

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[故障排除&解决方案](#)

[Catalyst 3850系列交换机](#)

[解决方案](#)

[Catalyst 4500 系列交换机](#)

[解决方案](#)

[Catalyst 6500系列交换机](#)

[解决方案](#)

[相关的思科支持社区讨论](#)

简介

本文描述在多种Catalyst平台的高CPU利用率由于充斥IPv6组播监听程序发现信息包和方式减轻此问题。

先决条件

没有前提条件。

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据Cisco Catalyst 6500系列交换机、Catalyst 4500系列交换机和Catalyst 3850系列交换机。

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。

问题

高CPU利用率在一些思科Catalyst平台可能被看到由于与MAC地址的IPv6组播流量在3333.xxxx.xxxx被踢的范围对CPU。

根据RFC7042，所有MAC-48组播标识符加了前缀"33-33" (即在范围的2**32组播MAC标识符从33-33-00-00-00-00到33-33-FF-FF-FF-FF)在[RFC2464]上指定使用IPv6组播。与组播目的地地址

DST的一IPv6数据包，包括十六个八位位组DST[1]通过DST[16]，传送对如图1所显示，前两个八位位组是十六进制值3333，并且为时四八位位组是最后四个八位位组DST的以太网组播地址。

某时被看到了，当主机设备使用某一NIC卡去静止方式时，他们充斥IPv6组播流量。此问题对特定主机供应商没有被限制，虽然某些芯片组比其他被看到经常显示此行为。

故障排除&解决方案

您能使用跟随的步骤发现，如果您的看到高CPU利用率的Catalyst交换机是受此问题的影响的和实现各自解决方案。

Catalyst 3850系列交换机

在Catalyst 3850交换机上，NGWC L2M进程使用CPU处理IPv6数据包。当组播监听程序监听的发现号(MLD)时在交换机禁用，MLD加入/事假数据包被充斥到所有成员端口。并且，如果有许多流入MLD加入/事假数据包，此进程将消耗更多CPU周期派出在所有成员端口的数据包。被看到，当某些主机去静止方式时，他们可能发送数千包/秒IGMPv6 MLD流量。

```
3850#show processes cpu detailed process iosd sorted | exc 0.0
Core 0: CPU utilization for five seconds: 43%; one minute: 35%; five minutes: 33%
Core 1: CPU utilization for five seconds: 54%; one minute: 46%; five minutes: 46%
Core 2: CPU utilization for five seconds: 75%; one minute: 63%; five minutes: 58%
Core 3: CPU utilization for five seconds: 48%; one minute: 49%; five minutes: 57%
PID      T C  TID      Runtime(ms) Invoked uSecs  5Sec      1Min      5Min      TTY      Process
12577    L   12577    2766882   2422952 291    23.52     23.67     23.69     34816   iosd
12577    L 3   12577    1911782   1970561 0        23.34     23.29     23.29     34818   iosd
12577    L 0   14135    694490    3264088 0        0.28      0.34      0.36      0       iosd.fastpath
162      I           2832830   6643     0        93.11     92.55     92.33     0       NGWC L2M
```

解决方案

配置监听在受影响的交换机的IPv6 mld全局启用监听IPv6的mld。这应该降低在CPU利用率下。

```
3850#conf t
Enter configuration commands, one per line. End with CNTL/Z.
3850(config)#ipv6 mld snooping
3850(config)#end
```

当监听的MLD启用时，每VLAN IPv6组播地址表在软件和硬件方面被修建。交换机在硬件方面然后执行IPv6组播地址基于桥接，防止软件将处理的这些数据包。

点击链路关于[配置监听的MLD的更多信息](#)

在IOS XE更早版本，发现CPU队列可能获得卡住由于从去将终止在该队列的控制数据包CPU的此问题。这通过在IOS版本3.3.3和3.6.0的[CSCuo14829](#)修复及以后。请参考此bug关于详细信息。

Catalyst 4500 系列交换机

Catalyst 4500系列交换机IPv6组播流量支持硬件转发使用三重内容可编址存储器。这在[思科Catalyst 4500E和4500X系列交换机的组播解释](#)

当谈到IPv6组播监听程序发现号流量，交换机需要执行软件转发(使用CPU资源)。按照[配置IPv6](#)

[MLD说明](#) [监听在Catalyst 4500交换机的MLD](#)可以是启用或禁用的全局或每个VLAN。当监听的MLD启用时，每VLAN IPv6组播MAC地址表在软件方面被修建，并且每VLAN IPv6组播地址表在软件和硬件方面被修建。交换机在硬件方面然后执行IPv6组播地址基于桥接。这是在Catalyst 4500系列交换机的预料之中的行为。

为了检查被踢对我们能运行的CPU的数据包的类型？**调试平台数据包全部缓冲？**跟随由？**显示平台缓冲的cpu数据包？**命令。

```
4500#debug platform packet all buffer
platform packet debugging is on
Cat4500#sh platform cpu packet buffered
Total Received Packets Buffered: 1024
-----
Index 0:
33 days 11:42:21:833532 - RxVlan: 214, RxPort: Te1/15
Priority: Normal, Tag: Dot1Q Tag, Event: L2 Router, Flags: 0x40, Size: 90
Eth: Src 44:39:C4:39:5A:4A Dst 33:33:FF:7F:EB:DB Type/Len 0x86DD
Remaining data:
0: 0x60 0x0 0x0 0x0 0x0 0x20 0x0 0x1 0xFE 0x80
10: 0x0 0x0 0x0 0x0 0x0 0x0 0x46 0x39 0xC4 0xFF
20: 0xFE 0x39 0x5A 0x4A 0xFF 0x2 0x0 0x0 0x0 0x0
30: 0x0 0x0 0x0 0x0 0x0 0x1 0xFF 0x7F 0xEB 0xDB
40: 0x3A 0x0 0x5 0x2 0x0 0x0 0x1 0x0 0x83 0x0
```

此数据包在VLAN 214的接口Tengigabitethernet1/15到达从源MAC地址44:39:C4:39:5A:4A。协议0x86DD是IPv6，并且Dst MAC 33:33:FF:7F:EB:DB在这种情况下使用组播IPv6 MLD节点。

解决方案

我们有两个选项修复高CPU利用率由于此流量。

1. 禁用IPv6组播监听程序在终端主机的发现号流量的生成。这能执行通过升级NIC驱动程序或禁用在发送IPv6数据包的主机BIOS的功能。您能联系可帮助禁用在BIOS的功能或升级NIC驱动程序的您的客户端机器的供应商。
1. 使控制平面策略(CoPP)为了降低超出数量IPv6组播监听程序被踢对CPU的发现号流量。并且，这些数据包是一链路本地跳限制，因而是预料之中的行为这些数据包将被踢对CPU。

```
4500#debug platform packet all buffer
platform packet debugging is on
Cat4500#sh platform cpu packet buffered
Total Received Packets Buffered: 1024
-----
Index 0:
33 days 11:42:21:833532 - RxVlan: 214, RxPort: Te1/15
Priority: Normal, Tag: Dot1Q Tag, Event: L2 Router, Flags: 0x40, Size: 90
Eth: Src 44:39:C4:39:5A:4A Dst 33:33:FF:7F:EB:DB Type/Len 0x86DD
Remaining data:
0: 0x60 0x0 0x0 0x0 0x0 0x20 0x0 0x1 0xFE 0x80
10: 0x0 0x0 0x0 0x0 0x0 0x0 0x46 0x39 0xC4 0xFF
20: 0xFE 0x39 0x5A 0x4A 0xFF 0x2 0x0 0x0 0x0 0x0
30: 0x0 0x0 0x0 0x0 0x0 0x1 0xFF 0x7F 0xEB 0xDB
40: 0x3A 0x0 0x5 0x2 0x0 0x0 0x1 0x0 0x83 0x0
```

在CPU to32000数据包处理每秒的上述示例中，我们限制相当数量IPv6流量。

Catalyst 6500系列交换机

Catalyst 6500交换机在通常不需要CPU协助的硬件方面做出转发决策使用TCAM，只要TCAM有转发条目。

Supervisor在Catalyst 6500交换机的Enginet 720有两CPU。一个CPU是网络管理处理器(NMP)或交换机处理器(SP)。另一个CPU是第3层CPU，呼叫路由处理器(RP)。

进程和中断CPU利用率在show process cpu命令列出。如下所示，

```
4500#debug platform packet all buffer
platform packet debugging is on
Cat4500#sh platform cpu packet buffered
Total Received Packets Buffered: 1024
-----
Index 0:
33 days 11:42:21:833532 - RxVlan: 214, RxPort: Te1/15
Priority: Normal, Tag: Dot1Q Tag, Event: L2 Router, Flags: 0x40, Size: 90
Eth: Src 44:39:C4:39:5A:4A Dst 33:33:FF:7F:EB:DB Type/Len 0x86DD
Remaining data:
0: 0x60 0x0 0x0 0x0 0x0 0x20 0x0 0x1 0xFE 0x80
10: 0x0 0x0 0x0 0x0 0x0 0x0 0x46 0x39 0xC4 0xFF
20: 0xFE 0x39 0x5A 0x4A 0xFF 0x2 0x0 0x0 0x0 0x0
30: 0x0 0x0 0x0 0x0 0x0 0x1 0xFF 0x7F 0xEB 0xDB
40: 0x3A 0x0 0x5 0x2 0x0 0x0 0x1 0x0 0x83 0x0
```

检查任何接口或第3层VLAN是否下降大量数据流。(输入队列丢弃)。如果那样，流量可能踢给到RP从该VLAN。

```
Vlan19 is up, line protocol is up
  Input queue: 0/75/6303532/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  5 minute input rate 19932000 bits/sec, 26424 packets/sec
  5 minute output rate 2662000 bits/sec, 1168 packets/sec
```

跟随的命令可以用于查找在Input queue缓冲区的所有信息包接口VLAN的19。

```
Vlan19 is up, line protocol is up
  Input queue: 0/75/6303532/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  5 minute input rate 19932000 bits/sec, 26424 packets/sec
  5 minute output rate 2662000 bits/sec, 1168 packets/sec
```

或者，您能使用NetDR捕获捕获去在Catalyst 6500交换机的CPU的流量。[本文](#)解释如何解释使用NetDR捕获捕获的数据包。

```
----- dump of incoming inband packet -----interface Vl16, routine
mistral_process_rx_packet_inlin, timestamp 03:17:56.380dbus info: src_vlan 0x10(16), src_indx
0x1001(4097), len 0x5A(90) bpdu 0, index_dir 0, flood 1, dont_lrn 0, dest_indx 0x4010(16400)
E8820000 00100000 10010000 5A080000 0C000418 01000008 00000008 4010417Emistral_hdr: req_token
0x0(0), src_index 0x1001(4097), rx_offset 0x76(118) requeue 0, obl_pkt 0, vlan 0x10(16)destmac
33.33.FF.4A.C3.FD, srcmac C8.CB.B8.29.33.62, protocol 86DDprotocol ipv6: version 6, flow
1610612736, payload 32, nexthdr 0, hoplt 1class 0, src FE80::CACB:B8FF:FE29:3362, dst
FF02::1:FF4A:C3FD
```

解决方案

请使用一个或很多下面的解决方案。

1. 通过使用以下配置，丢弃IPv6组播数据包。

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. 重定向IPv6组播流量对一个未使用或admin关闭接口(在本例中的Gi1/22)。

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. 请使用VLAN访问控制列表(VACL)降低IPv6组播流量。

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. 禁用监听IPv6的MLD。

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. 降低IPv6组播流量使用控制平面策略(CoPP)

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. 请使用在入口接口的storm-control。storm-control监视器流入的数据流成水平—1秒的粒，并且在此间隔期间数据流级别与已配置的流量控制层比较。流量控制层是端口的百分比总可用的带宽。每个端口有使用所有流量类型的单个流量控制层(广播，组播和单播)。

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

7. 万一，如果CPU是高在SP (交换处理器)，请应用下面应急方案。

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

如果无法确定根据信息的原因提供在本文，请打开TAC服务请求进一步调查。