Utilisation élevée du CPU sur les commutateurs Catalyst en raison du trafic de multidiffusion IPv6

Contenu

Introduction

Ce document décrit l'utilisation élevée du CPU sur différentes plates-formes Catalyst en raison de l'inondation de paquets de détection de l'écouteur multidiffusion IPV6 et des moyens d'atténuer ce problème.

Conditions préalables

Il n'y a aucune condition préalable.

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

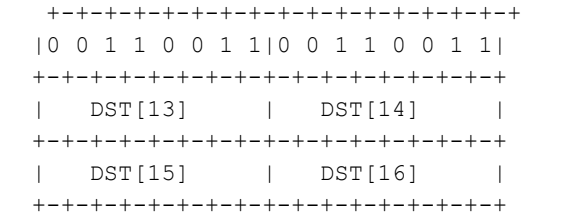
Les informations de ce document sont basées sur les commutateurs de la gamme Cisco Catalyst 6500, Catalyst 4500 et Catalyst 3850.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration.

Problème

L'utilisation élevée du CPU peut être vue sur certaines plates-formes Cisco Catalyst en raison du trafic de multidiffusion IPv6 dont l'adresse MAC se situe dans la plage 3333.xxxx.xxxx et qui est transmis au CPU.

Conformément à la RFC7042, tous les identificateurs de multidiffusion MAC-48 prédéfinis « 33-33 » (c'est-à-dire les identificateurs MAC de multidiffusion 2**32 dans la plage de 33-33-00-00-00 à 33-33-FF-FF-FF-FF) sont utilisés comme spécifié dans [RFC2464] pour la multidiffusion IPv6. Un paquet IPv6 avec une adresse de destination de multidiffusion DST, composée des seize octets DST[1] à DST[16], est transmis à l'adresse de multidiffusion Ethernet dont les deux premiers octets sont la valeur hexadécimale 333 et dont les quatre derniers octets sont les quatre derniers octets de DST, comme illustré à la Figure 1.



(Figure 1: Address Mapping - Multicast)

Il a été constaté à certaines occasions que lorsque des périphériques hôtes utilisant une certaine carte réseau passent en mode veille, ils inondent le trafic de multidiffusion IPv6. Ce problème ne se limite pas à un fournisseur d'hôte particulier, bien que certains chipsets aient été vus comme présentant ce comportement plus souvent que d'autres.

Dépannage et solution

Vous pouvez utiliser les procédures suivantes pour savoir si votre commutateur Catalyst qui voit une utilisation élevée du CPU est affecté par ce problème et implémenter les solutions correspondantes.

Commutateurs de la gamme Catalyst 3850

Sur les commutateurs Catalyst 3850, NGWC L2M Process utilise le CPU pour traiter les paquets IPv6. Lorsque la surveillance MLD (Multicast Listener Discovery) est désactivée sur le commutateur, le paquet de jonction/sortie MLD est diffusé à tous les ports membres. Et, s'il y a beaucoup de paquets entrants de jonction/sortie MLD, ce processus consommera plus de cycles CPU pour envoyer les paquets sur tous les ports membres. Il a été constaté que lorsque certaines machines hôtes passent en mode veille, elles peuvent envoyer plusieurs milliers de paquets/s de trafic IGMPv6 MLD.

```
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
```

Solution

Configurez **ipv6 mld snooping** sur les commutateurs concernés pour activer globalement **ipv6 mld snooping**. Cela devrait réduire l'utilisation du processeur.

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

Lorsque la surveillance MLD est activée, une table d'adresses de multidiffusion IPv6 par VLAN est créée dans le logiciel et le matériel. Le commutateur effectue ensuite un pontage IPv6 basé sur les adresses de multidiffusion dans le matériel, ce qui empêche le traitement de ces paquets par le logiciel.

Cliquez sur le lien pour plus d'informations sur la configuration de la surveillance MLD

Sur les versions antérieures d'IOS XE, il a été constaté que la file d'attente du processeur pouvait être bloquée en raison de ce problème qui empêcherait tous les paquets de contrôle de cette file d'attente d'accéder au processeur. Ceci a été corrigé via CSCuo14829 dans IOS versions 3.3.3 et 3.6.0 et ultérieures. Veuillez consulter ce bogue pour plus de détails.

Commutateurs de la gamme Catalyst 4500

Les commutateurs de la gamme Catalyst 4500 prennent en charge le transfert matériel du trafic de multidiffusion IPv6 à l'aide de la mémoire TCAM (Ternary Content Addressable Memory). Ceci est expliqué dans Multicast sur les commutateurs Cisco Catalyst 4500E et 4500X

Lorsqu'il s'agit du trafic de découverte de l'écouteur multidiffusion IPv6, le commutateur doit effectuer le transfert logiciel (en utilisant les ressources du processeur). Comme expliqué dans Configuration de la surveillance IPv6 MLD sur les commutateurs Catalyst 4500, la surveillance MLD peut être activée ou désactivée globalement ou par VLAN. Lorsque la surveillance MLD est activée, une table d'adresses MAC de multidiffusion IPv6 par VLAN est créée dans le logiciel et une table d'adresses de multidiffusion IPv6 par VLAN est construite dans le logiciel et le matériel. Le commutateur effectue ensuite un pontage IPv6 basé sur les adresses de multidiffusion dans le matériel. Voici le comportement attendu sur les commutateurs de la gamme Catalyst 4500.

Afin de vérifier le type de paquet qui est pointé sur le CPU, nous pouvons exécuter “ **paquet de plateforme de débogage tous les** ” de **tampon** suivi de “ **show platform cpu packet buffered** ”.

```
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
```

Ce paquet est arrivé sur l'interface Tengigabitethernet1/15 sur le VLAN 214 à partir de l'adresse MAC source 44:39:C4:39:5A:4A. Le protocole 0x86DD est IPv6 et Dst MAC 33:33:FF:7F:EB:DB est utilisé pour les noeuds MLD IPv6 multidiffusion dans ce cas.

Solution

Nous avons deux options pour corriger l'utilisation élevée du CPU en raison de ce trafic.

1. Désactivez la génération du trafic de découverte de l'écouteur multidiffusion IPv6 sur l'hôte final. Cela peut se faire en mettant à niveau les pilotes de carte réseau ou en désactivant la fonctionnalité du BIOS des hôtes qui envoient des paquets IPv6. Vous pouvez contacter le fournisseur de votre ordinateur client qui peut vous aider à désactiver la fonctionnalité du BIOS ou à mettre à niveau les pilotes de la carte réseau.
2. Activez la fonction CoPP (Control Plane Policing) afin d'abandonner la quantité excessive de trafic de découverte de l'écouteur multidiffusion IPv6 qui est pointé vers le processeur. Et, ces paquets sont la limite de saut d'une liaison locale, ainsi il est prévu que le comportement de ces paquets sera puni au 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
```

Dans l'exemple ci-dessus, nous limitons la quantité de trafic IPv6 qui est traitée par le processeur à 32 000 paquets par seconde.

Commutateurs de la gamme Catalyst 6500

Les commutateurs Catalyst 6500 prennent des décisions de transfert dans le matériel à l'aide de TCAM qui n'a normalement pas besoin d'assistance CPU tant que TCAM a l'entrée de transfert.

Supervisor Engine 720 sur les commutateurs Catalyst 6500 ont deux processeurs. Un processeur est le NMP (Network Management Processor) ou le SP (Switch Processor). L'autre processeur est le processeur de couche 3, appelé processeur de routage (RP).

L'utilisation du processeur de processus et d'interruption est répertoriée dans la commande **show process cpu**. Comme indiqué ci-dessous, Élevé Le processeur provoqué par les interruptions est principalement basé sur le trafic. Le trafic commuté d'interruption est un trafic qui ne correspond pas à un processus spécifique, mais qui doit encore être transféré. L'exemple suivant illustre un commutateur Catalyst 6500 dont l'utilisation du CPU sur le RP est élevée en raison d'interruptions.

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

Vérifiez si une interface ou un VLAN de couche 3 abandonne une grande quantité de trafic. (La file d'attente d'entrée est abandonnée). Si c'est le cas, le trafic peut être acheminé vers le RP à partir de ce 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
```

La commande suivante peut être utilisée pour rechercher tous les paquets dans la mémoire tampon de file d'attente d'entrée pour l'interface vlan 19.

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

Vous pouvez également utiliser la capture NetDR pour capturer le trafic allant au CPU sur un commutateur Catalyst 6500. Ce document explique comment interpréter les paquets capturés à l'aide de la capture NetDR.

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

Solution

Utilisez une ou plusieurs des solutions ci-dessous.

1. Supprimez les paquets de multidiffusion IPv6 en utilisant la configuration suivante.

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

2. Rediriger le trafic de multidiffusion IPv6 vers une interface inutilisée ou d'arrêt d'administration (Gi1/22 dans cet exemple).

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

3. Utilisez Vlan Access Control List (VACL) pour supprimer le trafic de multidiffusion IPv6.

```
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. Désactivez la surveillance IPv6 MLD.

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

5. Déposer le trafic de multidiffusion IPv6 à l'aide de Control Plane Policing (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. Utilisez le contrôle de tempête sur les interfaces d'entrée. le contrôle des tempêtes surveille les niveaux de trafic entrants sur un intervalle d'une seconde et, au cours de cet intervalle, il compare le niveau de trafic au niveau configuré de contrôle des tempêtes de trafic. Le niveau de contrôle des tempêtes de trafic est un pourcentage de la bande passante totale disponible du port. Chaque port a un niveau de contrôle de tempête de trafic unique qui est utilisé pour tous les types de trafic (diffusion, multidiffusion et monodiffusion).

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

7. Si le processeur est élevé sur le SP (processeur de commutation), appliquez la solution de contournement ci-dessous.

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

Si vous n'arrivez pas à déterminer la raison en fonction des informations fournies dans ce document, veuillez ouvrir une demande de service TAC pour approfondir votre enquête.