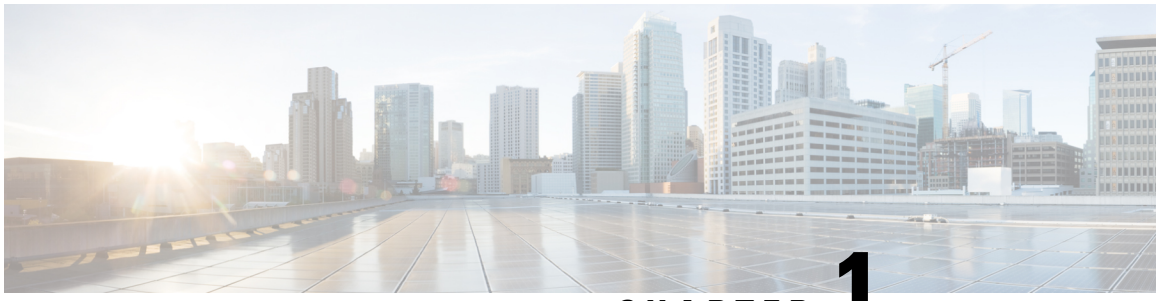
Network Management Systems Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 Series)

First Published: 2019-11-14

Last Modified: 2020-01-12

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

CONTENTS



CHAPTER 1

Configuration of Onboard Failure Logging

This chapter describes how to configure Onboard Failure Logging (OBFL).

Restrictions for OBFL

- Software Restrictions—If a device (router or switch) intends to use *linear* flash memory as its OBFL storage media, Cisco IOS software must reserve a minimum of two physical sectors (or physical blocks) for the OBFL feature. Because an erase operation for a linear flash device is done on per-sector (or per-block) basis, one extra physical sector is needed. Otherwise, the minimum amount of space reserved for the OBFL feature on any device must be at least 8 KB.
- Hardware Restrictions—To support the OBFL feature, a device must have at least 8 KB of nonvolatile memory space reserved for OBFL data logging.

Overview of OBFL

The Onboard Failure Logging (OBFL) feature collects data such as operating temperatures, hardware uptime, interrupts, and other important events and messages from system hardware installed in a Cisco router or switch. The data is stored in nonvolatile memory and helps technical personnel diagnose hardware problems.

Data Collected by OBFL

The OBFL feature records operating temperatures, hardware uptime, interrupts, and other important events and messages that can assist with diagnosing problems with hardware cards (or modules)installed in a Cisco router or switch. Data is logged to files stored in nonvolatile memory. When the onboard hardware is started up, a first record is made for each area monitored and becomes a base value for subsequent records. The OBFL feature provides a circular updating scheme for collecting continuous records and archiving older (historical) records, ensuring accurate data about the system. Data is recorded in one of two formats: continuous information

that displays a snapshot of measurements and samples in a continuous file, and summary information that provides details about the data being collected. The data is displayed using the show logging onboard command. The message “No historical data to display” is seen when historical data is not available.

The following sections describe the type of data collected:

Temperature

Temperatures surrounding hardware modules can exceed recommended safe operating ranges and cause system problems such as packet drops. Higher than recommended operating temperatures can also accelerate component degradation and affect device reliability. Monitoring temperatures is important for maintaining environmental control and system reliability. Once a temperature sample is logged, the sample becomes the base value for the next record. From that point on, temperatures are recorded either when there are changes from the previous record or if the maximum storage time is exceeded. Temperatures are measured and recorded in degrees Celsius.

Example for Temperature

```
Router# show logging onboard slot <R0/R1> temperature
Name              Id     Data (C)  Poll      Last Update
-------------------------------------------------------------------------
Temp: FC PWM1     80           24  1         01/31/12 14:36:30
Temp: FC PWM1     80           25  1         01/31/12 14:37:30
Temp: FC PWM1     80           23  1         01/31/12 14:38:30
Temp: FC PWM1     80           25  1         01/31/12 14:40:30
Temp: FC PWM1     80           24  1         01/31/12 14:41:30
Temp: FC PWM1     80           25  1         01/31/12 14:43:31
Temp: FC PWM1     80           23  1         01/31/12 14:46:31
Temp: FC PWM1     80           25  1         01/31/12 14:50:31
Temp: FC PWM1     80           24  1         01/31/12 14:54:31
Temp: FC PWM1     80           26  1         01/31/12 14:56:31
Temp: FC PWM1     80           24  1         01/31/12 14:57:31
Temp: FC PWM1     80           26  1         01/31/12 15:00:31
Temp: FC PWM1     80           24  1         01/31/12 15:02:31
Temp: FC PWM1     80           25  1         01/31/12 15:03:31
Temp: FC PWM1     80           24  1         01/31/12 15:04:32
Temp: FC PWM1     80           26  1         01/31/12 15:08:32
Temp: FC PWM1     80           24  1         01/31/12 15:11:32
```

To interpret this data:

- A column for each sensor is displayed with temperatures listed under the number of each sensor, as available.
- The ID column lists an assigned identifier for the sensor.
- Temp indicates a recorded temperature in degrees Celsius in the historical record. Columns following show the total time each sensor has recorded that temperature.
- Sensor ID is an assigned number, so that temperatures for the same sensor can be stored together.
- Poll indicates the number of times a given sensor has been polled.
- The Last Update column provides the most recent time that the data was updated.

Voltage

OBFL allows you to track the voltage of system components, as shown in the following example.

Example for Voltage

```
Router# show logging onboard slot R1 voltage
Name               Id    Data (mV)  Poll      Last Update
-------------------------------------------------------------------
VNILE: VX1         20         1002  1         01/30/12 03:45:46
VNILE: VX2         21         1009  1         01/30/12 03:45:46
VNILE: VX3         22         1492  1         01/30/12 03:45:46
VNILE: VX4         23         1203  1         01/30/12 03:45:46
VNILE: VP1         24         1790  1         01/30/12 03:45:46
VNILE: VP2         25         2528  1         01/30/12 03:45:47
VNILE: VP3         26         3305  1         01/30/12 03:45:47
VNILE: VH          27        12076  1         01/30/12 03:45:47
VCPU : VX1         32          997  1         01/30/12 03:45:47
VCPU : VX2         33         1054  1         01/30/12 03:45:47
VCPU : VX3         34         1217  1         01/30/12 03:45:47
VCPU : VX4         35         1526  1         01/30/12 03:45:47
VCPU : VP1         36         4992  1         01/30/12 03:45:47
VCPU : VP2         37         3368  1         01/30/12 03:45:47
VCPU : VP3         38         2490  1         01/30/12 03:45:47
VCPU : VP4         39         1803  1         01/30/12 03:45:48
VCPU : VH          40        12034  1         01/30/12 03:45:48
VNILE: VX1         20         1001  1         01/30/12 03:48:11
VNILE: VX2         21         1008  1         01/30/12 03:48:11
VNILE: VX3         22         1492  1         01/30/12 03:48:11
VNILE: VX4         23         1200  1         01/30/12 03:48:11
VNILE: VP1         24         1790  1         01/30/12 03:48:11
VNILE: VP2         25         2530  1         01/30/12 03:48:11
VNILE: VP3         26         3305  1         01/30/12 03:48:11
VNILE: VH          27        12066  1         01/30/12 03:48:11
VCPU : VX1         32          997  1         01/30/12 03:48:11
VCPU : VX2         33         1054  1         01/30/12 03:48:11
VCPU : VX3         34         1218  1         01/30/12 03:48:11
VCPU : VX4         35         1526  1         01/30/12 03:48:11
```

To interpret this data:

- The Name and ID fields identify the system component.
- The Data (mV) indicates the component voltage
- The poll field indicates the number of times the component voltage has been polled.
- A timestamp shows the date and time the message was logged.

Message Logging

The OBFL feature logs standard system messages. Instead of displaying the message to a terminal, the message is written to and stored in a file, so the message can be accessed and read at a later time.

Example for Error Message Log

```
-------------------------------------------------------------------------------
ERROR MESSAGE SUMMARY INFORMATION
-------------------------------------------------------------------------------
Facility-Sev-Name      | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
-------------------------------------------------------------------------------
No historical data to display
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
ERROR MESSAGE CONTINUOUS INFORMATION
```

```
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS Facility-Sev-Name
--------------------------------------------------------------------------------
03/06/2007 22:33:35  %GOLD_OBFL-3-GOLD : Diagnostic OBFL: Diagnostic OBFL testing
```

To interpret this data:

- A timestamp shows the date and time the message was logged.
- Facility-Sev-Name is a coded naming scheme for a system message, as follows:
  - The Facility code consists of two or more uppercase letters that indicate the hardware device (facility) to which the message refers.
  - Sev is a single-digit code from 1 to 7 that reflects the severity of the message.
  - Name is one or two code names separated by a hyphen that describe the part of the system from where the message is coming.
- The error message follows the Facility-Sev-Name codes. For more information about system messages, see the Cisco System Messages.
- Count indicates the number of instances of this message that is allowed in the history file. Once that number of instances has been recorded, the oldest instance will be removed from the history file to make room for new ones.
- The Persistence Flag gives a message priority over others that do not have the flag set.

Enabling OBFL

Note The OBFL feature is enabled by default. Because of the valuable information this feature offers technical personnel, it should not be disabled. If you find the feature has been disabled, use the following steps to reenable it.

SUMMARY STEPS

1. Router# **enable**
2. Router# **configure terminal**
3. Router(config)# **hw-module slot {R0 | R1} logging onboard enable**
4. Router(config)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **enable**	Enables privileged EXEC mode (enter your password if prompted).
Step 2	Router# **configure terminal**	Enters global configuration mode.
Step 3	Router(config)# **hw-module slot {R0 | R1} logging onboard enable** **Example:**	Enables OBFL on the specified hardware module.

	Command or Action	Purpose
	`hw-module slot R0 logging onboard enable`	
Step 4	Router(config)# **end**	Ends global configuration mode.

Disabling OBFL

SUMMARY STEPS

1. Router# **enable**
2. Router# **configure terminal**
3. Router(config)# **hw-module slot {R0 | R1} logging onboard disable**
4. Router(config)# **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **enable**	Enables privileged EXEC mode (enter your password if prompted).
Step 2	Router# **configure terminal**	Enters global configuration mode.
Step 3	Router(config)# **hw-module slot {R0 | R1} logging onboard disable** **Example:** `hw-module slot R0 logging onboard disable`	Enables OBFL on the specified hardware module.
Step 4	Router(config)# **end**	Ends global configuration mode.

Displaying OBFL Information

You can use the following commands to display OBFL information:

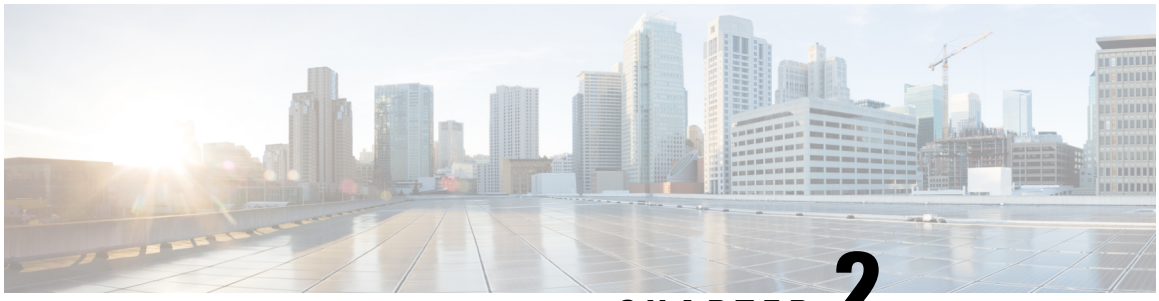
- show logging onboard slot status—To display the slot status.
- show logging onboard slot temperature—To display the slot temperature.
- show logging onboard slot voltage—To display the slot voltage.
- show logging onboard slot hw_errors—To display any hardware error in the setup.

Clearing OBFL Information

You can use the **clear logging onboard slot {R0 | R1} {temperature | voltage}** command to clear OBFL data:

Router#**clear logging onboard slot R1 voltage**

You can use the **show logging onboard temperature** or **show logging onboard voltage** command to verify that the OBFL data is cleared.



CHAPTER 2

Configuring TCAM Threshold Based Alarms

The Ternary Content-Addressable Memory (TCAM) threshold based alarms feature generates syslog and consequently a Simple Network Management Protocol (SNMP) trap when an application reaches the preset threshold for its allotted TCAM size. Alarms and traps are generated when the threshold value for the TCAM is reached.

New and Changed Information

Table 1: New and Changed Features

Feature	Description	Changed in Release	Where Documented
TCAM Threshold Based Alarms	This feature generates a Syslog and consequently a SNMP trap when the number of entries for an application on TCAM becomes equal or greater than a preset threshold level.	Cisco IOS XE Release 3.11S	• Information on TCAM Threshold Based Alarms, on page 8 • Configuring TCAM Threshold Based Alarms, on page 8
TCAM Threshold Based Alarm Frequency	This enhancement configures the frequency at which the TCAM Threshold based alarm should be generated.	Cisco IOS XE Release 3.12	• Information on TCAM Threshold Based Alarm Frequency, on page 8 • Configuring TCAM Threshold Based Alarms, on page 8

Information on TCAM Threshold Based Alarms

This feature generates a Syslog and consequently an SNMP trap when the number of entries for an application on TCAM becomes equal to or greater than the threshold percentage of the value defined in the license template. You can configure the threshold percentage value for notification before the TCAM limit specified by the license for an application is exhausted. The default threshold value for all TCAM applications is 80 percent. The frequency of the alert messages is rate limited to avoid flooding the router console when many entries are added or deleted in quick succession.

Note This feature can be enabled or disabled using the **platform tcam-threshold enable** or **no platform tcam-threshold enable** command.

Information on TCAM Threshold Based Alarm Frequency

This feature enables you to configure the frequency at which the TCAM Threshold Based alarm should be generated. You can configure the TCAM Threshold Based alarm frequency only if you have enabled the TCAM Threshold Based alarms.

Note By default, the **platform tcam-threshold alarm-frequency** command appears in the router configuration file with the default alarm frequency value 1.

Configuring TCAM Threshold Based Alarms

To configure TCAM threshold based alarms, complete the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform tcam-threshold enable** [*app-name* | **all**] [*threshold_percentage* | **default**]
4. **platform tcam-threshold alarm-frequency** [*frequency-value* | **default**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**platform tcam-threshold enable** [*app-name* | **all**] [*threshold_percentage* | **default**] **Example:** `Router(config)# platform tcam-threshold enable all 75`	Enables TCAM threshold based alarms. To disable, use the **no platform tcam-threshold enable** command. • *app-name*—Specifies the name of an application. • all—Selects all applications supported on the router. • *threshold_percentage*—Specifies the threshold percentage. • default—Uses the default threshold of 80 percent.
Step 4	**platform tcam-threshold alarm-frequency** [*frequency-value* | **default**] **Example:** `Router(config)# platform tcam-threshold alarm-frequency 75`	Configures the TCAM Threshold Based alarm frequency • *frequency-value*—Specifies the frequency [1 - 75] at which the alarm should be generated per hour. • default—Sets the default value 1.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Verifying TCAM Threshold Based Alarms

- Use the **show platform hardware pp active tcam utilization** *app-name* **detail** *asic-id* command to display the TCAM utilization for the applications.

  Following is a sample output using the **show platform hardware pp active tcam utilization** command to display the TCAM utilization for ACL application on ASIC 0:

```
Router# show platform hardware pp active tcam utilization acl detail 0
```

```
Router Tcam Utilization per Application and Region
ES == Entry size == Number of 80 bit TCAM words

App/Region                Start     Num Avail  ES  Region    Range     Used
     Range     Num Used
-------------------------------------------------------------------------------------------
ACL                      0x8000    0x1000     2   000000    000000    000000
    000000    172

Scale limit: 4000
Threshold configured: 4%
Current usage: 172 (4% approx.)
```

- Use the **show platform hardware pp active tcam usage** command to display the alarm status for the applications:

```
Router# show platform hardware pp active tcam usage
```

```
TCAM Size: Num of 80 bit entries: 0x010000, Number of Blocks: 16

Nile Tcam Application Table
New Column
Thld Alarm State = 1 if Threshold alarm raised, 0 if alarm cleared

App/Region             Start Index      Num Entries      Entry Size       Num
 Regions      Profile ID       Blk_sel_bits4    Bsb3             Bsb2
      Bsb1             Thld Alarm S...
-------------------------------------------------------------------------------
UCASTV4                000000           0x3000           1                34
               19                         0               0
0              0x7        1
MCASTV4                0x3000           0x1000           2                109
                 4                        0               0
0              0x18       0
INGRESS_VLAN_TRANS     0x5000           0x1000           1                25
                16                        0               0
0              0x20       0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Command List, All Releases

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support