Onboard Failure Logging on Cisco IOS XR Software

OBFL gathers boot, environmental, and critical hardware data for field-replaceable units (FRUs), and stores the information in the nonvolatile memory of the FRU. This information is used for troubleshooting, testing, and diagnosis if a failure or other error occurs, providing improved accuracy in hardware troubleshooting and root cause isolation analysis. Stored OBFL data can be retrieved in the event of a failure and is accessible even if the card does not boot.

Because OBFL is on by default, data is collected and stored as soon as the card is installed. If a problem occurs, the data can provide information about historical environmental conditions, uptime, downtime, errors, and other operating conditions.

Caution OBFL is activated by default in all cards. Do not deactivate OBFL without specific reasons, because the OBFL data is used to diagnose and resolve problems in FRUs.

Note For information about OBFL commands, console logging, alarms, and logging correlation, see Related Documents, page MNC-323.

Feature History for Implementing OBFL on Cisco IOS XR Software

Release	Modification
Release 3.4.0	This feature was introduced on the Cisco CRS-1.
Release 3.4.1	Message severity levels were added.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Contents

- Prerequisites, page MNC-314
- Information About OBFL, page MNC-314

- How to Implement OBFL, page MNC-317
- Configuration Examples for OBFL, page MNC-322
- Where to Go Next, page MNC-323
- Additional References, page MNC-323

Prerequisites

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About OBFL

To implement logging services, you need to understand the following concepts:

- Data Collection Types, page MNC-314
- Supported Cards and Platforms, page MNC-316
- Syslog Message Severity Level Definitions, page MNC-316

Data Collection Types

OBFL collects and stores both baseline and event- driven information in the nonvolatile memory of each supported card where OBFL is enabled. The data collected includes the following:

- FRU part serial number
- OS version
- Boot time
- Total run time (hours in use)
- Boot status
- Temperature and voltage at boot
- Temperature and voltage history
- Other board specific errors

This data is collected in two different ways: as baseline data and event- driven data:

- Baseline Data Collection, page MNC-315
- Event-Driven Data Collection, page MNC-315

Baseline Data Collection

Baseline data is stored independent of hardware or software failures. This includes:

Data Type	Details
Installation	Chassis name and slot number are stored at initial boot and for the most recent nine boots.
Temperature	Inlet and hotpoint temperatures are recorded 10 minutes after boot.
Run-time	Total run-time since initial installation. This is based on the local router clock with a granularity of 30 minutes.

Event-Driven Data Collection

Event driven data include card failure events. Failure events are card crashes, memory errors, ASIC resets, and similar hardware failure indications.

Data Type	Details	
Environmental Errors	Temperature Errors	Inlet and hot point temperature errors
	Voltage Errors	+5, and MBUS +5, +3.3, and +2.2 voltage errors
		An environmental reading is logged when the following temperature or voltage events occur: • Exceed the normal range • Change more than 10% • Return within range for more than five minutes. On reboot, these environmental readings are consolidated into a single environmental history record that shows the duration and extent out of normal range for a consecutive set of environmental readings.

Data Type	Details	
Calendar Time	Disabled	The time when OBFL logging was disabled with the **hw-module** {**all** | **subslot** *node-id*} **logging onboard disable** command in global configuration or administration configuration mode.
	Cleared	The time when OBFL logging was cleared with the **clear logging onboard** command in EXEC or administration EXEC mode.
	Reset to 0	The time when total line card runtime is reset to zero with the **clear logging onboard** command in EXEC or administration EXEC mode.

Supported Cards and Platforms

OBFL data collection is supported.

FRUs that have sufficient nonvolatile memory available for OBFL data storage support OBFL. For example, the processor supports the OBFL.

Table 33 OBFL Support by Card Type

Card Type	Cisco CRS-1
Route processor (RP)	Supported
Distributed route processor (DRP)	Supported
Modular service card (MSC)	Supported
Switch fabric cards (SFC)	Supported
Power supply cards: AC rectifier modules and DC power entry modules (PEMs)	Supported
Fan controller cards	Supported
Alarm modules	Supported
Optical interface module (OIM) and light emitting diode (LED)	Supported
Shared port adapters (SPA)	Supported
Physical layer interface module (PLIM)	Not Supported

Syslog Message Severity Level Definitions

By default, OBFL data is collected for alert and emergency messages.

How to Implement OBFL

OBFL logging is configured for the router. If a new node is inserted, and OBFL is enabled for that slot or for all slots, then OBFL is enabled for the new node. If a card is removed from a router and inserted into a different router, the card assumes the OBFL configuration for the new router.

This section contains the following procedures:

- Enabling or Disabling OBFL, page MNC-317
- Configuring Message Severity Levels, page MNC-318
- Monitoring and Maintaining OBFL, page MNC-320

Enabling or Disabling OBFL

OBFL is enabled for all nodes by default and is active until disabled for a specified node or for all nodes.

Caution Do not deactivate OBFL without specific reasons since the OBFL data is used to diagnose and resolve problems in FRUs.

There are no configuration requirements other than to enable and disable OBFL.

SUMMARY STEPS

1. **admin**
2. **configure**
3. **hw-module** {**all** | **subslot** *node-id*} **logging onboard disable**
4. **no hw-module** {**all** | **subslot** *node-id*} **logging onboard disable**
5. **end**
   or
   commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.

Step 2	**configure**
	
	Example:
	`RP/0/RP0/CPU0:router(admin)# configure`
	`RP/0/RP0/CPU0:router(admin-config)#`
		Enters administration configuration mode.

	Command or Action	Purpose

Step 3	**hw-module** {**all** | **subslot** *node-id*} **logging onboard disable**
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config)# hw-module all logging onboard disable`
	
	or
	
	`RP/0/RP0/CPU0:router(admin-config)# hw-module subslot 0/2/1 logging onboard disable`
		(Optional) Disables OBFL. Existing OBFL data is preserved, but no new data is collected.
		• Use the **all** keyword to disable OBFL data collection for all nodes.
		• Use the **subslot** *node-id* keyword and argument to disable OBFL data collection for a specific node. The *node-id* argument is entered in the *rack/slot/module* notation.

Step 4	**no hw-module** {**all** | **subslot** *node-id*} **logging onboard disable** **Example:** `RP/0/RP0/CPU0:router(admin-config)# no hw-module all logging onboard disable`	(Optional) Enables OBFL on the FRU and resets the message severity level to the default (**alert**). • Use the **all** keyword to collect OBFL data for all nodes. • Use the **subslot** *node-id* keyword and argument to enable OBFL for a specific node. The *node-id* argument is entered in the *rack/slot/module* notation.

Step 5	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config)# end`
	or
	`RP/0/RP0/CPU0:router(admin-config)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		– Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		– Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring Message Severity Levels

Perform this task to configure message severity levels.

SUMMARY STEPS

1. **admin**
2. **configure**

3. **hw-module** {**all** | **subslot** *node-id*} **logging onboard** [**disable** | **severity** {**alerts** | **emergencies**}]
4. **end**
   or
   commit

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.

Step 2	**configure**
	
	Example:
	`RP/0/RP0/CPU0:router(admin)# configure`
	`RP/0/RP0/CPU0:router(admin-config)#`
		Enters administration configuration mode.

	Command or Action	Purpose
Step 3	**hw-module** {**all** | **subslot** *node-id*} **logging onboard** [**disable** | **severity** {**alerts** | **emergencies**}] **Example:** `RP/0/RP0/CPU0:router(admin-config)# hw-module all logging onboard severity alerts`	Configures the severity level for the syslog messages that are logged into the OBFL storage device. • Use the **severity** keyword to specify the severity for the syslog message that is logged into the OBFL storage device. • Use the **alerts** keyword to specify that both emergency and alert syslog messages are logged. The default is the **alerts** keyword. • Use the **emergencies** keyword to specify only the emergency syslog messages are logged.

Step 4	**end**
	or
	commit
	
	Example:
	`RP/0/RP0/CPU0:router(admin-config)# end`
	or
	`RP/0/RP0/CPU0:router(admin-config)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		– Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		– Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Monitoring and Maintaining OBFL

Use the commands described in this section to display the status of OBFL, and the data collected by OBFL. Enter these commands in EXEC or administration EXEC mode.

SUMMARY STEPS

1. **admin**
2. **show logging onboard** [**all** | **cbc** {**dump-all** | **dump-range** {*start-address* | *end-address* | **most-recent** {**fans** *fan-tray-slot* | [**location** *node-id*]} | **diagnostic** | **environment** | **error** | **temperature** | **uptime** | **verbose** | **voltage**] [**continuous** | **historical** | **static-data**] [**detail** | **raw** | **summary**] [**location** *node-id*]

3. **show processes include obfl**
4. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**admin** **Example:** `RP/0/RP0/CPU0:router# admin`	Enters administration EXEC mode.
Step 2	**show logging onboard** [**all** | *cbc* {**dump-all** | **dump-range** {*start-address* | *end-address* | **most-recent** {**fans** *fan-tray-slot* | [**location** *node-id*]} | **diagnostic** | **environment** | **error** | **temperature** | **uptime** | **verbose** | **voltage**] [**continuous** | **historical** | **static-data**] [**detail** | **raw** | **summary**] [**location** *node-id*] **Example:** `RP/0/RP0/CPU0:router(admin)# show logging onboard uptime`	Displays stored OBFL data for all nodes or for a specified node. See the "Onboard Failure Logging Commands on Cisco IOS XR Software" module of *Onboard Failure Logging Commands on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco CRS-1 Router*.
Step 3	**show processes include obfl** **Example:** `RP/0/RP0/CPU0:router# show processes include obfl`	Confirms that the OBFL environmental monitor process is operating.
Step 4	**show running-config** **Example:** `RP/0/RP0/CPU0:router# show running-config`	Displays the status of OBFL configuration.

Clearing OBFL Data

To erase all OBFL data on a specific card or on all cards, use the following command:

clear logging onboard [**all** | **cbc** {**dump-all** | **dump-range** {*start-address* | *end-address* | **most-recent** {**fans** *fan-tray-slot* | [**location** *node-id*]} | **corrupted-files** | **diagnostic** | **environment** | **error** | **poweron-time** | **temperature** | **uptime** | **voltage**] [**location** *node-id*]

Caution The **clear logging onboard** command permanently deletes all OBFL data for a node or for all nodes. Do not clear the OBFL logs without specific reasons because the OBFL data is used to diagnose and resolve problems in FRUs.

Caution If OBFL is actively running on a card, issuing the **clear logging onboard** command can result in a corrupt or incomplete log at a later point in time. OBFL should always be disabled before this command is issued.

For more information, see the *Onboard Failure Logging Commands on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco CRS-1 Router*.

Configuration Examples for OBFL

This section provides the following configuration examples:

- Enabling and Disabling OBFL: Example, page MNC-322
- Configuring Message Severity Levels: Example, page MNC-322
- Clearing OBFL Messages: Example, page MNC-322
- Displaying OBFL Data: Example, page MNC-323

Enabling and Disabling OBFL: Example

The following example shows how to disable OBFL:

```
RP/0/RP0/CPU0:router(admin-config)# hw-module all logging onboard disable
```

The following example shows how to enable OBFL again:

```
RP/0/RP0/CPU0:router(admin-config)# no hw-module all logging onboard disable
```

The following example shows that OBFL is enabled and message severity level is reset to the default:

```
RP/0/RP0/CPU0:router(admin-config)# no hw-module all logging onboard
```

Configuring Message Severity Levels: Example

The following example shows how to save only the syslog message in which the severity level is set to 0 (emergency) to a storage device:

```
RP/0/RP0/CPU0:router(admin-config)# hw-module subslot 0/2/CPU0 logging onboard severity
emergencies
```

The following example shows how to save the syslog message in which the severity level is set to 0 (emergency) and 1 (alert) to a storage device:

```
RP/0/RP0/CPU0:router(admin-config)# hw-module subslot 0/2/CPU0 logging onboard severity
alerts
```

Clearing OBFL Messages: Example

In the following example, all OBFL messages are cleared for all nodes in the system:

```
RP/0/RP0/CPU0:router(admin)# clear logging onboard
```

Displaying OBFL Data: Example

The following example shows how to display uptime information from the OBFL feature:

```
RP/0/RP0/CPU0:router(admin)# show logging onboard uptime detail location 0/7/cpu0

--------------------------------------------------------------------------------
UPTIME CONTINUOUS DETAIL INFORMATION (Node: node0_7_CPU0)
--------------------------------------------------------------------------------
The first record     : 01/05/2009 00:58:41
The last record      : 01/17/2007916:07:13
Number of records    :        478
File size            :      15288 bytes
Current reset reason : 0x00
Current uptime       :    0 years  0 weeks 0 days  3 hours  0 minutes
--------------------------------------------------------------------------------
Time Stamp          |
MM/DD/YYYY HH:MM:SS | Users operation
--------------------------------------------------------------------------------
01/05/2009 01:44:35   File cleared by user request.
--------------------------------------------------------------------------------
```

Where to Go Next

To configure logging services for terminal display, see *Implementing Logging Services on Cisco IOS XR Software.*

To configure alarm log correlation, see *Implementing and Monitoring Alarms and Alarm Log Correlation on Cisco IOS XR Software*.

Additional References

The following sections provide references related to implementing logging services.

Related Documents

Related Topic	Document Title
OBFL commands	*Onboard Failure Logging Commands on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco CRS-1 Router*
Alarm and logging correlation commands	*Alarm Management and Logging Correlation Commands on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco CRS-1 Router*
Alarm and logging correlation configuration and monitoring tasks	*Implementing and Monitoring Alarms and Alarm Log Correlation on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco CRS-1 Router*

Related Topic	Document Title
Logging services configuration tasks	*Implementing Logging Services on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco CRS-1 Router*
Logging services commands	*Logging Services Commands on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco CRS-1 Router*
SNMP commands	*SNMP Commands on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco CRS-1 Router*
SNMP configuration tasks	*Implementing SNMP on Cisco IOS XR Software* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco CRS-1 Router*
Cisco IOS XR getting started material	*Cisco IOS XR Getting Started Guide for the Cisco CRS-1 Router*
Information about user groups and task IDs	*Configuring AAA Services on Cisco IOS XR Software* module in the *Cisco IOS XR System Security Configuration Guide for the Cisco CRS-1 Router*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport