目录

相关信息

简介

本文档介绍 Cisco Catalyst 6500/6000 系列交换机和基于虚拟交换系统 (VSS) 1440 的系统上高 CPU 使用率的原因。类似于 Cisco 路由器，交换机使用 **show processes cpu** 命令显示交换机 Supervisor 引擎处理器的 CPU 使用率。但是，由于 Cisco 路由器和交换机之间在体系结构和转发机制上存在差异，**show processes cpu** 命令的标准输出有很大的不同。输出的含义有所不同。本文澄清这些差异并且描述在交换机的CPU利用率和如何解释**show processes cpu命令**输出。

注意： 在本文档中，“交换机”一词是指 Catalyst 6500/6000 交换机。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于 Catalyst 6500/6000 交换机和基于虚拟交换系统 (VSS) 1440 的系统的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

注意： 基于虚拟交换系统(VSS)1440的系统的支持的软件是Cisco IOS软件版本12.2(33)SXH1或以后。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

CatOS 和 Cisco IOS 系统软件之间的区别

Supervisor 引擎上的 Catalyst OS (CatOS) 和 Multilayer Switch Feature Card (MSFC) 上的 Cisco IOS® 软件（混合）：可将 CatOS 映像用作系统软件，以在 Catalyst 6500/6000 交换机上运行 Supervisor 引擎。如果安装了可选的 MSFC，则将使用单独的 Cisco IOS 软件映像来运行 MSFC。

Supervisor 引擎和 MSFC 上的 Cisco IOS 软件（本地）：可将单个 Cisco IOS 软件映像用作系统软件，以在 Catalyst 6500/6000 交换机上同时运行 Supervisor 引擎和 MSFC。

注意： 有关详细信息，请参阅比较 Cisco Catalyst 6500 系列交换机的 Cisco Catalyst 和 Cisco IOS 操作系统。

了解 Catalyst 6500/6000 交换机上的 CPU 使用率

Cisco 基于软件的路由器使用软件来处理和路由数据包。当路由器执行更多数据包处理和路由操作

时，Cisco 路由器上的 CPU 使用率势必增加。因此，**show processes cpu** 命令可对路由器上的数据流处理负载提供一个相当准确的指示。

Catalyst 6500/6000 交换机使用 CPU 的方式不同。这些交换机在硬件而不是软件中做出转发决策。因此，当交换机对通过交换机的大多数帧做出转发或交换决策时，进程不会占用 Supervisor 引擎 CPU。

在 Catalyst 6500/6000 交换机上，有两个 CPU。一个 CPU 是 Supervisor 引擎 CPU，称为网络管理处理器 (NMP) 或交换机处理器 (SP)。另一个 CPU 是第 3 层路由引擎 CPU，称为 MSFC 或路由处理器 (RP)。

SP CPU 执行以下功能：

- 帮助执行 MAC 地址识别和老化操作**注意：** MAC 地址识别也称为路径设置。
- 运行提供网络控制的协议和进程示例包括生成树协议 (STP)、Cisco 发现协议 (CDP)、VLAN 中继协议 (VTP)、动态中继协议 (DTP) 和端口聚合协议 (PAgP)。
- 处理发往交换机 CPU 的网络管理数据流示例包括 Telnet、HTTP 和简单网络管理协议 (SNMP) 数据流。

RP CPU 执行以下功能：

- 构建和更新第 3 层路由和地址解析协议 (ARP) 表
- 生成 Cisco 快速转发 (CEF) 转发信息库 (FIB) 和邻接表，并将这些表下载到 Policy Feature Card (PFC)
- 处理发往 RP 的网络管理数据流示例包括 Telnet、HTTP 和 SNMP 数据流。

触发数据流进入软件的情况和功能

发往交换机的数据包

发往交换机的任何数据包都会进入软件。此类数据包包括：

- 控制数据包对于 STP、CDP、VTP、热备用路由器协议 (HSRP)、PAgP、链路聚合控制协议 (LACP) 和单向链路检测 (UDLD)，将收到控制数据包。
- 路由协议更新这些协议的示例包括路由信息协议 (RIP)、增强型内部网关路由协议 (EIGRP)、边界网关协议 (BGP) 和开放最短路径优先（OSPF 协议）。
- 发往交换机的 SNMP 数据流
- 对交换机的Telnet和安全套接协议(SSH)流量。高CPU ultilization由于SSH被看到如下：当CPU上升时，请包括这些in命令EEM脚本为了验证SSH会话数量建立：show usersshow line
- 对 ARP 请求的 ARP 响应

需要特殊处理的数据包和情况

此列表提供强制数据包在软件中进行处理的特定数据包类型和情况：

- 具有 IP 选项、过期存活时间 (TTL) 或非高级研究项目管理局 (ARPA) 封装的数据包
- 需要特殊处理（如建立隧道）的数据包
- IP 分段
- 需要来自 RP 或 SP 的 Internet 控制消息协议 (ICMP) 消息的数据包

- 最大传输单元 (MTU) 检查失败
- 具有 IP 错误（包括 IP 校验和长度错误）的数据包
- 如果输入信息包返回有点错误(例如一位错误(SBE))数据包被发送对处理的软件的CPU和被更正。系统分配他们的一缓冲区并且使用CPU资源更正它。
- 当PBR和自反访问列表在通信流的路径时，数据包是交换的软件，要求另外的CPU周期。
- 邻接同一接口
- 失败反向路径转发的数据包(RPF)检查？**rpf-failure**
- 收集/接收收集是指需要 ARP 解析的数据包，接收是指归入接收情况的数据包。
- Supervisor 引擎 720 上在 Cisco IOS 软件和 CatOS 中都进行软件交换的互联网分组交换 (IPX) 数据流IPX 数据流在 Supervisor 引擎 2/Cisco IOS 软件上也进行软件交换，但该数据流在 Supervisor 引擎 2/CatOS 上进行硬件交换。IPX 数据流在 Supervisor 引擎 1A 上对于两个操作系统都进行硬件交换。
- AppleTalk 数据流
- 硬件资源已满情况这些资源包括 FIB、内容可寻址存储器 (CAM) 和三重 CAM (TCAM)。

基于 ACL 的功能

- 已打开“ICMP 不可达”功能的被访问控制列表 (ACL) 拒绝的数据流**注意：** 这是默认设置。如果已启用“IP 不可达”功能，则 ACL 拒绝的某些数据包将被泄漏给 MSFC。需要“ICMP 不可达”的数据包将以用户可配置的速率泄漏。默认情况下，速率为每秒 500 个数据包（500 pps）。
- IPX 根据不支持的参数（如源主机）进行过滤在 Supervisor 引擎 720 上，第 3 层 IPX 数据流的处理始终在软件中进行。
- 具有 **log 关键字**的，需要日志记录的访问控制项 (ACE)这适用于 ACL 日志和 VLAN ACL (VACL) 日志功能。同一 ACL 中不需要日志记录的 ACE 仍在硬件中进行处理。具有 PFC3 的 Supervisor 引擎 720 支持对因 ACL 和 VACL 日志记录而重定向到 MSFC 的数据包进行速率限制。Supervisor 引擎 2 支持对因 VACL 日志记录而重定向到 MSFC 的数据包进行速率限制。Supervisor 引擎 2 上对 ACL 日志记录的支持计划在 Cisco IOS 软件版本 12.2S 分支中提供。
- 策略路由的数据流（使用 **match length**、set ip precedence 或其他不支持的参数）软件中支持 **set interface** 参数。但是，**set interface null 0** 参数是一个例外。在具有 PFC2 的 Supervisor 引擎 2 和具有 PFC3 的 Supervisor 引擎 720 上，此数据流在硬件中进行处理。
- 非 IP 和非 IPX 路由器 ACL (RACL)非 IP RACL 适用于所有 Supervisor 引擎。非 IPX RACL 仅适用于具有 PFC 的 Supervisor 引擎 1a 和具有 PFC2 的 Supervisor 引擎 2。
- 在 RACL 中被拒绝的广播数据流
- 在单播 RPF (uRPF) 检查中被拒绝的数据流，ACL ACE此 uRPF 检查适用于具有 PFC2 的 Supervisor 引擎 2 和具有 PFC3 的 Supervisor 引擎 720。
- 身份验证代理在 Supervisor 引擎 720 上可以对受身份验证代理控制的数据流进行速率限制。
- Cisco IOS 软件 IP 安全 (IPSec)在 Supervisor 引擎 720 上可以对受 Cisco IOS 加密控制的数据流进行速率限制。

基于 NetFlow 的功能

本部分介绍的基于 NetFlow 的功能仅适用于 Supervisor 引擎 2 和 Supervisor 引擎 720。

- 基于 NetFlow 的功能总是需要在软件中看到数据流的第一个数据包。数据流的第一个数据包到达软件后，将对同一数据流的后续数据包进行硬件交换。此数据流安排适用于自反 ACL、Web 缓存通信协议 (WCCP) 和 Cisco IOS 服务器负载均衡 (SLB)。**注意：** 在 Supervisor 引擎 1 上，自反 ACL 依靠动态 TCAM 条目创建特定数据流的硬件快捷方式。原理是相同的：数据流的第一个数据包进入软件。该数据流的后续数据包进行硬件交换。

- 使用 TCP 拦截功能，三次握手和会话关闭将在软件中进行处理。数据流的其余部分在硬件中进行处理。**注意：** 同步 (SYN)、SYN 确认 (SYN ACK) 和 ACK 数据包构成三次握手。会话关闭发生在完成 (FIN) 或重置 (RST) 时。
- 使用网络地址转换 (NAT)，数据流按如下方式进行处理：在 Supervisor 引擎 720 上：需要 NAT 的数据流在初始转换后在硬件中进行处理。流的第一个数据包的转换在软件中进行，该流的后续数据包进行硬件交换。对于 TCP 数据包，将在完成 TCP 三次握手后在 Netflow 表中创建硬件快捷方式。在 Supervisor 引擎 2 和 Supervisor 引擎 1 上：需要 NAT 的所有数据流都进行软件交换。
- 基于上下文的访问控制 (CBAC) 使用 Netflow 快捷方式将需要检查的数据流分类。然后，CBAC 仅将此数据流发送到软件。CBAC 是一个仅限软件的功能；受检查控制的数据流不进行硬件交换。**注意：** 在 Supervisor 引擎 720 上可以对受检查控制的数据流进行速率限制。

多播流量

- 独立于协议的多播 (PIM) 监听
- Internet 组管理协议 (IGMP) 监听 (TTL = 1)此数据流实际上被发往路由器。
- 多播监听程序发现 (MLD) 监听 (TTL = 1)此数据流实际上被发往路由器。
- FIB 缺失
- 与多播源直接连接的用于注册的多播数据包这些多播数据包通过隧道被传输到集合点。
- IP 版本 6 (IPv6) 多播

其它特性

- 基于网络的应用程序识别 (NBAR)
- ARP 检查，仅适用于 CatOS
- 端口安全，仅适用于 CatOS
- DHCP 监听

IPv6 情况

- 具有逐跳选项报头的数据包
- 与路由器具有相同目标 IPv6 地址的数据包
- 未能通过范围实施检查的数据包
- 超出输出链路的 MTU 的数据包
- TTL 小于或等于 1 的数据包
- 输入 VLAN 等于输出 VLAN 的数据包
- IPv6 uRPF软件为所有数据包执行此 uRPF。
- IPv6 自反 ACL软件处理这些自反 ACL。
- IPv6 站内自动隧道编址协议 (ISATAP) 隧道的 6to4 前缀软件处理此隧道。所有其他进入 ISATAP 隧道的数据流进行硬件交换。

LCP Schedular 和 DFC 模块

在 Distributed Forwarding Card (DFC) 中，在使用率较高的 CPU 上运行的 lcp schedular 进程不是问题，不会造成任何运行问题。LCP Schedular 是固件代码的一部分。在不需要 DFC 的所有模块上，固件在称为线路卡处理器 (LCP) 的一个特定处理器上运行。该处理器用于对 ASIC 硬件编程和与中央 Supervisor 模块通信。

当启动 lcp schedular 时，它将利用所有进程可用时间。但当新进程需要处理器时间时，lcp schedular 会为新进程释放进程时间。此高 CPU 使用率对系统性能没有影响。该进程只是获取所有未使用的 CPU 周期（只要没有更高优先级的进程需要它们）。

```
DFC#show process cpuPID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process  22
0         1      0   0.00%  0.00%  0.00%   0 SCP ChilisLC Lis   23           0         1      0
0.00%  0.00%  0.00%   0 IPC RTTYC Messag   24           0         9      0   0.00%  0.00%  0.00%
0 ICC Slave LC Req   25           0         1      0   0.00%  0.00%  0.00%   0 ICC Async mcast
26           0         2      0   0.00%  0.00%  0.00%   0 RPC Sync           27           0
1      0   0.00%  0.00%  0.00%   0 RPC rpc-master     28           0         1      0   0.00%
0.00%  0.00%   0 Net Input          29           0         2      0   0.00%  0.00%  0.00%   0
Protocol Filteri   30           8       105     76   0.00%  0.00%  0.00%   0 Remote Console P
31          40      1530     26   0.00%  0.00%  0.00%   0 L2 Control Task    32          72
986     73   0.00%  0.02%  0.00%   0 L2 Aging Task      33           4        21    190   0.00%
0.00%  0.00%   0 L3 Control Task    34          12       652     18   0.00%  0.00%  0.00%   0
FIB Control Task   35        9148       165  55442   1.22%  1.22%  1.15%   0 Statistics Task
36           4       413      9   0.00%  0.00%  0.00%   0 PFIB Table Manag   37      655016
64690036     10  75.33% 77.87% 71.10%   0 lcp schedular      38           0       762      0
0.00%  0.00%  0.00%   0 Constellation SP
```

高 CPU 使用率问题的常见原因和解决方案

IP 不可达

当访问组拒绝数据包时，MSFC 会发送 ICMP 不可达消息。此操作在默认情况下发生。

使用默认启用的 **ip unreachables** 命令，Supervisor 引擎将在硬件中丢弃大多数被拒绝的数据包。然后，Supervisor 引擎仅将数量很少的数据包（最多 10 pps）发送到 MSFC 进行丢弃。此操作会生成 ICMP 不可达消息。

丢弃被拒绝的数据包和生成 ICMP 不可达消息会造成 MSFC CPU 负载增加。为了降低负载，可以发出 **no ip unreachables** 接口配置命令。此命令将禁用 ICMP 不可达消息，这允许在硬件中丢弃所有被访问组拒绝的数据包。

如果 VACL 拒绝数据包，将不发送 ICMP 不可达消息。

NAT 转换

NAT 同时使用硬件和软件转发。NAT 转换的最初建立必须在软件中完成，进一步的转发在硬件中完成。NAT 还使用 Netflow 表（最大 128 KB）。因此，如果 Netflow 表已满，交换机也将开始通过软件应用 NAT 转发。这通常发生在流量突然升高时，并将导致 6500 CPU 使用率的增加。

流缓存表中 CEF FIB 表空间的使用

Supervisor 引擎 1 有一个支持 128,000 个条目的流缓存表。但是，根据散列算法的效率，这些条目的数量范围在 32,000 到 120,000 个之间。在 Supervisor 引擎 2 上，会生成 FIB 表并将其编程到 PFC 中。该表可容纳多达 256,000 个条目。具有 PFC3-BXL 的 Supervisor 引擎 720 支持多达 1,000,000 个条目。一旦超出此空间，便变为在软件中交换数据包。这可能在 RP 上导致高 CPU 使用率。为了检查 CEF FIB 表中的路由数，请使用以下命令：

```
Router#show processes cpuCPU utilization for five seconds:  99.26%                    one
minute: 100.00%                   five minutes: 100.00%PID Runtime(ms) Invoked    uSecs    5Sec
1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- --- -----
----------1   0           0          0          0.74%   0.00%   0.00% -2  Kernel and Idle2   2
245        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0           1          0
```

```
0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0          0.00%   0.00%
0.00% -2  L2L3PatchRev   5   653         11737      1000       0.00%   0.00%   0.00% -2  SynDi!-
-- Output is suppressed.26 10576 615970 1000 0.00% 0.00% 0.00% 0 L3Aging 27 47432 51696 8000
0.02% 0.00% 0.00% 0 NetFlow 28 6758259 1060831 501000 96.62% 96.00% 96.00% 0   Fib            29
0           1          0          0.00%   0.00%   0.00% -2  Fib_bg_task  !--- Output is
suppressed.CATOS% show mls cefTotal L3 packets switched:           124893998234Total L3 octets
switched:          530193789624 95Total route entries:                      112579  IP route
entries:                        112578  IPX route entries:                            1  IPM
route entries:                            0IP load sharing entries:                   295IPX
load sharing entries:                       0Forwarding entries:
112521Bridge entries:                                  56Drop entries:
2IOS% show ip cef summaryIP Distributed CEF with switching (Table Version 86771423), flags=0x0
112564 routes, 1 reresolve, 0 unresolved (0 old, 0 new)  112567 leaves, 6888 nodes, 21156688
bytes, 86771426inserts, 86658859invalidations  295 load sharing elements, 96760 bytes, 112359
references  universal per-destination load sharing algorithm, id 8ADDA64A  2 CEF resets, 2306608
revisions of existing leaves  refcounts:  1981829 leaf, 1763584 node!--- You see these messages
if the TCAM space is exceeded:%MLSCEF-SP-7-FIB_EXCEPTION: FIB TCAM exception, Some entries will
be software switched%MLSCEF-SP-7-END_FIB_EXCEPTION: FIB TCAM exception cleared, all CEF entries
will be hardware switched
```

在 Supervisor 引擎 2 上，如果已在接口上配置 RPF 检查，则 FIB 条目的数量将减少到一半。此配置可能导致对更多数据包进行软件交换，并因此导致高 CPU 使用率。

为了解决高CPU利用率问题， enable (event)路由总结。路由总结能通过减少处理器工作量、内存要求和带宽需求最小化在复杂网络的延迟。

有关 TCAM 使用率和优化的详细信息，请参阅了解 Catalyst 6500 系列交换机上的 ACL。

优化的 ACL 日志记录

优化的 ACL 日志记录 (OAL) 为 ACL 日志记录提供硬件支持。除非配置 OAL，否则对需要日志记录的数据包的处理将完全在 MSFC3 上的软件中进行。OAL 在 PFC3 上的硬件中允许或丢弃数据包。OAL 使用一个优化的例程向 MSFC3 发送信息以生成日志记录消息。

注意： 有关 OAL 的信息，请参阅了解 Cisco IOS ACL 支持的*使用 PFC3 的优化的 ACL 日志记录*部分。

到 CPU 的数据包的速率限制

在 Supervisor 引擎 720 上，速率限制器可以控制数据包进入软件的速率。此速率控制可帮助防止拒绝服务攻击。还可以在 Supervisor 引擎 2 上使用这些速率限制器中的一部分：

```
Router#show mls rate-limit   Rate Limiter Type       Status     Packets/s   Burst--------------
------   ----------   ---------   -----          MCAST NON RPF   Off                  -       -
MCAST DFLT ADJ   On              100000     100      MCAST DIRECT CON   Off                  -
-        ACL BRIDGED IN   Off                  -       -       ACL BRIDGED OUT   Off
-       -           IP FEATURES   Off                  -       -          ACL VACL LOG   On
2000       1           CEF RECEIVE   Off                  -       -             CEF GLEAN   Off
-       -      MCAST PARTIAL SC   On              100000     100        IP RPF FAILURE   On
500      10           TTL FAILURE   Off                  -       -ICMP UNREAC. NO-ROUTE   On
500      10ICMP UNREAC. ACL-DROP   On                500      10         ICMP REDIRECT   Off
-       -           MTU FAILURE   Off                  -       -           LAYER_2 PDU   Off
-       -            LAYER_2 PT   Off                  -       -             IP ERRORS   On
500      10           CAPTURE PKT   Off                  -       -            MCAST IGMP   Off
-       -Router(config)#mls rate-limit ?  all        Rate Limiting for both Unicast and
Multicast packets  layer2     layer2 protocol cases  multicast  Rate limiting for Multicast
packets  unicast    Rate limiting for Unicast packets
```

示例如下：

```
Router(config)#mls rate-limit layer2 l2pt 3000
```
为了限制所有 CEF 转出的数据包发往 MSFC 的速率，请发出本示例中的命令：

```
Router(config)#mls ip cef rate-limit 50000
```
为了减少由于 TTL=1 而被转出到 CPU 的数据包数量，请发出以下命令：

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```
例如，这是**netdr捕获的**输出，显示该IPv4 TTL是1 ：

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```
高 CPU 使用率也可能是由于泄漏给 CPU 的 TTL=1 的数据包引起的。为了限制泄漏给 CPU 的数据包的数量，请配置一个硬件速率限制器。速率限制器可以限制从硬件数据路径直到软件数据路径泄漏的数据包的速率。速率限制器可通过丢弃超过配置速率的数据流，来防止软件控制路径发生拥塞。速率限制是使用 mls rate-limit all ttl-failure 命令配置的。

由于不正确布线导致的 VLAN 物理合并

高 CPU 使用率也可能是由于因不正确布线而将两个或更多 VLAN 合并到一起引起的。此外，如果在发生 VLAN 合并的这些端口上已禁用 STP，则也可能出现高 CPU 使用率。

为了解决此问题，请识别布线错误并进行更正。如果您的要求允许，也可以在这些端口上启用 STP。

广播风暴

当广播或多播数据包泛洪 LAN 时，会出现 LAN 广播风暴，这会创建过多的数据流并且降低网络性能。协议堆栈实施或网络配置中的错误可能导致广播风暴。

由于 Catalyst 6500 系列平台的体系结构设计，广播数据包始终仅在软件级别被丢弃。

广播抑制可防止广播风暴破坏 LAN 接口。广播抑制使用测量 1 秒时段内 LAN 上的广播活动并将测量结果与预定义的阈值进行比较的过滤方法。如果达到阈值，则将在指定时段内抑制进一步的广播活动。广播抑制在默认情况下处于禁用状态。

注意： 从掌握的备份的VRRP飘荡由广播风暴导致也许导致高CPU利用率。

为了了解广播抑制的工作原理以及如何启用该功能，请参阅：

- 配置广播抑制（Cisco IOS 系统软件）
- 配置广播抑制（CatOS 系统软件）

BGP 下一跳地址跟踪（BGP 扫描程序进程）

BGP 扫描程序进程扫描 BGP 表并确认下一跳的可达性。此进程也检查条件通告以确定 BGP 是否应该通告条件前缀并/或执行路由衰减。默认情况下，该进程每 60 秒扫描一次。

在具有大型 Internet 路由表的路由器上执行 BGP 扫描程序进程时，您可以预料到会因此出现持续时间较短的高 CPU 使用率。每分钟一次，BGP 扫描程序扫描 BGP 路由信息库 (RIB) 表并执行重要维护任务。这些任务包括：

- 检查路由器 BGP 表中引用的下一跳
- 验证下一跳设备是否可以到达

因此，扫描和验证大型 BGP 表需要花费相当长的时间。BGP 扫描程序进程扫描 BGP 表以更新所有数据结构，并扫描路由表以进行路由重分配。两个表分别存储在路由器内存中。两个表都可能非常大，并因此可能会耗尽 CPU 周期。

有关 BGP 扫描程序进程的 CPU 使用率的详细信息，请参阅解决由 BGP 扫描器和 BGP 路由器进程引起的高 CPU 使用率问题的*由于 BGP 扫描程序而导致 CPU 使用率较高*部分。

有关 BGP 下一跳地址跟踪功能和启用/禁用或调整扫描间隔的过程的详细信息，请参阅对下一跳地址跟踪的 BGP 支持。

非 RPF 多播数据流

多播路由（不同于单播路由）只关心给定多播数据流的源。即发起多播数据流的设备的 IP 地址。基本原理是源设备将数据流“推”出到数量不确定的接收方（在其多播组内）。所有多播路由器都会创建分布树，这些分布树控制多播数据流通过网络将数据流发送到所有接收方所采用的路径。多播分布树的两种基本类型是源树和共享树。RPF 是多播转发中的一个重要概念。它使路由器可以沿分布树正确转发多播数据流。RPF 利用现有的单播路由表确定上游与下游邻居。只有当上游接口收到多播数据包时，路由器才会转发该数据包。此 RPF 检查可帮助保证分布树无环路。

根据 IEEE 802.3 CSMA/CD 规范，多播数据流在桥接的（第 2 层）LAN 上对于每个路由器始终可见。在 802.3 标准中，第一个八位组的位 0 用于指示广播和/或多播帧，具有此地址的所有第 2 层帧将被泛洪。即使配置了 CGMP 或 IGMP 监听，也是这种情况。这是因为，如果希望多播路由器做出正确的转发决策，多播路由器必须看到多播数据流。如果多个多播路由器中的每一个都在公共 LAN 上有接口，则只有一个路由器转发数据（通过选举过程选择）。由于 LAN 的泛洪性质，冗余路由器（不转发多播数据流的路由器）在该 LAN 的出站接口上收到此数据。冗余路由器通常会丢弃此数据流，因为该数据流已到达错误的接口，因此无法通过 RPF 检查。无法通过 RPF 检查的此数据流称为非 RPF 数据流或 RPF 故障数据包，因为它们已按照来自源的流向被反向传输回去。

可以将安装了 MSFC 的 Catalyst 6500 配置为充当功能完备的多播路由器。使用多播多层交换 (MMLS)，RPF 数据流通常在交换机内由硬件进行转发。ASIC 被提供了来自多播路由状态的信息（例如，(*,G) 和 (S,G)），因此可以将硬件快捷方式编程到 Netflow 和/或 FIB 表中。这种非 RPF 数据流在某些情况下仍然是必需的，MSFC CPU（在进程级别）需要它才能使用 PIM 主张机制。否则，它将被软件快速交换路径丢弃（假定未在 RPF 接口上禁用软件快速交换）。

使用冗余的 Catalyst 6500 在某些拓扑中可能无法有效处理非 RPF 数据流。对于非 RPF 数据流，冗余路由器中通常没有 (*,G) 或 (S,G) 状态，因此不能创建任何硬件或软件快捷方式来丢弃数据包。MSFC 路由处理器必须分别检查每个多播数据包，这通常被称为 CPU 中断数据流。使用第 3 层硬件交换和连接同一组路由器的多个接口/VLAN，到达冗余 MSFC 的 CPU 的非 RPF 数据流被放大为原始源速率的“N”倍（其中“N”是路由器以冗余方式连接到的 LAN 的数量）。如果非 RPF 数据流的速率超过系统的数据包丢弃能力，则可能导致高 CPU 使用率、缓冲区溢出和整体网络不稳定。

对于 Catalyst 6500，有一个使过滤能够以线速进行的访问列表引擎。在某些情况下，此功能可用于有效地处理稀疏模式组的非 RPF 数据流。只能在没有下游多播路由器（及对应的接收方）的稀疏模式“残域网络”中，才能使用基于 ACL 的方法。此外，由于 Catalyst 6500 的数据包转发设计，内部冗余的 MSFC 不能使用此实施。这将在 Cisco Bug ID CSCdr74908（仅限注册用户）中进行概述。对于密集模式组，必须在路由器上看到非 RPF 数据包，PIM 主张机制才能正常运行。不同的解决方案（如 CEF 或基于 Netflow 的速率限制和 QoS）用于控制密集模式网络和稀疏模式中转网络中的 RPF 故障。

在 Catalyst 6500 上，有一个使过滤能够以线速进行的访问列表引擎。此功能可用于有效地处理稀疏模式组的非 RPF 数据流。为了实施此解决方案，请在“残域网络”的传入接口上放置一个访问列表，以过滤不是源自“残域网络”的多播数据流。此访问列表被推入交换机的硬件中。此访问列表可防止 CPU 看到数据包，并允许硬件丢弃非 RPF 数据流。

注意： 请勿在中转接口上放置此访问列表。它只供残域网络（只包含主机的网络）使用。

有关详细信息，请参阅以下文档：

- 残域网络中 IP 多播的冗余路由器问题
- 非 RPF 数据流处理

显示命令

发出 **show** 命令时，CPU 使用率总是几乎 100%。发出 **show** 命令时出现高 CPU 使用率是正常的，高 CPU 使用率通常仅保持几秒钟。

例如，发出 **show tech-support** 命令时，虚拟 Exec 进程导致 CPU 使用率升高是正常的，因为此输出是一个中断驱动的输出。您只需关心执行 **show** 命令以外的其他进程时出现的高 CPU 使用率。

show cef not-cef-switched命令显示数据包为什么被踢对MSFC (接收、IP选项、没有邻接等等)，并且多少。例如：

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0         0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

当您监控CPU状态时，**显示ibc**和**显示ibc简化**show命令CPU队列，并且可以使用。

Exec 进程

Cisco IOS 软件中的 Exec 进程负责路由器 TTY 线路（控制台、辅助、异步）上的通信。虚拟 Exec 进程负责 vty 线路（Telnet 会话）。Exec 和虚拟 Exec 进程是中优先级进程，因此如果有具有更高优先级（“高”或“重要”）的其他进程，则更高优先级进程将获得 CPU 资源。

如果通过这些会话传输的数据很多，则 Exec 进程的 CPU 使用率将增加。这是因为当路由器需要通过这些线路发送一个简单字符时，它会使用一些 CPU 资源：

- 对于控制台 (Exec)，路由器为每个字符使用一个中断。
- 对于 VTY 线路（虚拟 Exec），Telnet 会话必须为每个字符建立一个 TCP 数据包。

此列表详细说明了执行 Exec 进程时 CPU 使用率较高的某些可能原因：

- **通过控制台端口发送的数据过多。**请查看是否已使用 show debugging 命令在路由器上启动了任何调试。使用 **no** 形式的 logging console 命令在路由器上禁用控制台日志记录。验证是否在控制台上显示了较长的输出。例如，**show tech-support** 或 show memory 命令。
- **exec 命令是为异步和辅助线路配置的。**如果线路只有传出数据流，则对此线路禁用 Exec 进程。这是因为，如果连接到此线路的设备（例如，调制解调器）发送一些主动提供的数据，Exec 进程将在此线路上启动。如果路由器用作终端服务器（以便可以执行到其他设备控制台的反向 Telnet），建议在连接到其他设备的控制台的线路上配置 **no exec** 命令。否则，从控制台返回

的数据可能会启动一个 Exec 进程，该进程将使用 CPU 资源。
执行虚拟 Exec 进程时 CPU 使用率较高的一个可能原因是：

- **通过 Telnet 会话发送的数据过多。**执行虚拟 Exec 进程时 CPU 使用率较高的最常见原因是从路由器传输到 Telnet 会话的数据过多。从 Telnet 会话执行具有较长输出的命令（如 **show tech-support**、show memory 等）时，可能出现这种情况。可以使用 **show tcp VTY <line number>** 命令验证通过每个 VTY 会话传输的数据量。

L3 老化进程

当 L3 老化进程使用 NetFlow 数据导出 (NDE) 导出大量 *IfIndex* 值时，CPU 使用率可能会达到 100%。

如果遇到此问题，请检查是否启用了以下两个命令：

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

如果启用这些命令，该进程必须使用 NDE 导出所有目标和源 IfIndex 值。L3 老化进程会导致 CPU 使用率升高，因为它必须对所有目标和源 *IfIndex* 值执行 FIB 查找。因此，表将变满，L3 老化进程导致 CPU 使用率升高，CPU 使用率达到 100%。

为了解决此问题，请禁用这些命令：

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

请使用这些命令验证值：

- show mls cef summary
- show mls cef maximum-routes

BPDU 风暴

生成树在冗余交换网络和网桥网络中维护一个无环路的第 2 层环境。**没有 STP，帧会无限循环并/或倍增。这将导致网络崩溃，因为高流量将中断广播域中的所有设备。**

在某些方面，STP 最初是为基于软件的缓慢网桥规范 (IEEE 802.1D) 开发的早期协议，但是要在具

有以下功能的大型交换网络中成功实施该协议，STP 可能非常复杂：

- 多个 VLAN
- STP 域中的许多交换机
- 多供应商支持
- 较新的 IEEE 增强功能

如果网络面临频繁的生成树计算或交换机必须处理更多 BPDU，则可能导致 CPU 使用率较高以及 BPDU 被丢弃。

为了解决这些问题，请执行下列步骤中的部分或全部：

1. 从交换机中删除部分 VLAN。
2. 使用 STP 的增强版，如 MST。
3. 升级交换机的硬件。

另请参阅在网络中实施生成树协议 (STP) 的最佳实践。

- 运行 CatOS 配置和管理的 Catalyst 4500/4000、5500/5000 和 6500/6000 系列交换机的最佳实践
- 运行 Cisco IOS 软件的 Catalyst 6500/6000 系列和 Catalyst 4500/4000 系列交换机的最佳实践

SPAN 会话

基于 Catalyst 6000/6500 系列交换机的体系结构，SPAN 会话不会影响交换机的性能，但是，如果 SPAN 会话中包括高流量/上行链路端口或 EtherChannel，则它可能增加处理器上的负载。如果它随后要选出一个特定 VLAN，这还会增加更多工作量。如果链路上存在不良数据流，这可能进一步增加工作量。

在某些情况下，RSPAN 功能可能导致环路，并可能导致处理器上的负载激增。有关详细信息，请参阅为何 SPAN 会话会产生桥接环路？

交换机可以像平常一样传递数据流，因为所有操作都在硬件中进行，但是如果它试图确定要发送哪个数据流，CPU 可能难以承受。建议只在必需时配置 SPAN 会话。

%CFIB-SP-STBY-7-CFIB_EXCEPTION ：FIB TCAM exception, Some entries will be software switched

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

当 TCAM 中的可用空间量被超出时，将收到此错误信息。这将导致 CPU 使用率较高。这是一个 FIB TCAM 限制。一旦 TCAM 已满，便将设置一个标志，并将收到 FIB TCAM 异常错误。这将停止向 TCAM 添加新的路由。因此，所有数据流都将进行软件交换。删除路由对恢复硬件交换没有帮助。一旦 TCAM 进入异常错误状态，必须重新加载系统才能脱离该状态。通过 **mls cef maximum-routes** 命令可以增加 TCAM 中可以安装的最大路由数。

运行以高CPU的Catalyst 6500/6000有IPv6 ACL用L4端口

Enable (event) MLS IPv6 ACL压缩地址单播。如果IPv6 ACL在L4协议端口端口号，匹配此命令是

需要的。如果此命令没有启用， IPv6流量将被踢对软件处理的CPU。默认情况下此命令没有配置。

铜缆 SPF

在 Cisco ME 6500 系列以太网交换机中，铜缆 SFP 比其他类型的 SFP 需要更多固件交互，这会使 CPU 使用率升高。

管理铜缆 SFP 的软件算法已在 Cisco IOS SXH 版本中改进。

模块化 IOS

在运行模块化 IOS 软件的 Cisco Catalyst 6500 系列交换机中，正常 CPU 使用率稍大于非模块化 IOS 软件。

模块化 IOS 软件为每个活动付出的代价多于它为每个数据包付出的代价。模块化 IOS 软件通过消耗特定的 CPU 来维护进程，即使没有多少数据包也是如此，因此 CPU 消耗并不基于实际数据流。但是，当处理的数据包比率升高时，在模块化 IOS 软件中消耗的 CPU 不应多于在非模块化 IOS 软件中消耗的 CPU。

检查 CPU 使用率

如果 CPU 使用率较高，请先发出 **show processes cpu** 命令。输出显示交换机上的 CPU 使用率以及每个进程的 CPU 使用率。

```
Router#show processes cpu CPU utilization for five seconds: 57%/48%; one minute: 56%; five
minutes: 48% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process    1
0         5          0  0.00%  0.00%  0.00%   0 Chunk Manager       2          12     18062
0  0.00%  0.00%  0.00%   0 Load Meter          4      164532     13717      11994  0.00%  0.21%
0.17%   0 Check heaps         5          0         1          0  0.00%  0.00%  0.00%   0 Pool
Manager     !--- Output is suppressed. 172 0 9 0 0.00% 0.00% 0.00% 0 RPC aapi_rp 173      243912
2171455        112  9.25%  8.11%  7.39%   0 SNMP ENGINE       174          68       463
146  0.00%  0.00%  0.00%   0 RPC pm-mp  !--- Output is suppressed.
```

在此输出中，总 CPU 使用率是 57%，中断 CPU 使用率是 48%。此处，这些百分比以粗体文本显示。由 CPU 进行的数据流中断交换将导致中断 CPU 使用率。命令输出列出了导致两种使用率之间的差异的进程。在本例中，原因是 SNMP 进程。

在运行 CatOS 的 Supervisor 引擎上，输出如下所示：

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410    3712736    106000    22.22%  21.84%  21.96% -2
SptBpduRx      63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

在此输出中，第一个进程是 Kernel and Idle，它显示空闲 CPU 使用率。通常，此进程显示的空闲 CPU 使用率较高，除非一些其他进程占用 CPU 周期。在本示例中，SptBpduRx 进程导致高 CPU 使用率。

如果 CPU 使用率较高是由于这些进程之一导致的，您可以排除故障并确定此进程导致高 CPU 使用率的原因。但是，如果 CPU 较高是由于被转出到 CPU 的数据流导致的，则您需要确定数据流被转出的原因。确定数据流被转出的原因可帮助您识别该数据流是什么。

对于排除故障，当您体验高CPU利用率时，请使用此EEM脚本示例为了从交换机收集输出：

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410    3712736    106000    22.22%  21.84%  21.96% -2
SptBpduRx      63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

注意： 当CPU是由于的高处理数据包交换而不是硬件时，**调试netdr捕获rx**命令是有用。当命令运行时，它获取4096数据包流入对CPU。命令是十分安全的并且是高CPU问题的最方便的工具在6500。它不引起额外的负载CPU。

用于确定被传送到 CPU 的数据流的实用程序和工具

本部分确定了可帮助您查看此数据流的一些实用程序和工具。

Cisco IOS 系统软件

在 Cisco IOS 软件中，Supervisor 引擎上的交换处理器称为 SP，MSFC 称为 RP。

show interface 命令提供有关接口状态和接口上数据流速率的基本信息。此命令也提供错误计数器。

```
Router#show interface gigabitethernet 4/1GigabitEthernet4/1 is up, line protocol is up
(connected)  Hardware is C6k 1000Mb 802.3, address is 000a.42d1.7580 (bia 000a.42d1.7580)
Internet address is 100.100.100.2/24  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255  Encapsulation ARPA, loopback not set  Keepalive
set (10 sec)  Half-duplex, 100Mb/s  input flow-control is off, output flow-control is off  Clock
mode is auto  ARP type: ARPA, ARP Timeout 04:00:00  Last input 00:00:00, output 00:00:00, output
hang never  Last clearing of "show interface" counters never  Input queue: 5/75/1/24075
(size/max/drops/flushes); Total output drops: 2  Queueing strategy: fifo  Output queue: 0/40
(size/max)  30 second input rate 7609000 bits/sec, 14859 packets/sec  30 second output rate 0
bits/sec, 0 packets/sec  L2 Switched: ucast: 0 pkt, 184954624 bytes - mcast: 1 pkt, 500 bytes
L3 in Switched: ucast: 2889916 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast  L3 out Switched:
ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes     2982871 packets input, 190904816 bytes, 0 no
buffer     Received 9 broadcasts, 0 runts, 0 giants, 0 throttles     1 input errors, 1 CRC, 0
frame, 28 overrun, 0 ignored     0 input packets with dribble condition detected     1256
packets output, 124317 bytes, 0 underruns     2 output errors, 1 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred     0 lost carrier, 0 no carrier     0 output buffer
failures, 0 output buffers swapped out
```

在此输出中，可以看到传入数据流是在第 3 层交换的（而不是在第 2 层交换的）。这表明数据流被转出到 CPU。

show processes cpu 命令告诉您这些数据包是常规数据流数据包还是控制数据包。

```
Router#show processes cpu | exclude 0.00              CPU utilization for five seconds: 91%/50%;
one minute: 89%; five minutes: 47% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY
Process   5      881160     79142      11133  0.49%  0.19%  0.16%   0 Check heaps       98
121064   3020704         40 40.53% 38.67% 20.59%   0 IP Input         245      209336    894828
233  0.08%  0.05%  0.02%   0 IFCOM Msg Hdlr
```

如果数据包是进程交换的，您会看到 IP Input process 的 CPU 使用率升高。发出此命令可以看到以下数据包：

show buffers input-interface

```
Router#show buffers input-interface gigabitethernet 4/1 packetBuffer information for Small
buffer at 0x437874D4  data_area 0x8060F04, refcount 1, next 0x5006D400, flags 0x280  linktype 7
(IP), enctype 1 (ARPA), encsize 14, rxtype 1  if_input 0x505BC20C (GigabitEthernet4/1),
if_output 0x0 (None)  inputtime 00:00:00.000 (elapsed never)  outputtime 00:00:00.000 (elapsed
never), oqnumber 65535  datagramstart 0x8060F7A, datagramsize 60, maximum size 308  mac_start
0x8060F7A, addr_start 0x8060F7A, info_start 0x0  network_start 0x8060F88, transport_start
0x8060F9C, caller_pc 0x403519B4  source: 100.100.100.1, destination: 100.100.100.2, id: 0x0000,
ttl: 63,  TOS: 0 prot: 17, source port 63, destination port 6308060F70:
000A 42D17580            ..BQu.08060F80: 00000000 11110800 4500002E 00000000
........E.......08060F90: 3F11EAF3 64646401 64646402 003F003F  ?.jsddd.ddd..?.?08060FA0:
001A261F 00010203 04050607 08090A0B  ..&.............08060FB0: 0C0D0E0F 101164
......d
```

如果数据流是**中断交换的**，则使用 show buffers input-interface 命令无法看到这些数据包。为了看到由于中断交换被转出到 RP 的数据包，可以执行 RP 端口的交换端口分析程序 (SPAN) 捕获。

注意： 有关中断交换与进程交换 CPU 使用率的详细信息，请参阅以下文档：

- 对 Cisco 路由器上的 CPU 使用率过高进行故障排除的*由于中断而导致 CPU 使用率较高* 部分

SPAN RP-Inband 和 SP-Inband

Cisco IOS 软件中用于 RP 或 SP 端口的 SPAN 在 Cisco IOS 软件版本 12.1(19)E 及更高版本中可用。

以下是命令语法：

```
test monitor session 1-66 add {rp-inband | sp-inband} [rx | tx | both]
```

对于 Cisco IOS 软件 12.2 SX 版本，使用以下语法：

```
test monitor add {1..66} {rp-inband | sp-inband} {rx | tx | both}
```

注意： 对于 SXH 版本，必须使用 **monitor session** 命令配置本地 SPAN 会话，然后使用此命令将 SPAN 会话与 CPU 关联：

```
source {cpu {rp | sp}} | single_interface | interface_list | interface_range |
mixed_interface_list | single_vlan | vlan_list | vlan_range | mixed_vlan_list} [rx | tx | both]
```

注意： 有关这些命令的详细信息，请参阅 *Catalyst 6500 版本 12.2SX 软件配置指南* 中的配置本地 SPAN（SPAN 配置模式）。

以下是 RP 控制台上的一个示例：

```
Router#monitor session 1 source interface fast 3/3!--- Use any interface that is
administratively shut down.Router#monitor session 1 destination interface 3/2
```

现在，转到 SP 控制台。示例如下：

```
Router-sp#test monitor session 1 add rp-inband rx
```

注意： 在 Cisco IOS 12.2 SX 版本中，此命令已更改为 **test monitor add 1 rp-inband rx**。

```
Router#show monitor Session 1---------Type : Local SessionSource Ports :Both : Fa3/3Destination
Ports : Fa3/2SP console:Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1
Egress Source Ports: 3/3 Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans:
<empty>Destination Ports: 3/2
```

注意： 在 Cisco IOS 12.2 SX 版本中，此命令已更改为 **test monitor show 1**。

以下是 SP 控制台上的一个示例：

```
Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1 Egress Source Ports: 3/3
Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans: <empty>Destination Ports:
3/2
```

CatOS 系统软件

对于运行 CatOS 系统软件的交换机，Supervisor 引擎运行 CatOS，MSFC 运行 Cisco IOS 软件。

如果发出 **show mac** 命令，可以看到被转出到 MSFC 的帧的数量。端口 15/1 是与 MSFC 的 Supervisor 引擎连接。

注意： 端口 16/1 用于插槽 2 中的 Supervisor 引擎。

```
Console> (enable) show mac 15/1Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast-
------- -------------------- -------------------- --------------------15/1
193576                    0                    1Port     Xmit-Unicast         Xmit-Multicast
Xmit-Broadcast-------- -------------------- -------------------- --------------------15/1
3                     0                     0Port     Rcv-Octet            Xmit-Octet-------- ----
---------------- --------------------15/1                 18583370                    0MAC
Dely-Exced MTU-Exced  In-Discard Out-Discard-------- ---------- ---------- ---------- ----------
-15/1              0          -          0           0
```

此数字快速增加表明数据包被转出到 MSFC，导致高 CPU 使用率。然后您可以通过以下方式查看数据包：

- SPAN MSFC 端口 15/1 或 16/1
- SPAN sc0

SPAN MSFC 端口 15/1 或 16/1

设置一个 SPAN 会话，其中源是 MSFC 端口 15/1（或 16/1），目标是以太网端口。

示例如下：

```
Console> (enable) set span 15/1 5/10Console> (enable) show spanDestination     : Port 5/10Admin
Source    : Port 15/1Oper Source     : NoneDirection       : transmit/receiveIncoming Packets:
disabledLearning        : enabledMulticast       : enabledFilter          : -Status          :
active
```

如果收集端口 5/10 上的嗅探器踪迹，嗅探器踪迹显示从 MSFC 传输的数据包和传输到 MSFC 的数据包。 将 SPAN 会话配置为 **tx** 以只捕获发往 MSFC 的数据包而不捕获来自 MSFC 的数据包。

SPAN sc0

设置一个以 **sc0** 接口作为源的 SPAN 会话，以捕获进入 Supervisor 引擎 CPU 的帧。

```
Console> (enable) set span ?  disable                  Disable port monitoring  sc0
Set span on interface sc0  <mod/port>                Source module and port numbers  <vlan>
Source VLAN numbers
```

注意： 对于光服务模块 (OSM)，不能执行数据流 SPAN 捕获。

建议

Supervisor 引擎 CPU 使用率不反映交换机的硬件转发性能。但是，仍必须以 Supervisor 引擎 CPU

使用率作为基线并对其进行监控。

1. 以稳定状态网络中具有正常数据流模式和负载的交换机的 Supervisor 引擎 CPU 使用率作为基线。请注意哪些进程导致最高的 CPU 使用率。
2. 在排除 CPU 使用率故障时，请考虑以下问题：哪些进程导致最高使用率？这些进程是否与您的基线不同？CPU 使用率是否一直高于基线？或者是否存在出现高使用率峰值，然后返回基线水平的情况？网络中是否存在拓扑更改通知 (TCN)？**注意：** 已禁用 STP Portfast 的抖动端口或主机端口将导致 TCN。管理子网/VLAN 中是否存在过多的广播或多播数据流？交换机上是否存在过多的管理数据流，如 SNMP 轮询？
3. 在高CPU时间期间(当CPU是75%以上)时，从这些命令请收集输出：show clockshow version排序的show processes cpushow proc cpu历史记录show log
4. 如果可能，请从具有用户数据流（特别是大量广播数据流）的 VLAN 中分离出管理 VLAN。这种数据流类型的示例包括 IPX RIP/服务通告协议 (SAP)、AppleTalk 和其他广播数据流。此类数据流可能影响 Supervisor 引擎 CPU 使用率，并且在特殊情况下可能干扰交换机的正常运行。
5. 如果由于数据流被转出到 RP 而导致 CPU 使用率很高，请确定该数据流是什么以及该数据流为什么被转出。为了进行此确定，请使用用于确定被传送到 CPU 的数据流的实用程序和工具部分介绍的实用程序。

相关信息

- 排除故障的高CPU有用的命令在有Sup720的Catalyst 6500's
- Catalyst 6000/6500 系列交换机上常见的 CatOS 错误消息
- 运行 Cisco IOS 软件的 Catalyst 6500/6000 系列交换机上常见的错误消息
- 排除运行 Cisco IOS 系统软件的 Catalyst 6500/6000 系列交换机上的硬件和常见问题
- 交换式园区网络中的单播泛洪
- Cisco Catalyst 6500 系列交换机产品支持
- 收集的数据EEM脚本在断断续续高CPU问题期间
- LAN 产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems