

Gebruik van hoge CPU's op Catalyst-switches door IPv6-multicast verkeer

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Problemen oplossen en oplossing](#)

[Catalyst 3850 Series switches](#)

[Oplossing](#)

[Catalyst 4500 Series switches](#)

[Oplossing](#)

[Catalyst 6500 Series switches](#)

[Oplossing](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding

In dit document wordt een hoog CPU-gebruik op verschillende Catalyst-platforms beschreven door overstroming van IP V6-multicast detectiepakketten en manieren om dit probleem op te lossen.

Voorwaarden

Er zijn geen voorwaarden.

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

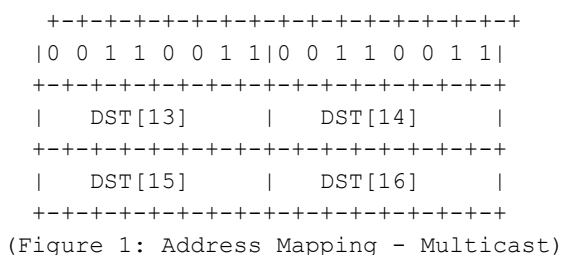
De informatie in dit document is gebaseerd op Cisco Catalyst 6500 Series-switches, Catalyst 4500 Series switches en Catalyst 3850 Series switches.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie.

Probleem

Het gebruik van hoge CPU's kan op sommige Cisco Catalyst-platforms worden gezien door IPv6-multicast verkeer met MAC-adres in het bereik 333.xxxx.xxx dat op CPU's wordt gestraft.

Volgens RFC7042 worden alle MAC-48 multicast-identificatoren vooraf ingesteld op "33-33" (dat wil zeggen de 2**32 multicast MAC-identificatoren in het bereik van 33-33-00-00-00-00 tot 33-33-FF-FF-FF [FF-FF] gebruikt zoals aangegeven in RFC2464] voor IPv6-multicast. Een IPv6-pakket met een multicast bestemmingsadres DST, dat bestaat uit de zestien octetten DST[1] via DST[16], wordt naar het Ethernet multicast-adres verzonden waarvan de eerste twee octetten de waarde 3333 hexadecimaal zijn en waarvan de laatste vier octetten de laatste vier pakketten van DST zijn zoals in afbeelding 1.



Er is bij sommige gelegenheden gezien dat wanneer hosts met apparaten die gebruik maken van een bepaalde NIC-kaart naar de slaapmodus gaan, zij in multicast IPv6-verkeer overspoelen. Deze kwestie is niet beperkt tot een bepaalde verkoper van ontvangst, hoewel bepaalde chipsets dit gedrag vaker laten zien dan andere.

Problemen oplossen en oplossing

U kunt de volgende procedures gebruiken om te weten te komen of uw Catalyst-switch wanneer u een hoog CPU-gebruik ziet, door dit probleem wordt beïnvloed en respectieve oplossingen implementeren.

Catalyst 3850 Series switches

Op Catalyst 3850-switches gebruikt NGWC L2M-proces CPU's voor het verwerken van IPv6-pakketten. Wanneer MLD-snooping (Multicast Luistener Discovery) via de schakelaar wordt uitgeschakeld, dient MLD zich aan te sluiten bij het pakket en het pakket achter te laten door alle lidstaten. En als er veel binnenkomende MLD-pakketten beschikbaar zijn om aan te sluiten of te verlaten, zal dit proces meer CPU-cycli vergen om de pakketten op alle afzonderlijke poorten te verzenden. Er is aangetoond dat wanneer bepaalde host-machines naar de slaapmodus gaan, zij duizenden pakketten per sec IGMPv6 MLD-verkeer kunnen verzenden.

```
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   3   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
```

Oplossing

Configureer **ipv6 mld** door op de getroffen switches te **snooping** om wereldwijd **ipv6 mld-snooping** mogelijk te maken. Dit zou het CPU-gebruik moeten verlagen.

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

Wanneer MLD-snooping is ingeschakeld, wordt een IPv6 multicast adrestabel per VLAN-VLAN in software en hardware geconstrueerd. De switch voert vervolgens IPv6 op multicast adres gebaseerde overbrugging in hardware uit, waardoor deze pakketten niet door software kunnen worden verwerkt.

Klik op een link voor meer informatie over het [configureren van MLD-decodering](#)

Op eerdere versies van IOS XE werd ontdekt dat de CPU-wachtrij klem kon komen te zitten door dit probleem, waardoor alle besturingspakketten in die wachtrij zouden stoppen om naar de CPU te gaan. Dit is vastgesteld door [CSCuo14829](#) in IOS-versies 3.3.3 en 3.6.0 en hoger. Raadpleeg deze bug voor meer informatie.

Catalyst 4500 Series switches

Catalyst 4500 Series switches ondersteunen hardware-expanderen van IPv6-multicast verkeer met Ternary Content Adresseerbare Geheugen (TCAM). Dit wordt uitgelegd in [Multicast voor Cisco Catalyst 4500E en 4500X Series-switches](#)

Wanneer het op IPv6 Multicast Detectieverkeer aankomt, moet de switch software doorsturen (met CPU-bronnen). Zoals wordt uitgelegd in het [configureren van IPv6 MLD-spinnen op Catalyst 4500 switches](#) kan MLD-snooping mondiaal of per VLAN ingeschakeld of uitgeschakeld worden. Wanneer MLD-snooping is ingeschakeld, wordt een IPv6 multicast MAC-adrestabel per VLAN in de software geconstrueerd en wordt een IPv6 multicast adrestabel per VLAN in de software en de hardware geconstrueerd. De switch voert vervolgens IPv6 op multicast adres gebaseerde overbrugging in hardware uit. Dit is het verwachte gedrag op Catalyst 4500 Series switches.

Om het type pakket te controleren dat op CPU wordt gestraft, kunnen we "**platform debug all buffer**" uitvoeren, gevolgd door de opdracht "**platform cpu gebufferde**" pakketsnelheid weergeven.

```
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

Dit pakket is aangekomen op interface Tengigabitethernet1/15 op VLAN 214 van bronmac adres 44:39:C4:39:5A:4A. Protocol 0x86D is IPv6 en Dst MAC 3:3:FF:7F:EB:DB wordt in dit geval gebruikt voor multicast IPv6 MLD-knooppunten.

Oplossing

We hebben twee opties om een hoog CPU-gebruik te repareren vanwege dit verkeer.

1. Uitschakelen van generatie van IPv6 Multicast listener Detectie op eindhost. Dit kan worden gedaan door het verbeteren van de NIC-stuurprogramma's of het uitschakelen van de functie in het configuratiescherm van hosts die IPv6-pakketten verzenden. U kunt contact opnemen met de verkoper van de client die kan helpen om de functie uit te schakelen op een upgrade van de NIC-stuurprogramma.
2. CoPP-toezicht (Control Plane Policing) inschakelen om de buitensporige hoeveelheid IPv6-multicast detectieverkeer te laten vallen die naar de CPU wordt gestraft. En, deze pakketten zijn hopgrens van één lokale verbinding, dus wordt het verwacht gedrag dat deze pakketten aan CPU zullen worden gestraft.

```
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
```

In het bovenstaande voorbeeld beperken we de hoeveelheid IPv6-verkeer die door de CPU wordt verwerkt tot 32000 pakketten per seconde.

Catalyst 6500 Series switches

Catalyst 6500-switches nemen verzendingsbeslissingen in hardware met behulp van TCAM die normaliter geen CPU-ondersteuning nodig hebben zolang TCAM de verzendende ingang heeft.

Supervisor Engine 720 op Catalyst 6500 switches heeft twee CPU's. Eén CPU is de netwerkbeheerprocessor (NMP) of de switchprocessor (SP). De andere CPU is Layer 3 CPU, wat de routeprocessor (RP) wordt genoemd.

Het gebruik van CPU's verwerken en onderbreken wordt in de opdracht **Cpu-proces** weergegeven. Zoals hieronder wordt getoond, Hoog CPU's die door onderbrekingen worden veroorzaakt, zijn vooral op verkeer gebaseerd. Onderbreek geschakeld verkeer, is verkeer dat geen specifiek proces past, maar moet nog worden doorgestuurd. Volgend voorbeeld toont een Catalyst 6500 switch met een hoog CPU-gebruik op RP door onderbrekingen.

```
6500#show process cpu
CPU utilization for five seconds: 98%/92%;
```

one minute: 99%; five minutes: 99% PID Runtime(ms) Invoked

Controleer of een interface of Layer 3 VLAN een hoge hoeveelheid verkeer vermindert. (Wachtrij invoeren). Als dat zo is, kan het verkeer worden gestraft naar RP van dat 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

Na deze opdracht kan worden gebruikt om alle pakketten in de ingangswachtrijbuffer te vinden voor interface VLAN 19.

6500#show buffer input-interface vlan 19 packet

U kunt ook NetDR gebruiken om verkeer naar CPU op een Catalyst 6500-switch op te nemen. [Dit document](#) legt uit hoe u opgenomen pakketten interpreteert met behulp van NetDR-opname.

----- 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

Oplossing

Gebruik één of meer van onderstaande oplossingen.

1. Laat IPv6 multicast pakketten vallen door de volgende configuratie te gebruiken.

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

2. Richt IPv6 multicast verkeer op een ongebruikte of admin shutdown interface (Gi1/22 in dit voorbeeld).

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

3. Gebruik VLAN Access Control List (VACL) om IPv6-multicast verkeer te verwijderen.

```
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. Schakel IPv6 MLD-snooping uit.

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

5. Drop IPv6 Multicastverkeer met behulp van controle-instantie (CoPP)

```
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. Gebruik stormcontrole op ingangsiinterfaces. stormcontrole controleert inkomend verkeer over een interval van 1 seconde en tijdens dit interval vergelijkt het verkeersniveau met het geconfigureerde stormcontroleneniveau. Het niveau van de verkeersonweerscontrole is een percentage van de totale beschikbare bandbreedte van de haven. Elke haven heeft één enkel verkeersnormcontroleneniveau dat voor alle types van verkeer (uitzending, multicast, en unicast) wordt gebruikt.

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

7. Als de CPU op SP (Switch Processor) hoog is, volgt u de onderstaande instructies.

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

Als u de reden niet kunt bepalen op basis van de informatie in dit document, opent u een TAC-serviceaanvraag om verder te onderzoeken.