6K-DFC3A      SAD0641029Y Hw : 0.501
                               Fw : 12.2(20020828:202911)
                               Sw : 12.2(20030125:231135)

 6  2   WS-X6K-SUP3-BASE          SAD064300GU Hw : 0.705
                               Fw : 7.1(0.12-Eng-02)TAM
                               Sw : 12.2(20030125:231135)
                               Sw1: 8.1(0.45)KIS

                               WS-X6K-SUP3-PFC3      SAD064200VR Hw : 0.701
                               Fw : 12.2(20021016:001154)
                               Sw : 12.2(20030125:231135)

                               WS-F6K-PFC3          SAD064300M7 Hw : 0.301

 9 48   WS-X6548-RJ-45          SAD04490BAC Hw : 0.301
                               Fw : 6.3(1)
                               Sw : 7.5(0.30)CFW11
```

```
Sup#
```

This example shows how to display administration and operating status of modules:

```
Sup# show module power
```

```
Mod Card Type                Admin Status Oper Status
-----
 1 SFM-capable 48-port 10/100 Mbps RJ45 on on
 4 SFM-capable 16 port 1000mb GBIC on on
 5 Supervisor Engine 720 (Active) on on
```

```
Sup#
```

This example shows how to display module provisioning information:

```
Sup# show module provision
```

```
Module Provision
 1 dynamic
 2 dynamic
 3 dynamic
 4 dynamic
 5 dynamic
 6 dynamic
 7 dynamic
 8 dynamic
 9 dynamic
10 dynamic
11 dynamic
12 dynamic
13 dynamic
```

```
Sup#
```

show sami module

To display SAMI traffic counters, use the **show sami module** command in privileged EXEC mode.

```
show sami module slot_number [port port_number] traffic
```

Syntax Description		
	<i>slot_number</i>	Number of the slot in which the SAMI is installed.
	port <i>port_number</i>	(Optional) Number of the data port on the SAMI.
	traffic	Displays traffic counters.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRC	This command was introduced.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use this command to display the traffic counters of a SAMI.

Examples The following example illustrates how to use the counters displayed by the **show sami module** command:

```
Sup#show sami module 2 port 1 traffic
Specified interface is up line protocol is up (connected)
Hardware is c7600 10Gb 802.3, address is 0030.f276.41e4 (bia 0030.f276.41e4)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 10Gb/s
input flow-control is on, output flow-control is unsupported
    202 packets input
    0 input errors,
    0 CRC
    6 packets output
```

Related Commands	Command	Description
	clear sami module	Clears traffic counters on the SAMI.

show svclc module

To view the state or traffic statistics for the backplane port of the module, use the **show svclc module** command in privileged EXEC mode.

```
show svclc module module_number {state | traffic | vlan-group}
```

Syntax Description		
<i>module_number</i>		Number of the slot in which the module is installed.
state		Displays state-related statistics.
traffic		Displays traffic-related statistics.
vlan-group		Displays the group configuration for the SVCLC module, and the associated VLANs.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use this command to display the state or traffic statistics for the backplane port of the module.



Note

If the module is running a software application that supports Layer 2 Transparent Bridging, the **show svclc module** command displays SVCLC traffic information for the seven TenGigabitEthernet interfaces that are automatically created by the supervisor engine module for Layer 2 Transparent Bridging-enabled applications.

Examples The following example illustrates how to use the **show svclc module** command to display the SVCLC module traffic:

```
Sup> show svclc module 4 traffic
SAMI Module 4:

Specified interface is up line protocol is up (connected)
Hardware is c7600 10Gb 802.3, address is 0030.f275.c3de (bia 0030.f275.c3de)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 10Gb/s
input flow-control is on, output flow-control is unsupported
123 packets input
```

■ show svclic module

```
0 input errors, 0 CRC
7 packets output
svclic module 4:
```

```
Sup>
```

This example shows how to display SVCLC module VLAN group configuration:

```
Sup> show svclic module 2 vlan-group
Module Vlan-groups
-----
02    100,101,102
Sup>
```

show upgrade software progress

To display information about the progress of a software upgrade, use the **show upgrade software progress** command in privileged EXEC mode.

show upgrade software progress

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use this command to display the status of any software upgrades in progress.

Examples The following example illustrates the results of issuing the **show upgrade software process** command:

```
Sup# show upgrade software progress
% There is no software upgrade in progress.
```

```
Sup# show upgrade software progress
Slot      Software File
9         sb-csg2-mzg.bin
```

Related Commands	Command	Description
	upgrade hw-module	Upgrades the software image on a module.

show vlans dot1q

To display statistics about 802.1Q VLAN subinterfaces, use the **show vlans dot1q** command in privileged EXEC mode.

```
show vlans dot1q [internal | interface-type interface-number.subinterface-number [detail] |
  outer-id [interface-type interface-number | second-dot1q [inner-id | any]] [detail]
```

Syntax Description		
internal	(Optional) Displays internal QinQ VLAN tag termination information. Used for troubleshooting purposes. The QinQ VLAN Tag Termination feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated.	
<i>interface-type</i>	(Optional) Interface type.	
<i>interface-number</i>	(Optional) Interface number.	
<i>.subinterface-number</i>	(Optional) Subinterface number in the range 1 to 4294967293. A period (.) must be entered between the <i>interface-number</i> argument and the <i>subinterface-number</i> argument.	
detail	(Optional) Displays detailed information.	
<i>outer-id</i>	(Optional) Outer VLAN identifier. The allowed range is from 1 to 4095.	
second-dot1q	(Optional) Displays inner VLAN subinterface information.	
<i>inner-id</i>	(Optional) Inner VLAN identifier. The allowed range is from 1 to 4095.	
any	(Optional) Displays information for all the inner VLAN subinterfaces configured as “any.”	
	Note The any keyword is not supported on a subinterface configured for IPoQinQ because IP routing is not supported on ambiguous subinterfaces.	

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3(7)T	This command was introduced.
	12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines If no arguments or keywords are entered, statistics for all of the 802.1Q VLAN IDs are displayed. The **any** keyword is not supported for IPoQinQ because IP routing is not supported on ambiguous subinterfaces. However, the **second-dot1q inner-id** keyword and argument can be used on IPoQinQ for a specific inner VLAN ID that is not an ambiguous subinterface.

Examples

The output from the **show vlans dot1q** command displays the statistics for all the 802.1Q VLAN IDs. Only the outer VLAN IDs are displayed here.

```
Router# show vlans dot1q

Total statistics for 802.1Q VLAN 1:
  441 packets, 85825 bytes input
  1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
  5173 packets, 510384 bytes input
  3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
  1012 packets, 119254 bytes input
  1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
  3163 packets, 265272 bytes input
  1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
  1012 packets, 119254 bytes input
  1010 packets, 119108 bytes output
```

[Table 7](#) describes the significant fields shown in the display.

Table 7 *show vlans dot1q Field Descriptions*

Field	Description
Total statistics for 802.1Q VLAN 1	Statistics are shown for the VLAN ID with the specified outer ID.
packets	Number of packets encapsulated by the 802.1Q QinQ VLAN.
bytes input	Number of bytes input.
bytes output	Number of bytes output.

The following sample output from the **show vlans dot1q** command displays the statistics for the 802.1Q VLAN subinterface configured on Gigabit Ethernet interface 5/0:

```
Router# show vlans dot1q GigabitEthernet 5/0.1011001

GigabitEthernet5/0.1011001 (101/1001)
  1005 packets, 122556 bytes input
  1023 packets, 125136 bytes output
```

[Table 8](#) describes the significant fields shown in the display.

Table 8 *show vlans dot1q (subinterface) Field Descriptions*

Field	Description
GigabitEthernet5/0.1011001 (101/1001)	Statistics are shown for subinterface Gigabit Ethernet 5/0.1011001 with an outer VLAN ID of 101 and an inner VLAN ID of 1001.
packets	Number of packets encapsulated by the 802.1Q QinQ VLAN.
bytes input	Number of bytes input.
bytes output	Number of bytes output.

The following sample output from the **show vlans dot1q** command displays the summary statistics for all of the VLAN subinterfaces under the physical interface Gigabit Ethernet 5/0 that have an outer VLAN ID of 101:

```
Router# show vlans dot1q 101 GigabitEthernet 5/0

Total statistics for 802.1Q VLAN 101 on GigabitEthernet5/0:
    5218 packets, 513444 bytes input
    3042 packets, 369567 bytes output
```

The following sample output from the **show vlans dot1q** command displays the individual subinterface statistics and summary statistics for all the VLAN subinterfaces under the physical interface Gigabit Ethernet 5/0 that have an outer VLAN ID of 101:

```
Router# show vlans dot1q 101 GigabitEthernet 5/0 detail

GigabitEthernet5/0.101 (0)
    3220 packets, 269148 bytes input
    1008 packets, 119622 bytes output
GigabitEthernet5/0.1019999 (101/1-1000,1003-2000)
    0 packets, 0 bytes input
    3 packets, 1143 bytes output
GigabitEthernet5/0.1011001 (101/1001)
    1005 packets, 122556 bytes input
    1023 packets, 125136 bytes output
GigabitEthernet5/0.1011002 (101/1002)
    1005 packets, 122556 bytes input
    1008 packets, 123666 bytes output
Total statistics for 802.1Q VLAN 101 on GigabitEthernet5/0:
    5230 packets, 514260 bytes input
    3042 packets, 369567 bytes output
```

The following sample output from the **show vlans dot1q** command displays the statistics for an outer VLAN and inner VLAN ID combination. This is a summary that displays the total for all the subinterfaces on the router that are configured with the specified IDs.



Note

When multiple inner VLANs are used, the statistics displayed are at subinterface-level granularity, not VLAN-ID granularity. For example, when a range of inner VLAN IDs is assigned to a subinterface, the statistics are reported only at the subinterface level. Statistics are not available for each inner VLAN ID.

```
Router# show vlans dot1q 101 second-dot1q 1001 detail

GigabitEthernet5/0.1011001 (101/1001)
    1005 packets, 122556 bytes input
    1023 packets, 125136 bytes output
Total statistics for Outer/Inner VLAN 101/1001:
    1005 packets, 122556 bytes input
    1023 packets, 125136 bytes output
```

The following sample output from the **show vlans dot1q** command displays the statistics for a specific outer VLAN ID of 301 and an inner VLAN ID of any. This is a summary that displays the total for all of the subinterfaces on the router that are configured with the specified IDs.

```
Router# show vlans dot1q 301 second-dot1q any

GigabitEthernet5/0.301999 (301/any)
    0 packets, 0 bytes input
    3 packets, 1128 bytes output
```

```
Total statistics for Outer/Inner VLAN 301/"any":
  0 packets, 0 bytes input
  3 packets, 1128 bytes output
```

The following sample output from the **show vlans dot1q** command displays some internal information about the QinQ subsystem and is used for troubleshooting purposes (typically by Cisco engineers):

```
Router# show vlans dot1q internal

Internal VLAN representation on FastEthernet0/0:
VLAN Id: 1 (.1Q, Fa0/0)
VLAN Id: 201 (.1Q-in-.1Q tree, 3 elements)
  Inner VLAN Id: (0 -0 ) Fa0/0.201
  dot1q software subblock bitlist missing
  Inner VLAN Id: (2001-2001) Fa0/0.2012001
  2001
  Inner VLAN Id: (2002-2002) Fa0/0.2012002
  2002
  "any" Fa0/0.201999
VLAN Id: 401 (.1Q-in-.1Q tree, 3 elements)
  Inner VLAN Id: (0 -0 ) Fa0/0.401
  dot1q software subblock bitlist missing
  Inner VLAN Id: (100 -900 ) Fa0/0.4019999
  100-900,1001-2000
  Inner VLAN Id: (1001-2000) Fa0/0.4019999
  100-900,1001-2000
Internal VLAN representation on GigabitEthernet5/0:
VLAN Id: 1 (.1Q, Gi5/0)
VLAN Id: 101 (.1Q-in-.1Q tree, 5 elements)
  Inner VLAN Id: (0 -0 ) Gi5/0.101
  dot1q software subblock bitlist missing
  Inner VLAN Id: (1 -1000) Gi5/0.1019999
  1-1000,1003-2000
  Inner VLAN Id: (1001-1001) Gi5/0.1011001
  1001
  Inner VLAN Id: (1002-1002) Gi5/0.1011002
  1002
  Inner VLAN Id: (1003-2000) Gi5/0.1019999
  1-1000,1003-2000
VLAN Id: 301 (.1Q-in-.1Q tree, 1 elements)
  Inner VLAN Id: (0 -0 ) Gi5/0.301
  dot1q software subblock bitlist missing
  "any" Gi5/0.301999
```

svclc console

To establish a session with the LCP console when the LCP is in ROM-monitor state, use the **svclc console** command in privileged EXEC mode.

svclc console *slot*

Syntax Description

<i>slot</i>	Number of the slot in which the module is installed.
-------------	--

Defaults

No default behavior or values exist.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

To establish a session with the LCP when the LCP is in ROM-monitor state, use the **svclc console** command.

If the LCP is in ROM-monitor state, the module status displays as other in the **show module** command output.

Examples

The following example illustrates how to use the **svclc console** command:

```
Sup# svclc console 3
```

svclc module

To assign a VLAN group to a SAMI, use the **svclc module** command in global configuration mode. To remove the VLAN assignment, use the **no** form of the command.

```
svclc module module_number vlan-group group_number_range
```

```
no svclc module module_number vlan-group group_number_range
```

Syntax Description

<i>module_number</i>	Number of the slot in which the SAMI is installed.
vlan-group <i>group_number_range</i>	VLAN group number identified as a single number (n), as a range of numbers (n-x), or as separate numbers, or range of numbers, separated by commas (for example, 3,5,7-10). Only VLAN groups created using the svclc vlan-group global configuration command can be specified.

Defaults

No default behavior or values exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

Use this command to apply a VLAN group created using the **svclc module** command to a SAMI. This is the allowed VLAN.

One VLAN group can be assigned to multiple SAMIs.

Examples

The following example shows how to assign VLAN groups 50 and 52 to a SAMI installed in slot 5 of the chassis:

```
Sup(config)# svclc module 5 vlan-group 50,52
```

Related Commands

Command	Description
svclc vlan-group	Assigns VLANs to a VLAN groups.
svclc multiple-vlan-interfaces	Enables multiple SVIs to be configured for a SAMI.

svclc multiple-vlan-interfaces

To enable multiple switched virtual interfaces (SVIs) to be configured for a SAMI, use the **svclc multiple-vlan-interfaces** command in global configuration mode. To remove this configuration, use the **no** form of the command.

svclc multiple-vlan-interfaces

no svclc multiple-vlan-interfaces

Syntax Description This command has no keywords or arguments.

Defaults No default behavior or values exist.

Command Modes Global configuration

Command History

Release	Modification
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

The SVI configuration defines the Layer 3 instance on the MSFC (the router). If you assign the VLAN used for the SVI to a SAMI PPC, then the MSFC routes between the SAMI PPC and other Layer 3 VLANs.

By default, only one SVI can exist between the MSFC and a SAMI. However, you must configure multiple SVIs for unique VLANs on each SAMI.



Note

For Layer 2 forwarding, configuring a switched virtual interface (SVI) is not required for allowing VLAN traffic to the SAMI PPCs. Configuring a SVI is only required if the supervisor participates in Layer 3 forwarding.

Examples

The following example illustrates how to use the **svclc multiple-vlan-interfaces** command:

```
Sup> enable
Sup# configure terminal
Sup(config)# svclc multiple-vlan-interfaces
Sup(config)# interface vlan 100
Sup(config-if)# ip address 127.0.0.0 255.255.255.0
Sup(config-if)# no shutdown
```

Related Commands	Command	Description
	svclc module vlan-group	Assigns a VLAN group to a SAMI.
	svclc vlan-group	Assigns VLANs to a VLAN group.

svc1c vlan-group

To assign VLANs to a group, use the **svc1c vlan-group** command in global configuration mode. To remove the configuration, use the **no** form of this command.

svc1c vlan-group *group_number* *vlan_range*

no svc1c vlan-group *group_number* *vlan_range*

Syntax Description

<i>group_number</i>	Number of the group.
<i>vlan_range</i>	Number of the VLAN or VLANs identified as a single number (<i>n</i>), as a range of numbers (<i>n-x</i>), or as separate numbers, or range of numbers, separated by commas (for example, 5,7-10,13,45-100).

Defaults

No default behavior or values exist.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines

Use this command to assign VLANs to a group.

You can create one or more VLAN groups, and then assign the groups to the SAMI. You cannot assign the same VLAN to multiple groups; however, you can assign multiple groups to a SAMI. VLANs that you want to assign to multiple SAMIs, for example, can reside in a separate group from VLANs that are unique to each SAMI.

Examples

The following example illustrates how to assign VLANs 50, 56, and 57 to VLAN group 50:

```
Sup(config)# svc1c vlan-group 50 55-57
```

Related Commands

Command	Description
svc1c	Enables multiple SVIs to be configured for a SAMI.
multiple-vlan-interfaces	
svc1c module vlan-group	Assigns a VLAN group to a SAMI.

upgrade hw-module

To upgrade the software image on a module, use the **upgrade hw-module** command in privileged EXEC mode.

```
upgrade hw-module slot slot_number software url/filename
```

Syntax Description	slot <i>slot_number</i>	Number of the slot in which the SAMI is installed.
	software	Specifies that a software file will be downloaded
	<i>url/file-name</i>	Location and name of the file you want to use to upgrade the SAMI.

Defaults No default behavior or values exist.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
	12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.

Usage Guidelines Use this command to copy a bundle image from a specified URL to the compact flash of a SAMI installed in a specific slot of the router chassis.

Note This command is required to ensure that future reboots of the SAMI will automatically come up with the specified image.

Examples The following example illustrates how to use the **upgrade hw-module** command:

```
Sup# upgrade hw-module slot 9 software tftp.10.102.16.25/sb-csg2-mzg.bin
Loading sb-csg2-mzg.bin from 64.102.16.25 (via FastEthernet2/6):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 37541640 bytes]
```

Related Commands	Command	Description
	show upgrade software progress	Displays the progress of module upgrades.

