CPU 占用率高怎么办

文档版本 01

发布日期 2020-11-13

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 CPU 占用率高怎么办?

1.1 简介

当设备转发面上送CPU的报文速率过快或者某任务长时间占用CPU时，CPU将高负荷运行，可能无法及时调度其他任务，进而引发业务异常。

本文档简要介绍了CPU占用率高的定位步骤、CPU占用率高的解决方法、以及CPU占用率高的典型案例。

1.2 引起 CPU 占用率高的常见原因

根据现网排查情况，常见引起交换机CPU占用率高的原因如下：

- 网络攻击
- 网络震荡（包括STP震荡和路由协议震荡）
- 网络环路
- 设备配置流采样功能，占用大量CPU资源
- 设备产生海量日志，占用大量CPU资源

1.3 如何定位 CPU 占用率高

1.3.1 查看设备及版本信息

使用**display version**和**display device**命令查看交换机的版本信息及部件类型，将获取的信息记录下来，以供后续排查时使用。

步骤1 通过**display version**命令的回显，查看交换机的版本信息。

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 8.160 (CE12800 V200R003C00SPC200)
Copyright (C) 2012-2017 Huawei Technologies Co., Ltd.
HUAWEI CE12804 uptime is 11 days, 1 hour, 27 minutes

BKP  version information:
1.PCB      Version  : DE01BAK04A VER C
2.Board    Type     : CE-BAK04A
3.MPU Slot Quantity : 2
4.LPU Slot Quantity : 4
5.SFU Slot Quantity : 6
......
```

关注“VRP (R) software, Version 8.160”字段，可以看出这台CE12800系列框式交换机为V200R003C00版本。

步骤2 通过**display device**命令的回显，查看交换机的型号、是否是堆叠系统、交换机上使用的业务板（仅框式交换机有业务板）有哪些类型等。

```
<HUAWEI> display device
CE12804's Device status:
-------------------------------------------------------------------------------
Slot  Card  Type                Online   Power Register     Alarm     Primary
-------------------------------------------------------------------------------
2     -     CE-L12LQ-EA          Present  On    Registered   Normal    NA
4     -     CE-L48XS-EF          Present  On    Registered   Normal    NA
6     -     CE-MPUA              Present  On    Registered   Normal    Master
7     -     CE-CMUA              Present  On    Registered   Normal    Slave
8     -     CE-CMUA              Present  On    Registered   Normal    Master
9     -     CE-SFU04C            Present  On    Registered   Normal    NA
10    -     CE-SFU04C            Present  On    Registered   Normal    NA
11    -     CE-SFU04B            Present  On    Registered   Normal    NA
PWR1  -     PAC-2700WA           Present  On    Registered   Normal    NA
FAN1  -     FAN-12C              Present  On    Registered   Normal    NA
FAN2  -     FAN-12C              Present  On    Registered   Normal    NA
FAN3  -     FAN-12C              Present  On    Registered   Normal    NA
FAN4  -     FAN-12C              Present  On    Registered   Normal    NA
FAN5  -     FAN-12C              Present  On    Registered   Normal    NA
FAN6  -     FAN-12C              Present  On    Registered   Normal    NA
FAN7  -     FAN-12C              Present  On    Registered   Normal    NA
FAN8  -     FAN-12C              Present  On    Registered   Normal    NA
FAN9  -     FAN-12C              Present  On    Registered   Normal    NA
-------------------------------------------------------------------------------
```

----结束

1.3.2 查看 CPU 占用率

查看CPU占用率，方法有以下几种：

- 执行**display cpu** [**slot** *slot-id*]命令，查看CPU占用率。

  隔几秒连续执行**display cpu** [**slot** *slot-id*]命令，观察“System CPU Using Percentage”字段是否持续保持较高百分比。

说明

如果CPU平均使用率（“System CPU Using Percentage”字段）持续高于75%，或者单个CPU的使用率（“Current”字段）持续高于75%，那么可以确认CPU使用率偏高。

```
<HUAWEI> display cpu
CPU utilization statistics at 2017-12-01 11:17:44 945 ms
System CPU Using Percentage :  12%
CPU utilization for five seconds: 12%, one minute: 12%, five minutes: 11%.
Max CPU Usage :              37%
Max CPU Usage Stat. Time : 2017-11-28 16:55:21 599 ms
State: Non-overload
Overload threshold:  90%, Overload clear threshold:  75%, Duration:  480s
----------------------------
ServiceName  UseRate
----------------------------
SYSTEM          12%
AAA             0%
... ...
----------------------------
CPU Usage Details
-------------------------------------------------------------------
CPU     Current  FiveSec   OneMin  FiveMin  Max MaxTime
-------------------------------------------------------------------
cpu0       21%      22%      21%      19%  59% 2017-11-20 09:43:19
cpu1       12%      12%      13%      12%  64% 2017-11-20 09:43:19
cpu2       12%      11%      11%      11%  69% 2017-11-20 09:43:09
cpu3        3%       3%       3%       3%   8% 2017-11-20 09:43:09
-------------------------------------------------------------------
```

通过显示信息，获取CPU占用率较高的任务，并重点关注占用率最高的前3个任务，以判断引起CPU占用率高的初步原因，详细信息请参考**1.3.3 根据任务的CPU占用率排序判断初步原因**。

- 在网管系统上查看是否有相关告警。

  当交换机部署了网管系统时，可以在网管系统上查看CPU占用率高的相关告警。

  当CPU占用率超过告警阈值（可在系统视图下通过**set cpu threshold**命令配置，缺省情况下，V100R005C00及之前版本告警阈值为95%，V100R005C10及之后版本为90%），系统会向网管发送告警**SYSTEM_1.3.6.1.4.1.2011.5.25.129.2.4.1 hwCPUUtilizationRisingAlarm**，管理用户可通过这些信息获取CPU占用率过高的记录。

- 查看日志是否有CPU占用率高的记录。

  通过查看系统日志文件或执行**display logbuffer**命令查看设备的日志信息，查看设备是否产生了CPU占用率高的日志。

  系统日志可以查看历史及当前是否有CPU占用率高的记录。

  相关日志信息为：**SYSTEM/1/hwCPUUtilizationRisingAlarm_active**。

1.3.3 根据任务的 CPU 占用率排序判断初步原因

通过查看**display cpu** [**slot** *slot-id*]命令的显示信息，获取CPU占用率较高的任务，并重点关注占用率最高的前3个任务。

请根据**表1-1**来查询引起CPU占用率高的原因及解决措施。

表 1-1 常见 CPU 占用率高的任务及解决措施

任务名称	任务解释	导致CPU占用率高的可能原因	解决措施
SYSTEM	系统管理	大量协议报文处理	检查是否存在网络攻击
DEVICE	设备管理	接口闪断	检查是否存在网络震荡
CMF	配置管理框架	批量配置下发或SNMP查询	检查是否存在大量SNMP报文上送或配置下发
NETSTREAM	流采样	大量报文采样	检查是否配置流采样功能
SFLOW	采样流	大量报文采样	检查是否配置采样流功能
FEA	业务适配层	执行批量配置备份或任务	检查是否存在批量任务执行
IP STACK	协议栈	路由协议震荡	检查是否存在路由协议震荡
LOCAL PKT	主机报文收发	大量协议报文上送	检查是否存在网络攻击

如果您的交换机CPU占用率高的任务不在以上表格里，请参考《什么是CPU和CPU占用率？》，查询是什么业务引起。

如果您的交换机CPU占用率高的任务既不在以上表格里，也不在《什么是CPU和CPU占用率？》里，请联系技术支持人员进行处理。

通过上述表格，只能大致判断出引起CPU占用率高的原因，具体原因还要结合后续排查手段进行问题定位并处理，详细信息请参考**1.4 如何解决CPU占用率高**。

1.4 如何解决 CPU 占用率高

1.4.1 判断为网络攻击引起

现网中导致CPU占用率高的原因，很大一部分是由于网络攻击引起。网络攻击是由于网络中的主机或者网络设备通过发起大量的非正常网络交互对交换机产生冲击，影响交换机的安全性和正常的业务运行。发生网络攻击时，交换机忙于处理来自于攻击源的非正常网络交互请求，具体表现均为某些任务大量占用CPU，导致CPU占用率高。

常见的网络攻击

常见的网络攻击包括ARP、ARP-Miss以及DHCP等协议报文攻击，这些攻击行为的共同特点是攻击源产生大量的协议报文对设备进行冲击，因此可以在设备上看到大量上送CPU的报文统计。

- ARP协议报文攻击和ARP-Miss协议报文攻击
  - ARP和ARP-Miss泛洪攻击
  - ARP欺骗攻击

- DHCP协议报文攻击
- 其他攻击
  - ICMP攻击
  - DDoS攻击
  - 广播报文攻击
  - TTL-expired报文攻击
  - 目的IP为设备IP的报文攻击
  - SSH/FTP/Telnet等应用层协议报文攻击

网络攻击的定位方法

步骤1 使用**display version**和**display device**命令查看交换机的版本信息及部件类型，将获取的信息记录下来，以供后续排查时使用。

步骤2 使用**display cpu-defend statistics all**命令查看上送CPU报文的统计信息，判断是否存在过多由于来不及处理而丢弃的协议报文。

1. 执行**reset cpu-defend statistics all**命令，清除上送CPU报文的统计信息。
2. 隔几秒后执行**display cpu-defend statistics all**命令，查看上送CPU报文的统计信息。

   如果观察到某种协议报文过多，根据组网判断是否可能出现这么多的协议报文。如果不可能出现这么多协议报文，则可基本判断为协议报文的攻击。

```
<HUAWEI> reset cpu-defend statistics all
<HUAWEI> display cpu-defend statistics all
Statistics(packets) on slot 1 :
------------------------------------------------------------------------------
PacketType             Total Passed       Total Dropped   Last Dropping Time
                 Last 5 Min Passed   Last 5 Min Dropped
------------------------------------------------------------------------------
arp                      784824               0   -
                           8                  0
arp-miss                    0                 0   -
                           0                  0
fib-hit                  25993                0   -
                           0                  0
snmp                     4922372                0   -
                         599                 0
telnet                     425                0   -
                           0                  0
......
------------------------------------------------------------------------------
```

步骤3 使用本机防攻击的攻击溯源功能找出攻击源。

设备提供本机防攻击功能来保护CPU，解决CPU因处理大量正常上送CPU的报文或者恶意攻击报文造成的业务中断问题。

1. 创建基于攻击溯源的本机防攻击策略。

```
<HUAWEI> system-view
[~HUAWEI] cpu-defend policy policy1   //创建防攻击策略
[*HUAWEI-cpu-defend-policy-policy1] auto-defend enable   //使能攻击溯源功能
[*HUAWEI-cpu-defend-policy-policy1] auto-defend trace-type source-ip source-mac   //配置攻击溯源的溯源模式为基于源MAC地址和源IP地址
[*HUAWEI-cpu-defend-policy-policy1] auto-defend protocol all   //匹配防范所有协议报文
[*HUAWEI-cpu-defend-policy-policy1] quit
[*HUAWEI] cpu-defend-policy policy1   //全局应用攻击溯源策略
[*HUAWEI] commit
```


配置基于攻击溯源的本机防攻击功能后，可以执行命令**display auto-defend attack-source**查看攻击源的信息（IP和MAC地址）。

```
<HUAWEI> display auto-defend attack-source
 Attack Source User Table on Slot 1 :
 ------------------------------------------------------------------------------
 MAC Address      Interface       PacketType    VLAN:Outer/Inner     Total
 ------------------------------------------------------------------------------
 0000-c102-0102   10GE1/0/1       ICMP          1000/                4832
 ------------------------------------------------------------------------------
 Total: 1
 Attack Source IP Table on Slot 1 :
 ------------------------------------------------------------------------------
 IP Address      PacketType    Total
 ------------------------------------------------------------------------------
 10.1.1.2        ICMP          1144
 ------------------------------------------------------------------------------
 Total: 1
 Attack Source Port Table on Slot 1 :
 ------------------------------------------------------------------------------
 Interface       VLAN:Outer/Inner     PacketType     Total
 ------------------------------------------------------------------------------
 10GE1/0/1       1000/--              ICMP           4832
 ------------------------------------------------------------------------------
 Total: 1
```

----结束

网络攻击的处理建议

根据查看到的攻击源信息，结合现网情况，选择处理方法。

- 配置ARP安全功能，防范ARP协议攻击。

  针对ARP和ARP-Miss协议报文攻击，可以部署ARP安全功能，来防止设备后续遭受这类攻击。

  设备提供了多种ARP安全的解决方案，请参考产品文档的“配置-安全配置指南-ARP安全配置”进行配置。

- 配置攻击溯源的惩罚功能，在指定周期内丢弃识别为攻击的报文。

  # 使能攻击溯源的惩罚功能，在300秒内，将识别为攻击的报文全部丢弃。

  ```
  <HUAWEI> system-view
  [~HUAWEI] cpu-defend policy policy1
  [*HUAWEI-cpu-defend-policy-policy1] auto-defend enable
  [*HUAWEI-cpu-defend-policy-policy1] auto-defend action deny timeout 300  //（缺省情况下，未使能攻击溯源的惩罚功能）
  [*HUAWEI-cpu-defend-policy-policy1] commit
  ```

- 配置黑名单功能，直接丢弃黑名单用户上送的报文。

  如果判断攻击源为特定用户的恶意报文攻击，可通过ACL把符合特定特征的用户纳入到黑名单中，被纳入黑名单的用户发送的攻击报文到达设备CPU后均会被丢弃。

  假设攻击源的IP为10.1.1.0/24，配置ACL匹配该IP，丢弃攻击报文。

  ```
  <HUAWEI> system-view
  [~HUAWEI] acl number 2001
  [*HUAWEI-acl4-basic-2001] rule permit source 10.1.1.0 0.0.0.255
  [*HUAWEI-acl4-basic-2001] quit
  [*HUAWEI] cpu-defend policy policy1
  [*HUAWEI-cpu-defend-policy-policy1] blacklist 1 acl 2001
  [*HUAWEI-cpu-defend-policy-policy1] commit
  ```

- 配置攻击溯源的惩罚功能，将攻击报文进入的接口**Error-down**，避免攻击源继续攻击设备。

如果判断攻击报文来自某端口，并且将该端口**Error-down**，不会对设备业务造成影响，可以使用该方法。

须知

如果配置攻击溯源的惩罚措施是将攻击报文进入的接口**Error-down**，有可能会造成设备业务的中断，接口下合法的用户会受牵连，请谨慎使用。

配置攻击溯源的惩罚措施为将攻击报文进入的端口**Error-down**。

```
<HUAWEI> system-view
[~HUAWEI] cpu-defend policy policy1
[*HUAWEI-cpu-defend-policy-policy1] auto-defend enable
[*HUAWEI-cpu-defend-policy-policy1] auto-defend action error-down
[*HUAWEI-cpu-defend-policy-policy1] commit
```

1.4.2 判断为网络震荡引起

出现网络震荡时，网络频繁变动，设备忙于处理网络切换事件，导致CPU占用率高。常见的网络震荡情况包括STP震荡和OSPF路由协议震荡。

STP 震荡

在STP频繁震荡时，设备需要不断进行STP拓扑计算，更新MAC表、ARP表等转发表，引起CPU占用率高。

1. **定位方法**

   当怀疑网络中存在频繁的STP震荡时，可以通过隔几秒连续执行**display stp topology-change**命令查看当前STP的拓扑变化信息，也可以查看设备输出的告警和日志信息观察设备是否产生过STP拓扑变化。

   隔几秒连续执行一次该命令，查看设备上STP拓扑变化统计信息，观察“Number of topology changes”是否有增长。

```
<HUAWEI> display stp topology-change
 CIST topology change information
   Number of topology changes           :5
   Time since last topology change      :0 days 0h:23m:19s
   Topology change initiator(detected)    :10GE1/0/1
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3
```

   确认存在频繁的网络拓扑变化后，隔几秒连续执行**display stp tc-bpdu statistics**命令查看端口接收到的TC-BPDU统计，以确定TC（Topology Change）报文的来源，找到发送拓扑变化的设备。

```
<HUAWEI> display stp tc-bpdu statistics
 ------------------------- STP TC/TCN information -------------------------
 MSTID Port                  TC(Send/Receive)      TCN(Send/Receive)
 0     10GE1/0/3             2/3                   0/0
 1     10GE1/0/5             1/0                   -/-
```

   - 如果显示信息中只有“TC(Send)”计数增长，表明是本设备发生拓扑变化。
     - 如果只是单个接口的“TC(Send)”计数增长，确定是该接口产生震荡。
     - 如果是多个接口的“TC(Send)”计数增长，请查看网管事件和日志信息分析STP拓扑变化的根因，确定是哪个端口频繁震荡。
   - 如果显示信息中“TC(Send/Receive)”计数均有增长，先查看本设备网管事件和日志信息排查本设备是否发生拓扑变化，产生STP震荡，再排查与发生问题的端口连接的设备是否产生STP震荡。

2. **处理建议**

   a. 打开TC保护的告警开关，帮助管理用户了解设备对TC报文的具体处理情况。

   系统视图下，执行命令**snmp-agent trap enable feature-name mstp**和**stp tc-protection**，打开TC保护功能和告警。

   说明

   - 告警开关打开后，设备会触发MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.15 hwMstpiTcGuarded和MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.16 hwMstpProTcGuarded两个告警。
   - 设备开启防拓扑变化攻击功能后，在**stp tc-protection threshold** *interval-value* 命令指定的生成树协议处理最大数量的TC报文所需的时间内（默认2s），设备只会处理**stp tc-protection threshold** *threshold*指定的最大数量的TC报文（默认1个）。

   b. 根据拓扑变化情况进行处理。

   对于接入侧端口Up/Down引起的STP拓扑变化，可以配置STP边缘端口或开启STP-BPDU保护功能，减少BPDU对CPU的冲击，配置命令如下：

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] stp edged-port enable   //配置端口为边缘端口
[*HUAWEI-10GE1/0/1] quit
[*HUAWEI] stp bpdu-protection   //使能BPDU保护功能
[*HUAWEI] commit
```

OSPF 路由协议震荡

路由协议震荡会导致路由信息的重新扩散和路由表的重新计算，对设备CPU产生影响。交换机的实际应用中，通常使用OSPF协议对动态路由信息进行管理，因此这里介绍常见的OSPF路由协议震荡。

1. **定位方法**

   – 通过命令**display ospf peer last-nbr-down**查看OSPF邻居状态Down的原因。

   根据输出信息的“Immediate Reason”字段和“Primary Reason”字段查看原因。

   – 通过日志查看OSPF邻居状态Down的原因。

   执行**display logbuffer**命令，查看如下日志信息：

```
OSPF/3/NBR_DOWN_REASON: Neighbor state left full or changed to Down.
(ProcessId=[ProcessId], NeighborRouterId=[NbrRouterId], NeighborIp=[NbrIp],
NeighborAreaId=[NbrAreaId], NeighborInterface=[IfName], NeighborDownImmediate
reason=[NbrImmReason], NeighborDownPrimeReason=[NbrPriReason], CpuUsage=[CpuUsage])
```

   “NeighborDownImmediate reason”关键字记录的是OSPF邻居Down的原因。

2. **处理建议**

   根据关键字段判断原因并采取相应措施。

   OSPF邻居Down的原因一般会有以下几种：

   – Neighbor Down Due to Inactivity

   表示在deadtime时间（在接口视图下通过**ospf timer dead** *interval*命令配置）内没有收到Hello报文导致OSPF邻居Down。

   OSPF邻居Down一般包括OSPF邻居震荡和OSPF邻居建立不起来。持续执行**display ospf peer brief**命令，查看当前是OSPF邻居震荡还是OSPF邻居无法建立。

- OSPF邻居震荡

  设备上OSPF CPCAR值过小、接口链路震荡或接口链路拥塞、大量LSA flooding都会导致OSPF邻居关系震荡。

  1) 执行命令**display cpu-defend statistics packet-type ospf**查看上送CPU的OSPF报文统计信息，如果OSPF丢包过多，请排查设备是否受到OSPF报文攻击或OSPF的CPCAR值设置过小。
  2) 通过日志信息查看接口Up/Down的记录情况。如果出现链路震荡或链路拥塞，请对接口链路进行检查。
  3) 如果配置的OSPF邻居失效时间小于20s，建议在接口视图下通过**ospf timer dead** *interval*命令将OSPF邻居失效时间配置为20s以上。
  4) 如果执行上述措施后仍然无法解决问题，建议联系技术支持人员。

- OSPF邻居无法建立

  排查两端OSPF视图下的配置是否一致，如果区域ID，区域类型（NSSA区域、STUB区域、普通区域）等配置不一致，会导致邻居无法建立。

  执行命令**display ospf** [*process-id*] **interface**查看Interface字段，检查对应的接口是否被成功使能OSPF。

  ```
  <HUAWEI> display ospf 1 interface

  OSPF Process 1 with Router ID 192.168.5.5

   Area: 0.0.0.0          MPLS TE not enabled

   Interface           IP Address      Type        State    Cost    Pri
   Vlanif200           192.168.3.1     Broadcast   DR       1       1
  ```

  - 如果对应的接口没有使能OSPF，请在接口视图下执行命令**ospf enable** [*process-id*] **area** *area-id*将接口使能OSPF。
  - 如果对应的接口已经被使能到OSPF进程，请隔几秒连续执行**display ospf error**命令，查看Bad authentication type和Bad authentication key字段，确认两端设备的OSPF认证信息是否匹配：

    ```
    <HUAWEI> display ospf error
            OSPF Process 1 with Router ID 10.1.1.1
                  OSPF error statistics

    General packet errors:
     0      : IP: received my own packet     0      : Bad packet
     0      : Bad version                    0      : Bad checksum
     0      : Bad area id                    0      : Drop on unnumbered interface
     0      : Bad virtual link               0      : Bad authentication type
     0      : Bad authentication key         0      : Packet too small
     0      : Packet size > ip length        0      : Transmit error
     0      : Interface down                 0      : Unknown neighbor
    ```

    如果Bad authentication type或者Bad authentication key计数持续增长，说明两端的OSPF认证信息不匹配，请在接口视图下执行**ospf authentication-mode**命令或者在OSPF区域视图下执行**authentication-mode**命令将两端设备配置相同的认证信息。

– Neighbor Down Due to Kill Neighbor

  表示因为接口Down、BFD Down或执行了**reset ospf process**操作。

  请查看NeighborDownPrimeReason字段判断具体原因。

– Neighbor Down Due to 1-Wayhello Received或Neighbor Down Due to SequenceNum Mismatch

表示因为对端OSPF状态首先变成Down，从而向本端发送1-Wayhello，导致本端OSPF状态也变成Down。

请先排查对端设备的原因。

其它导致OSPF邻居Down的原因，请参考“OSPF/3/NBR_DOWN_REASON”的日志详细信息。

1.4.3 判断为网络环路引起

出现网络环路时，设备上MAC表频繁漂移，同时产生的广播风暴造成大量协议报文上送设备处理，导致CPU占用率高。

1. **定位方法**

   网络出现环路后，一般会有如下现象产生：

   - 设备出现MAC漂移告警，执行**display mac-address flapping**命令可以查询到有MAC漂移记录。
   - 设备CPU占用率偏高。
   - 设备上发生环路的VLAN的接口指示灯频繁闪烁。
   - 管理用户无法远程登录设备，并且使用Console口登录设备进行操作时，操作比较慢。
   - 通过**ping**命令进行网络测试时丢包严重。
   - 执行**display interface**命令查看接口统计信息时，接口有大量广播/组播报文。
   - 设备下接的PC机上能收到大量的广播报文或未知单播报文。

2. **处理建议**

   如果明确故障发生前有配置或连线变更，优先建议回退变更，否则按照如下步骤进行排查：

   a. 通过接口指示灯的闪烁情况和接口流量情况，确认存在广播风暴的接口。

   b. 根据链路拓扑，逐跳排查产生环路的设备。

   c. 判断产生环路的接口并破环。

   d. 如果执行上述措施后仍然无法解决问题，请收集组网信息、设备配置文件、日志信息和告警信息，联系技术支持人员。

1.4.4 判断为流采样功能引起

设备配置了流采样功能时，由于流量较高、采样比较高可能会导致CPU占有率偏高。

1. **定位方法**

   如果通过命令**display cpu** [**slot** *slot-id*]查询到“FEA”+“NETSTREAM”或“FEA”+“SFLOW”任务占用CPU高，表示设备配置了流采样功能，且流量较高或采样比较高。

2. **处理建议**

   查询流采样配置，根据接口的流量，调低流量采样比，观察CPU占有率是否有下降到合适水平。

   - 调整NetStream采样比。

     - 在系统视图下调整所有接口的采样功能。

       ```
       <HUAWEI> system-view
       [~HUAWEI] netstream sampler random-packets 32768 inbound
       ```

```
[*HUAWEI] netstream sampler random-packets 32768 outbound
[*HUAWEI] commit
```

- 在接口视图下调整该接口的采样功能。

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] netstream sampler random-packets 32768 inbound
[*HUAWEI-10GE1/0/1] netstream sampler random-packets 32768 outbound
[*HUAWEI-10GE1/0/1] commit
```

– 调整sFlow采样比。

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] sflow sampling rate 32768
[*HUAWEI-10GE1/0/1] commit
```

1.4.5 判断为海量日志引起

某些异常情况下如受到攻击、运行中发生了错误、端口频繁Up/Down等，设备会不停打印诊断信息或日志信息。此时对存储器要进行频繁的读写操作，会造成CPU占用率升高。

1. **定位方法**

   执行命令**display logbuffer**，查看是否有大量的异常日志，例如某一条信息不断地大量重复出现。

2. **处理建议**

   根据日志名称查询相应产品的日志参考手册，参照其处理步骤进行处理。

   如果执行上述措施后仍然无法解决问题，请收集组网信息、设备配置文件、日志信息和告警信息，联系技术支持人员。

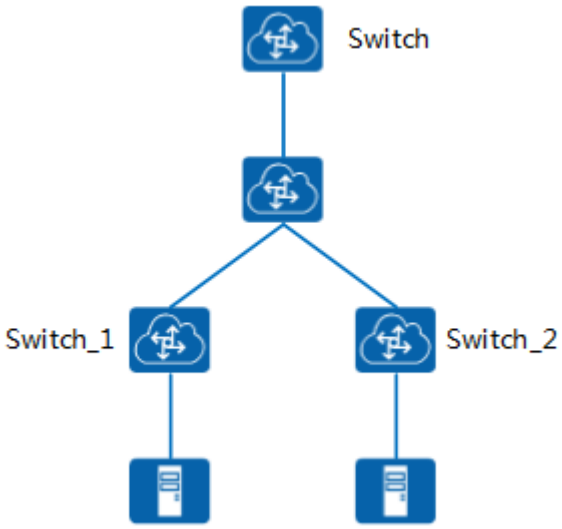
1.5 CPU 占用率高的典型案例

1.5.1 交换机受到 ARP 报文攻击

问题现象描述

如图1-1所示，Switch为网关，Switch_1经常脱管，且Switch_1下用户存在掉线、Ping网关存在时延、不通等现象，而Switch_2下联业务正常、Ping网关正常。

图 1-1 故障组网图



问题根因说明

Switch_1上存在源MAC固定的ARP攻击导致用户无法进行正常ARP交互。

问题判断方法

在Switch_1上执行以下操作：

步骤1 查看设备CPU占用率，判断CPU占用率较高。

```
<HUAWEI> display cpu
CPU utilization statistics at 2015-12-04 11:04:40 820 ms
System CPU Using Percentage :  82%
CPU utilization for five seconds: 82%, one minute: 82%, five minutes: 82%.
Max CPU Usage :              87%
Max CPU Usage Stat. Time : 2015-11-28 16:55:21 599 ms
```

发现CPU占用率达到82%。

步骤2 查看存在临时ARP表项，初步判断设备的ARP表项学习存在问题。

```
<HUAWEI> display arp
ARP Entry Types: D - Dynamic, S - Static, I - Interface, O - OpenFlow
EXP: Expire-time VLAN:VLAN or Bridge Domain

IP ADDRESS      MAC ADDRESS    EXP(M) TYPE/VLAN      INTERFACE       VPN-INSTANCE
-------------------------------------------------------------------------------
10.137.222.139  00e0-fc01-4422       I -           MEth0/0/0
10.1.1.1        200b-c739-130c       I             Vlanif10
10.2.3.4        200b-c739-1316       I             Vlanif200
12.1.1.1        200b-c739-1302       I             10GE4/0/8
12.1.1.2        f84a-bff0-cac2   12  D             10GE4/0/8
50.1.1.2        Incomplete       1   D             10GE4/0/22
50.1.1.3        Incomplete       1   D             10GE4/0/22
......
-------------------------------------------------------------------------------
```

发现有两条ARP表项的“MAC ADDRESS”字段为“Incomplete”即为临时表项，表示有ARP表项学习不到。

步骤3 判断设备正遭受ARP攻击。

1. 由于有未学习到的ARP表项，查看上送CPU的ARP-Request报文统计信息。

```
<HUAWEI> display cpu-defend statistics packet-type arp all
Statistics(packets) on slot 2 :
-------------------------------------------------------------------------------
PacketType            Total Passed       Total Dropped   Last Dropping Time
               Last 5 Min Passed   Last 5 Min Dropped
-------------------------------------------------------------------------------
arp                          0                0   -
                             0                0
-------------------------------------------------------------------------------
Statistics(packets) on slot 4 :
-------------------------------------------------------------------------------
PacketType            Total Passed       Total Dropped   Last Dropping Time
               Last 5 Min Passed   Last 5 Min Dropped
-------------------------------------------------------------------------------
arp                     106549          44380928   -
                          3                0
-------------------------------------------------------------------------------
```

   发现交换机的4号单板上存在大量ARP报文丢包。

2. 配置攻击溯源识别攻击源。

```
<HUAWEI> system-view
[~HUAWEI] cpu-defend policy policy1
[*HUAWEI-cpu-defend-policy-policy1] auto-defend enable
[*HUAWEI-cpu-defend-policy-policy1] auto-defend attack-packet sample 5  //每5个报文抽样识别一次，抽样值过小会消耗过多CPU
[*HUAWEI-cpu-defend-policy-policy1] auto-defend threshold 30  //报文达30pps即被识别为攻击，若攻击源较多可调低该值
[*HUAWEI-cpu-defend-policy-policy1] auto-defend trace-type source-mac  //基于源MAC进行攻击源识别
[*HUAWEI-cpu-defend-policy-policy1] auto-defend protocol arp  //针对ARP攻击进行识别
[*HUAWEI-cpu-defend-policy-policy1] quit
[*HUAWEI] cpu-defend-policy policy1
[*HUAWEI] commit
```

3. 查看攻击源信息。

```
[~HUAWEI] display auto-defend attack-source
Attack Source User Table on Slot 4 :
 ------------------------------------------------------------------------------
 MAC Address      Interface       PacketType    VLAN:Outer/Inner      Total
 ------------------------------------------------------------------------------
 0000-c102-0102   10GE4/0/22      ARP           1000/                 4832
 ------------------------------------------------------------------------------
```

   发现攻击源的MAC地址为0000-c102-0102，位于10GE4/0/22端口。

----结束

解决方案

- 配置黑名单。

```
#
acl number 4000
 rule 10 permit type arp source-mac 0000-c102-0102
#
cpu-defend policy 1
 blacklist 1 acl 4000  //针对来自特定用户恶意报文的攻击，设备通过ACL把符合特定特征的用户纳入到黑名单中，被纳入黑名单的用户所发的报文到达设备后均会被丢弃
#
cpu-defend-policy 1
#
```

- 配置攻击溯源的惩罚功能。

```
#
cpu-defend policy policy1
 auto-defend enable
 auto-defend action deny  //使能攻击溯源的惩罚功能，并指定惩罚措施。在默认惩罚时间300s内，将识别为攻击的报文全部丢弃
 auto-defend alarm enable
```



```
 auto-defend threshold 30
 auto-defend trace-type source-mac
 auto-defend protocol arp
#
cpu-defend-policy policy1
#
```

1.5.2 STP 震荡引起 CPU 占用率高

问题现象描述

一台盒式交换机的CPU占用率过高，交换机输出大量的ARP报文超过CPCAR后丢弃的日志，同时采集端口信息时，发现所有使能STP的端口接收的TC报文计数均在增长。

问题根因说明

端口收到大量的TC报文引起STP震荡，触发大量MAC表项删除、ARP表项刷新，使交换机需要处理大量ARP-Miss、ARP-Request和ARP-Reply报文，导致CPU占用率升高。

问题判断方法

1. 查看告警，设备上出现CPU占用率过高的告警信息。

   ```
   Dec  4 2016 11:37:34 HUAWEI %%01SYSTEM/1/hwCPUUtilizationRisingAlarm(t):CID=0x80020106-OID=1.3.6.1.4.1.2011.5.25.129.2.4.1;The CPU usage exceeded the pre-set overload threshold. (TrapSeverity=3, ProbableCause=74240, EventType=3, PhysicalIndex=17170433, PhysicalName=MPU slot 6, RelativeResource=CPU, UsageType=1, SubIndex=0, CpuUsage=92, Unit=1, CpuUsageThreshold=90)
   ```

2. 设备上还有ARP报文超过CPCAR后丢弃的告警信息。

   ```
   Dec  4 2016 11:45:47 HUAWEI %%01DEFEND/4/hwCpcarDropPacketAlarm(t):CID=0x80e70402-OID=1.3.6.1.4.1.2011.5.25.165.2.2.7.1;Rate of packets to cpu exceeded the CPCAR limit in slot 4. (Protocol=ARP, PPS/CBS=0/0, ExceededPacketCount=20699)
   ```

3. 采集端口TC（Topology Change）报文收发情况。

   隔几秒执行一次**display stp tc-bpdu statistics**命令，查看端口TC/TCN报文收发计数，发现所有使能STP的端口，接收的TC报文计数均在增长。

解决方案

1. 系统视图下执行**stp tc-protection**命令，打开TC保护的告警开关。缺省情况下，TC保护告警开关处于关闭状态。

   打开TC保护告警开关后，可以保证设备频繁收到TC报文时，每2秒周期内最多只处理1次表项刷新，从而减少MAC、ARP表项频繁刷新对设备造成的CPU处理任务过多。

   同时设备会触发MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.15 hwMstpiTcGuarded和MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.16 hwMstpProTcGuarded两个告警。

2. 系统视图下执行**arp topology-change disable**命令，去使能设备响应TC报文的功能。缺省情况下，设备会对收到TC报文进行响应。

   当设备收到TC报文后，默认会对ARP表项进行老化。执行该命令后，当设备收到TC报文时，不对ARP表项进行老化或删除，避免网络拓扑变化频繁时，设备重新的学习ARP表项造成网络中ARP报文过多，导致设备的CPU占用率过高。

3. 系统视图下执行**mac-address update arp enable**命令，使能MAC刷新ARP功能。缺省情况下，MAC刷新ARP功能处于使能状态。

   当设备收到TC报文后，默认会清除MAC表项。执行该命令后，在MAC地址表项出接口刷新时，设备将直接刷新ARP表项的出接口，可以减少大量不必要的ARP表项刷新。

经验总结

在处理CPU高的问题时，需要多关注CPCAR丢包情况。

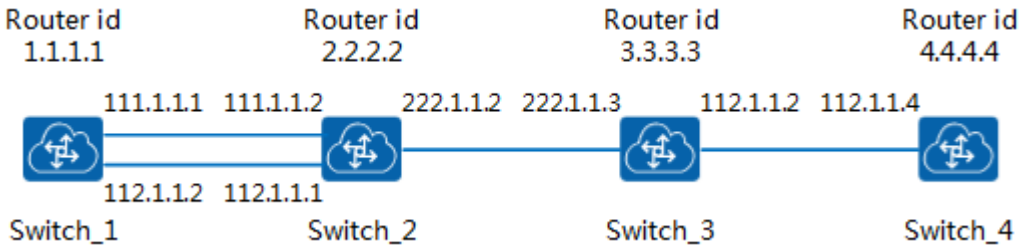
在部署STP时，建议配置TC保护功能，并将所有连接终端的接口配置成边缘端口，这样可以避免某些端口的状态变化引起整个STP网络震荡而重新收敛。

1.5.3 OSPF 震荡引起 CPU 占用率高

问题现象描述

如图1-2所示，Switch_1、Switch_2、Switch_3和Switch_4配置了OSPF协议，发现Switch_1设备的CPU占用率高，ROUT任务占用率明显高于其他任务并且产生路由震荡。

图 1-2 故障组网图



问题根因说明

网络中IP地址冲突导致路由震荡。

问题判断方法

步骤1 在各交换机上每隔一秒执行一次**display ospf lsdb**命令，查看每台交换机的OSPF的LSDB链路状态数据库信息。

步骤2 根据各交换机的回显信息，判断故障点。

- 如果同时出现以下情况，说明LSA老化异常。
  - 一台交换机上发现网段LSA的老化时间（Age）为3600或者没有这条LSA，且Sequence字段增加很快。
  - 其他交换机的相同网段LSA的Age不断在3600和其他较小值之间切换，而且Sequence字段增加很快。

```
<HUAWEI> display ospf lsdb

OSPF Process 100 with Router ID 3.3.3.3
Link State Database

Area: 0.0.0.0
--------------------------------------------------------------------------
Type      LinkState ID    AdvRouter       Age    Len Sequence       Metric
Router    4.4.4.4         4.4.4.4           2     48 8000000D           1
Router    3.3.3.3         3.3.3.3           6     72 80000016           1
Router    2.2.2.2         2.2.2.2         228     60 8000000D           1
Router    1.1.1.1         1.1.1.1         258     60 80000009           1
Network   112.1.1.4       4.4.4.4         121     32 80000001           0
Network   112.1.1.2       1.1.1.1        3600     32 80000015           0
```

```
Network   222.1.1.3       3.3.3.3         227     32 80000003     0
Network   111.1.1.1       1.1.1.1         259     32 80000002     0
```

a. 在各交换机上每隔一秒执行一次**display ospf routing**，如果看到有路由振荡且没有邻居振荡，则可以判断为IP地址冲突或Router ID冲突。结合**display ospf lsdb**的回显信息，可以判断为DR/BDR和非DR的IP地址冲突。

b. 根据AdvRouter字段找到其中的一台设备进而定位出是哪个接口，与其冲突的设备只能够通过网络IP地址规划找到，很难通过OSPF自身携带的信息找到冲突设备。

如本例中，可以首先判断出冲突的IP地址为112.1.1.2，其中一台冲突设备的Router ID为1.1.1.1，与其冲突的另外一台设备（3.3.3.3）无法通过OSPF自身携带的信息找到。

- 如果任意一台交换机上出现两个LinkState ID为112.1.1.2的Network LSA，并且这两个LSA的Age字段一直都很小，Sequence字段增加比较快。说明IP地址冲突发生在DR和BDR上。

```
<HUAWEI> display ospf lsdb

OSPF Process 100 with Router ID 3.3.3.3
Link State Database

Area: 0.0.0.0
--------------------------------------------------------------------------------
 Type      LinkState ID    AdvRouter       Age    Len Sequence      Metric
 Router    4.4.4.4         4.4.4.4          17     48 8000011D          1
 Router    3.3.3.3         3.3.3.3          21     72 8000015A          1
 Router    2.2.2.2         2.2.2.2         151     60 80000089          1
 Router    1.1.1.1         1.1.1.1        1180     60 8000002A          1
 Network   112.1.1.2       3.3.3.3           3     32 8000016A          0
 Network   112.1.1.2       1.1.1.1           5     32 80000179          0
 Network   222.1.1.3       3.3.3.3         145     32 8000002D          0
 Network   212.1.1.4       4.4.4.4          10     32 80000005          0
 Network   111.1.1.2       2.2.2.2         459     32 80000003          0
```

----结束

解决方案

根据规划修改冲突一方的IP地址。

经验总结

- 网络中时常会出现由于接口IP地址配置冲突而导致的路由问题。出现此问题时，设备通常伴随下面两个现象：
  - 设备CPU占用率高。
  - 发生路由振荡。
- 在OSPF网络中，接口IP地址配置冲突时可能导致OSPF的LSA频繁的老化和产生，进而导致网络不稳定，引起路由振荡，消耗CPU处理资源。

因此，网络中接口IP地址需要根据规划配置，不要随意改动网络规划参数。

1.6 如何尽量避免 CPU 占用率高

1. 配置ARP安全功能，防止设备受到ARP和ARP-Miss协议报文攻击。

   设备提供了多种ARP安全的解决方案，请参考产品文档的“配置-安全配置指南-ARP安全配置”进行配置。

2. 在经常出现DHCP、ARP协议报文攻击的网络，配置基于DHCP、ARP协议报文的本机防攻击策略。

   下面给出通用情况下本机防攻击策略的建议配置，由于不同的设备和版本可能在少数地方存在差异，不同的场景也对各种协议报文的上送存在不同的要求，不能一概而论。在实际配置的时候请根据具体的设备型态、版本并按照现网实际的业务要求，对配置进行审视之后再操作，避免出现配置不成功甚至业务受损的问题。

   ```
   #
   cpu-defend policy policy1
    auto-defend enable
    auto-defend action deny
    auto-defend trace-type source-mac source-ip
    auto-defend protocol arp dhcp
    auto-defend whitelist 1 interface 10GEx/x/x  //将互联口加入白名单
    auto-defend whitelist 2 interface 10GEx/x/x  //将上行口加入白名单
   #
   cpu-defend-policy policy1
   #
   ```

3. 管理用户通过SSH、Telnet、SNMP等方式登录设备时，配置基于ACL的访问限制，只允许指定的管理用户登录设备。

   # 在VTY0~14用户界面上，通过ACL指定只有源IP为10.1.1.1/32的用户可以登录到本设备。

   ```
   <HUAWEI> system-view
   [~HUAWEI] acl 2001
   [*HUAWEI-acl4-basic-2001] rule 5 permit source 10.1.1.1 0
   [*HUAWEI-acl4-basic-2001] quit
   [*HUAWEI] user-interface vty 0 14
   [*HUAWEI-ui-vty0-14] acl 2001 outbound
   [*HUAWEI-ui-vty0-14] commit
   ```

4. MAC频繁漂移可能导致CPU占用率高，因此，在可能产生MAC频繁漂移场景，建议在接口视图下通过命令**mac-address flapping trigger error-down**配置接口发生MAC漂移后的处理动作为Error-down。

5. 及时加载并激活版本对应最新的补丁文件。

   请登录**http://support.huawei.com/enterprise/**网站获取补丁的软件和安装补丁需要参考的文档（包括补丁说明书和补丁安装指导书）。

6. 设备针对每类协议报文都有缺省的CPCAR值，一般情况下，缺省的CPCAR值即可满足需要。如果存在正常业务的流量过大的问题，请联系技术支持人员根据实际业务规模和具体的用户网络环境进行调整。

1.7 相关信息

CloudEngine 12800, 12800E, 8800, 7800, 6800, 5800系列交换机 CPU占用率高技术专题

