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 details 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. It also 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. When the **show memory** command is used in a system with 4 GB RAM running a single Cisco IOS process, the following memory usage is displayed:

```
Router# show memory
          Tracekey : 1#24c450a57e03d03a6788866ae1d462e4
 Address      Bytes      Prev       Next    Ref   PrevF     NextF          what        Alloc
 PC

                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor  7F51210010   1499843648   303330248   1196513400   786722360   713031588
 lsmpi_io  7F506281A8     6295128     6294304         824         824         412
Dynamic heap limit(MB) 680       Use(MB) 0



          Processor memory

 Address      Bytes      Prev       Next    Ref   PrevF     NextF          what
    Alloc PC
7F51210010 0000000568 00000000 7F512102A0 001  -------- -------- *Init*
:400000+896EB88
7F512102A0 0000032776 7F51210010 7F51218300 001  -------- -------- Managed Chunk Q
:400000+295B3C8
7F51218300 0000000056 7F512102A0 7F51218390 001  -------- -------- *Init*
:400000+896EB88
7F51218390 0000012808 7F51218300 7F5121B5F0 001  -------- -------- *Init*
:400000+896EB88
 Address      Bytes      Prev       Next    Ref   PrevF     NextF          what
    Alloc PC
7F5121B5F0 0000032776 7F51218390 7F51223650 001  -------- -------- List Elements
:400000+2948680
7F51223650 0000010008 7F5121B5F0 7F51225DC0 001  -------- -------- List Headers
:400000+2948680
7F51225DC0 0000032776 7F51223650 7F5122DE20 001  -------- -------- IOSXE Process S
:400000+295B3C8
7F5122DE20 0000032776 7F51225DC0 7F51235E80 001  -------- -------- IOSXE Queue Pro
:400000+295B3C8
7F51235E80 0000065544 7F5122DE20 7F51245EE0 001  -------- -------- IOSXE Queue Bal
:400000+295B3C8
7F51245EE0 0000000112 7F51235E80 7F51245FA8 001  -------- -------- *Init*
:400000+2951DE0
7F51245FA8 0000036872 7F51245EE0 7F5124F008 001  -------- -------- *Init*
:400000+2950FB4
7F5124F008 0000010008 7F51245FA8 7F51251778 001  -------- -------- Platform VM Pag
:400000+295B3C8
7F51251778 0000000328 7F5124F008 7F51251918 001  -------- -------- *Init*
:400000+896EB88
7F51251918 0000000328 7F51251778 7F51251AB8 001  -------- -------- *Init*
:400000+896EB88
7F51251AB8 0000000896 7F51251918 7F51251E90 001  -------- -------- Watched Message
:400000+295B3C8

...
```

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

```
Router# show process cpu
CPU utilization for five seconds: 1%/1%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0          21          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        5692       12584        452  0.00%  0.00%  0.00%   0 Load Meter
   3           0           1          0  0.00%  0.00%  0.00%   0 PKI Trustpool
   4           0           1          0  0.00%  0.00%  0.00%   0 Retransmission o
   5           0           1          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6          16          12       1333  0.00%  0.00%  0.00%   0 RF Slave Main Th
   7           4           1       4000  0.00%  0.00%  0.00%   0 EDDRI_MAIN
```

```
  8           0           1           0  0.00%  0.00%  0.00%   0 RO Notify Timers
  9       38188        8525        4479  0.00%  0.04%  0.05%   0 Check heaps
 10          12        1069          11  0.00%  0.00%  0.00%   0 Pool Manager
 11           0           1           0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 12           0           2           0  0.00%  0.00%  0.00%   0 Timers
 13           0          29           0  0.00%  0.00%  0.00%   0 WATCH_AFS
 14           0           1           0  0.00%  0.00%  0.00%   0 MEMLEAK PROCESS
 15        3840       23732         161  0.00%  0.00%  0.00%   0 ARP Input
 16        1156       65637          17  0.00%  0.00%  0.00%   0 ARP Background
 17           0           2           0  0.00%  0.00%  0.00%   0 ATM Idle Timer
 18           0           1           0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
 19           0           1           0  0.00%  0.00%  0.00%   0 CEF MIB API
 20           0           1           0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
 21           0           1           0  0.00%  0.00%  0.00%   0 Policy Manager
 22           0           2           0  0.00%  0.00%  0.00%   0 DDR Timers
PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 23          76          19        4000  0.00%  0.00%  0.00%   0 Entity MIB API
 24         124          38        3263  0.00%  0.00%  0.00%   0 PrstVbl
 25           0           2           0  0.00%  0.00%  0.00%   0 Serial Backgroun
 26           0           1           0  0.00%  0.00%  0.00%   0 RMI RM Notify Wa
 27           0           2           0  0.00%  0.00%  0.00%   0 ATM AutoVC Perio
 28           0           2           0  0.00%  0.00%  0.00%   0 ATM VC Auto Crea
 29         768       31455          24  0.00%  0.00%  0.00%   0 IOSXE heartbeat
 30         180        1866          96  0.00%  0.00%  0.00%   0 DB Lock Manager
 31           0           1           0  0.00%  0.00%  0.00%   0 DB Notification
 32           0           1           0  0.00%  0.00%  0.00%   0 IPC Apps Task
 33           0           1           0  0.00%  0.00%  0.00%   0 ifIndex Receive

...
```

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 system 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: 0.90, status: healthy, under 5.00
  5-Min: 0.87, status: healthy, under 5.00
  15-Min: 0.95, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3448368
  Used: 1979068 (57%), status: healthy
  Free: 1469300 (43%)
  Committed: 2002904 (58%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.54, System:  1.33, Nice:  0.00, Idle: 97.11
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  1.53, System:  0.82, Nice:  0.00, Idle: 97.64
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
```

```
  User:  2.77, System:  9.38, Nice:  0.00, Idle: 87.84
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 12.62, System: 64.63, Nice:  0.00, Idle: 22.74
  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   0.87   0.87   0.94

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  3448368  1996720 (58%)  1451648 (42%)   2003380 (58%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   1.54   0.92   0.00  97.53   0.00   0.00   0.00
         1   1.64   1.12   0.00  97.22   0.00   0.00   0.00
         2   3.32   8.36   0.00  88.30   0.00   0.00   0.00
         3  12.58  64.44   0.00  22.97   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:

```
Oct  6 14:10:56.292: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota exceeded

[free space is 1429020 kB] - Please clean up files on bootflash.
```

Approaches for Monitoring Hardware Alarms

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

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.

Alarms

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

```
Device# show facility-alarm status
Source          Severity            Description [Index]
------                             --------      -------------------------
Cellular0/2/0   INFO                Physical Port Administrative State Down [2]
Cellular0/2/1   INFO                Physical Port Administrative State Down [2]
```

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

```
Device# show facility-alarm status critical
ystem Totals Critical: 4 Major: 0 Minor: 0
Source               Time                 Severity Description           [Index]
------               ------               -------- ------------          -------
GigabitEthernet0/1/0 Jul 12 2017 22:27:25 CRITICAL Physical Port Link Down [1]
GigabitEthernet0/1/1 Jul 12 2017 22:27:25 CRITICAL Physical Port Link Down [1]
GigabitEthernet0/1/2 Jul 12 2017 22:27:25 CRITICAL Physical Port Link Down [1]
GigabitEthernet0/1/3 Jul 12 2017 22:27:25 CRITICAL Physical Port Link Down [1]
```

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

```
Device# show platform diag

Chassis type: C1117-4PLTEEA

Slot: 0, C1117-4PLTEEA
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:52 (09:02:14 ago)
  Software declared up time   : 00:03:12 (09:00:54 ago)
  CPLD version                : 17100501
  Firmware version            : 16.6(1r)RC3

Sub-slot: 0/0, C1117-1x1GE
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:34 (08:59:32 ago)
  Logical insert detect time  : 00:04:34 (08:59:32 ago)
```

```
Sub-slot: 0/1, C1117-ES-4
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:34 (08:59:32 ago)
  Logical insert detect time  : 00:04:34 (08:59:32 ago)

Sub-slot: 0/2, C1117-LTE
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:34 (08:59:32 ago)
  Logical insert detect time  : 00:04:34 (08:59:32 ago)

Sub-slot: 0/3, C1117-VADSL-A
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:34 (08:59:32 ago)
  Logical insert detect time  : 00:04:34 (08:59:32 ago)

Slot: R0, C1117-4PLTEEA
    Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:52 (09:02:14 ago)
  Software declared up time   : 00:01:52 (09:02:14 ago)
  CPLD version                : 17100501
  Firmware version            : 16.6(1r)RC3

Slot: F0, C1117-4PLTEEA
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:52 (09:02:14 ago)
  Software declared up time   : 00:04:06 (09:00:00 ago)
  Hardware ready signal time  : 00:02:44 (09:01:22 ago)
  Packet ready signal time    : 00:04:31 (08:59:35 ago)
  CPLD version                : 17100501
  Firmware version            : 16.6(1r)RC3

Slot: P0, PWR-12V
  State                       : ok
  Physical insert detect time : 00:02:24 (09:01:43 ago)

Slot: GE-POE, Unknown
  State                       : NA
  Physical insert detect time : 00:00:00 (never 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.

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, RFC4133(required for the CISCO-ENTITY-ALARM-MIB, ENTITY-STATE-MIB and CISCO-ENTITY-SENSOR-MIB to work)
- CISCO-ENTITY-ALARM-MIB
- ENTITY-STATE-MIB
- CISCO-ENTITY-SENSOR-MIB(for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)