Process Health Monitoring

This chapter describes how to manage and monitor the health of various components of your router. It contains the following sections:

Monitoring Control Plane Resources

The following sections explain the of memory and CPU monitoring from the perspective of the Cisco IOS process and the overall control plane:

Avoiding Problems Through Regular Monitoring

Processes should provide monitoring and notification of their status/health to ensure correct operation. When a process fails, a syslog error message is displayed and either the process is restarted or the router is rebooted. A syslog error message is displayed when a monitor detects that a process is stuck or has crashed. If the process can be restarted, it is restarted; else, the router is restarted.

Monitoring system resources enables you to detect potential problems before they occur, thus avoiding outages. The following are the advantages of regular monitoring:

- Lack of memory on line cards that are in operation for a few years can lead to major outages. Monitoring memory usage helps to identify memory issues in the line cards and enables you to prevent an outage.
- Regular monitoring establishes a baseline for a normal system load. You can use this information as a basis for comparison when you upgrade hardware or software—to see if the upgrade has affected resource usage.

Cisco IOS Process Resources

You can view CPU utilization statistics on active processes and see the amount of memory being used in these processes using the **show memory** command and the **show process cpu** command. These commands provide a representation of memory and CPU utilization from the perspective of only the Cisco IOS process; they do not include information for resources on the entire platform. For example, when the **show memory** command is used in a system with 8 GB RAM running a single Cisco IOS process, the following memory usage is displayed:

```
Router# show memory
           Head            Total(b)     Used(b)      Free(b)      Lowest(b)    Largest(b)
Processor  2ABEA4316010    4489061884   314474916    4174586968   3580216380   3512323496
lsmpi_io   2ABFAFF471A8    6295128      6294212      916          916          916
Critical   2ABEB7C72EB0    1024004      92           1023912      1023912      1023912
```

The **show process cpu** command displays Cisco IOS CPU utilization average:

```
Router# show process cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1         583     48054         12  0.00%  0.00%  0.00%   0 Chunk Manager
   2         991    176805          5  0.00%  0.00%  0.00%   0 Load Meter
   3           0         2          0  0.00%  0.00%  0.00%   0 IFCOM Msg Hdlr
   4           0        11          0  0.00%  0.00%  0.00%   0 Retransmission o
   5           0         3          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6      230385    119697       1924  0.00%  0.01%  0.00%   0 Check heaps
   7          49        28       1750  0.00%  0.00%  0.00%   0 Pool Manager
   8           0         2          0  0.00%  0.00%  0.00%   0 Timers
   9       17268    644656         26  0.00%  0.00%  0.00%   0 ARP Input
  10         197    922201          0  0.00%  0.00%  0.00%   0 ARP Background
  11           0         2          0  0.00%  0.00%  0.00%   0 ATM Idle Timer
  12           0         1          0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
  13           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  14           0         1          0  0.00%  0.00%  0.00%   0 Policy Manager
  15           0         2          0  0.00%  0.00%  0.00%   0 DDR Timers
  16           1        15         66  0.00%  0.00%  0.00%   0 Entity MIB API
  17          13      1195         10  0.00%  0.00%  0.00%   0 EEM ED Syslog
  18          93        46       2021  0.00%  0.00%  0.00%   0 PrstVbl
  19           0         1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
```

Overall Control Plane Resources

Control plane memory and CPU utilization on each control processor allows you to keep a tab on the overall control plane resources. You can use the **show platform software status control-processor brief** command (summary view) or the **show platform software status control-processor** command (detailed view) to view control plane memory and CPU utilization information.

All control processors should show status, Healthy. Other possible status values are Warning and Critical. Warning indicates that the router is operational, but that the operating level should be reviewed. Critical implies that the router is nearing failure.

If you see a Warning or Critical status, take the following actions:

- Reduce the static and dynamic loads on the system by reducing the number of elements in the configuration or by limiting the capacity for dynamic services.
- Reduce the number of routes and adjacencies, limit the number of ACLs and other rules, reduce the number of VLANs, and so on.

The following sections describe the fields in the **show platform software status control-processor** command output.

Load Average

Load average represents the process queue or process contention for CPU resources. For example, on a single-core processor, an instantaneous load of 7 would mean that seven processes are ready to run, one of which is currently running. On a dual-core processor, a load of 7 would mean that seven processes are ready to run, two of which are currently running.

Memory Utilization

Memory utilization is represented by the following fields:

- Total—Total line card memory
- Used—Consumed memory
- Free—Available memory
- Committed—Virtual memory committed to processes

CPU Utilization

CPU utilization is an indication of the percentage of time the CPU is busy, and is represented by the following fields:

- CPU—Allocated processor
- User—Non-Linux kernel processes
- System—Linux kernel process
- Nice—Low-priority processes
- Idle—Percentage of time the CPU was inactive
- IRQ—Interrupts
- SIRQ—System Interrupts
- IOwait—Percentage of time CPU was waiting for I/O

Example: show platform software status control-processor Command

The following are some examples of using the **show platform software status control-processor** command:

```
Router# show platform software status control-processor
RP0: online, statistics updated 5 seconds ago
Load Average: healthy
  1-Min: 0.07, status: healthy, under 5.00
  5-Min: 0.11, status: healthy, under 5.00
  15-Min: 0.09, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3971216
  Used: 3415976 (86%)
  Free: 555240 (14%)
```

```
  Committed: 2594412 (65%), status: healthy, under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.40, System:  1.20, Nice:  0.00, Idle: 97.39
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  0.89, System:  0.79, Nice:  0.00, Idle: 98.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  0.80, System:  2.50, Nice:  0.00, Idle: 96.70
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  3.09, System:  6.19, Nice:  0.00, Idle: 90.60
  IRQ:  0.00, SIRQ:  0.09, IOwait:  0.00
CPU4: CPU Utilization (percentage of time spent)
  User:  0.10, System:  0.30, Nice:  0.00, Idle: 99.60
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU5: CPU Utilization (percentage of time spent)
  User:  0.89, System:  1.59, Nice:  0.00, Idle: 97.50
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU6: CPU Utilization (percentage of time spent)
  User:  0.80, System:  1.10, Nice:  0.00, Idle: 98.10
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU7: CPU Utilization (percentage of time spent)
  User:  0.20, System:  3.40, Nice:  0.00, Idle: 96.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00


Router# show platform software status control-processor brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.09   0.10   0.09

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  3971216  3426452 (86%)   544764 (14%)   2595212 (65%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   1.60   0.90   0.00  97.30   0.10   0.10   0.00
         1   0.09   1.29   0.00  98.60   0.00   0.00   0.00
         2   0.10   0.10   0.00  99.79   0.00   0.00   0.00
         3   0.00   0.00   0.00 100.00   0.00   0.00   0.00
         4   0.60   4.90   0.00  94.50   0.00   0.00   0.00
         5   0.70   1.30   0.00  98.00   0.00   0.00   0.00
         6   0.10   0.00   0.00  99.90   0.00   0.00   0.00
         7   1.39   0.49   0.00  98.10   0.00   0.00   0.00
```

Monitoring Hardware Using Alarms

Router Design and Monitoring Hardware

The router sends alarm notifications when problems are detected, allowing you to monitor the network remotely. You do not need to use **show** commands to poll devices on a routine basis; however, you can perform onsite monitoring if you choose.

BootFlash Disk Monitoring

The bootflash disk must have enough free space to store two core dumps. This condition is monitored, and if the bootflash disk is too small to store two core dumps, a syslog alarm is generated, as shown in the following example:

```
Aug 22 13:40:41.038 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 7084440 kB] - Please clean up files on bootflash.
```

The size of the bootflash disk must be at least of the same size as that of the physical memory installed on the router. If this condition is not met, a syslog alarm is generated as shown in the following example:

```
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Flash capacity (8 GB) is insufficient for fault
analysis based on
installed memory of RP (16 GB)
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Please increase the size of installed flash to at
least 16 GB (same as
physical memory size)
```

Approaches for Monitoring Hardware Alarms

- Onsite Network Administrator Responds to Audible or Visual Alarms, on page 5
- Viewing the Console or Syslog for Alarm Messages, on page 6
- Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP, on page 8

Onsite Network Administrator Responds to Audible or Visual Alarms

- About Audible and Visual Alarms, on page 5
- Clearing an Audible Alarm, on page 5
- Clearing a Visual Alarm, on page 6

About Audible and Visual Alarms

An external element can be connected to a power supply using the DB-25 alarm connector on the power supply. The external element is a DC light bulb for a visual alarm and a bell for an audible alarm.

If an alarm illuminates the CRIT, MIN, or MAJ LED on the faceplate of the router, and a visual or audible alarm is wired, the alarm also activates an alarm relay in the power supply DB-25 connector, and either the bell rings or the light bulb flashes.

Clearing an Audible Alarm

To clear an audible alarm, perform one of the following tasks:

- Press the **Audible Cut Off** button on the faceplate.
- Enter the **clear facility-alarm** command.

Clearing a Visual Alarm

To clear a visual alarm, you must resolve the alarm condition. The **clear facility-alarm** command does not clear an alarm LED on the faceplate or turn off the DC light bulb. For example, if a critical alarm LED is illuminated because an active module was removed without a graceful deactivation, the only way to resolve that alarm is to replace the module.

Viewing the Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a system message log (syslog).

- Enabling the logging alarm Command, on page 6
- Examples of Alarm Messages, on page 6
- Reviewing and Analyzing Alarm Messages, on page 8

Enabling the logging alarm Command

The **logging alarm** command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of the alarms to be logged. All the alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

Examples of Alarm Messages

The following are examples of alarm messages that are sent to the console when a module is removed before performing a graceful deactivation. The alarm is cleared when the module is reinserted.

Module Removed

```
*Aug 22 13:27:33.774: %ISR4451-X_OIR-6-REMSPA: Module removed from subslot 1/1, interfaces
 disabled
*Aug 22 13:27:33.775: %SPA_OIR-6-OFFLINECARD: Module (SPA-4XT-SERIAL) offline in subslot
1/1
```

Module Reinserted

```
*Aug 22 13:32:29.447: %ISR4451-X_OIR-6-INSSPA: Module inserted in subslot 1/1
*Aug 22 13:32:34.916: %SPA_OIR-6-ONLINECARD: Module (SPA-4XT-SERIAL) online in subslot 1/1
*Aug 22 13:32:35.523: %LINK-3-UPDOWN: SIP1/1: Interface EOBC1/1, changed state to up
```

Alarms

To view alarms, use the **show facility-alarm status** command. The following example shows a critical alarm for the power supply:

```
Router# show facility-alarm status
System Totals  Critical: 5  Major: 0  Minor: 0

Source                    Severity      Description [Index]
------                    --------      -------------------
Power Supply Bay 0        CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/1      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/2      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/3      INFO          Physical Port Link Down [1]
xcvr container 0/0/0      INFO          Transceiver Missing [0]
xcvr container 0/0/1      INFO          Transceiver Missing [0]
xcvr container 0/0/2      INFO          Transceiver Missing [0]
xcvr container 0/0/3      INFO          Transceiver Missing [0]
```

To view critical alarms, use the **show facility-alarm status critical** command, as shown in the following example:

```
Router# show facility-alarm status critical
System Totals  Critical: 5  Major: 0  Minor: 0

Source                    Severity      Description [Index]
------                    --------      -------------------
Power Supply Bay 0        CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/1      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/2      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/3      INFO          Physical Port Link Down [1]
```

To view the operational state of the major hardware components on the router, use the **show platform diag** command. This example shows that power supply P0 has failed:

```
Router# show platform diag
Chassis type: ISR4451/K9

Slot: 0, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:42 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Sub-slot: 0/0, ISR4451-4X1GE
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:02:48 (1w0d ago)
  Logical insert detect time  : 00:02:48 (1w0d ago)

Slot: 1, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:43 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Slot: 2, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
```

```
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:44 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Slot: R0, ISR4451/K9
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:09 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Slot: F0, ISR4451-FP
  Running state               : init, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:37 (1w0d ago)
  Hardware ready signal time  : 00:00:00 (never ago)
  Packet ready signal time    : 00:00:00 (never ago)
  CPLD version                :
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA 101]

Slot: P0, Unknown
  State                       : ps, fail
  Physical insert detect time : 00:00:00 (never ago)

Slot: P1, XXX-XXXX-XX
  State                       : ok
  Physical insert detect time : 00:01:26 (1w0d ago)

Slot: P2, ACS-4450-FANASSY
  State                       : ok
  Physical insert detect time : 00:01:26 (1w0d ago)
```

Reviewing and Analyzing Alarm Messages

To facilitate the review of alarm messages, you can write scripts to analyze alarm messages sent to the console or syslog. Scripts can provide reports on events such as alarms, security alerts, and interface status.

Syslog messages can also be accessed through Simple Network Management Protocol (SNMP) using the history table defined in the CISCO-SYSLOG-MIB.

Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP

The SNMP is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network. Of all the approaches to monitor alarms, SNMP is the best approach to monitor more than one router in an enterprise and service provider setup.

SNMP provides notification of faults, alarms, and conditions that might affect services. It allows a network administrator to access router information through a network management system (NMS) instead of reviewing logs, polling devices, or reviewing log reports.

To use SNMP to get alarm notification, use the following MIBs:

- ENTITY-MIB, RFC 4133 (required for the CISCO-ENTITY-ALARM-MIB and CISCO-ENTITY-SENSOR-MIB to work)

- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-SENSOR-MIB (for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)