CHAPTER 3

Configuring the Cisco SAMI

This chapter describes how to configure the Cisco Service and Application Module for IP (SAMI). It includes the following sections:

For a description of some of the commands used in this chapter, see Appendix A, "Using the Command-Line Interfaces."

To locate documentation about other commands that appear in this chapter, refer to the *Cisco 7600 Series Internet Router IOS Software Configuration Guide*.

Before You Begin

Before configuring the SAMI, ensure that you have reviewed the following sections:

- System Requirements and Specifications, page 1-12
- Using the Command-Line Interfaces, page A-1
- Establishing Console Sessions, page 3-2

Establishing Console Sessions

When configuring the SAMI in your Cisco 7600 Series Router, you establish a console session with the SAMI LCP and PPCs and enter commands.

To establish a session with a SAMI LCP or PPC, complete the tasks in the following sections:

Configuring a Virtual Terminal Line Settings

Line configuration mode commands allow you to configure the virtual terminal line settings which are used solely to control inbound Telnet connections.

Note Typically, vty0 and line 66 are used for **session** command support from supervisor.

To configure the virtual terminal line settings for the **session** command to a remote console, use the following commands from the supervisor console:

Step 1	`Sup> enable`	Enables privileged EXEC mode.
Step 2	`Sup# line vty line-number [ending-line-number]`	Identifies a specific line for configuration and enters line configuration collection mode where: • *line-number*—Relative number of the terminal line (or the first line in a contiguous group) that you want to configure when the line type is specified. Numbering begins with zero. • *ending-line-number*—(Optional) Relative number of the last line in a contiguous group that you want to configure. If you omit any keyword, then line-number and ending-line-number are absolute rather than relative line numbers.

Establishing a Console Session with the SAMI LCP

Establishing a console session with the SAMI LCP is not required to set up the SAMI in the Cisco 7600 Series Router chassis, however, you can establish a session to perform various maintenance tasks (manage files or issue **show** commands), and you can configure a hostname for the SAMI LCP that assists you in keeping track when you have sessions to multiple SAMIs open. From the SAMI LCP console, you can also configure the amount of time that a session can remain inactive before it is closed (inactivity timeout).

A session to the LCP console can be established from the supervisor or from a serial console connected to the front panel of the SAMI. For information about establishing a session using a connected serial console, see the "Establishing a Console Connection on the SAMI" section on page 4-23.

To establish a console session to the SAMI LCP from the supervisor, use the following commands:

Step 1	`Sup>` **`enable`**	Enables privileged EXEC mode.
Step 2	`Sup#` **`session slot`** *`slot_number`* **`processor 0`**	Establishes a session to the LCP on the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. • *proc_number*—Number of the LCP, which is **0**. **Note** One session per processor can be established.

Assigning a Hostname to the SAMI LCP

The hostname is used for the command line prompts and default configuration filenames. If you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. By default, the hostname for the the SAMI LCP is "switch."

To configure a hostname for the SAMI LCP, from the LCP console, use the following commands:

Step 1	`switch#` **`configure`**	Enables configuration mode.
Step 2	`switch(config)#` **`hostname`** *`name`*	New hostname for the SAMI LCP. Enter a case sensitive text string that contains from 1 to 32 alphanumeric characters.

For example, to change the hostname of the SAMI LCP from switch to host1, enter:

```
switch# configure
switch(config)# hostname host1

host1(config)#
```

Configuring the SAMI Inactivity Timeout

By default, the inactivity timeout value is 5 minutes. You can modify the length of time that can occur before the SAMI automatically logs off an inactive session by using the **login timeout** command in configuration mode.

To specify the length of time a session can be idle before the SAMI logs off the inactive session, use the **login timeout** command in configuration mode, from the LCP console:

Step 1	`switch#` **`configure`**	Enables configuration mode.
Step 2	`switch(config)#` **`login timeout`** *`minutes`*	Length of time a session can be idle before the SAMI terminates the session. Valid entries are 0 to 60 minutes. A value of 0 instructs the never to timeout. The default is 5 minutes. To restore the default timeout value, use the **no** form of the command.

To display the value configured for the inactivity timer, use the **show login timeout** command in EXEC mode from the LCP console:

Step 1	`switch# show login timeout`	Displays the value configured for the inactivity timer.

For example, to specify a timeout period of 10 minutes, enter:

```
switch# configure
switch(config)# login timeout 10
```

To display the configured login time value, use the **show login timeout** command in EXEC mode. For example, enter:

```
switch# show login timeout

Login Timeout 10 minutes.
```

Establishing a Session with a SAMI PPC

Note Under certain conditions such as low processor memory, a session to the SAMI might fail. If this occurs, you will need to use the physical front-panel console connections to access the SAMI (see "Establishing a Console Connection on the SAMI" section on page 4-23).

To establish a session with a SAMI PPC from the supervisor engine console, use the following commands:

Step 1	`Sup> enable`	Enables privileged EXEC mode.
Step 2	`Sup# session slot` *slot_number* `processor` *proc_number*	Establishes a session to a PPC on the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. • *proc_number*—Number of the PPC on the SAMI. Valid values are 3 through 8. **Note** One session per processor can be established.

When you establish a session with a Cisco IOS PPC, the default session prompt is "router."

When you establish a session with a COSLI PPC, the default session prompt is "switch."

Assigning a Hostname to a SAMI PPC

Assigning a hostname to the SAMI PPCs helps you keep track of the PPC sessions.

To assign a hostname to a Cisco IOS PPC, use the following command, in global configuration mode:

Step 1	`Sup# session slot slot_number processor proc_number`	Establishes a session to a PPC on the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. • *proc_number*—Number of the PPC on the SAMI. Valid values are 3 through 8. One session per processor can be established.
Step 2	`Router> enable`	Enters privilege EXEC mode.
Step 3	`Router# config`	Enters global configuration mode.
Step 4	`Router(config)# hostname name`	New hostname for the PPC. Enter a case sensitive text string that contains from 1 to 32 alphanumeric characters.

In the following example, a session with Cisco IOS PPC 3 on a SAMI in slot 6 is established, and the hostname is changed to "PPC3."

```
Sup> enable
Sup# session slot slot_number processor proc_number

Router# enable
Router# configure
Router(config)# hostname PPC3

PPC3(config)#
```

To assign a hostname to a COSLI PPC, use the following command, in global configuration mode:

Step 1	`Sup# session slot slot_number processor proc_number`	Establishes a session to a PPC on the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. • *proc_number*—Number of the PPC on the SAMI. Valid values are 3 through 8. One session per processor can be established.
Step 2	`switch# config`	Enters global configuration mode.
Step 3	`switch(config)# hostname name`	New hostname for the PPC. Enter a case sensitive text string that contains from 1 to 32 alphanumeric characters.

In the following example, a session with Cisco COSLI PPC 3 on a SAMI in slot 6 is established, and the hostname is changed to "PPC3."

```
Sup> enable
Sup# session slot slot_number processor proc_number

switch# config
switch(config)# hostname PPC3

PPC3(config)#
```

Enabling the Supervisor to Store PPC Startup Configuration Files

The Configuration File Storage on Supervisor feature enables you to configure the supervisor engine to save and store the startup configuration file of each of the PPCs on the SAMI in the supervisor's bootflash memory.

Note The Configuration File Storage on Supervisor feature only stores the PPC startup configuration files. Crypto configurations, such as RSA key generation for Secure Shell (SSH) is stored locally on nvram:private-config. Therefore, if a SAMI card containing crypto configuration needs to be replaced, the crypto configuration must be reapplied by either by manually reconfiguring it on the new card, or by exporting the crypto configuration to the supervisor and then importing the configuration onto the new card. For information on exporting and importing the crypto configuration, see "Configuring, Exporting, and Importing RSA Keys on a SAMI PPC" section on page 4-20.

Note For information about using the bootflash on a supervisor engine, see the *Cisco 7600 Series Cisco IOS Software Configuration Guide*.

The ability to store PPC startup configuration files on the supervisor enables a SAMI to be replaced while retaining the configurations associated with each of the PPCs on the module.

When a SAMI is inserted into the Cisco 7600 Series Router chassis, an empty configuration file is automatically created for each of the PPCs with the following naming convention:

```
SLOTxSAMICy.cfg
```

where *x* is the number of the chassis slot in which the SAMI is installed and *y* is the PPC number (numbers 3 through 8) on the SAMI.

When a PPC comes up, it copies its configuration file from the supervisor bootflash and uses it. When you save the configuration changes on a PPC using the **write memory** command, the configuration file in the supervisor bootflash is updated.

The following example shows the configuration files stored on the supervisor module for PPCs of a SAMI installed in slot 9 of a Cisco 7600 Series Router chassis:

```
Sup# dir bootflash:
Directory of bootflash:/
  172  -rw-          42   Mar 8 2007 12:30:07 -07:00  SLOT9SAMIC3.cfg
  173  -rw-          42   Mar 8 2007 12:30:07 -07:00  SLOT9SAMIC4.cfg
  174  -rw-          42   Mar 8 2007 12:30:07 -07:00  SLOT9SAMIC5.cfg
  175  -rw-          42   Mar 8 2007 12:30:07 -07:00  SLOT9SAMIC6.cfg
  176  -rw-          42   Mar 8 2007 12:30:07 -07:00  SLOT9SAMIC7.cfg
  177  -rw-          42   Mar 8 2007 12:30:07 -07:00  SLOT9SAMIC8.cfg
```

Note If a standby supervisor engine is installed, the bootflash on the standby supervisor engine backs up the SAMI PPC configuration files that are on the active supervisor. If a difference is detected between corresponding files on the active and standby supervisor engines, the file in the bootflash of the active supervisor engine is copied over the file in the bootflash of the standby supervisor engine. This compare and copy operation occurs after a SAMI is replaced or when the active supervisor engine detects that a standby supervisor engine has been installed.

Caution If a standby supervisor engine does not exist, periodically copy the SAMI PPC configuration files from the bootflash of the active supervisor engine to a TFTP server. Failure to take this precaution might result in the loss of the SAMI PPC configuration files if a supervisor engine failure should occur.

Configuration File Storage and the Remote Copy Protocol

The remote copy protocol (RCP) is used to read and write the PPC configuration files between the SAMI and the supervisor.

The RCP server, configured on the supervisor, accepts the RCP requests from the RCP client, which is configured on each the PPCs on the SAMI. The PPCs use their internal Ethernet Out of Band Channel (EOBC) IP address (address format 127.0.0.*slot_num proc_num*) when sending read/write requests to the RCP server.

To enable PPC configuration files to be stored on the supervisor, on the supervisor, you must first enable RCP support for each of the SAMI PPCs using the **ip rcmd remote-host enable** global configuration command—six **ip rcmd remote-host enable** configuration statements for each SAMI installed in the router chassis.

Note To facilitate the process of enabling RCP support for each of the PPCs, we recommend that you create an access list on the supervisor engine that permits RCP requests from all IP addresses that begin with the internal EOBC IP address of the PPCs (127*), and specify the access list when configuring the **ip rcmd remote host enable** command on the supervisor.

To configure an access list permitting the RCP requests from all SAMI PPCs, use the following commands from the supervisor engine console:

	Command	Purpose
Step 1	`Sup> enable`	Enables privileged EXEC mode.
Step 2	`Sup# configure terminal`	Enters global configuration mode.

	Command	Purpose
Step 3	`Sup(config)# access-list` *access-list-number* **permit** *source*	Configures the access list mechanism for filtering frames where: • *access-list-number* is the number that identifies the access list. • **permit** is the keyword option to specify to permit the frames if conditions are matched. • source is the number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: – Use a 32-bit quantity in four-part, dotted-decimal format. – Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255.
Step 4	`Sup(config-ip-acl) exit`	Exits access-list configuration mode.

To enable RCP and apply the access list when configuring the remote hosts (the Cisco software application running on the SAMI PPCs) that can execute commands using RCP, use the following commands from the supervisor engine console:

	Command	Purpose
Step 1	`Sup> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	`Sup# configure terminal`	Enters global configuration mode.
Step 3	`Sup(config)# ip rcmd rcp-enable`	Configures the supervisor engine to allow remote hosts to copy files to and from using RCP.

	Command	Purpose
Step 4	`Sup(config)# ip rcmd remote-host local-username {ip-address | host-name | access-list} remote-username [enable [level]]`	Creates an entry for a remote host in a local authentication database so that the remote host can execute commands using RCP where: • *local-username* is the name of the SAMI PPC on the local router. • *ip-address* is the IP address of the remote host from which the local router will accept remotely executed commands. • *host-name* is the name of the remote host. • *access-list* is the name of an access list of remote hosts. • *remote-username* is the name of the SAMI PPC on the remote host. • **enable** enables the PPC to execute privileged EXEC commands using rsh, or to copy files to the router using rcp. • *level* is the privilege level assigned to the PPC. The default is 15, the highest level.
Step 5	`Sup(config-ip-acl) exit`	Exits global configuration mode.

For example:

- To create an access-list that when applied will permit RCP requests from all SAMI PPCs, enter the following commands on the supervisor:

```
Sup> enable
Sup# configure terminal
Sup(config)# access-list 24 permit 127.0.0.0 0.0.0.255
Sup(config)# exit
```

- To configure the supervisor engine to allow remote hosts to copy files to and from using RCP, and to define the remote hosts allowed to use RCP, enter the following commands on the supervisor:

```
Sup> enable
Sup# configure terminal
Sup(config)# ip rcmd rcp-enable
Sup(config)# ip rcmd remote-host * 24 * enable
Sup(config)# exit
```

Note The asterisks (*) are specified for the **ip rcmd remote-host** command *local-username* and *remote-user name* to enable any user for the 127.0.0.*xy* addresses so that all SAMIs are supported.

Configuring VLAN Support

The SAMI does not include any external physical interfaces to receive traffic from clients and servers. Instead, it uses internal VLAN interfaces.

Before configuring VLAN support, note the following:

- You must configure virtual LANs (VLANS) on the Cisco 7600 Series Router and assign physical interfaces to the VLAN before you configure VLANs for the SAMI PPCs. The VLAN IDs for the router and for the PPCs must be the same. For details on configuring VLANs on the Cisco 7600 Series Router, refer to the *Cisco 7600 Series Cisco IOS Software Configuration Guide*.
- If the Multilayer Switch Function Card (MSFC) (Supervisor Engine 720 only) is used as the next-hop router on either the subscriber-side VLAN or the network-side VLAN, then a corresponding Layer 3 VLAN interface must be configured.

To enable VLAN traffic, you must complete the following:

- On the supervisor:
  - Configure a VLAN and VLAN interface for each PPC.
  - Assign the VLANs to a VLAN group.
  - Associate the group to a SAMI installed in the chassis.
  - Configure a default gateway VLAN
- On the SAMI PPCs:
  - Configure the corresponding VLAN interfaces. (All VLAN interfaces are routed mode interfaces.)
  - Define the default gateway on each SAMI PPC
  - Configure a static route

To configure VLAN support between the supervisor engine and the SAMI PPCs, complete tasks in the following sections:

- Permitting VLAN Traffic to Cisco SAMI, page 3-10 (Required)
- Configuring a Switched Virtual Interface on the MSFC, page 3-13 (Optional)
- Configuring the VLAN Interfaces on the SAMI PPCs, page 3-14 (Required)

Permitting VLAN Traffic to Cisco SAMI

In order for the PPCs on the SAMI to receive traffic from the supervisor engine, complete the following tasks on the supervisor engine:

- Configure a VLAN for each SAMI PPC
- Assign the VLANs to a VLAN group
- Determine which VLAN groups you want to allow to which SAMI
- Assign the VLAN groups to the SAMIs
- Configure a default gateway VLAN

After the VLAN configuration has been completed on the supervisor engine, establish a session with each of the PPCs on the SAMI, and configure the corresponding VLAN interface on the PPC.

Configuring VLANs for the SAMI PPCs

To configure the VLANs for each SAMI PPC on the supervisor, use the following commands on the supervisor engine console:

	Command	Purpose
Step 1	`Sup> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	`Sup# configure terminal`	Enters global configuration mode.
Step 3	`Sup(config)# vlan` *vlan-id*	Configures a VLAN where *vlan-id* is the number of the VLAN. Valid values are from 1 to 4094.
Step 4	`Sup(config-vlan)# description` *interface_description*	(Optional) Provides a description for the VLAN.
Step 5	`Sup(config-vlan)# end`	Exits VLAN configuration mode.

For example:

- To create VLANs 71 to 76 on the supervisor, enter the following commands:

```
Sup> enable
Sup# configure terminal
Sup(config)# vlan 71
Sup(config-vlan) exit
Sup(config)# vlan 72
Sup(config-vlan) exit
Sup(config)# vlan 73
Sup(config-vlan) exit
Sup(config)# vlan 74
Sup(config-vlan) exit
Sup(config)# vlan 75
Sup(config-vlan) exit
Sup(config)# vlan 76
Sup(config-vlan) exit
```

Creating and Assigning VLANs Groups to the SAMI

The PPC VLANs on a SAMI must be assigned to the same VLAN group. You cannot assign the same VLAN to multiple groups, however, you can assign a group to multiple SAMIs.

By default, one switched virtual interface (SVI) (required if the supervisor participates in Layer-3 forwarding) can exist between an MSCFC and a SAMI. However, on the SAMI, you must create multiple SVIs, therefore you must enable multiple SVIs to be configured using the **svclc multiple-vlan-interfaces** command.

To assign VLANs to a SAMI, use the following commands at the supervisor engine console:

Step 1	`Sup> enable`	Enables privileged EXEC mode.
Step 2	`Sup# configure terminal`	Enters global configuration mode.

Step 3	`Sup(config)# svclc vlan-group vlan_group_number vlan_range`	Assigns the VLANs to a group. • *vlan_group_number*—Number of the VLAN group. • *vlan_range*—Number of the VLAN or VLANs 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, 5,7-10,13,45-100).
Step 4	`Sup(config)# svclc module slot_num vlan-group group_number_range`	Assigns VLAN groups to the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. To display slot numbers and modules in the chassis, use the **show module** privilege EXEC command. • *group_number_range*—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 specified. **Note** One VLAN group can be assigned to multiple SAMIs.

For example:

- To create a VLAN group, group 50, with a VLAN range of 71 to 76, enter the following commands:

```
Sup> enable
Sup# configure terminal
Sup(config)# svclc vlan-group 50 71-76
```

- To assign VLAN group 50 to the SAMI in slot 5, enter:

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

- To enable multiple SVIs to be configured for a SAMI, enter:

```
Sup(config)# svclc multiple-vlan-interfaces
```

- To view the group configuration for the SAMI and the associated VLANs, enter:

```
Sup(config)# exit
Sup# show svclc vlan-group
```

- To view VLAN group numbers for all modules, enter:

```
Sup# show svclc module
```

Configuring a Switched Virtual Interface on the MSFC

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 engine participates in Layer-3 forwarding.

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 a MSFC and a SAMI. However, on each SAMI, you need to configure multiple SVIs for unique VLANs.

To configure the SVI and enable multiple SVIs to be configured for a SAMI, use the following commands at the supervisor engine console:

	Command	Purpose
Step 1	`Sup> enable`	Enables privileged EXEC mode.
Step 2	`Sup# configure terminal`	Enters global configuration mode.
Step 1	`Sup(config)# svclc multiple-vlan-interfaces`	Enables multiple SVIs to be configured for a SAMI.
Step 2	`Sup(config)# interface vlan` *vlan_number*	Creates or accesses a dynamic SVI where *vlan-number* is the number of the VLAN. Valid values are from 1 to 4094.
Step 3	`Sup(config-if)# ip address` *ip_address vlan vlan_number*	IP address and IP subnet for this interface.
Step 4	`Sup(config-if)# no shutdown`	Enables the interface.

For example:

- To enable multiple SVIs to be configured for a SAMI and to configure the SVI on the MSFC, enter the following commands:

```
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
```

- To view the SVI configuration, enter:

```
Sup(config-if)# exit
Sup(config)# exit
Sup# show interface vlan 100
```

Configuring the VLAN Interfaces on the SAMI PPCs

The way you configure the VLAN interfaces on the SAMI PPCs is dependent on the PPC operating system being used by the Cisco software application.

If your application is using Cisco IOS, see "Configuring Cisco IOS PPCs" section on page 3-14.

If you application is using COSLI, see "Configuring COSLI PPCs" section on page 3-16.

Configuring Cisco IOS PPCs

To complete the configuration tasks for VLAN support, on each SAMI PPC, complete the following:

- Configure an interface to the PPCs corresponding VLAN created on the supervisor engine.
- Enable IEEE 802.1Q encapsulation on the interface.
- Configure a static route for traffic to the PPC.

To configure a SAMI Cisco IOS PPC, use the following commands beginning in privilege EXEC mode at the supervisor engine console:

	Command	Purpose
Step 1	`Sup> enable`	Enables privileged EXEC mode.
Step 2	`Sup# configure terminal`	Enters global configuration mode.
Step 3	`Sup# session slot` *slot_number* `processor` *proc_number*	Establishes a session to a PPC on the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. • *proc_number*—Number of the PPC on the SAMI. Valid values are 3 through 8. One session per processor can be established.
Step 4	`Router> enable`	Enables privileged EXEC mode.
Step 5	`Router# configure terminal`	Enters global configuration mode.

	Command	Purpose
Step 6	`Router(config)# interface gigabitethernet`	Specifies a subinterface on which IEEE 802.1Q is used.
Step 7	`Router(config-if)# encapsulation dot1Q` *vlan_id*	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier (configured on the supervisor engine).
Step 8	`Router(config-if)# ip address` *ip-address mask*	Sets a primary IP address for the interface.
Step 9	`Router(config-if)# exit`	Exits interface configuration mode.
Step 10	`Router(config)# ip route`	Creates a static route for traffic to the PPC.

For example:

- To create two interfaces on PPC3 (on a SAMI in slot 5) on which IEEE 802.1Q is enabled, enter the following commands:

```
Sup# session 5 processor 3
Router> enable
Router(config)# interface GigabitEthernet0/0
Router(config-if)# no ip address
Router(config-if)# exit
Router(config)#
Router(config)# interface GigabitEthernet0/0.310
Router(config-if)# encapsulation dot1Q 310
Router(config-if)# ip address 10.3.10.1 255.255.255.0
Router(config-if)# exit
Router(config)#
Router(config)# interface GigabitEthernet0/0.401
Router(config-if)# encapsulation dot1Q 401
Router(config-if)# ip address 10.4.1.1 255.255.255.0
Router(config-if)# exit
Router(config)#
```

- To verify the interface configurations, enter:

```
Router(config)# exit
Router# show interface
```

Configuring COSLI PPCs

To complete the configuration tasks for VLAN support, on each of the SAMI PPCs, complete the following tasks:

- Configure an interface to the corresponding VLAN created on the supervisor engine
- Configure a default gateway.

To configure a SAMI COSLI PPCs, use the following commands beginning in privilege EXEC mode at the supervisor engine console:

	Command	Purpose
Step 1	`Sup> enable`	Enables privileged EXEC mode.
Step 2	`Sup# configure terminal`	Enters global configuration mode.
Step 3	`Sup# session slot` *slot_number* `processor` *proc_number*	Establishes a session to a PPC on the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. • *proc_number*—Number of the PPC on the SAMI. Valid values are 3 through 8. One session per processor can be established.
Step 4	`switch# config`	Enters configuration mode.
Step 5	`switch(config)# interface vlan` *number*	Creates a VLAN interface for the specified VLAN, and enters interface configuration mode.
Step 6	`switch(config-if)# description` *interface_description*	(Optional) Provides a description for the interface.
Step 7	`switch(config-if)# ip address` *ipv4-addr*	Assigns an IPv4 address to the VLAN interface for connectivity. This IP address will be used by the IKE and ESP traffic from the end points.
Step 8	`switch(config-if)# no shutdown`	Enables the VLAN interface.
Step 9	`switch(config-if)# do show interface vlan` *number*	Verifies that the VLAN is active. **Note** When you are in a configuration mode, you can use the **do** command to use a **show** command or any other command that is only available in EXEC mode.
Step 10	`switch(config-if)# do ping` *ip_address*	Verifies network connectivity.
Step 11	`switch(config-if)# do show arp`	Displays the ARP table.
Step 12	`switch(config-if)# exit`	Exit interface configuration mode.
Step 13	`switch(config)#ip default-gateway` *ip-addr*	Defines a default gateway (router) when IP routing is disabled.

For example:

- To create a VLAN interface on PPC3 on a SAMI in slot 5, enter the following commands:

```
Sup# session slot 5 processor 3
switch> config
switch(config)# interface vlan71
switch(config-if)# ip address 10.22.22.2/32
switch(config-if)# exit
```

- To configure a default gateway, enter the following commands:

```
Sup# session slot 5 processor 3
switch> config
switch(config)# ip default-gateway 88.88.38.100
```

- To verify the interface configuration of VLAN71, enter:

```
switch# show interface vlan71
```

Verifying the Configuration

To verify the configuration on the supervisor engine, use the following **show** commands:

Note In the following examples, the SAMI is installed in slot 2 of the chassis.

- **show spanning-tree vlan**

  The following example shows how to display the spanning tree state for the specified VLAN.

```
Sup> show spanning-tree vlan 46

VLAN0046
  Spanning tree enabled protocol rstp
  Root ID    Priority    32814
             Address     0011.5ddb.fc00
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID   Priority    32814  (priority 32768 sys-id-ext 46)
             Address     0011.5ddb.fc00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Te2/1               Desg FWD 2         128.257  Edge P2p
Sup>
```

- **show sami module**

  The following example shows how to display the trunk and VLAN configuration.

```
Sup> show sami module 2 port 1 state
SAMI module 2 data-port 1:

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
```

```
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1,10,46,220,250,301,501,1100,2066
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1,10,46,220,250,301,501,1100,2066
Vlans allowed and active in management domain: 1,10,46,220,250,301,501,1100,2066
Vlans in spanning tree forwarding state and not pruned:
1,10,46,220,250,301,501,1100,2066
Sup>
```

The following example shows how to display SAMI port traffic:

```
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.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
  Keepalive set (10 sec)
  Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is unsupported
  Last input never, output 00:00:47, output hang never
  Last clearing of "show interface" counters 1d02h
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     730149 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     22035 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Sup>
```

- **show svclc module**

  The following example shows how to display the SVCLC module traffic:

```
Sup> show svclc module 2 traffic
Module 4:

Specified interface is up line protocol is up (connected)
  Hardware is C6k 10000Mb 802.3, address is 001f.ca08.892c (bia 001f.ca08.892c)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 10Gb/s
  input flow-control is on, output flow-control is unsupported
  Last input never, output 00:00:57, output hang never
  Last clearing of "show interface" counters 1d02h
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     732861 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     22116 packets output, 0 bytes, 0 underruns
```

```
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Sup>
```

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

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

Sup>
```

Configuring Network Clock Synchronization

If the supervisor engine is not already configured as a Cisco Network Time Protocol (NTP) client, configure it as an NTP master clock to which the applications running on the SAMI PPCs can synchronize themselves.

To configure the supervisor engine as an NTP client, use the following commands in global configuration mode at the supervisor engine console:

Step 1	`Sup(config)# ntp master`	Configures an NTP master clock to which peers synchronize themselves.
Step 2	`Sup(config)# ntp update-calendar`	Periodically updates the hardware clock (calendar) from an NTP time source.

To enable a Cisco software application running on a SAMI PPC to synchronize its software clock with the one in the supervisor engine, use the following commands beginning in privileged EXEC mode at the supervisor engine console:

Step 1	`Sup# session slot` *slot_number* `processor` *proc_number*	Establishes a session to a PPC on the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. • *proc_number*—Number of the PPC on the SAMI. Valid values are 3 through 8. One session per processor can be established.
Step 2	`Router> enable` **Note** If establishing a session to a COSLI PPC, skip this step and proceed to Step 3.	Enters privilege EXEC mode.

Step 3	`Router# config`	Enters global configuration mode.
Step 4	`Router(config)# ntp server 127.0.0.xy`	Enables the software clock to be synchronized by a Network Time Protocol (NTP) time server where: • *x* is the slot in which the supervisor engine is installed. • *y* identifies the supervisor engine—1 for Supervisor Engine 720.

Note For NTPv4, the NTP synchronization takes more time to complete unlike NTPv3, which synchronizes in seconds or in a maximum of 1 to 2 minutes. The acceptable time for synchronization in case of NTPv4 is 15 to 20 minutes.

To achieve faster NTP synchronization, enable the burst or iburst mode by using the burst or iburst keyword. With the **burst** or **iburst** mode configured, NTP synchronization takes about 1 to 2 minutes to sync.

Step 1	`Sup# ntp server [burst] [iburst]`	**burst** enables burst mode. Burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval in order to reduce the effects of network jitter. **iburst** enables initial burst (iburst) mode. Iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This feature allows rapid time setting at system startup or when an association is configured.

For further details, please refer to the *Cisco IOS Network Management Command Reference* for NTP commands.

Configuring Remote Console and Logging

The command line interface (CLI) is the primary interface for configuring and managing the SAMI processors. The CLI is designed for a single processor system, therefore, on a multiprocessor system such as the SAMI, managing and monitoring the processors on a module requires that you establish a session with each processor.

For a description of the various Cisco SAMI CLIs, see "Using the Command-Line Interfaces" section on page A-1.

Establishing a session with each PPC on each SAMI in a Cisco 7600 Series Router chassis. can be a cumbersome task. To facilitate the management and monitoring of the multiple SAMI processors, the remote console and logging (RCAL) feature enables you to use the supervisor console as a single connection point, from which you can control debugging, display **show** command output, and view logging output from all the PPCs on a SAMI (and/or all SAMIs in a chassis) without having to establish a session with each PPC.

To use RCAL to manage and monitor SAMI processors, complete the tasks in the following sections:

- Configuring RCAL Support on the Supervisor, page 3-21

Configuring RCAL Support on the Supervisor

The supervisor functions as the RCAL client—receiving messages sent by the SAMI processors. When configuring a supervisor as an RCAL client, you specify the port on which to receive system messages from the SAMI processors, and configure the level of messages to receive and display (levels below are filtered).

To configure the supervisor as an RCAL client, use the following commands beginning in global configuration mode at the supervisor console:

	Command	Purpose
Step 1	`Sup# configure terminal`	Enters global configuration mode.
Step 2	`Sup(config)# logging listen` *udp_port*	Configures the port on which the supervisor listens for system messages from the SAMI processors on which RCAL is enabled. **Note** The UDP port specified must match the port specified on the SAMI processors using the **logging main-cpu** global configuration command. We recommend that you use port 4000. If a port other than 4000 is used, RCAL to SAMI processor 0 does not work.
Step 3	`Sup(config)# sami module` {*mod_num* | **all** {**cpu** {*cpu_num* | **all**} **logging** *severity*	Specifies the RCAL server (or servers) from which to receive system messages, and configures the level of system messages to receive on the supervisor, where: • *mod_num*—Number of the slot in which the SAMI is installed. • **all**—Specifies all SAMIs installed in the chassis. • **cpu** {*cpu-num* | **all**} – *cpu_num*—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. By default, the supervisor receives all system messages sent by SAMI processors. To define the level of messages sent by a processor to the supervisor, establish a session with the processor and use the **logging main-cpu** global configuration command. For a list of severity levels, see Table 3-1.
Step 4	`Sup(config)# exit`	Exits global configuration mode.

Table 3-1 lists the logging levels.

Table 3-1 Severity Level Definitions

Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

Configuring RCAL Support on a SAMI PPC

Note By default, RCAL support is enabled on SAMI COSLI PPCs. Therefore, to use RCAL, no configuration tasks are required on the SAMI COSLI PPC.

When RCAL is enabled on a SAMI PPC, the SAMI PPC functions as an RCAL server. When configuring a SAMI PPC to function as an RCAL server, you can define the level of system messages to send to the RCAL client.

By default, RCAL is enabled on PPCs 3 through 8 using port 4000 for severity level errors (level 3) and the EXEC command.

Note The log level defined on the supervisor when specifying an RCAL client (**sami module** global configuration command) can be used to filter out all of the messages below a certain severity level.

To configure RCAL support on a SAMI PPCs 3 through 8, use the following commands beginning in privileged EXEC mode at the supervisor console:

	Command	Purpose
Step 1	`Sup# session slot slot_number processor proc_number`	Establishes a session to a SAMI PPC.
Step 2	`Router> enable`	Enters privilege EXEC mode.
Step 3	`Router# configure`	Enters global configuration mode.
Step 4	`Router(config)# logging main-cpu udp_port [log_level] ip_address`	Enables logs to be generated and sent to the supervisor at and above the specified level. By default, RCAL is enabled on a processor and the processor sends messages for level 3 and above. For a list of severity levels, see Table 3-1. **Note** The UDP port specified must match the port specified on the supervisor. By default, port 4000 is used. Optionally, a VLAN IP address can be specified for transporting this traffic from PPCs 3-8.
Step 5	`Router(config)# exit`	Exits global configuration mode.

Configuring RCAL Support on the SAMI LCP

To configure RCAL support on the SAMI LCP (processor 0), use the following commands beginning in privileged EXEC mode at the supervisor console:

	Command	Purpose
Step 1	`Sup# session slot slot_number processor 0`	Establishes a session to the SAMI LCP.
Step 2	`switch# config`	Enters global configuration mode.
Step 3	`switch(config)# logging enable`	Enables logging to send syslog messages to one or more output locations.
Step 4	`switch(config)# logging supervisor level`	Sets the severity level at which syslog messages are sent to the supervisor. The default is level 3.

Using RCAL

After the supervisor and SAMI processors are enabled for RCAL, you can execute certain commands to the SAMI LCP or SAMI PPC directly from the supervisor console. The command set that you can issue depends on whether you are executing the commands remotely to a SAMI LCP or SAMI PPC.

Table 3-2 lists the command sets that you can execute remotely from the supervisor to a SAMI PPC (processor numbers 3 through 8).

Table 3-2 PPC RCAL Command Set

Command	Description
clear	Clears counters and statistics
debug	Enables debugging functions
dir	Lists files in a file system
log dir	Logs the **dir** command to syslog
log show	Logs the **show** command to syslog
log systat	Logs the **systat** command to syslog
ping *ip_address*	Executes a ping on a remote processor
set memory	Executes the **set memory debug** command
show	Displays running system information
systat	Displays information about terminal lines
undebug	Disables debugging functions

Table 3-3 lists the command sets that you can execute remotely from the supervisor to a SAMI LCP (processor number 0).

Table 3-3 LCP RCAL Command Set

Command	Description
clear	Clears counters and statistics
confreg	Sets the config register for processors
console-select	Specifies console selection for front panel consoles DB1 and DB2
reload	Reloads the entire SAMI or SAMIs
show	Displays system information

To execute a command to a SAMI PCC from the supervisor, use the following commands beginning in privileged EXEC mode from the supervisor console:

Step 1	`Sup> enable`	Enables privileged EXEC mode.
Step 2	`Sup# configure terminal`	Enters global configuration mode.
Step 3	`Sup(config)# execute-on {{slot_num [, slot_number] | all-mwams | all-samis} {cpu_number [,cpu_num] | all | all-ppc} command}}`	Executes commands remotely when RCAL is enabled, where: • *slot_num*—Specifies the number of the slot in which the module is installed. Optionally, you can specify additional slot numbers, separated by a comma (,). • **all-mwam**—Specifies all Cisco Multiprocessor WAN Application Modules (MWAMs) in the chassis. • **all-sami**—Specifies all SAMIs in the router chassis. • *cpu_num*—Specifies the processor number. 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**—Executes the command on all processors. • **all-ppc**—Executes the command on all SAMI processors 3 through 8. • *command*—Specifies the command to execute on the processor remotely. Table 3-2 lists commands supported for the PPC. Table 3-3 lists supported LCP commands.

Note When you specify a keyword option that applies to multiple processors (**all-mwam**, **all-sami**, **all**, and **all-ppc**), the command is executed on active processors but is not executed on processors that are inactive. To show the processor state, use the **show logging slot** command.

Logs received by the supervisor are prefixed with hostname information that identifies which PPC generated the log.

For example:

- Processor 5 on a SAMI in slot 6 generates the following error message:

```
SAMI 06/5: 00:02:05: %SNMP-5-MODULETRAP: Module 6 [Up] Trap
```

- Processor 4 on a SAMI in slot 2 generates the following debug message:

```
SAMI 02/4: 00:03:42: ICMP: echo reply sent, src 10.10.10.2, dst 10.10.10.1
```

At the supervisor, the logs can be directed to one or more destinations including console, buffer, or syslog.

Usage Notes

When using RCAL, note the following:

- To prevent the supervisor CPU from being overloaded when the command output is expected to exceed more than 100 lines, two options are available:
  a. Ensure that the logging console feature is configured as follows:

     ```
     no logging console guaranteed
     ```

     This configuration allows the output to be dropped when the console backs up. This is the default configuration.
  b. Configure the logging console debug as follows:

     ```
     no logging console debug
     ```

     This configuration directs the output to other logging endpoints, such as buffer or syslog.
- To display logging information for all PPCs on all SAMIs in a router chassis with one command from the supervisor:
  a. Configure the PPCs to locally store logs (in each processor).
  b. Set the buffer logging level on each processor to include the required level of information (the default setting is the debug level).
  c. Display the logs for all the PPCs for all SAMIs in the router chassis, enter the following commands:

     ```
     Sup# execute-on all-samis all-ppc show logging
     ```

- To display the software image versions running on all the PPCs in a chassis with one command from the supervisor, use the following command:

```
Sup# execute-on all-samis all-ppc show version

----------- Slot 3/CPU 3, show ver-------------
Cisco Internetwork Operating System Software
IOS (tm) SAMI Software (SAMI-G7IS-M), Experimental Version

----------- Slot 3/CPU 4, show ver-------------
Cisco Internetwork Operating System Software
IOS (tm) SAMI Software (SAMI-G7IS-M), Experimental Version
```

Tip To minimize command output, you can use the pipe (|) support to include only lines of text that match the regular expression following the pipe. For example:

```
Sup# execute-on |
```

To display logging status and counters for all processors on a SAMI using RCAL, use the **show logging slot** command.

Configuring the Cisco Software Application on a SAMI PPC

To configure a Cisco software application on a SAMI PPC, use the following commands beginning in global configuration mode at the supervisor console:

	Command	Purpose
Step 1	`Sup# session slot slot_number processor proc_number`	Establishes a session to a PPC on the SAMI, where: • *slot_number*—Number of the slot in which the SAMI is installed. • *proc_number*—Number of the PPC on the SAMI. Valid values are 3 through 8. One session per processor can be established.
Step 2	`Router> enable` **Note** If establishing a session to a COSLI PPC, skip this step and proceed to Step 3.	Enters privilege EXEC mode.
Step 3	`Router# config`	Enters global configuration mode.
Step 4	`Router(config)#` Configure the application as outlined in the application documentation.	Refer to the Cisco software application documentation (see the "Related Documentation" section on page 9).
Step 5	`Router(config)# exit`	Exits global configuration mode.
Step 6	`Router# copy running-config startup-config`	Copies the running configuration to NVRAM on the SAMI (if in local mode) or supervisor bootflash (if in supervisor mode).

The following example shows how to establish a session to a SAMI Cisco IOS PPC and begin configuring a Cisco software application:

```
Sup> enable
Sup# session slot 6 processor 4
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.64 ... Open

Router> enable
Router# config
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Enter application configuration commands. For information on configuring your application, see the documentation for the application list in "Related Documentation" section on page -9.

```
Router(config)# exit
```

Note In the example above, the "64" part of IP address indicates slot 6, processor 4.

The following example shows how to make a backup of the configuration after the application is configured.

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

L2 Connectivity Between SAMIs

SAMI does not support L2 connectivity among processors of the same card. The only exception to this is if the SAMI is running the Cisco Broadband Wireless Gateway 2.0 image, and the Supervisor is running SRE.

If you require connectivity among processors of the same card, then it needs to be provided at L3, with the Supervisor routing packets between the different SAMI processors. This requires the following configurations on the Supervisor and the SAMI processors.

1. The IP addresses used for inter-processor connectivity have to be from different IP subnets.
2. Each processor needs to have a different VLAN (i.e., different Gi0/0 sub-interface) for the purpose of inter-processor connectivity. In order to force the inter-processor traffic to be routed at L3 by the Supervisor, each processor should only contain the sub-interface corresponding to its own VLAN.
3. On the Supervisor, L3 VLAN interfaces need to be configured corresponding to each of the 6 VLANs configured on the SAMI processors in the previous step.
4. IP connectivity between the SAMI processor sub-interface and the corresponding L3 VLAN interfaces on the Supervisor needs to be verified for all SAMI processors.
5. Either static routes need to be configured on the Supervisor, or a dynamic routing protocol needs to be run on the Supervisor, and each of the SAMI processors to enable the Supervisor to route traffic between the subnets corresponding to each SAMI processor.

4GB DRAM Support

The SAMI platform supports 4GB DIMMs. Refer to your specific Cisco software application documentation to determine if the application supports 4GB DIMMs.

- Changes are downward compatible—the same image supports 2GB and 4GB configurations.
- Because of the larger available memory, the IOS "Check heaps" process requires higher usage of the CPU. This is reflected as a higher average use of the CPU depending on the heap usage.
- There is no upgrade procedure for 4GB DIMMS. You will have to order and install new cards to upgrade to the 4GB.

SAMI Coredump, Crashinfo and Debuginfo Support

When any of the processors crash (PPC or IXP), the LCP collects the crashinfo and debuginfo files from each of the processors and bundles it together in a tar file. The tar file is stored in the directory core: in the LCP. Execute command **dir core**: from the LCP to check for the crashinfo files.

The .tar file contains the following information:

- Crashinfo of the PPC crashed and debuginfo of the rest.
- LCP debuginfo.
- Crashinfo of IXP1 and IXP2.
- IXP coredumps (see the"exception ixp" section on page E-17 to enable coredump collection for IXPs).

The tar filename will have the following format

crashinfo_collection-%Y%m%d-%H%M%S.tar

So, for example, crashinfo_collection-20100506-160941.tar means the tar file was created on May 6, 2010 at 16:09:41 hours

The following list identifies the contents of the above example tar file. In this instance, processor 3 reloads. Additionally, IXP coredump collection is enabled for both IXPs

crashinfo_proc3_20100506-160534

debuginfo_proc4_20100506-160535

debuginfo_proc5_20100506-160535

debuginfo_proc6_20100506-160535

debuginfo_proc7_20100506-160536

debuginfo_proc8_20100506-160536

debuginfo_proc0-20100506-160941

coredump_proc1-20100506-160941.gz

coredump_proc2-20100506-160941.gz

qnx_1_mecore_ucdump

qnx_2_mecore_ucdump

Note Please ensure that you have enough space in LCP core:/ directory to store the tar file.

- To find out how much free space is available, use the **dir core**: command from the LCP console.
- To delete files from LCP core use the **delete core**: *filename* command.
- To delete all the files at once use the **clear core** command.

Debug Info Generation During RF-Induced Reload

An RF-Induced reload occurs when the redundancy facility identifies a failure in the system. For example, when there is a communication issues between the redundant systems. Previously, the SAMI would simply reload, and the information about the condition of the system before the SAMI reloaded were lost. Now, the SAMI can write debug info during RF-Induced reload. This provides information regarding the state of the system before the SAMI reloaded. Debuginfo generation will lead to a slower reload of the SAMI.

Singleip

Redundancy-Facility induced reloads cause the PPCs and LCP to write debuginfo, and the IXP to write crashinfo and coredump if configured. All of the debuginfo, crashinfo and coredump files are collected and stored together as **crashinfo_collection.tar** in the LCP core directory. This behaviour is similar to the behaviour seen in the case of PPC - IXP Health-monitoring failure.