

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Problème](#)

[Dépannage et solution](#)

[Commutateurs de gamme Catalyst 3850](#)

[Solution](#)

[Commutateurs de la gamme Catalyst 4500](#)

[Solution](#)

[Commutateurs de gamme Catalyst 6500](#)

[Solution](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit l'utilisation du CPU élevé sur de diverses plates-formes Catalyst dues à l'inondation des paquets et des manières de détection d'auditeur de Multidiffusion IPv6 d'atténuer ce problème.

Conditions préalables

Il n'y a aucune condition préalable.

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut).

Problème

L'utilisation du CPU élevé peut être vue sur quelques Plateformes de Cisco Catalyst dues au trafic de Multidiffusion IPv6 avec l'adresse MAC dans la plage 3333.xxxx.xxxx étant donnée un coup de

volée à la CPU.

Selon RFC7042, tous les identifiants de la Multidiffusion MAC-48 ont préfixé "33-33" (c'est-à-dire, les identifiants de MAC multicast $2^{**}32$ dans la plage de 33-33-00-00-00-00 à 33-33-FF-FF-FF-FF) sont utilisés comme spécifié dans [RFC2464] pour la Multidiffusion IPv6. Un paquet d'IPv6 avec une adresse de destination multicast DST, comprenant les seize octets DST[1] par DST[16], est transmis à l'adresse de multidiffusion d'Ethernets dont les deux premiers octets sont la valeur 3333 hexadécimale et dont les quatre derniers octets sont les quatre derniers octets de DST suivant les indications de figure 1.

On l'a vu à quelques occasions que quand les périphériques d'hôtes utilisant une certaine carte NIC vont au mode de sommeil, ils inondent le trafic de Multidiffusion IPv6. Cette question n'est pas limitée à un constructeur d'hôte spécifique, bien que certains jeux de puces aient été vus pour montrer ce comportement plus souvent que d'autres.

Dépannage et solution

Vous pouvez employer des procédures suivantes pour découvrir si votre commutateur de Catalyst voyant l'utilisation du CPU élevé est affecté par ce problème, et des solutions respectives de mise en place.

Commutateurs de gamme Catalyst 3850

Sur des Commutateurs du Catalyst 3850, le processus NGWC L2M utilise la CPU pour traiter des paquets d'IPv6. Quand Multicast Listener Discovery (MLD) pillant est désactivé sur le commutateur, MLD se joignent/paquet de congé sont inondés à tous les ports membres. Et, s'il y a beaucoup de MLD entrants se joignent/paquets de congé, ce processus consomment plus de cycles CPU pour envoyer les paquets sur tous les ports membres. On l'a vu que quand certains ordinateurs hôte vont au mode de sommeil, ils peuvent envoyer plusieurs milliers de paquets/sec du 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 l'**ipv6 mld snooping** sur les Commutateurs affectés pour activer globalement l'**ipv6 mld snooping**. Ceci devrait diminuer en bas de 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
```

Quand piller MLD est activé, une table d'adresse de la Multidiffusion IPv6 par-VLAN est construite

dans le logiciel et le matériel. Le commutateur exécute alors la transition basée par adresse de multidiffusion d'IPv6 dans le matériel, qui empêche ces paquets à traiter par le logiciel.

Cliquez sur en fonction le lien pour plus d'informations sur [configurer piller MLD](#)

Sur des versions antérieures d'IOS XE, on l'a constaté que la file d'attente CPU pourrait être bloqué en raison de ce problème qui arrêterait tous les paquets de contrôle dans cette file d'attente d'aller à la CPU. Ceci a été réparé par [CSCuo14829](#) dans les versions IOS 3.3.3 et 3.6.0 et plus tard. Veuillez se référer cette bogue pour des détails.

Commutateurs de la gamme Catalyst 4500

Expédition de matériel de support de Commutateurs de gamme Catalyst 4500 du trafic de Multidiffusion IPv6 utilisant la mémoire associative ternaire (TCAM). Ceci est expliqué dans la [Multidiffusion des Commutateurs sur de Cisco Catalyst gamme 4500E et 4500X](#)

Quand il s'agit de trafic de détection d'auditeur de Multidiffusion IPv6, commutateur doit exécuter l'expédition de logiciel (utilisant des ressources CPU). Comme expliqué [en configurant l'ipv6 mld snooping sur](#) piller des [Commutateurs](#) MLD du [Catalyst 4500](#) peut être activé ou désactivé globalement ou par VLAN. Quand piller MLD est activé, une table d'adresse MAC de la Multidiffusion IPv6 par-VLAN est construite en logiciel et une table d'adresse de la Multidiffusion IPv6 par-VLAN est construite dans le logiciel et le matériel. Le commutateur exécute alors la transition basée par adresse de multidiffusion d'IPv6 dans le matériel. C'est le comportement prévu sur des Commutateurs de gamme Catalyst 4500.

Afin de vérifier le type de paquet étant donné un coup de volée à la CPU que nous pouvons exécuter ? **mettez au point le paquet de plate-forme toute la mémoire tampon ?** suivi de ? **paquet CPU de show platform mis en mémoire tampon ?** commande.

```
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
```

Ce paquet est arrivé sur l'interface TENGIGABITETHERNET1/15 sur le VLAN 214 du MAC address 44:39:C4:39:5A:4A de source. Protocol 0x86DD est IPv6 et le MAC 33:33:FF:7F:EB:DB de Dst est utilisé pour des Nœuds de l'IPv6 MLD de Multidiffusion dans ce cas.

Solution

Nous avons deux options de réparer l'utilisation du CPU élevé due à ce trafic.

1. Génération de débordement du trafic de détection d'auditeur de Multidiffusion IPv6 sur l'hôte d'extrémité. Ceci peut être fait en améliorant des pilotes de carte NIC ou en désactivant la

caractéristique sur le BIOS des hôtes envoyant des paquets d'IPv6. Vous pouvez contacter le constructeur de votre machine cliente qui peut aider à désactiver la configuration sur le BIOS ou à améliorer des pilotes de carte NIC.

1. Réglementation du plan de commande d'enable (CoPP) afin de relâcher la quantité excessive du trafic de détection d'auditeur de Multidiffusion IPv6 qui est donné un coup de volée à la CPU. Et, ces paquets sont limite de saut d'un gens du pays de lien, ainsi il est comportement prévu que ces paquets seront donnés un coup de volée à la 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: Tel1/15
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
```

Dans l'exemple ci-dessus, nous limitons la quantité du trafic d'IPv6 qui est traité par la CPU à 32000 paquets par seconde.

Commutateurs de gamme Catalyst 6500

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

Le superviseur Enginet 720 sur des Commutateurs de Catalyst 6500 ont deux CPU. Une CPU est le processeur de gestion de réseau (NMP) ou le processeur de commutateur (fournisseur de services). L'autre CPU est la CPU de la couche 3, qui s'appelle le processeur d'artère (RP).

L'utilisation du processeur de processus et d'interruption sont répertoriées dans la commande **CPU de processus d'exposition**. Comme affiché ci-dessous, la CPU de haute provoquée par des interruptions sont en grande partie le trafic basé. Le trafic commuté par interruption, est le trafic qui n'apparie pas un processus spécifique, mais toujours les besoins d'être expédié. L'exemple suivant affiche un commutateur de Catalyst 6500 ayant l'utilisation du CPU élevé sur le RP dû aux interruptions.

```
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: Tel1/15
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
```

Vérifiez si n'importe quel VLAN d'interface ou de couche 3 relâche la grande quantité de trafic. (Pertes de file d'attente d'entrée). Si oui, le trafic peut obtenir a donné un coup de volée au RP 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 trouver tous les paquets dans la mémoire tampon de file d'attente d'entrée pour l'interface vlan 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
```

Alternativement, vous pouvez utiliser la capture de NetDR pour capturer le trafic allant à la CPU sur un commutateur de Catalyst 6500. [Ce document](#) explique comment interpréter des paquets capturés utilisant la capture de NetDR.

```
----- dump of incoming inband packet -----interface Vl16, routine
mistral_process_rx_packet_inlin, timestamp 03:17:56.380dbus info: src_vlan 0x10(16), src_idx
0x1001(4097), len 0x5A(90) bpdn 0, index_dir 0, flood 1, dont_lrn 0, dest_idx 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
```

Solution

Utilisez un ou plusieurs de solutions ci-dessous.

1. Paquets de Multidiffusion IPv6 de baisse à l'aide de configuration suivante.

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

1. Réorientez le trafic de Multidiffusion IPv6 à une interface inutilisée ou d'admin d'arrêt (Gi1/22 dans cet exemple).

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

1. Liste de contrôle d'accès de VLAN d'utilisation (VACL) pour relâcher le trafic de Multidiffusion IPv6.

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

1. Ipv6 mld snooping de débranchement.

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

1. Le trafic de Multidiffusion IPv6 de baisse utilisant la Réglementation du plan de commande (CoPP)

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

1. Storm-control d'utilisation sur des interfaces d'entrée. le trafic entrant de moniteurs de storm-control nivelle pendant un 1 seconde intervalle et pendant cet intervalle il compare le niveau du trafic au storm-control level configuré du trafic. Le storm-control level du trafic est un

pourcentage de toute la bande passante disponible du port. Chaque port a un storm-control level simple du trafic qui est utilisé pour tous les types de trafic (émission, Multidiffusion, et unicast).

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

7. Au cas où si la CPU est élevée sur le fournisseur de services (processeur de commutateur), appliqueriez le contournement ci-dessous.

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

Si vous ne pouvez pas déterminer la raison basée sur des informations fournies dans ce document, ouvrez s'il vous plaît une demande de services TAC d'étudier plus plus loin.