



**CloudEngine 12800, 12800E, 8800, 7800, 6800,
5800 系列交换机**

CPU 占用率高技术专题

文档版本 02

发布日期 2018-09-10

版权所有 © 华为技术有限公司 2018。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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：<http://e.huawei.com>

前言

概述

本文档介绍了CloudEngine系列交换机CPU和CPU占用率的相关原理，描述了CPU占用率高时的定位方法和解决步骤，同时提供了相关的典型案例及参考信息，为维护工程师处理现网CPU占用率高的故障问题提供一些参考。

特别申明

由于硬件形态的差异，不同设备支持的功能特性及支持的命令行可能不同。使用时请参考设备对应版本的产品文档。

修改记录

文档版本	发布日期	修改说明
01	2018-02-01	第一次正式发布。

目录

前言.....	ii
1 CPU 和 CPU 占用率简介.....	1
2 CPU 和 CPU 占用率原理.....	4
2.1 CPU 处理报文原理.....	4
2.2 CPU 占用率高造成的影响.....	5
2.3 CPU 占用率高属于正常现象的场景.....	6
3 引起 CPU 占用率高的常见原因.....	8
4 如何定位 CPU 占用率高.....	9
4.1 查看设备及版本信息.....	9
4.2 查看 CPU 占用率.....	10
4.3 根据任务的 CPU 占用率排序判断初步原因.....	11
5 如何解决 CPU 占用率高.....	12
5.1 判断为网络攻击引起.....	12
5.2 判断为网络震荡引起.....	15
5.3 判断为网络环路引起.....	18
5.4 判断为流采样功能引起.....	18
5.5 判断为海量日志引起.....	19
6 CPU 占用率高的典型案例.....	20
6.1 交换机受到 ARP 报文攻击.....	20
6.2 STP 震荡引起 CPU 占用率高.....	22
6.3 OSPF 震荡引起 CPU 占用率高.....	23
7 如何尽量避免 CPU 占用率高.....	26
8 A 附录.....	28
8.1 CPU 占用率高相关命令/告警/日志/网管 OID 信息.....	28
8.1.1 命令信息.....	28
8.1.2 告警信息.....	29
8.1.3 日志信息.....	30
8.1.4 网管 OID 信息.....	34
8.2 CPU 各任务名称及功能说明.....	35

1 CPU 和 CPU 占用率简介

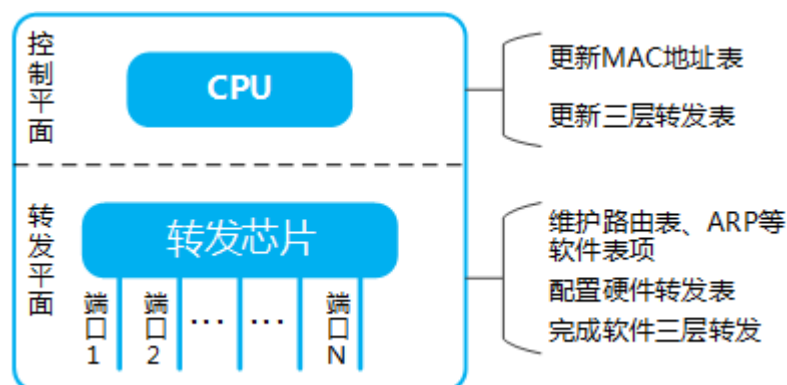
交换机的核心--CPU

交换机采用分布式架构，主要包括转发平面和控制平面。其中转发平面用于实现二层转发；而控制平面主要用于实现转发的控制。

如图1-1所示，交换机的控制平面采用通用嵌入式CPU实现，转发平面采用转发芯片实现：

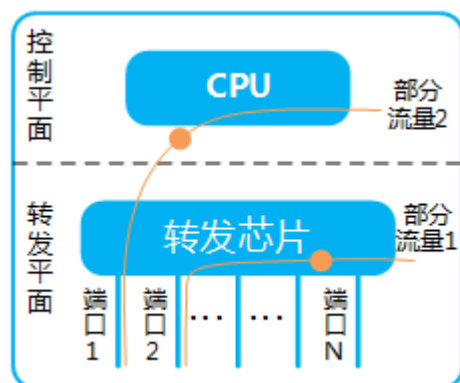
- 转发芯片完成主要的二三层转发功能，如更新用于二层转发的MAC地址表以及用于IP转发的三层转发表。转发芯片的特点是能够实现大吞吐量的数据转发。
- CPU主要维护软件表项（如路由表、ARP表等），并根据软件表项的转发信息来配置转发芯片的硬件三层转发表。同时，CPU本身也可以完成软件三层转发。CPU的特点是数据处理能力低。

图 1-1 交换机的分布式架构



在网络中，可将报文按照功能分为控制报文和数据报文。当交换机上还未建立任何硬件转发表项时，如果报文到达交换机，首包由CPU转发并建立三层转发硬件表项，后续包（即非首包）流量由入端口进入转发芯片，如图1-2所示：

图 1-2 交换机对非首包流量的处理



- 后续包的**部分流量1**（一般为数据报文）直接由转发芯片转发出去这部分流量不经过CPU，所以该流量的处理也不消耗CPU。这部分流量一般为数据报文。
- 后续包的**部分流量2**（一般为控制报文和部分数据报文）经由转发芯片上送CPU，由CPU来决定是否需要将其转发出去或直接在CPU终结。该流量需要消耗CPU，不能进行高速转发。

总的来说，真正决定交换机高速交换转发的是转发芯片中的二三层硬件表项，而转发芯片的硬件表项来源于CPU维护的软件表项。可以看出，CPU是交换机的核心。

CPU 占用率

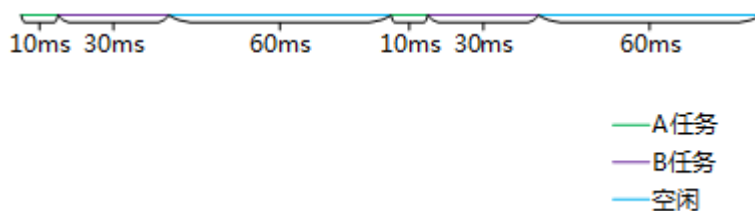
交换机正常启动后，为了维持系统的正常运行，CPU上有多个活跃的任务用于完成对设备的管理、监控和三层表项学习。通常交换机支持的特性越多，系统运行的任务也越多。

设备的CPU占用率指一段时间内系统中非空闲任务占用CPU处理的时间比率，是对设备CPU使用情况的一个宏观统计，具有以下几个重要特点：

- 持续变化性：系统的CPU占用率不是保持不变的，它是随着系统的运行和外部环境的变化而持续变化的。
- 非实时性：系统的CPU占用率反映的是一个CPU统计周期内的CPU使用情况，并不是特指某一个时间点的实时占用情况。
- 实体强相关性：CPU占用率是以物理CPU为粒度进行统计的，通常而言，设备上的每块业务板均有一个单独的物理CPU，因此它们的CPU占用率都是相互独立的。

CPU占用率表示交换机在某个时间点的运行任务情况。如图1-3所示，A任务占用10ms，B任务占用30ms，然后空闲60ms，再又是A任务占10ms，B任务占30ms，空闲60ms。如果在一段时间内都是如此，那么这段时间内的占用率为40%。CPU占用率越高，说明交换机在这个时间上运行了很多任务，反之则很少。

图 1-3 任务占用 CPU 运行时间



可以看出，CPU 占用率的高低与CPU的强弱有直接关系，因此，CPU 占用率是衡量设备性能的重要指标之一。

2 CPU 和 CPU 占用率原理

2.1 CPU处理报文原理

2.2 CPU占用率高造成的影响

2.3 CPU占用率高属于正常现象的场景

2.1 CPU 处理报文原理

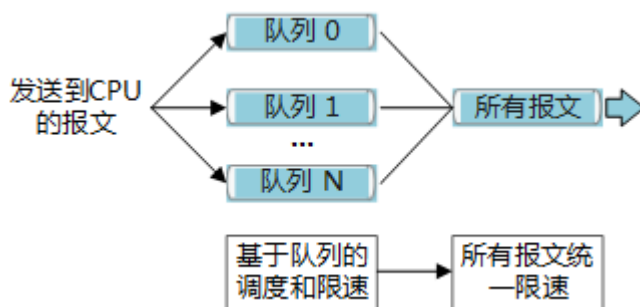
交换机由转发芯片转发普通数据报文，无需CPU参与。以下场景会将报文发送给CPU处理：

- 需要交换机终结的协议报文
所有目的地址为本机的报文均需要上送CPU处理：
 - 各种协议控制报文，如STP、LLDP、LACP、DLDP、EFM、GVRP、VRRP等
 - 路由更新报文，如RIP、OSPF、BGP、IS-IS等
 - SNMP、Telnet、SSH报文
 - ARP、ND回应报文
- 需要特殊处理的报文
 - 带option选项的ICMP报文
 - 带hop-by-hop选项的IPv6报文
 - TTL小于或等于1的IPv4/IPv6数据报文
 - 目的IP地址为本机的数据报文
 - ARP/ND/FIB Miss报文
- 应用了ACL，需要CPU处理的报文
 - 开启logging功能后，通过ACL deny动作丢弃的报文
 - 流策略重定向到CPU的报文
- 组播特性相关的报文
 - IGMP协议报文
 - 未知IP组播流
- 其他特性的相关报文
 - DHCP协议报文

- ARP、ND广播请求报文

交换机根据报文的权重，将上送CPU的不同类型的报文划分到优先级不同的多个队列，确保重要报文优先处理。同时，还可以针对上送CPU的报文进行限速，使单位时间内上送CPU报文的数量限制在一定的范围之内，从而保证CPU对业务的正常处理。

图 2-1 将不同类型报文分发到 CPU 队列



在稳定的网络环境下，上送CPU的报文数量控制在适当的范围内，CPU占用率也稳定在一个合理的区间。如果一段时间内上送CPU的报文数量过大，则CPU会因为忙于处理这些报文而表现为CPU占用率过高。

2.2 CPU 占用率高造成的影响

当设备转发面上送CPU的报文速率过快（如因网络环路导致CPU短时间内收到大量报文）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。

CPU占用率过高会影响系统处理能力，导致网络业务表现不如预期，可能导致出现的网络故障现象有：

- 交换机不能响应正常的管理请求。
 - Telnet或SSH会话不能建立，导致无法管理设备或者设备反应慢，命令执行有延迟等。
 - SNMP超时。
 - MAC/IP Ping耗时很长甚至超时。
- 交换机不能及时转发或回应客户端请求，导致DHCP失败或IEEE 802.1x认证失败。
- STP拓扑改变甚至出现网络环路。

交换机通过CPU周期性的接收BPDU报文维持其Root/Alternate端口角色，如果因上游设备CPU繁忙导致BPDU报文不能及时发出或本机CPU繁忙不能及时处理收到的BPDU报文，交换机会认为到根桥的原路径故障而重新选择Root端口，引起网络重新收敛；如果交换机原来同时存在Alternate端口，则将Alternate端口作为新的Root端口，这时就可能导致网络出现环路。
- 路由拓扑改变。

动态路由协议的保活由CPU完成，如果因CPU繁忙不能及时接收和发送hello报文，就会导致路由震荡，如OSPF震荡、BGP震荡、VRRP震荡。
- 可靠性检测协议震荡。

802.3ah、802.1ag、DLDP、BFD、MPLS OAM等检测协议均由CPU完成定时保活，如果因为CPU繁忙不能及时接收和发送协议报文，将会导致协议震荡，进而影响相关业务流量转发。

- LACP类型的Eth-Trunk链路震荡。
LACP的保活由CPU完成，如果因CPU繁忙不能及时接收和发送LACP报文，Eth-Trunk会将链路关闭，产生链路震荡。
- 通过CPU软转发的报文被丢弃或转发时延增大。
- 交换机内存消耗增加。

2.3 CPU 占用率高属于正常现象的场景

在网络运行中，CPU占用率过高常常会导致业务异常，例如BGP震荡、VRRP频繁切换甚至用户无法登录交换机。但某些情况下，CPU占用率高并不会导致网络问题，例如，交换机在某一时刻集中读取光模块信息、瞬间流量增多等各种具体情况，导致CPU占用率暂时性高的现象是正常的、可接受的，所以不能简单的将CPU占用率高当作故障处理。只有当设备长时间不能正常处理业务时，才需要定位是否由于CPU占用率高而引起的。

如下一些场景可能导致CPU占用率高，属于正常现象，而不是故障场景。如果过了一段时间后，CPU占用率恢复到正常值，则可以不处理：

- 网络中瞬间流量增多。
- 交换机单板刚启动。
- 网管系统在频繁操作交换机。
- 批量读取光模块信息（执行命令**display interface transceiver**或者在网管读取光模块信息）。
- 交换机在执行**copy flash:**或输出信息量大、执行时间长的命令，如**debugging**、**display diagnostic-information**命令。
- 交换机在进行生成树的计算。

对于MSTP，CPU占用率同实例数和活跃端口数成正比。对于VBST，由于每个VLAN独立运行一个实例，因此在相同VLAN和端口数目下，VBST比MSTP占用更多的CPU资源。

- 交换机接收到路由更新信息，大规模更新路由表。

当接收到路由更新消息时，设备需占用CPU资源将路由信息更新到转发面。对于堆叠系统，路由信息还需要同步到其他成员交换机。

在路由表更新过程中影响CPU占用率大小的因素有：

- 路由表项的规模
- 更新的频率
- 接收更新的路由协议进程数
- 堆叠系统成员交换机数量
- 导致CPU占用率高的其他事件：
 - 将大量端口同时加入大量VLAN（如通过端口组操作，将大批端口加入大量VLAN、修改大批端口的链路类型等）。
 - 频繁或大量的IGMP请求。
 - 大量并发的DHCP请求（如交换机作为DHCP服务器时，恢复与大量用户的连接）。

- ARP广播风暴。
- 以太网广播风暴。
- 软转发大量并发协议报文（如短时间内L2PT透传大量BPDU报文，DHCP Relay/Snooping软转发DHCP报文等）。
- 大量不能由转发芯片直接转发的数据报文上送CPU（如ARP-Miss）。
- 端口频繁Up/Down。

3 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

4 如何定位 CPU 占用率高

- 4.1 查看设备及版本信息
- 4.2 查看CPU占用率
- 4.3 根据任务的CPU占用率排序判断初步原因

4.1 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

4.2 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[4.3 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。

关于以上告警的具体信息，请查看[8.1.2 告警信息](#)。

- 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**，关于该日志的具体信息，请查看[8.1.3 日志信息](#)。

4.3 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4-1](#)来查询引起CPU占用率高的原因及解决措施。

表 4-1 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
NETSTRE AM	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[8.2 CPU各任务名称及功能说明](#)，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[8.2 CPU各任务名称及功能说明](#)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[5 如何解决CPU占用率高](#)。

5 如何解决 CPU 占用率高

5.1 判断为网络攻击引起

5.2 判断为网络震荡引起

5.3 判断为网络环路引起

5.4 判断为流采样功能引起

5.5 判断为海量日志引起

5.1 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 Last 5 Min Passed	Total Dropped Last 5 Min Dropped	Last Dropping Time
arp	784824 8	0 0	-
arp-miss	0 0	0 0	-
fib-hit	25993 0	0 0	-
snmp	4922372 599	0 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传的报文。

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。



注意

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
```

5.2 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 hwMstpTcGuarded和MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.16 hwMstpProTcGuarded两个告警。关于以上告警的详细信息，请参考[8.1.2 告警信息](#)。
- 设备开启防拓扑变化攻击功能后，在`stp tc-protection interval 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[8.1.3 日志信息](#)的“OSPF/3/NBR_DOWN_REASON”的日志详细信息。

5.3 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坏。
- 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。

5.4 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
```

5.5 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。

6 CPU 占用率高的典型案例

6.1 交换机受到ARP报文攻击

6.2 STP震荡引起CPU占用率高

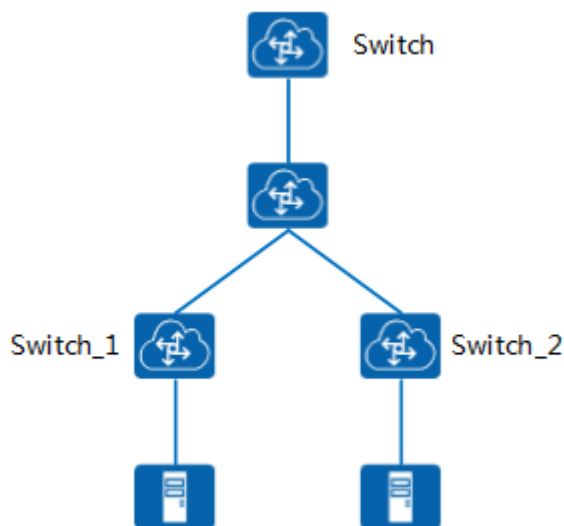
6.3 OSPF震荡引起CPU占用率高

6.1 交换机受到 ARP 报文攻击

问题现象描述

如图6-1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 6-1 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 Last 5 Min Passed	Total Dropped Last 5 Min Dropped	Last Dropping Time
arp	0 0	0 0	-

```
Statistics(packets) on slot 4 :
```

PacketType	Total Passed Last 5 Min Passed	Total Dropped Last 5 Min Dropped	Last Dropping Time
arp	106549 3	44380928 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
#
```

6.2 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)
```

- 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)
```

- 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

- 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。

- 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。

- 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。

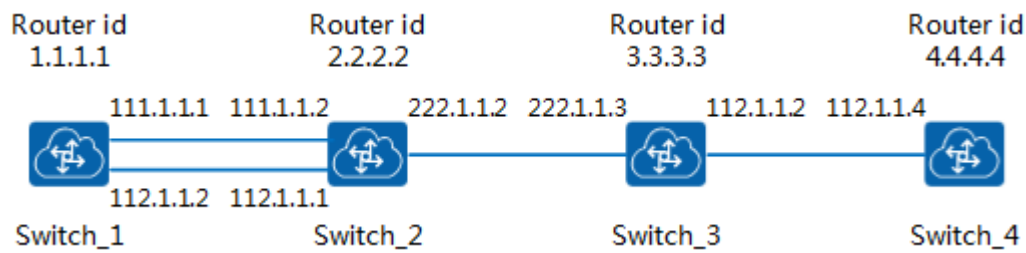
在部署STP时，建议配置TC保护功能，并将所有连接终端的接口配置成边缘端口，这样可以避免某些端口的状态变化引起整个STP网络震荡而重新收敛。

6.3 OSPF 震荡引起 CPU 占用率高

问题现象描述

如图6-2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 6-2 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。

7 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。

8

A 附录

- 8.1 CPU占用率高相关命令/告警/日志/网管OID信息
- 8.2 CPU各任务名称及功能说明

8.1 CPU 占用率高相关命令/告警/日志/网管 OID 信息

8.1.1 命令信息

表 8-1 CPU 占用率高常用命令信息

命令	描述
display interface counters [inbound outbound] [interface-type [interface-number]]	查看设备上各接口收发报文统计信息。
display cpu [slot slot-id]	查看设备CPU占用率的统计信息。
display cpu threshold [slot slot-id]	查看设备CPU占用率的阈值信息。
display cpu-defend statistics [history] [packet-type packet-type] { all slot slot-id }	查看协议报文上送CPU的统计信息。
display arp packet statistics [interface [interface-type interface-number]]	查看ARP报文统计信息。
display dhcp statistics	查看DHCP报文统计信息。
display cpu-defend rate [packet-type packet-type] { all slot slot-id }	查看协议报文上送CPU的速率。
display cpu-defend policy [policy-name]	查看防攻击策略的配置信息。
display cpu-defend configuration [packet-type packet-type] { all slot slot-id }	查看CAR（包括上送CPU的报文限速信息，协议报文上送的CPU队列）的配置信息。

命令	描述
display logbuffer [security] [slot slot-id module module-name starttime starttime [endtime endtime] level { severity level } size size] *	查看设备日志信息。
display trapbuffer [size value]	查看设备告警信息。
display stp [process process-id] [instance instance-id] topology-change	查看STP拓扑变化信息。
display stp [process process-id] [instance instance-id] [interface interface-type interface-number slot slot-id] [brief]	查看STP TC BPDU统计信息。
reset cpu-defend statistics [packet-type packet-type] { all slot slot-id }	清除上送CPU报文的统计信息。
cpu-defend policy policy-name	配置本机防攻击策略。
blacklist blacklist-id acl { acl-number ipv6 acl6-number } [interface { interface-type interface-number1 [to interface-type interface-number2] } &<1-8>] [vlan { vlan-id1 [to vlan-id2] } &<1-8>]	通过ACL配置本机防攻击策略的黑名单。
auto-defend enable	使能攻击溯源功能。
auto-defend trace-type { source-mac source-ip source-portvlan } *	配置攻击溯源的溯源模式。
auto-defend protocol { all { arp dhcp dhcpv6 icmp icmpv6 igmp mld nd ttl-expired } * }	配置攻击溯源防范的报文类型。
auto-defend whitelist whitelist-number { acl { acl-number ipv6 acl6-number } interface interface-type interface-number }	配置攻击溯源的白名单，对白名单用户不做溯源。
auto-defend alarm enable	使能攻击溯源事件上报功能。
auto-defend action { deny [timeout time-length] error-down }	使能攻击溯源的惩罚功能，并指定惩罚措施。
cpu-defend-policy policy-name [slot slot-id batch slot { slot-id1 [to slot-id2] } &<1-12>]	应用防攻击策略。

8.1.2 告警信息

1. **SYSTEM_1.3.6.1.4.1.2011.5.25.129.2.4.1 hwCPUUtilizationRisingAlarm** //设备的CPU占用率超过门限阈值。
The CPU usage exceeded the pre-set overload threshold. (TrapSeverity=[TrapSeverity], ProbableCause=[ProbableCause], EventType=[EventType], PhysicalIndex=[PhysicalIndex],

PhysicalName=[PhysicalName], RelativeResource=[RelativeResource], UsageType=[UsageType], SubIndex=[SubIndex], CpuUsage=[CpuUsage], Unit=[Unit], CpuUsageThreshold=[CpuUsageThreshold])

2. **MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.15 hwMstpTcGuarded** //在启用MSTP的设备上启用TC保护功能，单位时间内收到的TC报文超过阈值，超过阈值的TC消息将被延迟到TC保护时间超时后处理。
With the TC protection enabled, if TC BPDUs were received after the number of TC BPDUs received by an instance exceeded the threshold, these TC BPDUs were processed after the TC protection time expires. (InstanceID=[InstanceID], bridgePriority=[bridgePriority])
3. **MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.16 hwMstpProTcGuarded** //MSTP进程启用TC保护功能，单位时间内收到的TC报文超过阈值，超过阈值的TC消息将被延迟到该MSTP进程TC保护时间超时后处理。
With the TC protection enabled, if TC BPDUs were received after the number of TC BPDUs received by an instance exceeded the threshold, these TC BPDUs were processed after the TC protection time expires. (ProcessID=[ProcessID], proTcGuard=[proTcGuard], InstanceID=[InstanceID], proInstBridgePriority=[proInstBridgePriority])

8.1.3 日志信息

1. **SYSTEM/1/hwCPUUtilizationRisingAlarm_active** //设备的CPU占用率超过门限值。
The CPU usage exceeded the pre-set overload threshold. (TrapSeverity=[TrapSeverity], ProbableCause=[ProbableCause], EventType=[EventType], PhysicalIndex=[PhysicalIndex], PhysicalName=[PhysicalName], RelativeResource=[RelativeResource], UsageType=[UsageType], SubIndex=[SubIndex], CpuUsage=[CpuUsage], Unit=[Unit], CpuUsageThreshold=[CpuUsageThreshold])

参数名称	参数含义
TrapSeverity	告警级别。
ProbableCause	告警原因。
EventType	告警类别。
PhysicalIndex	物理索引。
PhysicalName	实体名称。
RelativeResource	相关资源名称。
UsageType	过载类型。
SubIndex	实体子索引。
CpuUsage	CPU使用率。
Unit	单位。
CpuUsageThreshold	CPU门限值。
2. **DEFEND/4/hwCpcarDropPacketAlarm_active** //协议报文上送CPU的速率超过相应的CPCAR值。
DEFEND/4/hwCpcarDropPacketAlarm_active:Rate of packets to cpu exceeded the CPCAR limit in slot [SlotId]. (Protocol=[Protocol], PPS/CBS=[Pps]/[Cbs], ExceededPacketCount=[DropPacketNum])

参数名称	参数含义
SlotId	槽位号。

参数名称	参数含义
Protocol	协议类型。
Pps	每秒允许通过的报文数。
Cbs	承诺突发尺寸。
DropPacketNum	丢弃报文个数。

3. SECURITYTRAP/4/LDM_STRACK_IFVLAN //某接口+VLAN下上送CPU的报文超过了告警阈值。

SECURITYTRAP/4/LDM_STRACK_IFVLAN: Attack occurred. (Interface=[Interface], CVLAN=[CVLAN], PVLAN=[PVLAN], EndTime=[EndTime], TotalPackets=[TotalPackets])

参数名称	参数含义
Interface	接口索引。
CVLAN	攻击用户报文的内层VLAN。
PVLAN	攻击用户报文的外层VLAN。
EndTime	攻击的最后时间。
TotalPackets	收到攻击用户的报文数目。

4. OSPF/3/NBR_DOWN_REASON //邻居状态改变为Down。

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])

参数名称	参数含义
ProcessId	进程号。
NeighborRouterId	邻居路由器标识。
NeighborIp	邻居IP地址。
NeighborAreaId	邻居区域ID。
NeighborInterface	邻居接口。

参数名称	参数含义
NeighborDownImmediate reason	<p>OSPF邻居Down的直接原因，一般会有以下几种：</p> <ul style="list-style-type: none">● Neighbor Down Due to Inactivity: Inactivity定时器超时● Neighbor Down Due to LL Down: 链路状态Down，比如接口由Up变为Down、链路上的IP地址被删除● Neighbor Down Due to Kill Neighbor: 本接口的邻居状态机发生“Kill Neighbor”事件● Neighbor Down Due to 1-Wayhello: 由于接收到1-way报文，邻居状态变为Down● Received: Neighbor Down Due to AdjOK?: 本接口发生“AdjOK?”事件● Neighbor Down Due to SequenceNum Mismatch: 本接口的邻居状态机发生“SequenceNum Mismatch”事件● Neighbor Down Due to BadLSreq: 本接口的邻居状态机发生“BadLSreq”事件

参数名称	参数含义
NeighborDownPrimeReason	<p>邻居Down的根本原因，一般会有以下几种：</p> <ul style="list-style-type: none"> ● Hello Not Seen: 没有收到Hello报文 ● Interface Parameter Mismatch: 链路两端的接口配置参数不匹配 ● I Bit Incorrect in DD: 邻居振荡场景下DD报文乱序导致邻居关系Down ● Logical Interface State Change: 逻辑接口状态发生变化 ● Physical Interface State Change: 物理接口状态发生变化 ● OSPF Process Reset: OSPF进程发生重启 ● Area reset: 区域类型发生变化导致区域重启 ● Area Option Mis-match: 链路两端接口所属的区域Option不匹配 ● Vlink Peer Not Reachable: 虚连接邻居不可达 ● Sham-Link Unreachable: Sham-Link邻居不可达 ● Undo Network Command: network命令被删除 ● Undo NBMA Peer: NBMA类型接口上的邻居配置被删除 ● Passive Interface Down: 由于本端配置了silent-interface命令，导致邻居关系Down ● Opaque Capability Enabled: 使能了Opaque能力 ● Opaque Capability Disabled: 去使能Opaque能力 ● Virtual Interface State Change: 虚连接接口状态变化 ● BFD Session Down: BFD会话Down ● Down Retransmission Limit Exceed: 达到重传限制 ● 1-Wayhello Received: 收到1-Way的Hello报文 ● Router State Change from DR or BDR to DROTHER: 接口状态机由DR或BDR变为DROTHER ● Neighbor State Change from DR or BDR to DROTHER: 接口状态机由DR或BDR变为DROTHER ● NSSA Area Configure Change: NSSA区域配置发生变化 ● Stub Area Configure Change: Stub区域配置发生变化

参数名称	参数含义
	<ul style="list-style-type: none"> ● Received Invalid DD Packet: 收到无效的DD报文 ● Not Received DD during RouterDeadInterval: 在Dead定时器启动期间, 没有收到DD报文 ● M,I,MS bit or SequenceNum Incorrect: 收到的DD报文中M、I、MS比特位与协议规定不符 ● Unable Opaque Capability,Find 9,10,11 Type Lsa: 收到了9,10,11类型的LSA, 但是Opaque能力并没有被使能 ● Not NSSA,Find 7 Type Lsa in Summary List: 本区域不属于NSSA, 却在Summary表中发现了Tpye-7 LSA ● LSrequest Packet,Unknown Reason: 由于未知原因收到LSR报文 ● NSSA or STUB Area,Find 5 ,11 Type Lsa: 本区域属于NSSA或者Stub, 却发现了Tpye-5、Tpye-11 LSA ● LSrequest Packet,Request Lsa is Not in the Lsdb: 邻居向本进程或区域通过LSR请求一条LSA, 但该LSA不在本进程的LSDB中 ● LSrequest Packet, exist same lsa in the Lsdb: 本进程收到一条本地LSDB中已存在的相同LSA, 该LSA在邻居的请求列表中 ● LSrequest Packet, exist newer lsa in the Lsdb: 本进程收到一条更新的LSA, 该LSA在本地LSDB中已存在, 并且在邻居的请求列表中 ● Neighbor state was not full when LSDB overflow: LSDB已经溢出, 但是邻居状态机还没有达到Full ● Filter LSA configuration change: LSA filter配置发生变化 ● ACL changed for Filter LSA: LSA filter的ACL配置发生变化 ● Reset Ospf Peer: 重启OSPF邻居
CpuUsage	CPU使用率。

8.1.4 网管 OID 信息

节点名称	节点OID	数据类型	含义	实现规格
hwEntityCpuUsage	1.3.6.1.4.1.2011 5.25.31.1.1.1.1.5	Integer32	CPU占用率 取值范围: 0~100	read-only

节点名称	节点OID	数据类型	含义	实现规格
hwEntityCpuUsageThreshold	1.3.6.1.4.1.2011 . 5.25.31.1.1.1.1. 6	Integer32	CPU占用率门限 取值范围：0~100 缺省值：90	read-write

8.2 CPU 各任务名称及功能说明

任务名称	任务描述
AAA	认证鉴权计费
AM	地址管理
ARP	地址解析协议
BGP	边界网关协议
CMF	配置管理框架
CSPF	最短路径优先算法
DEVICE	设备管理
DHCP	动态主机配置协议
ETRUNK	跨框TRUNK协议
EUM	以太网用户管理
EVPN	以太网虚拟网络
FEA	功能实体动作
FEC	功能实体控制
FIBRESM	资源管理
IFM	接口管理
IGMP	因特网组管理协议
IP STACK	协议栈
ISIS	ISIS路由协议
L2VPN	二层虚拟私有网络
LDP	标签分发协议
LLDP	链路层发现协议
LOCAL PKT	主机收发
MACM	静态MAC管理

任务名称	任务描述
MSTP	多实例stp
ND	ICMPv6邻居发现
NETSTREAM	网络流采样
OAM	操作管理维护
OSPF	开放最短路径转发
PEM	节能管理
PIM	协议无关组播
PNP	即插即用服务
RBS	远端备份服务
RGM	冗余网关管理
RM	路由管理
SFLOW	采样流
SLA	服务等级承诺
SMLK	smart link协议
STACKMNG	堆叠管理
SYSTEM	系统管理
TNLM	隧道管理
TRILL	TRILL
TUNNEL	隧道
VLAN	虚拟LAN
VRRP	虚拟路由器冗余协议
VXLAN	虚拟扩展Lan