Hohe CPU-Auslastung bei Catalyst Switches aufgrund von IPv6-Multicast-Datenverkehr

Inhalt

Einführung

In diesem Dokument wird die hohe CPU-Auslastung auf verschiedenen Catalyst-Plattformen durch die Überflutung mit IPV6 Multicast Listener Discovery-Paketen und Möglichkeiten zur Behebung dieses Problems beschrieben.

Voraussetzungen

Es gibt keine Voraussetzungen.

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

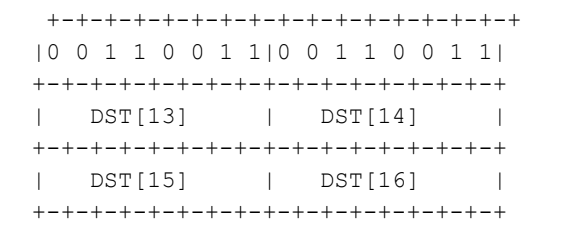
Die Informationen in diesem Dokument basieren auf Cisco Catalyst Switches der Serie 6500, Catalyst Switches der Serie 4500 und Catalyst Switches der Serie 3850.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen.

Problem

Bei einigen Cisco Catalyst-Plattformen ist eine hohe CPU-Auslastung zu beobachten, da IPv6-Multicast-Datenverkehr mit MAC-Adressen im Bereich 333.xxxx.xxxx auf die CPU abgestraft wird.

Gemäß RFC7042 werden alle MAC-48-Multicast-Identifikatoren mit dem Präfix "33-33" (d. h. die 2**32 Multicast-MAC-Identifikatoren im Bereich von 33-33-00-00-00 bis 33-33-FF-FF-FF-FF-FF-FF) verwendet. wie in [RFC2464] für IPv6-Multicast festgelegt. Ein IPv6-Paket mit einer Multicast-Zieladresse DST, bestehend aus den 16 Oktetten DST[1] bis DST[16], wird an die Ethernet-Multicast-Adresse übertragen, deren erste beiden Oktette der Wert 333 hexadezimal sind und deren letzte vier Oktette die letzten vier Oktette von DST sind, wie in Abbildung 1 gezeigt.



(Figure 1: Address Mapping - Multicast)

Es wurde gelegentlich festgestellt, dass Hosts, die Geräte mit einer bestimmten NIC-Karte in den Ruhemodus wechseln, IPv6-Multicast-Datenverkehr überfluten. Dieses Problem ist nicht auf einen bestimmten Host-Anbieter beschränkt, aber es wurde festgestellt, dass bestimmte Chipsätze dieses Verhalten häufiger aufweisen als andere.

Fehlerbehebung und Lösung

Mithilfe der folgenden Verfahren können Sie herausfinden, ob der Catalyst Switch eine hohe CPU-Auslastung durch dieses Problem beeinträchtigt, und die entsprechenden Lösungen implementieren.

Catalyst Switches der Serie 3850

Auf Catalyst 3850-Switches verwendet der NGWC L2M-Prozess CPU zur Verarbeitung von IPv6-Paketen. Wenn das Multicast Listener Discovery (MLD)-Snooping auf dem Switch deaktiviert ist, wird das MLD-Join-/Leave-Paket an alle Mitglieds-Ports geleitet. Und wenn es viele eingehende MLD-Join-/Late-Pakete gibt, verbraucht dieser Prozess mehr CPU-Zyklen, um die Pakete auf allen Mitglieds-Ports zu senden. Es wurde festgestellt, dass bestimmte Host-Systeme, die in den Ruhemodus wechseln, möglicherweise mehrere Tausend Pakete/s IGMPv6-MLD-Datenverkehr senden.

```
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           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
```

Lösung

Konfigurieren Sie **ipv6 mld Snooping** auf den betroffenen Switches, um **ipv6 mld Snooping** global zu aktivieren. Dadurch sollte die CPU-Auslastung verringert werden.

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

Wenn MLD-Snooping aktiviert ist, wird eine IPv6-Multicast-Adresstabelle pro VLAN in Software und Hardware erstellt. Der Switch führt dann ein hardwarebasiertes Bridging auf Basis der IPv6-Multicast-Adresse durch, wodurch die Verarbeitung dieser Pakete durch die Software verhindert wird.

Klicken Sie auf den Link, um weitere Informationen zur Konfiguration von MLD Snooping zu erhalten.

Bei früheren Versionen von IOS XE wurde festgestellt, dass die CPU-Warteschlange aufgrund dieses Problems blockiert werden konnte, wodurch alle Steuerungspakete in dieser Warteschlange nicht an die CPU weitergeleitet werden konnten. Dies wurde durch CSCuo14829 in IOS-Versionen 3.3.3 und 3.6.0 und höher behoben. Weitere Informationen finden Sie in diesem Bug.

Catalyst Switches der Serie 4500

Catalyst Switches der Serie 4500 unterstützen die Hardware-Weiterleitung von IPv6-Multicast-Datenverkehr mithilfe von Ternary Content Addressable Memory (TCAM). Dies wird in Multicast auf Cisco Catalyst Switches der Serien 4500E und 4500X erläutert.

Beim IPv6 Multicast Listener Discovery-Datenverkehr muss der Switch die Software-Weiterleitung (mithilfe von CPU-Ressourcen) durchführen. Wie unter Konfigurieren von IPv6 MLD Snooping auf Catalyst 4500-Switches erläutert, kann MLD-Snooping global oder pro VLAN aktiviert oder deaktiviert werden. Wenn MLD-Snooping aktiviert ist, wird eine IPv6-Multicast-MAC-Adresstabelle für VLANs in der Software erstellt und eine IPv6-Multicast-Adresstabelle für VLANs in der Software und Hardware erstellt. Der Switch führt dann ein hardwarebasiertes Bridging auf Basis der IPv6-Multicast-Adresse durch. Dies ist das erwartete Verhalten für Switches der Catalyst Serie 4500.

Um die Art des Pakets zu überprüfen, das auf die CPU angewendet wird, können wir den Befehl **"Debug-Plattform-Paket-Gesamt-Puffer"** gefolgt vom Befehl "**show plattform cpu paket gepuffert**" ausführen.

```
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
```

Dieses Paket kam von der MAC-Quelladresse 44:39:C4:39:5A:4A auf der Schnittstelle Tengigabitethernet1/15 für VLAN 214 an. Protokoll 0x86DD ist IPv6 und Dst MAC 33:33:FF:7F:EB:DB wird in diesem Fall für Multicast-IPv6-MLD-Knoten verwendet.

Lösung

Wir haben zwei Optionen, um eine hohe CPU-Auslastung aufgrund dieses Datenverkehrs zu reparieren.

1. Deaktivieren Sie die Generierung von IPv6 Multicast Listener Discovery-Datenverkehr auf dem End-Host. Dies kann durch ein Upgrade der NIC-Treiber oder die Deaktivierung der Funktion von Hosts, die IPv6-Pakete senden, im BIOS erfolgen. Sie können sich an den Anbieter Ihres Client-Computers wenden, der Ihnen bei der Deaktivierung der Funktionen im BIOS oder beim Upgrade der Netzwerkkartentreiber helfen kann.

2. Aktivieren Sie Control Plane Policing (CoPP), um die übermäßige Menge an IPv6-Multicast-Listener-Erkennungsverkehr, der an die CPU geleitet wird, zu verwerfen. Diese Pakete sind Hop-Limit für eine lokale Verbindung. Daher wird erwartet, dass diese Pakete an die CPU übergeben werden.

```
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
```

Im obigen Beispiel beschränken wir die Menge des IPv6-Datenverkehrs, der von der CPU verarbeitet wird, auf 3.200 Pakete pro Sekunde.

Catalyst Switches der Serie 6500

Catalyst Switches der Serie 6500 treffen Entscheidungen zur Weiterleitung in der Hardware mithilfe von TCAM, der normalerweise keine CPU-Unterstützung benötigt, solange TCAM über einen Weiterleitungseintrag verfügt.

Das Supervisor Enginet 720 auf Catalyst 6500-Switches verfügt über zwei CPUs. Eine CPU ist der Network Management Processor (NMP) oder der Switch Processor (SP). Die andere CPU ist die Layer-3-CPU, die als Route Processor (RP) bezeichnet wird.

Die CPU-Auslastung für Prozess und Interrupt wird im Befehl **show process cpu** aufgelistet. Wie unten gezeigt, hoch CPUs, die durch Interrupts verursacht werden, basieren hauptsächlich auf Datenverkehr. Interrupt Switched Traffic ist ein Datenverkehr, der nicht mit einem bestimmten Prozess übereinstimmt, aber trotzdem weitergeleitet werden muss. Das folgende Beispiel zeigt

einen Catalyst Switch der Serie 6500, der aufgrund von Interrupts eine hohe CPU-Auslastung auf RP aufweist.

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

Überprüfen Sie, ob eine Schnittstelle oder ein Layer-3-VLAN hohe Datenverkehrsmengen verwirft. (Eingabewarteschlange wird verworfen). Wenn dies der Fall ist, wird der Datenverkehr von diesem VLAN an den RP geleitet.

```
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
```

Der folgende Befehl kann verwendet werden, um alle Pakete im Puffer der Eingabewarteschlange für das Schnittstellen-VLAN 19 zu suchen.

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

Alternativ können Sie die NetDR-Erfassung verwenden, um Datenverkehr zu CPU auf einem Catalyst 6500-Switch zu erfassen. In diesem Dokument wird erläutert, wie mithilfe der NetDR-Erfassung erfasste Pakete interpretiert werden.

```
------- 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
```

Lösung

Verwenden Sie eine oder mehrere der folgenden Lösungen.

1. Löschen von IPv6-Multicast-Paketen mithilfe der folgenden Konfiguration:

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

2. Umleitung des IPv6-Multicast-Datenverkehrs an eine nicht verwendete oder Admin-Shutdown-Schnittstelle (in diesem Beispiel Gi1/22).

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

3. Verwenden Sie die VLAN Access Control List (VACL), um IPv6-Multicast-Datenverkehr zu verwerfen.

```
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. Deaktivieren Sie IPv6 MLD Snooping.

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

5. IPv6-Multicast-Datenverkehr mithilfe von CoPP (Control Plane Policing) verwerfen

```
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. Verwenden Sie Sturmkontrolle an Eingangsschnittstellen. Die Sturmkontrolle überwacht den eingehenden Datenverkehr in einem Intervall von 1 Sekunde und vergleicht in diesem Intervall die Datenverkehrsebene mit der konfigurierten Sturmkontrolle. Die Traffic Storm Control Level ist ein Prozentsatz der gesamten verfügbaren Bandbreite des Ports. Jeder Port verfügt über eine einzelne Datenverkehrs-Storm-Control-Ebene, die für alle Arten von Datenverkehr (Broadcast, Multicast und Unicast) verwendet wird.

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

7. Falls CPU High on SP (Switch Processor) ist, wenden Sie unten eine Problemumgehung an.

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

Wenn Sie auf der Grundlage der Informationen in diesem Dokument den Grund nicht ermitteln können, öffnen Sie bitte eine TAC-Serviceanfrage, um weitere Informationen zu erhalten.