

由于IPv6组播流量，Catalyst交换机上的CPU使用率较高

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[故障排除和解决方案](#)

[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

本文档介绍由于IPV6组播侦听程序发现数据包泛洪而导致的各种Catalyst平台上的高CPU使用率，以及缓解此问题的方法。

先决条件

没有先决条件。

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。

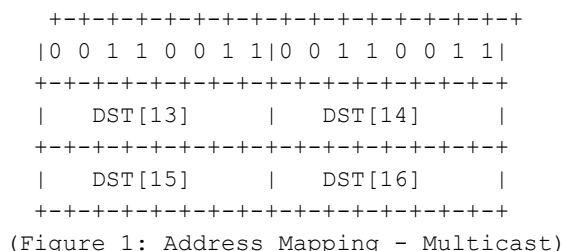
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。

问题

由于MAC地址范围为3333.xxxx.xxxx的IPv6组播流量正被传送到CPU，因此某些Cisco Catalyst平台

上可能会出现CPU使用率较高的情况。

根据RFC7042，所有MAC-48组播标识符前缀“33-33”(即，2**32个组播MAC标识符，范围从33-33-00-00-00-00到33-33-FF-FF-FF-FF)均按照[RFC2464]中为IPv6组播指定。组播目的地址为DST的IPv6数据包由16个八位组DST[1]到DST[16]组成，它被传输到以太网组播地址，其前两个八位组是值333十六进制，其后四个八位组是DST的后四个八位组，如图1所示。



有时，使用特定NIC卡的主机设备进入休眠模式时，会泛洪IPv6组播流量。此问题不限于特定主机供应商，尽管某些芯片组比其他芯片组更频繁地表现出此行为。

故障排除和解决方案

您可以使用以下步骤了解发现CPU使用率较高的Catalyst交换机是否受此问题的影响，并实施相应的解决方案。

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。当交换机上禁用组播侦听程序发现(MLD)监听时，MLD加入/离开数据包将泛洪到所有成员端口。而且，如果有许多传入的MLD加入/离开数据包，此进程将消耗更多CPU周期，以在所有成员端口上发送数据包。已经看到，当某些主机进入休眠模式时，它们可能会发送数千个数据包/秒的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

在受影响的交换机上配置ipv6 mld监听，以全局启用ipv6 mld监听。这会降低CPU利用率。

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

启用MLD监听时，在软件和硬件中构建每VLAN IPv6组播地址表。然后，交换机在硬件中执行基于IPv6组播地址的桥接，从而防止这些数据包由软件处理。

有关配置MLD监听的详细信息，请单[击链接](#)

在IOS XE的早期版本中，发现CPU队列可能因此问题而卡住，这将阻止该队列中的所有控制数据包进入CPU。这是通过IOS版本[3.3.3](#)和[3.6.0](#)及更高版本的CSCuo14829修复的。有关详细信息，请参阅[此漏洞](#)。

Catalyst 4500 系列交换机

Catalyst 4500系列交换机支持使用三态内容可寻址存储器(TCAM)的IPv6组播流量硬件转发。这在Cisco Catalyst 4500E和[4500X系列交换机上的组播中解释](#)

当涉及IPv6组播侦听程序发现流量时，交换机需要执行软件转发（使用CPU资源）。如在Catalyst 4500交换机[上配置IPv6 MLD监听中所述](#)，MLD监听可以全局启用或禁用或按VLAN启用。启用MLD监听时，在软件中构建每VLAN IPv6组播MAC地址表，在软件和硬件中构建每VLAN IPv6组播地址表。然后，交换机在硬件中执行基于IPv6组播地址的桥接。这是Catalyst 4500系列交换机上的预期行为。

为了检查被传送到CPU的数据包的类型，我们可以运行“`debug platform packet all buffer`”，然后运行“`show platform cpu packet buffered`”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&colon;
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
```

此数据包从源mac地址44:39:C4:39:5A:4A到达VLAN 214上的接口Tengigabitethernet1/15。协议0x86DD是IPv6，在本例中，目的MAC 33:33:FF:7F:EB:DB用于组播IPv6 MLD节点。

解决方案

由于此流量，我们有两种解决CPU使用率过高问题的方法。

1. 禁用在终端主机上生成IPv6组播侦听程序发现流量。这可以通过升级NIC驱动程序或禁用发送IPv6数据包的主机的BIOS上的功能来实现。您可以联系客户机的供应商，该供应商可以帮助禁用BIOS功能或升级NIC驱动程序。
2. 启用控制平面策略(CoPP)以丢弃传送到CPU的过多IPv6组播侦听程序发现流量。而且，这些数据包是本地链路的跳数限制，因此这些数据包预期会被传送到CPU。

```

ipv6 access-list IPv6-Block
permit ipv6 any any
!
class-map TEST
match access-group name IPv6-Block
!
policy-map ipv6
class TEST
police 32000 conform-action drop exceed-action drop
!
control-plane
service-policy input ipv6

```

在上例中，我们将CPU处理的IPv6流量限制为每秒32000个数据包。

Catalyst 6500 系列交换机

Catalyst 6500交换机使用TCAM在硬件中做出转发决策，TCAM通常不需要CPU协助，只要TCAM有转发条目。

Catalyst 6500交换机上的Supervisor Engine 720有两个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，称为路由处理器(RP)。

进程和中断CPU利用率列在**show process cpu**命令中。如下所示，高中断引起的CPU大多基于流量。中断交换流量，是指与特定进程不匹配但仍需要转发的流量。以下示例显示Catalyst 6500交换机由于中断而在RP上具有高CPU利用率。

```

6500#show process cpu
CPU utilization for five seconds: 98%/92%;
one minute: 99%; five minutes: 99% PID Runtime(ms) Invoked

```

检查是否有接口或第3层VLAN丢弃高流量。(输入队列丢弃)。如果是，流量可能会从该VLAN传送到RP。

```

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

```

以下命令可用于查找接口vlan 19的输入队列缓冲区中的所有数据包。

```
6500#show buffer input-interface vlan 19 packet
```

或者，您可以使用NetDR捕获捕获Catalyst 6500交换机上发往CPU的流量。本文[档](#)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 03:17:56.380
dbus 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 4010417E
mistral_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 86DD
protocol ipv6: version 6, flow 1610612736, payload 32, nexthdr 0, hoplt 1
class 0, src FE80::CACB:B8FF:FE29:3362, dst FF02::1:FF4A:C3FD

```

解决方案

使用以下一个或多个解决方案。

1. 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
```

2. 将IPv6组播流量重定向到未使用或管理员关闭接口 (本例中为Gi1/22)。

```
6500(config)#mac-address-table 3333.FF4A.C3FD vlan 19 interface Gi1/22
```

3. 使用VLAN访问控制列表(VACL)丢弃IPv6组播流量。

```
6500(config)#mac access-li extended Multicast_MAC
6500(config-ext-macl)#permit any host 3333.FF4A.C3FD
6500(config-ext-macl)#exit
6500(config)#vlan access-map block-ipv6 10
6500(config-access-map)#action drop
6500(config-access-map)#match mac address Multicast_MAC
6500(config-access-map)#exit
6500(config-access-map)#vlan access-map block-ipv6 20
6500(config-access-map)#action forward
6500(config-access-map)#exit
6500(config)#vlan filter block-ipv6 vlan-list <vlan #>
```

4. 禁用IPv6 MLD监听。

```
6500(config)#no ipv6 mld snoopin
```

5. 使用控制平面策略(CoPP)丢弃IPv6组播流量

```
6500(config)#ipv6 access-list test
6500(config-ipv6-acl)#permit ipv6 any any
6500(config-ipv6-acl)#exit

6500(config)#class-map TEST
6500(config-cmap)#match access-group name test
6500(config-cmap)#exit

6500(config)#policy-map ipv6
6500(config-pmap)#class TEST
6500(config-pmap-c)#police 320000 conform-action drop exceed-action drop
6500(config-pmap-c)#exit

6500(config)#control-plane
6500(config-cp)#service-policy in ipv6
6500(config-cp)#exit
```

6. 在入口接口上使用风暴控制。风暴控制在1秒间隔内监控传入流量级别，在此间隔内，它会将流量级别与已配置的流量风暴控制级别进行比较。流量风暴控制级别是端口总可用带宽的百分比。每个端口都有一个流量风暴控制级别，用于所有类型的流量 (广播、组播和单播)。

```
6500(config)#interface Gi2/22
6500(config-if)#storm-control multicast level 10
```

7.如果SP (交换机处理器) 上的CPU使用率较高，请应用以下解决方法。

```
6500(config)#mls rate-limit ipv6 mld 10 1
```

如果您无法根据本文档中提供的信息确定原因，请提交TAC服务请求以进一步调查。