CPU 占用率高技术专题

资料版本：6W100-20230927

目 录

1 简介

交换机作为网络设备的核心组件，负责转发数据包和管理网络流量。当交换机的 CPU 占用率高时，可能会导致网络性能下降和故障发生，影响通信的稳定性和可靠性。

本文档详细介绍交换机 CPU 占用率高的常见原因、影响以及如何定位和处理 CPU 占用率高的问题。

2 引起 CPU 占用率高的常见原因

CPU 占用率高的常见原因包括：

- 网络拥塞：当交换机处理大量的数据流量时，CPU 可能会过载，导致占用率升高
- 网络攻击：恶意软件或病毒可能会通过网络攻击交换机，对 CPU 资源造成极大的消耗。
- 协议震荡：通常为 STP 或路由协议震荡，导致设备进行频繁的重新计算和更新。
- 网络环路：流量不断循环，需要设备不断进行计算和处理。
- 设备启用流量采样功能：需要处理的流量太大或采样频率太高，导致采样功能占用大量 CPU 资源。
- 设备产生海量日志，生成和管理这些日志占用了大量 CPU 资源。
- 错误配置：错误的交换机配置可能导致 CPU 占用率升高，例如错误的 ACL 配置、广播风暴等。

3 CPU 占用率过高的影响

当 H3C 设备的 CPU 占用率过高时，可能会产生以下影响：

- 性能下降：高 CPU 占用率会使设备的处理速度下降，导致数据包的处理延迟增加。进而致网络的响应时间变慢，可能会对用户的网络体验产生负面影响。
- 丢包和延迟增加：高 CPU 占用率会影响设备对数据包的处理能力，可能会导致数据包在设备内部的丢失，或者在转发过程中的延迟增加。
- 系统稳定性降低：当 CPU 占用率过高时，设备的负载压力会增加，可能会导致设备在处理大量流量时无法正常工作，从而影响整个网络的稳定性。
- 服务中断：在极端情况下，当设备的 CPU 占用率过高且持续时间较长时，交换机可能会无法正常运行，导致网络服务的中断，从而影响用户的正常使用。
- 安全风险：高 CPU 占用率可能会导致设备的负载增加，使其无法正常检测和阻止恶意流量，从而给网络安全带来潜在的风险。
- 系统崩溃：当 CPU 资源超过其承载能力时，交换机可能会出现系统崩溃和重启的情况。

高 CPU 占用率会影响 H3C 设备的性能和稳定性。因此，及时监测和解决高 CPU 占用率问题对于网络正常运行和提供良好用户体验至关重要。

4 如何定位 CPU 占用率高

当出现以下情况时，说明设备的 CPU 控制核占用率高，需要确认 CPU 占用率高的具体原因。

- 对设备进行每日巡检时，连续使用 display cpu-usage 命令查看 CPU 的占用率，CPU 占用率持续在 60%以上，或占用率明显比日常平均值高。

  # 执行 **display cpu-usage summary** 命令显示最近 5 秒、1 分钟、5 分钟内 CPU 占用率的平均值。

  ```
  <Sysname> display cpu-usage summary
  Slot CPU        Last 5 sec        Last 1 min        Last 5 min
  1    0          5%                5%                4%
  ```

  # 执行 **display cpu-usage history** 命令以图表的方式显示最近 60 个采样点的 CPU 占用率，观察到 CPU 占用率持续在增长或者明显比日常平均值高。
- 通过 Telnet/SSH 等方式登录设备，并执行命令行时，设备反应缓慢，出现卡顿现象。
- 设备上打印 CPU 占用率高的相关日志。
- SNMP 网管上出现 CPU 占用率高的相关告警。

4.1 查看设备型号和版本信息

查看设备的型号与版本信息，方便后续排查时使用。

(1) 任意视图下执行 **display device** 命令，查看设备型号等信息。

显示设备信息。（集中式 IRF 设备）

```
<Sysname> display device
Slot Type             State    Subslot  Soft Ver             Patch Ver
1    S6820-32H        Master   0        S6820-6103           None
```

显示设备信息。（分布式设备—独立运行模式）

```
<Sysname> display device
Slot Type             State    Subslot  Soft Ver             Patch Ver
0    LSXM1SUPB1       Master   0        S12508X-AF-0502      None
1    LSXM1SUPB1       Standby  0        S12508X-AF-0502      None
2    NONE             Absent   0        NONE                 None
3    LSXM1TGS48C2HB1  Normal   0        S12508X-AF-0502      None
4    NONE             Absent   0        NONE                 None
5    NONE             Absent   0        NONE                 None
6    NONE             Absent   0        NONE                 None
7    NONE             Absent   0        NONE                 None
8    NONE             Absent   0        NONE                 None
9    NONE             Absent   0        NONE                 None
10   NONE             Absent   0        NONE                 None
11   NONE             Absent   0        NONE                 None
12   NONE             Absent   0        NONE                 None
13   NONE             Absent   0        NONE                 None
14   NONE             Absent   0        NONE                 None
15   LSXM1SFH08D1     Normal   0        S12508X-AF-0502      None
```

(2) 任意视图下执行 **display version** 命令，查看系统版本信息。

```
<Sysname> display version
H3C Comware Software, Version 7.1.070, Feature 2607
Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.
H3C S6800-54QT uptime is 0 weeks, 0 days, 2 hours, 14 minutes
Last reboot reason : Cold reboot

Boot image: flash:/s6800-cmw710-boot-f2607.bin
Boot image version: 7.1.070, Feature 2607
  Compiled May 15 2017 16:00:00
System image: flash:/s6800-cmw710-system-f2607.bin
System image version: 7.1.070, Feature 2607
  Compiled May 15 2017 16:00:00
...
```

4.2 查看CPU占用率

如下方式可以查看 CPU 占用率：

- 任意视图下执行 **display cpu-usage** 命令，查看 CPU 占用率信息。正常情况下，盒式设备、框式设备业务板和主控板的 CPU 占用率一般都是在 60%以内的，应根据 CPU 的 5 分钟内的平均占用率来判断该设备或单板的 CPU 占用率是否异常。如果确认 CPU 占用率高，请按照后续步骤继续排查。

  例如：通过命令可以判断出 3 号槽位的单板 CPU 占用率异常高。

  ```
  <H3C>display cpu
  Slot 0 CPU usage:
         11% in last 5 seconds
         13% in last 1 minute
         13% in last 5 minutes
  Slot 3 CPU usage:
         85% in last 5 seconds
         79% in last 1 minute
         71% in last 5 minutes
  ```

- 查看 CPU 占用率高的相关日志。

  执行 **display logbuffer** 命令查看日志缓冲区记录的日志信息，查看是否生成了 CPU 占用率高的日志信息。

  ```
  <Sysname> display logbuffer
  Log buffer: Enabled
  Max buffer size: 1024
  Actual buffer size: 512
  Dropped messages: 0
  Overwritten messages: 718
  Current messages: 512
  %Jun 17 15:57:09:578 2019 Sysname SYSLOG/7/SYS_RESTART:System restarted –
  ...
  ```

  CPU 占用率的相关日志信息为：

  - DIAG/5/CPU_MINOR_RECOVERY

- DIAG/4/CPU_MINOR_THRESHOLD
- DIAG/5/CPU_SEVERE_RECOVERY
- DIAG/3/CPU_SEVERE_THRESHOLD

- SNMP 网管上出现 CPU 占用率高的相关告警。

  如果设备上部署了网管系统，则可以在网管系统上查看 CPU 占用率高的告警。当 CPU 占用率超过告警阈值时（通过 **monitor cpu-usage threshold** 命令可以配置 CPU 占用率告警门限），系统会发送告警。

4.3 收集CPU占用率相关信息，找到CPU占用率高的业务模块

4.3.1 确定对 CPU 占用率高的任务进程

方法一：在设备上执行 **display process cpu** 命令查看一段时间内占用 CPU 最多的任务。下面以 slot 1 上的操作为例。pppd 进程的 CPU 占用率为高于 3%（经验值供参考），则需要针对该进程继续定位。

```
<Sysname> display process cpu slot 1
CPU utilization in 5 secs: 0.4%; 1 min: 0.2%; 5 mins: 0.2%
    JID      5Sec      1Min      5Min    Name
      1      0.0%      0.0%      0.0%    scmd
      2      5.5%      5.1%      5.0%    [kthreadd]
      3      0.0%      0.0%      0.0%    [ksoftirqd/0]
...
```

方法二：在设备上执行 **monitor process dumbtty** 命令实时查看进程在指定 CPU 上的占用率。下面以 slot 1 CPU 0 为例。

```
<Sysname> system-view
[Sysname] monitor process dumbtty slot 1 cpu 0
206 processes; 342 threads; 5134 fds
Thread states: 4 running, 338 sleeping, 0 stopped, 0 zombie
CPU0: 99.04% idle, 0.00% user, 0.96% kernel, 0.00% interrupt, 0.00% steal
CPU1: 98.06% idle, 0.00% user, 1.94% kernel, 0.00% interrupt, 0.00% steal
CPU2: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
CPU3: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
CPU4: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
Memory: 7940M total, 5273M available, page size 4K
        JID        PID  PRI State  FDs     MEM  HH:MM:SS    CPU   Name
        515        322  115   R     0       0K  01:48:03  20.02%  pppd
        376        376  120   S    22  159288K  00:00:07   0.37%  diagd
          1          1  120   S    18   30836K  00:00:02   0.18%  scmd
        379        379  120   S    22  173492K  00:00:11   0.18%  devd
          2          2  120   S     0       0K  00:00:00   0.00%  [kthreadd]
          3          3  120   S     0       0K  00:00:02   0.00%  [ksoftirqd/0]
...
```

- 在 **monitor process dumbtty** 命令显示信息中，pppd 进程 CPU 占用率超过 3%（经验值供参考）的进程的 JID，再对这些进程执行 **display process job** 命令，收集进程的详细信息，并确认该进程是否运行在控制核上。

如果 **display process job** 命令的显示信息中 LAST_CPU 字段的取值为控制核的编号（例如 0～1），则说明该进程运行在 CPU 控制核上，则需要进一步定位；如果显示信息中 LAST_CPU 字段的取值为非控制核的编号，则说明该进程运行在 CPU 转发核上，无需关注。下面以 pppd 进程为例，通过显示信息可以看到，该进程包含多个线程，这些线程都运行在控制核上。

```
<Sysname> display process name pppd
                                 Job ID: 515
                                    PID: 515
                              Parent JID: 1
                              Parent PID: 1
                         Executable path: /sbin/pppd
                                Instance: 0
                                 Respawn: ON
                           Respawn count: 1
                  Max. spawns per minute: 12
                            Last started: Wed Nov  3 09:52:00 2021
                           Process state: sleeping
                               Max. core: 1
                                    ARGS: --MaxTotalLimit=2000000 --MaxIfLimit=65534
--CmdOption=0x01047fbf --bSaveRunDb --pppoechastenflag=1 --pppoechastennum=6
--pppoechastenperiod=60 --pppoechastenblocktime=300 --pppchastenflag=1
--pppchastennum=6 --pppchastenperiod=60 --pppchastenblocktime=300 --PppoeKChasten
--bSoftRateLimit --RateLimitToken=2048
       TID  LAST_CPU    Stack      PRI    State   HH:MM:SS:MSEC  Name
       515      0        136K      115      S     0:0:0:90       pppd
       549      0        136K      115      S     0:0:0:0        ppp_misc
       557      0        136K      115      S     0:0:0:10       ppp_chasten
       610      0        136K      115      S     0:0:0:0        ppp_work0
       611      1        136K      115      S     0:0:0:0        ppp_work1
       612      1        136K      115      S     0:0:0:0        ppp_work2
       613      1        136K      115      S     0:0:0:0        mp_main
       618      1        136K      115      S     0:0:0:110      pppoes_main
       619      1        136K      115      S     0:0:0:100      pppoes_mesh
       620      1        136K      115      S     0:0:0:120      l2tp_mesh
       621      1        136K      115      S     0:0:0:20       l2tp_main
```

- 对于运行在控制核、CPU 占用率超过 5%的进程，查看进程的 Name 字段的取值来确定该进程是否为用户态进程。

  如果 Process 的 Name 取值中包含“[]”，表示它是内核线程，无需执行 **monitor thread dumbtty** 命令；如果 Process 的 Name 取值中未包含“[]”，表示它是用户态进程，它可能包含多个线程。对于多线程的用户态进程，还需要对该用户态进程执行 **monitor thread dumbtty** 命令，如果显示信息中某线程 LAST_CPU 字段的取值为 CPU 控制核的编号，且 CPU 字段取值大于 5%，则该线程可能为导致 CPU 控制核占用率高的线程，需要进一步定位。

```
<Sysname> monitor thread dumbtty slot 1 cpu 0
   206 processes; 342 threads; 5134 fds
   Thread states: 4 running, 338 sleeping, 0 stopped, 0 zombie
   CPU0: 98.06% idle, 0.97% user, 0.97% kernel, 0.00% interrupt, 0.00% steal
   CPU1: 97.12% idle, 0.96% user, 0.96% kernel, 0.96% interrupt, 0.00% steal
```

```
    CPU2: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
    CPU3: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
    CPU4: 0.00% idle, 0.00% user, 100.00% kernel, 0.00% interrupt, 0.00% steal
    Memory: 7940M total, 5315M available, page size 4K
            JID      TID  LAST_CPU  PRI  State  HH:MM:SS MAX   CPU     Name
            322      322      2      115    R    00:04:21    0  20.15%   [kdrvfwdd2]
            323      323      3      115    R    00:04:21    0  20.15%   [kdrvfwdd3]
            324      324      4      115    R    00:04:21    0  20.15%   [kdrvfwdd4]
              1        1      1      120    S   00:00:02   21   0.19%   scmd
            376      376      1      120    S   00:00:00    1   0.19%   diagd
              2        2      0      120    S   00:00:00    0   0.00%   [kthreadd]
...
```

4.3.2 确认异常任务的调用栈

通过 Probe 视图下的 **follow job** 命令确认异常任务的调用栈，请查询 5 次以上，发送给技术支持人员分析，以便于分析该任务具体在做什么处理导致 CPU 占用率持续升高。。下面以 Sysname 上（slot 1）pppd 进程（进程编号为 515）的操作为例。

```
<Sysname> system-view
[Sysname] probe
[Sysname-probe] follow job 515 slot 1
Attaching to process 515 (pppd)
Iteration 1 of 5
------------------------------
Thread LWP 515:
Switches: 3205
User stack:
#0  0x00007fdc2a3aaa8c in epoll_wait+0x14/0x2e
#1  0x0000000000441745 in ppp_EpollSched+0x35/0x5c
#2  0x0000000000000004 in ??
Kernel stack:
[<ffffffff811f0573>] ep_poll+0x2f3/0x370
[<ffffffff811f06c0>] SyS_epoll_wait+0xd0/0xe0
[<ffffffff814aed79>] system_call_fastpath+0x16/0x1b
[<ffffffffffffffff>] 0xffffffffffffffff
Thread LWP 549:
Switches: 20
User stack:
#0  0x00007fdc2a3aaa8c in epoll_wait+0x14/0x2e
#1  0x00000000004435d4 in ppp_misc_EpollSched+0x44/0x6c
Kernel stack:
[<ffffffffffffffff>] 0xffffffffffffffff
...
```

4.3.3 处理业务模块的问题

根据[确定对 CPU 占用率高的任务、确认异常任务的调用栈]两步找到的任务名称，再根据任务名称找到对应的业务模块，定位并处理业务模块的问题。例如，如果任务 snmpd 的 CPU 占用率较高，

可能是因为设备受到了 SNMP 攻击，或者 NMS 对设备的访问太频繁。需要进一步定位 SNMP 业务模块的问题；如果任务 nqad 的 CPU 占用率较高，可能是因为 NQA 探测太频繁，需要进一步定位 NQA 业务模块的问题。

4.3.4 常见任务进程

1. comsh

定义

comsh 是 H3C 设备上的一个系统进程，全称为 Command Shell Process，是指命令行解释器。comsh 进程负责解释和执行命令行命令，以及管理用户和用户操作。在用户登录设备后，系统会自动启动 comsh 进程，等待用户输入相应的命令行指令。如果 comsh 进程出现异常或错误，可能会导致命令行操作不稳定或错误，从而影响到设备的管理和维护。

comsh 进程占用率过高可能有以下原因：

- 操作不当：comsh 进程是响应用户命令操作的进程，如果在操作时出现错误或者卡住，就容易导致 comsh 进程占用率过高。
- 设备负载高：如果设备的负载过高，导致资源紧张，就会出现 comsh 进程占用率过高的情况。
- 系统软件异常：系统中的一些软件可能出现异常导致 comsh 进程占用率过高。
- 用户连接过多：如果设备上存在大量用户同时登录，就会增加 comsh 进程的压力，从而出现 comsh 进程占用率过高的情况。

解决措施：

- 检查用户操作，确认没有卡住或错误的操作。
- 可以尝试升级硬件或者降低一些应用的使用。
- 尝试重启重启设备。
- 联系技术支持进行更进一步的排查和解决。

2. Ifmgr

定义

ifmgr 是 H3C 设备上的一个系统进程，全称为 Interface Manager Process，是指接口管理程序。ifmgr 进程负责管理设备的各个接口，包括物理接口、逻辑接口、隧道接口等。对接口进行实时监控、配置及状态管理等操作。如果 ifmgr 进程出现异常或错误，可能会导致接口管理和维护出现问题，从而影响到设备的正常运行和管理。

ifmgr 进程占用率过高可能有以下原因：

- 接口配置异常：如果设备中存在接口配置异常，例如重复配置、配置错误、不当配置等，可能会导致 ifmgr 进程异常，占用大量系统资源。
- 硬件问题：设备中的一些硬件设备可能会出现问题，例如接口模块损坏、电源电压不稳等，这些问题也可能会导致 ifmgr 进程占用率过高。
- 系统软件错误：如果设备中的一些系统软件存在错误或漏洞，可能会导致 ifmgr 进程异常，进而占用大量 CPU 或内存资源。
- 大量接口监控：如果设备中需要监控大量的接口，例如多线路的负载均衡，可能会导致 ifmgr 进程占用大量系统资源。

解决措施：

- 检查接口配置，确认没有重复或者错误的配置。
- 检查设备是否存在硬件问题。
- 尝试重启设备。
- 联系技术支持进行更进一步的排查和解决。

3. nqad

定义

nqad 是 H3C 设备上的一个系统进程，是指网络质量自动检测系统进程（Network Quality Auto Detection）。nqad 进程负责监控设备接口的质量状况，通过定期发送探测数据包来检测链路的质量，包括连接延迟、丢包率、带宽利用率等指标，并将检测结果回传给设备的管理平台。对于故障事件，如链路丢包，nqad 还会自动降低接口的速率，并发出告警通知操作者。如果 nqad 进程出现异常，可能会导致链路检测失败，导致链路质量不稳定，影响节点间通信。

nqad 进程占用率过高可能有以下原因：

- 链路质量差：nqad 进程负责检测链路质量，如果链路质量较差，可能导致 nqad 进程占用大量系统资源。
- 数据采集间隔过短：nqad 进程采集链路数据的间隔时间过短，可能会导致 nqad 进程占用率过高。
- 运行环境异常：如果 nqad 进程所在的运行环境不稳定或出现异常，就可能导致 nqad 进程异常，占用 CPU 过高。
- 设备资源不足：如果设备的运行资源不足，可能会导致 nqad 进程占用率过高，这种情况下，可以升级硬件或者关闭一些不必要的应用来减轻负载。

解决措施：

- 根据日志或网络数据分析出链路质量是否存在异常问题，如果存在，建议进一步查找并修复相关问题。
- 调整 nqad 进程采集间隔时间。
- 尝试重启设备。
- 联系厂商技术支持进行更进一步的排查和解决。

4. scmd

定义

scmd 是 H3C 设备上的一个系统进程，全称为 System Command Process，是指令处理程序，是设备运行的重要组成部分。scmd 进程负责处理并执行从用户终端发来的命令请求。如果 scmd 进程出现异常，可能会导致用户无法进行正常的命令操作，从而影响到设备的管理和维护。

scmd 进程占用率过高的原因可能有很多，以下是一些常见的可能原因：

- 操作不当：scmd 进程是响应用户命令操作的进程，如果用户在操作时出现错误或者卡住，就容易导致 scmd 进程占用率过高。
- 设备负载高：如果设备的负载过高，导致资源紧张，就会出现 scmd 进程占用率过高的情况，这种情况下，你可以尝试升级硬件或者降低一些应用的使用。
- 系统软件异常：系统中的一些软件可能出现异常导致 scmd 进程占用率过高。

解决措施：

- 检查用户操作，确认没有卡住或错误的操作。
- 通过 top 命令查看当前系统的负载情况，如果负载过高，可以关闭一些不必要的应用来减轻负载。
- 尝试重启设备。
- 联系技术支持进行更进一步的排查和解决。

5. snmpd

定义

snmpd 是指 Simple Network Management Protocol (SNMP) Daemon，即简单网络管理协议守护进程。在计算机网络中，SNMP 是一种用于管理和监控网络设备的标准协议。snmpd 进程（守护进程）负责监听和响应 SNMP 协议的请求，提供网络设备的状态信息、性能数据、配置信息等供网络管理系统使用。通过 SNMP 协议，管理员可以远程监控和管理设备、检测故障、收集性能数据等。

snmpd 进程占用率过高可能有以下原因：

- SNMP 请求过多或 SNMP 攻击：SNMP 协议具有广泛的适用性，可能会有大量的请求发送到设备上，如果 snmpd 进程同时响应多个请求，就会导致进程占用 CPU 资源过多。
- 设备负载高：如果设备的负载过高，导致资源紧张，就会出现 snmpd 进程占用率过高的情况，这种情况下，你可以尝试升级硬件或者降低一些应用的使用。
- SNMP 配置异常：SNMP 协议除了基本的通用对象外，还有许多特定于设备和应用的对象需要配置支持。如果 SNMP 配置不当，可能会导致 snmpd 进程异常或错误。
- 系统软件异常：系统中的一些软件可能出现异常导致 snmpd 进程占用率过高。

解决措施：

- 检查 SNMP 请求，确认没有过多或非正常的请求。
- 关闭一些不必要的应用来减轻负载。
- 检查 SNMP 配置，确认配置正确。
- 尝试重启设备。
- 联系厂商技术支持进行更进一步的排查和解决。

6. sshd

定义

sshd 指的是 Secure Shell Daemon，也就是 SSH 安全壳守护进程。SSH 是一种用来安全远程连接、远程登录和文件传输的加密协议。sshd 进程是 SSH 服务器守护进程，负责接受和处理 SSH 客户端的连接请求，提供远程登录和文件传输等服务。通常，sshd 进程会在后台持续运行，等待用户的连接请求。

sshd 进程占用率过高可能有以下原因：

- 大量并发连接：如果服务器上存在大量的 SSH 连接请求，sshd 进程可能会因同时处理多个连接而消耗较高的系统资源。
- 密钥负载过大：密钥认证是 SSH 的一种常见身份验证方式，如果服务器上存在大量密钥对或复杂的密钥认证配置，sshd 进程可能会占用较高的 CPU 资源来处理密钥的解析和验证。
- 配置不当：sshd 的配置文件中的参数设置可能会导致进程占用率过高。例如，配置过多的认证方式或启用了高级的加密算法可能会增加 sshd 进程的负担。

- 恶意攻击：如果服务器受到 SSH 暴力破解、密码爆破或拒绝服务攻击等恶意行为攻击，大量的攻击尝试可能导致 sshd 进程资源被耗尽，使其占用率升高。

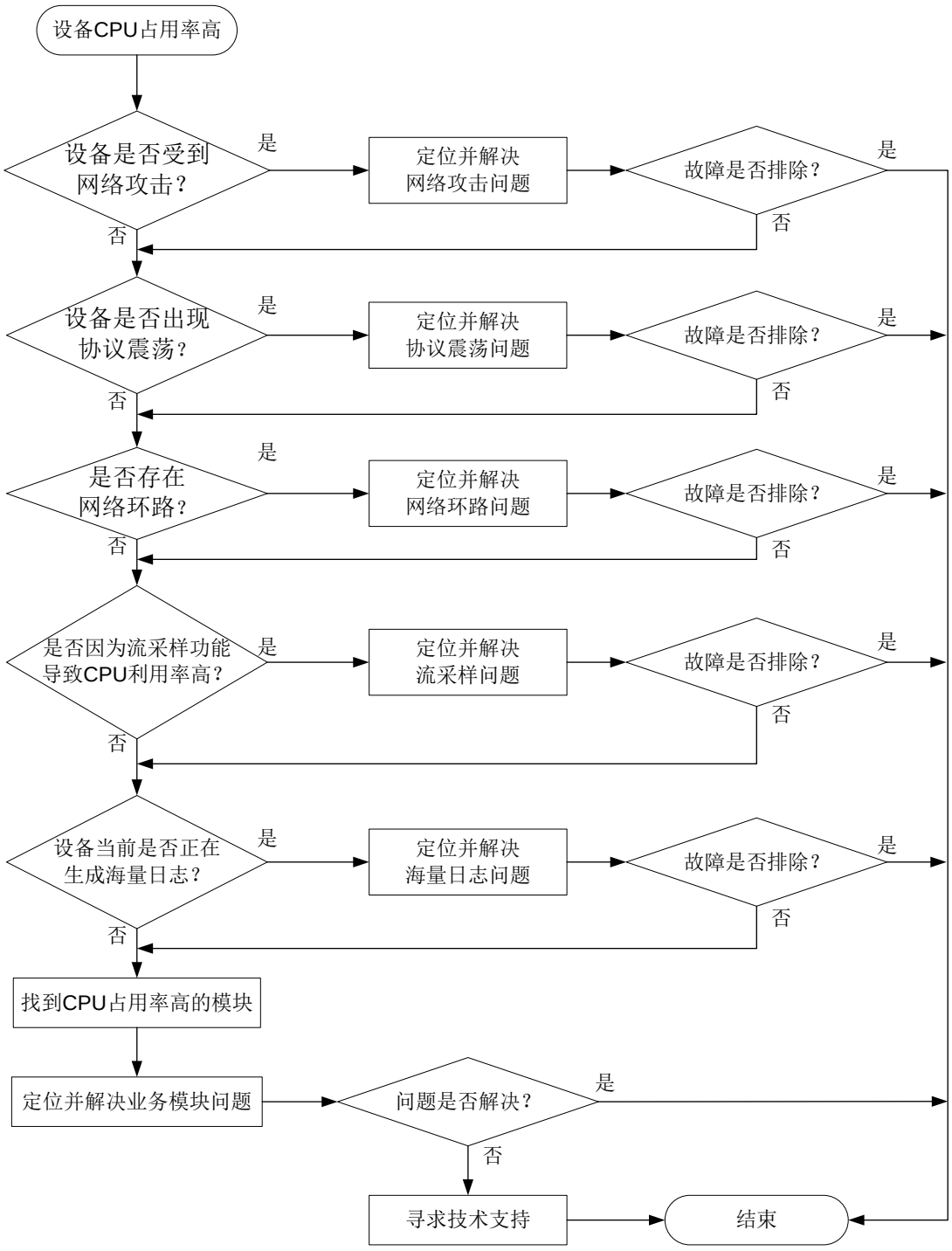
解决措施：

- 优化服务器资源：确保服务器有足够的 CPU 和内存资源，以支持大量并发连接和密钥负载。
- 优化 ssh 配置：检查并调整 sshd_config 文件中的参数设置，避免配置过多的认证方式或启用过于复杂的加密算法。
- 添加访问控制：限制 SSH 访问只允许受信任的 IP 地址或特定用户，可以减少无效连接请求对 sshd 进程的影响。
- 强化安全策略：采取措施防止恶意攻击，如启用 IP 防火墙、使用智能 SSH 防暴力破解工具、定期更换密钥等，以减少危害。

5 如何处理 CPU 占用率高

CPU 占用率高的处理流程如图 5-1 所示。

图5-1 CPU 占用率高的处理流程图



5.1 确认设备是否受到网络攻击

现网中，导致设备 CPU 占用率高最常见的原因是网络攻击。攻击者发起大量非正常网络交互对设备产生冲击，例如短时间内发送大量 TCP 连接建立请求报文或者 ICMP 请求报文，设备忙于处理这些攻击报文，导致 CPU 占用率高，从而影响设备正常业务的运行。

Probe 视图下执行 **display system internal control-plane statistics** 命令，查看控制平面报文的统计信息，关注丢弃报文的数量。如果当前 CPU 占用率高，且 Dropped 字段取值较大，则设备大概率受到了报文攻击。（**display system internal control-plane statistics** 的支持情况与设备的型号有关，请以设备的实际情况为准）

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] probe
[Sysname-probe] display system internal control-plane statistics slot 1
Control plane slot 1
  Protocol: Default
    Bandwidth: 15360 (pps)
    Forwarded: 108926 (Packets), 29780155 (Bytes)
    Dropped  : 0 (Packets), 0 (Bytes)
  Protocol: ARP
    Bandwidth: 512 (pps)
    Forwarded: 1489284 (Packets), 55318920 (Bytes)
    Dropped  : 122114 (Packets), 491421 (Bytes)
...
```

- 如果受到了网络攻击，则先解决网络攻击问题。
- 如果未受到网络攻击，则执行 5.2 确认设备是否出现协议震荡。

5.2 确认设备是否出现协议震荡

协议震荡会导致设备不断地处理协议报文、计算拓扑、更新表项，引起 CPU 占用率高。在实际应用中，最常见的协议震荡为 STP 协议震荡和 OSPF 协议震荡。

- 对于 STP 协议震荡，在系统视图执行 **stp port-log** 命令打开端口状态变化日志显示开关，如果命令行界面频繁输出以下日志，则说明出现了 STP 协议震荡。

  ```
  STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/0/1 detected a topology change.
  STP/6/STP_DISCARDING: Instance 0's port GigabitEthernet1/0/1 has been set to discarding state.
  STP/6/STP_NOTIFIED_TC: Instance 0's port GigabitEthernet1/0/1 was notified a topology change.
  ```

  - 如果 STP 协议震荡，请先排除 STP 协议震荡问题。
  - 如果 STP 协议没有震荡，则继续定位。
- 对于 OSPF 协议震荡，执行 **display ip routing-table** 命令，查看路由信息。如果路由表项中相同网段的路由条目被频繁反复地创建和删除，则表示路由震荡。
  - 如果路由震荡，或者路由一直不存在，则先排除链路问题和 IGP 路由问题。
  - 如果路由没有震荡，则执行 5.3 确认是否存在网络环路。

5.3 确认是否存在网络环路

当以太网接口工作在二层模式并且链路存在环路时，可能出现广播风暴和网络振荡。大量的协议报文上送 CPU 处理，从而导致 CPU 占用率升高。当存在网络环路时，设备很多端口的流量会明显变大，且广播和组播报文占比较大。可通过以下步骤来确认设备是否存在网络环路，设备是否存在广播、组播、未知单播报文风暴。

(1) 清除接口的统计信息。

```
<Sysname> reset counters interface
```

(2) 多次执行 **display counters rate inbound interface** 命令查看端口使用率是否明显增大。

```
<Sysname> display counters rate inbound interface
Usage: Bandwidth utilization in percentage
Interface                Usage(%)     Total(pps) Broadcast(pps) Multicast(pps)
GE5/3/0                      0.01              7            --             --
MGE0/31/0                    0.01              1            --             --
MGE0/32/0                    0.01              5            --             --
VMC1/1/0                     0.05             60            --             --
VMC1/2/0                     0.04             52            --             --

 Overflow: More than 14 digits.
       --: Not supported.
```

(3) 如果端口使用率明显增大，可继续多次执行 **display counters inbound interface** 命令查看接口收到的总报文数、广播和组播报文的数量，分别对应显示信息中 Total(pkt)、Broadcast(pkt)、Multicast(pkt)字段的取值。如果广播和组播报文的增长速度快，广播、组播报文在接口收到的总报文数中占比大，则可能出现广播/组播风暴。如果广播和组播报文数量没有明显增加，但是接口收到的总报文数明显增加，则可能出现未知单播报文风暴。

```
<Sysname> display counters inbound interface
Interface                  Total(pkt) Broadcast(pkt) Multicast(pkt) Err(pkt)
GE5/3/0                           141            27            111        0
MGE0/31/0                      274866         47696              0       --
MGE0/32/0                     1063034        684808              2       --
VMC1/1/0                     11157797       7274558             50        0
VMC1/2/0                      9653898       5619640             52        0

 Overflow: More than 14 digits (7 digits for column "Err").
       --: Not supported.
```

- 如链路出现环路，可进行如下处理：
  - 排查链路连接，避免物理拓扑出现环路。
  - 使用 **display stp** 命令检查 STP 协议是否使能，配置是否正确。如果配置错误，请修改配置。
  - 使用 **display stp brief** 和 **display stp abnormal-port** 命令检查邻接设备 STP 状态是否正常。请根据 **display stp abnormal-port** 命令显示信息中的 BlockReason 字段的取值，定位并解决 STP 异常问题。

如 STP 配置均正确，可能为 STP 协议计算错误或协议计算正确但端口驱动层没有正常 Block 阻塞，可以在发生环路的接口上执行 **shutdown/undo shutdown** 命令或者拔插网线让 STP 重新计算来快速恢复 STP 功能，消除环路。

  - 在以太网接口视图下，使用 **broadcast-suppression** 命令开启端口广播风暴抑制功能，使用 **multicast-suppression** 命令开启端口组播风暴抑制功能，使用 **unicast-suppression** 命令开启端口未知单播风暴抑制功能。或者使用 **flow-control** 命令配置流量控制功能。（**broadcast-suppression**、**multicast-suppression**、**unicast-suppression** 和 **flow-control** 命令的支持情况与设备的型号有关，请以设备的实际情况为准）
  - 使用 QoS 策略针对组播、广播和未知单播报文进行限速。
- 如未出现环，请执行 5.4 确认是否配置了流统计和采样功能，以及配置的参数是否合适

5.4 确认是否配置了流统计和采样功能，以及配置的参数是否合适

当设备上配置了 NetStream、sFlow 等网络流量监控功能后，设备会对网络流量进行统计分析。如果网络流量较高，可能会导致 CPU 占用率偏高。此时，可进行以下处理：

- 配置过滤条件来精确匹配流量，仅统计分析用户关心的流量。
- 配置采样器，调整采样比例，使得 NetStream、sFlow 收集到的统计信息既能基本反映整个网络的状况，又能避免统计报文过多影响设备转发性能。

5.5 确认设备当前是否正在生成海量日志

某些异常情况下，例如，设备受到攻击、运行中发生了错误、端口频繁 Up/Down 等，设备会不停地产生诊断信息或日志信息。此时系统软件要频繁的读写存储器，会造成 CPU 占用率升高。

可通过以下方式来判断设备是否正在生成海量日志：

- Telnet 登录到设备，配置 **terminal monitor** 命令允许日志信息输出到当前终端。

  ```
  <Sysname> terminal monitor
  The current terminal is enabled to display logs.
  ```

  配置该命令后，如果有大量异常日志或者重复日志输出到命令行界面，则说明设备正在生成海量日志。
- 重复执行 **display logbuffer summary** 命令，如果日志信息总量有明显的增加，再使用 **display logbuffer reverse** 命令查看日志详情，确认是否有大量异常日志或者某一条信息大量重复出现。

  ```
  <Sysname> display logbuffer summary
    Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
       1     0     0     2     9    24    12   128     0
       5     0     0     0    41    72     8     2     0
      97     0     0    42    11    14     7    40     0
  <Sysname> display logbuffer reverse
  Log buffer: Enabled
  Max buffer size: 1024
  Actual buffer size: 512
  Dropped messages: 0
  Overwritten messages: 0
  ```

```
Current messages: 410
%Jan 15 08:17:24:259 2021 Sysname SHELL/6/SHELL_CMD:
-Line=vty0-IPAddr=192.168.2.108-User=**; Command is display logbuffer
%Jan 15 08:17:19:743 2021 Sysname SHELL/4/SHELL_CMD_MATCHFAIL:
-User=**-IPAddr=192.168.2.108; Command display logfile in view shell failed to be
matched.
...
```

如果设备正在生成海量日志，可以通过以下方法减少日志的生成：

- 关闭部分业务模块的日志输出功能。
- 使用 **info-center logging suppress** 命令禁止指定模块日志的输出。
- 使用 **info-center logging suppress duplicates** 命令开启重复日志抑制功能。

如果设备未生成海量日志，则执行步 5.6 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员

5.6 如果故障仍然未能排除，请收集如下信息，并联系技术支持人员

- 上述步骤的执行结果。
- 设备的配置文件、日志信息、告警信息。

6 CPU 占用率高的典型案例

6.1 网络存在二层环路引起的CPU占用率高

6.1.1 现象描述

设备的 CPU 占用率出现大幅度的上升，设备的端口出现异常的波动，一些端口在短时间内重复收到相同的数据包。

6.1.2 根源说明

端口在短时间内重复收到相同的数据包，可能是由于网络存在二层环路所引起。二层环路是指在网络拓扑结构中出现的一个或多个路径，这些路径将形成一个环路，导致广播暴风和网络流量的无限循环。

6.1.3 判断方法

(1) 执行 **display cpu-usage summary** 命令查看 CPU 占用率的统计信息，CPU 占用率达 88%，判断 CPU 占用率过高。

```
<Sysname> display cpu-usage summary
Slot CPU        Last 5 sec        Last 1 min        Last 5 min
1    0          88%                83%                81%
```

(2) 清除接口的统计信息。

```
<Sysname> reset counters interface
```

(3) 多次执行 **display counters rate inbound interface** 命令查看端口使用率有明显增大。

第二次执行 **display counters rate inbound interface** 命令

```
<Sysname> display counters rate inbound interface
Usage: Bandwidth utilization in percentage
Interface               Usage(%)     Total(pps) Broadcast(pps) Multicast(pps)
GE1/0/1                  10.01       4527863793  2677938345     2683457793
GE1/0/2                  9.23        5727856379  2476385793     2876453793
......
 Overflow: More than 14 digits.
       --: Not supported.
```

第二次执行 **display counters rate inbound interface** 命令

```
<Sysname> display counters rate inbound interface
Usage: Bandwidth utilization in percentage
Interface               Usage(%)     Total(pps) Broadcast(pps) Multicast(pps)
GE1/0/1                  78.12       Overflow     Overflow      Overflow
GE1/0/2                  80.81       Overflow     Overflow      Overflow
......
 Overflow: More than 14 digits.
       --: Not supported.
```

(4) 执行 **display mac-address mac-move** 命令，查看设备的 MAC 地址迁移记录。

```
<Sysname> display mac-address mac-move
MAC address    VLAN Current port  Source port   Last time           Times
0000-0001-002c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0000-0001-002c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
0000-0001-003c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0000-0001-003c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
0000-0001-004c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0000-0001-004c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
0100-0001-005c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0100-0001-005c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
0100-0001-006c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0100-0001-006c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
0100-0001-007c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0100-0001-007c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
......
---  121 MAC address moving records found  ---
```

由此可确认设备发生大量 MAC 地址迁移，网络存在二层环路。

6.1.4 解决方法

- 排查链路连接，避免物理拓扑出现环路。
- 使用 **display stp** 命令检查 STP 协议是否使能，配置是否正确。如果配置错误，请修改配置。
- 使用 **display stp brief** 和 **display stp abnormal-port** 命令检查邻接设备 STP 状态是否正常。请根据 **display stp abnormal-port** 命令显示信息中的 BlockReason 字段的取值，定位并解决 STP 异常问题。
- 如 STP 配置均正确，可能为 STP 协议计算错误或协议计算正确但端口驱动层没有正常 Block 阻塞，可以在发生环路的接口上执行 **shutdown/undo shutdown** 命令或者拔插网线让 STP 重新计算来快速恢复 STP 功能，消除环路。
- 在以太网接口视图下，使用 **broadcast-suppression** 命令开启端口广播风暴抑制功能，使用 **multicast-suppression** 命令开启端口组播风暴抑制功能，使用 **unicast-suppression** 命令开启端口未知单播风暴抑制功能。或者使用 **flow-control** 命令配置流量控制功能。（**broadcast-suppression**、**multicast-suppression**、**unicast-suppression** 和 **flow-control** 命令的支持情况与设备的型号有关，请以设备的实际情况为准）
- 使用 QoS 策略针对组播、广播和未知单播报文进行限速。

6.2 设备受到ARP报文攻击引起CPU占用率高

6.2.1 现象描述

一台核心交换机的 CPU 占用率上升到 95%以上，该交换机连接的所有设备均无法正常通信，导致网络中断和服务停止。

6.2.2 根源说明

由于攻击者向网络中发送了大量的 ICMP 报文，导致交换机的 CPU 负载过高，无法处理正常的网络流量。

6.2.3 判断方法

(1) 执行 display cpu-usage summary 命令查看 CPU 占用率的统计信息，CPU 占用率达 88%，判断 CPU 占用率过高。

```
<Sysname> display cpu-usage summary
Slot CPU        Last 5 sec        Last 1 min        Last 5 min
1    0          98%                93%                91%
```

(2) Probe 视图下执行 **display system internal control-plane statistics** 命令，查看控制平面报文的统计信息

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] probe
[Sysname-probe] display system internal control-plane statistics slot 1
Control plane slot 1
  Protocol: Default
    Bandwidth: 15360 (pps)
    Forwarded: 108926 (Packets), 29780155 (Bytes)
    Dropped  : 0 (Packets), 0 (Bytes)
  Protocol: ARP
    Bandwidth: 512 (pps)
    Forwarded: 1489284 (Packets), 55318920 (Bytes)
    Dropped  : 1221124 (Packets), 4491421 (Bytes)
...
```

设备控制平面存在大量 ARP 报文丢弃。

(3) Probe 视图下执行 **debug rxtx softcar show** 命令，

```
[Sysname-probe] debug rxtx softcar show slot 1

ID  Type                RcvPps Rcv_All    DisPkt_All Pps  Dyn Swi Hash Am APps
0   ROOT                0      0          0          200  S   On  SMAC 0 0
1   ISIS                0      0          0          200  D   On  SMAC 8 512
2   ESIS                0      0          0          100  S   On  SMAC 8 512
…
31  ARP                 143    183008857  59300      750  S   On  SMAC 8 -
…
```

有大量 ARP 报文上送 CPU

以上信息标明，判断设备正在遭受 ARP 攻击。

6.2.4 解决方法

(1) 执行 **debugging arp packet** 命令用来打开 ARP 的报文调试信息开关。

```
<Sysname> debugging arp packet
```

```
*May 14 18:14:36:453 2023 S105-IRF ARP/7/ARP_RCV: -MDC=1-Chassis=1-Slot=7; Received an
ARP message, operation: 1, sender MAC: 0024-7e04-578d, sender IP: 192.168.50.30, target
MAC: 0000-0000-0000, target IP: 192.168.50.1
*May 14 18:14:36:453 2023 S105-IRF ARP/7/ARP_RCV: -MDC=1-Chassis=1-Slot=7; Received an
ARP message, operation: 1, sender MAC: 0024-7e04-578d, sender IP: 192.168.50.30, target
MAC: 0000-0000-0000, target IP: 192.168.50.2
*May 14 18:14:36:453 2023 S105-IRF ARP/7/ARP_RCV: -MDC=1-Chassis=1-Slot=7; Received an
ARP message, operation: 1, sender MAC: 0024-7e04-578d, sender IP: 192.168.50.30, target
MAC: 0000-0000-0000, target IP: 192.168.50.3
*May 14 18:14:36:453 2023 S105-IRF ARP/7/ARP_RCV: -MDC=1-Chassis=1-Slot=7; Received an
ARP message, operation: 1, sender MAC: 0024-7e04-578d, sender IP: 192.168.50.30, target
MAC: 0000-0000-0000, target IP: 192.168.50.4
…
```

以上信息标明，设备受到源 MAC 地址为 0024-7e04-578d 的 ARP 攻击。

(2) 配置指定源 MAC 地址的 ARP 报文限速功能

```
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]arp rate-limit source-mac 0024-7e04-578d 50
```

(3) 配置源 MAC 地址固定的 ARP 攻击检测功能

```
[Sysname]arp source-mac filter
```

7 如何避免 CPU 占用率高

- 开启环路检测与生成树功能，并避免出现环路
- 配置攻击防御相关功能，防止设备受到网络攻击。
- 设备提供了多种攻击防御技术对局域网中的攻击、检测和解决方法。有关攻击防御的详细介绍请参见“安全配置指导”中的相关内容。
- 定期更新操作系统和固件版本：定期更新操作系统和固件版本可以避免安全漏洞和性能问题，确保设备的正常运行和安全性。
- 按需设置端口镜像：端口镜像可用于监控和检测网络流量，并及早发现网络中的异常流量和威胁。
- 配置合理的端口安全策略：运用合理的端口安全策略，可以限制网络中的恶意流量，保护设备和网络的安全性。
- 启用防御大流量攻击功能：大流量攻击是一种常见的网络攻击，启用防御大流量攻击功能可以有效地防止设备被占用过高的 CPU 资源。

8 相关告警与日志

8.1.1 相关告警

- hh3cEntityExtCpuUsageThresholdNotfication
- hh3cEntityExtCpuUsageThresholdRecover
- hh3cCpuUsageSevereNotification
- hh3cCpuUsageSevereRecoverNotification
- hh3cCpuUsageMinorNotification
- hh3cCpuUsageMinorRecoverNotification

8.1.2 相关日志

- DIAG/5/CPU_MINOR_RECOVERY
- DIAG/4/CPU_MINOR_THRESHOLD
- DIAG/5/CPU_SEVERE_RECOVERY
- DIAG/3/CPU_SEVERE_THRESHOLD