Contenu

[Informations connexes](#)

Introduction

Ce document décrit les causes d'utilisation élevée de la CPU sur les commutateurs de la gamme Cisco Catalyst 6500/6000 et les systèmes basés sur le système de commutation virtuelle (VSS) 1440. Comme les routeurs Cisco, les commutateurs utilisent la commande **show processes cpu** pour afficher l'utilisation de la CPU pour le processeur de commutation du Supervisor Engine. Cependant, en raison des différences en matière d'architecture et de mécanismes de transmission entre les commutateurs et les routeurs Cisco, le résultat type de la commande **show processes cpu** diffère considérablement. La signification de la sortie diffère aussi bien. Ce document clarifie ces différences et décrit l'utilisation du processeur sur les Commutateurs et comment interpréter la sortie de commande de **show processes cpu**.

Remarque: Dans ce document, les mots « commutateur » et « commutateurs » font référence aux commutateurs Catalyst 6500/6000.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations de ce document sont basées sur les versions logicielles et matérielles pour les commutateurs Catalyst 6500/6000 et les systèmes basés sur le Système de commutation virtuelle (VSS) 1440.

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). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Remarque: Le logiciel pris en charge pour le Système de commutation virtuelle (VSS) 1440 systèmes basés est version de logiciel 12.2(33)SXH1 ou ultérieures de Cisco IOS®.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Différence entre CatOS et la plate-forme logicielle Cisco IOS

Catalyst OS (CatOS) sur le Supervisor Engine et le logiciel Cisco IOS® sur la carte de commutation multicouche (MSFC) (hybride) : Vous pouvez utiliser une image CatOS comme plate-forme logicielle pour exécuter le Supervisor Engine sur les commutateurs Catalyst 6500/6000. Si la MSFC facultative est installée, une image de logiciel Cisco IOS distincte est utilisée pour exécuter la MSFC.

Logiciel Cisco IOS sur le moteur de superviseur et la MSFC (natif) : Vous pouvez utiliser une seule image logicielle Cisco IOS comme plate-forme logicielle pour exécuter à la fois le Supervisor Engine et la MSFC sur les commutateurs Catalyst 6500/6000.

Remarque: Pour plus d'informations, reportez-vous à Comparaison des systèmes d'exploitation Cisco Catalyst et Cisco IOS pour le commutateur de la gamme Cisco Catalyst 6500.

Comprendre l'utilisation de la CPU sur les commutateurs Catalyst 6500/6000

Les routeurs basés sur un logiciel Cisco utilisent le logiciel afin de traiter et acheminer des paquets. L'utilisation de la CPU sur un routeur Cisco tend à augmenter lorsque le routeur effectue davantage de traitement et d'acheminement de paquets. Par conséquent, la commande **show processes cpu** peut fournir une indication assez précise de la charge du traitement du trafic du routeur.

Les commutateurs Catalyst 6500/6000 n'utilisent pas la CPU de la même manière. Ces commutateurs prennent des décisions de transfert dans le matériel, pas dans le logiciel. Par conséquent, quand les commutateurs prennent une décision de transfert ou de commutation pour la plupart des trames qui traversent le commutateur, le processus n'implique pas la CPU du Supervisor Engine.

Les commutateurs Catalyst 6500/6000 comprennent deux CPU. Une CPU est la CPU du Supervisor Engine, qui est appelée le processeur de gestion du réseau (NMP) ou le processeur du commutateur (SP). L'autre CPU est la CPU du moteur de routage de la couche 3, qui est appelée la MSFC ou le processeur de routage (RP).

La CPU du SP remplit entre autres les fonctions suivantes :

- Aide au vieillissement et à l'apprentissage d'adresses MAC**Remarque:** L'apprentissage d'adresses MAC est également appelé configuration de chemin.
- Exécute des protocoles et des processus qui fournissent le contrôle du réseauLes exemples incluent le protocole Spanning Tree (STP), le Cisco Discovery Protocol (CDP), le protocole de jonction VLAN (VTP), le Dynamic Trunking Protocol (DTP) et le protocole d'agrégation de ports (PAgP).
- Traite le trafic de gestion du réseau qui est destiné à la CPU du commutateurDes exemples incluent le trafic telnet, le trafic HTTP et le trafic du protocole SNMP (Simple Network Management Protocol).

La CPU du RP remplit entre autres les fonctions suivantes :

- Crée et met à jour le routage de la couche 3 et les tables du protocole de résolution d'adresse (ARP)
- Génère la base d'informations de transfert (FIB) Cisco Express Forwarding (CEF) et des tables de juxtaposition, et télécharge les tables dans la carte de fonctionnalité de politique (PFC)
- Traite le trafic de gestion du réseau qui est destiné au RPDes exemples incluent le trafic Telnet, HTTP et SNMP.

Situations et fonctionnalités qui déclenchent le routage du trafic

vers le logiciel

Paquets qui sont destinés au commutateur

Tout paquet qui est destiné au commutateur va au logiciel. De tels paquets incluent :

- Paquets de contrôleDes paquets de contrôle sont reçus pour le STP, le CDP, le VTP, le protocole HSRP (Hot Standby Router Protocol), le PAgP, le protocole de contrôle d'agrégation de liaisons (LACP) et le protocole UDLD (UniDirectional Link Detection).
- Mises à jour du protocole de routageDes exemples de ces protocoles sont le protocole d'informations de routage (RIP), le Enhanced Interior Gateway Routing Protocol (EIGRP), le protocole BGP (Border Gateway Protocol) et le protocole OSPF (Open Shortest Path First).
- Trafic SNMP destiné au commutateur
- Le telnet et le Secure Shell Protocol (SSH) trafiquent au commutateur.L'ultilization élevé CPU dû au SSH est vu en tant que :Incluez ces commandes dans le script EEM afin de vérifier le nombre de sessions de SSH établies quand la CPU passe à 1 :affichez les utilisateursshow line
- Réponses ARP aux requêtes ARP

Paquets et conditions qui requièrent un traitement spécial

Cette liste fournit des types de paquets et des conditions spécifiques qui forcent la prise en charge des paquets dans le logiciel :

- Paquets avec des options IP, un temps de vie (TTL) expiré ou une encapsulation non-ARPA (Advanced Research Projects Agency)
- Paquets avec traitement spécial, tel que la transmission tunnel
- Fragmentation IP
- Paquets qui requièrent des messages du protocole ICMP (Internet Control Message Protocol) du RP ou du SP
- Panne de contrôle de l'unité de transmission maximale (MTU)
- Paquets avec les erreurs d'IP, qui incluent des erreurs de somme de contrôle et de longueur d'IP
- Si les paquets en entrée renvoient une erreur de bits (telle que l'erreur à bit unique (SBE)), les paquets sont envoyés à la CPU pour traitement logiciel et sont corrigés. Le système alloue une mémoire tampon pour eux et utilise la ressource CPU pour la corriger.
- Quand un PBR et une liste d'accès réflexive sont dans le chemin d'un flux de trafic, le paquet est commuté par logiciel, ce qui requiert un cycle de CPU supplémentaire.
- Juxtaposition de la même interface
- Paquets qui échouent le contrôle du Reverse Path Forwarding (RPF) ? **RPF-panne**
- Glaner/recevoirGlaner fait référence aux paquets qui requièrent une résolution ARP et recevoir fait référence aux paquets qui tombent dans le cas de réception.
- Le trafic du protocole IPX (Internetwork Packet Exchange) qui est commuté par logiciel sur le Supervisor Engine 720 dans le logiciel Cisco IOS et CatOSLe trafic IPX est également commuté par logiciel sur le Supervisor Engine 2/logiciel Cisco IOS, mais le trafic est commuté par matériel sur le Supervisor Engine 2/CatOS. Le trafic IPX est commuté par matériel sur le Supervisor Engine 1A pour les deux systèmes d'exploitation.

- Trafic AppleTalk
- Conditions complètes des ressources matériellesCes ressources incluent la FIB, la mémoire de contenu adressable (CAM) et la CAM ternaire (TCAM).

Fonctionnalités basées sur l'ACL

- Trafic refusé par la liste de contrôle d'accès (ACL) avec la fonctionnalité d'ICMP inaccessibles activée**Remarque:** Il s'agit de la configuration par défaut.Certains paquets refusés par l'ACL sont intégrés au MSFC si les IP inaccessibles sont activées. Les paquets qui requièrent des ICMP inaccessibles sont intégrés à un débit configurable par l'utilisateur. Par défaut, le débit est de 500 paquets par seconde (PPS).
- Filtrage IPX sur la base de paramètres non pris en charge, tels que l'hôte sourceSur le Supervisor Engine 720, le processus du trafic IPX de la couche 3 est toujours dans le logiciel.
- Entrées de contrôle d'accès (ACE) qui requièrent une journalisation, avec le **mot-clé de journal**Cela s'applique aux fonctionnalités de journal de l'ACL et de journal de la VLAN ACL (VACL). Les ACE dans la même ACL qui ne requièrent pas de journalisation sont toujours traitées dans le matériel. Le Supervisor Engine 720 avec PFC3 prend en charge la limite de débit de paquets qui sont redirigés vers le MSFC pour la journalisation de l'ACL et la VACL. Le Supervisor Engine 2 support la limite de débit de paquets qui sont redirigés vers le MSFC pour la journalisation de la VACL. La prise en charge de la journalisation de l'ACL sur le Supervisor Engine 2 est planifiée pour le logiciel Cisco IOS version 12.2S.
- Trafic routé par une politique, avec l'utilisation de **match length**, **set ip precedence** ou d'autres paramètres non pris en chargeLe paramètre de **set interface** est pris en charge par le logiciel. Cependant, le paramètre **set interface null 0** est une exception. Ce trafic est traité dans le matériel sur le Supervisor Engine 2 avec PFC2 et le Supervisor Engine 720 avec PFC3.
- ACL de routeur (RACL) non-IP et non-IPXLes RACL non-IP s'appliquent à tous les Supervisor Engines. Les RACL non-IPX s'appliquent au Supervisor Engine 1a avec PFC et au Supervisor Engine 2 avec PFC2 seulement.
- Trafic de diffusion qui est refusé dans une RACL
- Trafic qui est refusé dans un contrôle Unicast RPF (uRPF), ACE d'ACLCe contrôle uRPF s'applique au Supervisor Engine 2 avec PFC2 et au Supervisor Engine 720 avec PFC3.
- Proxy d'authentificationLe trafic qui est sujet au proxy d'authentification peut être limité en débit sur le Supervisor Engine 720.
- Sécurité IP (IPsec) du logiciel Cisco IOSLe trafic qui est sujet au cryptage Cisco IOS peut être limité en débit sur le Supervisor Engine 720.

Fonctionnalités basées sur Netflow

Les fonctionnalités basées sur Netflow que cette section décrit s'appliquent au Supervisor Engine 2 et au Supervisor Engine 720 seulement.

- Les fonctionnalités basées sur Netflow doivent toujours avoir le premier paquet d'un flux dans le logiciel. Une fois que le premier paquet du flux atteint le logiciel, les paquets suivants du même sont commutés par matériel.Cette configuration du flux s'applique aux listes de contrôle d'accès réflexives, au protocole WCCP (Web Cache Communication Protocol) et à l'Équilibrage de charge de serveur (SLB) Cisco IOS.**Remarque:** Sur le Supervisor Engine 1, les listes de contrôle d'accès réflexives se fondent sur les entrées dynamiques TCAM pour créer des raccourcis matériels pour un flux particulier. Le principe est identique : le premier

paquet d'un flux va au logiciel. Les paquets suivants de ce flux sont commutés par matériel.
- Avec la configuration d'interception TCP, la connexion à trois et la fin de la session sont gérées dans le logiciel. Le reste du trafic est traité dans le matériel.**Remarque:** Les paquets Synchronize (SYN), SYN acknowledge (SYN ACK) et ACK incluent la connexion à trois. La fin de session se produit avec la finition (FIN) ou la réinitialisation (RST).
- Avec la Traduction d'adresses de réseau (NAT), le trafic est traité de cette façon :Sur le Supervisor Engine 720 :Le trafic qui requiert une NAT est pris en charge dans le matériel après la traduction initiale. La traduction du premier paquet d'un flux se produit dans le logiciel et les paquets suivants de ce flux sont commutés par matériel. Pour les paquets TCP, un raccourci matériel est créé dans la table Netflow à la fin de la connexion TCP à trois.Sur le Supervisor Engine 2 et le Supervisor Engine 1 :Tout le trafic qui requiert une NAT est commuté par logiciel.
- Le contrôle d'accès basé sur contexte (CBAC) utilise des raccourcis Netflow afin de classer le trafic qui requiert une inspection. Ensuite, le CBAC envoie seulement ce trafic vers le logiciel. Le CBAC est une fonctionnalité réservée au logiciel ; le trafic qui est sujet à une inspection n'est pas commuté par matériel.**Remarque:** Le trafic qui est sujet à une inspection peut être limité en débit sur le Supervisor Engine 720.

trafic multidiffusion

- Surveillance PIM (Protocol Independent Multicast)
- Surveillance IGMP (Internet Group Management Protocol) (TTL = 1)Ce trafic est en fait destiné au routeur.
- Surveillance MLD (Multicast Listener Discovery) (TTL = 1)Ce trafic est en fait destiné au routeur.
- Manque FIB
- Paquets multicast pour l'enregistrement qui ont une connexion directe à la source multicastCes paquets multicast sont transmis par tunnel au point de rendez-vous.
- Multicast d'IP version 6 (IPv6)

Autres fonctionnalités

- Network-Based Application Recognition (NBAR)
- Inspection ARP, avec CatOS seulement
- Sécurité de port, avec CatOS seulement
- Surveillance DHCP

Situations IPv6

- Paquets avec un en-tête d'option saut-par-saut
- Paquets avec le même adresse IPv6 de destination que celle des routeurs
- Paquets qui échouent le contrôle d'application de portée
- Paquets qui dépassent la MTU du lien de résultat
- Paquets avec un TTL qui est inférieur ou égal à 1
- Paquets avec un VLAN d'entrée qui est égal au VLAN de résultat
- IPv6 uRPFLe logiciel exécute cet uRPF pour tous les paquets.
- Listes de contrôle d'accès réflexives IPv6Le logiciel traite ces listes de contrôle d'accès

réflexives.
- Les préfixes 6to4 pour les tunnels ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)Le logiciel prend en charge cette transmission tunnel. Tout autre trafic qui entre dans un tunnel ISATAP est commuté par matériel.

Programmateur LCP et module DFC

Dans une carte de transfert distribué (DFC), le processus programmateur lcp qui s'exécute sur une CPU élevée n'est pas un problème et ne pose aucun problème à l'opération. Le programmateur LCP fait partie du code de microprogramme. Sur tous les modules qui ne requièrent pas une carte DFC, le microprogramme s'exécute sur un processeur particulier appelé le processeur de carte de lignes (LCP). Ce processeur est utilisé pour programmer le matériel ASIC et pour communiquer au module de supervision central.

Quand le programmateur lcp est lancé, il se sert de toute le temps de traitement disponible. Mais quand un nouveau processus a besoin de temps de processeur, le programmateur lcp libère du temps de traitement pour le nouveau processus. Il n'y a aucune incidence sur les performances du système en ce qui concerne cette utilisation élevée de la CPU. Le processus saisit simplement tous les cycles CPU inutilisés, tant que aucun processus de priorité plus élevée ne les requiert.

```
DFC#show process cpuPID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process  22
0          1       0   0.00%  0.00%  0.00%    0 SCP ChilisLC Lis   23           0          1       0
0.00%  0.00%  0.00%    0 IPC RTTYC Messag   24           0          9       0   0.00%  0.00%  0.00%
0 ICC Slave LC Req   25           0          1       0   0.00%  0.00%  0.00%    0 ICC Async mcast
26           0          2       0   0.00%  0.00%  0.00%    0 RPC Sync           27           0
1       0   0.00%  0.00%  0.00%    0 RPC rpc-master     28           0          1       0   0.00%
0.00%  0.00%    0 Net Input          29           0          2       0   0.00%  0.00%  0.00%    0
Protocol Filteri   30           8        105     76   0.00%  0.00%  0.00%    0 Remote Console P
31          40       1530     26   0.00%  0.00%  0.00%    0 L2 Control Task    32          72
986     73   0.00%  0.02%  0.00%    0 L2 Aging Task      33           4         21    190   0.00%
0.00%  0.00%    0 L3 Control Task    34          12        652     18   0.00%  0.00%  0.00%    0
FIB Control Task   35        9148       165  55442   1.22%  1.22%  1.15%    0 Statistics Task
36           4        413       9   0.00%  0.00%  0.00%    0 PFIB Table Manag   37       655016
64690036     10  75.33% 77.87% 71.10%   0 lcp schedular      38           0        762       0
0.00%  0.00%  0.00%    0 Constellation SP
```

Causes fréquentes et solutions pour les problèmes d'utilisation élevée de la CPU

IP inaccessibles

Quand un groupe d'accès refuse un paquet, le MSFC envoie des messages d'ICMP inaccessibles. Cette action se produit par défaut.

Avec l'activation par défaut de la commande **ip unreachables**, le Supervisor Engine rejette la plupart des paquets refusés vers le matériel. Ensuite, le Supervisor Engine envoie seulement un nombre restreint de paquets, au maximum 10 PPS, au MSFC. Cette action génère les messages d'ICMP inaccessibles.

L'abandon des paquets refusés et la génération des messages d'ICMP inaccessibles impose une charge à la CPU MSFC. Afin d'éliminer la charge, vous pouvez émettre la commande de configuration d'interface **no ip unreachables**. Cette commande désactive les messages d'ICMP inaccessibles, ce qui permet l'abandon dans le matériel de tous les paquets dont l'accès est refusé.

Les messages d'ICMP inaccessibles ne sont pas envoyés si une VACL refuse un paquet.

Traductions NAT

La NAT utilise à la fois le transfert matériel et logiciel. L'établissement initial des traductions NAT doit être fait dans le logiciel et le transfert supplémentaire est fait avec le matériel. La NAT utilise également la table Netflow (128 Ko maximum). Par conséquent, si la table Netflow est pleine, le commutateur démarrera également pour appliquer le transfert NAT par l'intermédiaire du logiciel. Cela se produit normalement avec des salves de trafic élevées et entraîne une augmentation sur la CPU de 6500.

Utilisation de l'espace de table FIB CEF dans la table de cache

Le Supervisor Engine 1 a une table de cache de flux qui prend en charge 128 000 entrées. Cependant, sur la base de l'efficacité de l'algorithme de hachage, ces entrées s'étendent de 32 000 à 120 000. Sur le Supervisor Engine 2, la table FIB est générée et programmée dans la PFC. La table contient jusqu'à 256 000 entrées. Le Supervisor Engine 720 avec PFC3-BXL prend en charge jusqu'à 1 000 000 entrées. Lorsque cet espace est dépassé, les paquets sont commutés dans le logiciel. Cela peut entraîner une utilisation élevée de la CPU sur le RP. Afin de vérifier le nombre de routes dans la table FIB CEF, utilisez ces commandes :

```
Router#show processes cpuCPU utilization for five seconds:  99.26%                      one
minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs    5Sec
1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- --- -----
----------1   0           0          0          0.74%   0.00%   0.00% -2  Kernel and Idle2   2
245        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0           1          0
0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0          0.00%   0.00%
0.00% -2  L2L3PatchRev   5   653         11737      1000       0.00%   0.00%   0.00% -2  SynDi!-
-- Output is suppressed.26 10576 615970 1000 0.00% 0.00% 0.00% 0 L3Aging 27 47432 51696 8000
0.02% 0.00% 0.00% 0 NetFlow 28 6758259 1060831 501000 96.62% 96.00% 96.00% 0   Fib            29
0           1          0          0.00%   0.00%   0.00% -2  Fib_bg_task  !--- Output is
suppressed.CATOS% show mls cefTotal L3 packets switched:          124893998234Total L3 octets
switched:          53019378962495Total route entries:                    112579  IP route
entries:                        112578  IPX route entries:                          1  IPM
route entries:                            0IP load sharing entries:                  295IPX
load sharing entries:                       0Forwarding entries:
112521Bridge entries:                                56Drop entries:
2IOS% show ip cef summaryIP Distributed CEF with switching (Table Version 86771423), flags=0x0
112564 routes, 1 reresolve, 0 unresolved (0 old, 0 new)  112567 leaves, 6888 nodes, 21156688
bytes, 86771426inserts, 86658859invalidations  295 load sharing elements, 96760 bytes, 112359
references  universal per-destination load sharing algorithm, id 8ADDA64A  2 CEF resets, 2306608
revisions of existing leaves  refcounts:  1981829 leaf, 1763584 node!--- You see these messages
if the TCAM space is exceeded:%MLSCEF-SP-7-FIB_EXCEPTION: FIB TCAM exception, Some entries will
be software switched%MLSCEF-SP-7-END_FIB_EXCEPTION: FIB TCAM exception cleared, all CEF entries
will be hardware switched
```

Sur le Supervisor Engine 2, le nombre d'entrées FIB est réduit de moitié si vous avez configuré le contrôle RPF sur les interfaces. Cette configuration peut mener à la commutation par logiciel de plus de paquets et, par conséquent, à une utilisation élevée de la CPU.

Afin de résoudre le problème d'utilisation élevée de la CPU, activez la récapitulation des routes. La récapitulation des routes peut réduire la latence dans un réseau complexe en réduisant les charges de processeur, les configurations requises en matière de mémoire et la demande de bande passante.

Consultez la page Comprendre l'ACL sur les commutateurs de la gamme Catalyst 6500 pour des informations supplémentaires sur l'utilisation et l'optimisation de la TCAM.

Journalisation de l'ACL optimisée

La journalisation de l'ACL optimisée (OAL) fournit la prise en charge matérielle pour le journalisation de l'ACL. À moins que vous configuriez l'OAL, le processus des paquets qui requièrent une journalisation a lieu entièrement dans le logiciel sur le MSFC3. L'OAL autorise ou rejette des paquets dans le matériel sur la PFC3. L'OAL utilise une routine optimisée pour envoyer les informations au MSFC3 afin de générer les messages de journalisation.

Remarque: Pour obtenir des informations sur OAL, consultez la section *Journalisation optimisée de l'ACL avec une PFC3* de Comprendre la prise en charge des ACL par Cisco IOS.

Limite de débit de paquets vers la CPU

Sur le Supervisor Engine 720, des limiteurs de débit peuvent contrôler le débit auquel les paquets peuvent accéder au logiciel. Ce contrôle du débit aide à éviter les attaques de déni de service. Vous pouvez également utiliser quelques uns de ces limiteurs de débit sur le Supervisor Engine 2 :

```
Router#show mls rate-limit   Rate Limiter Type       Status     Packets/s   Burst---------------
------   ----------   ---------   -----          MCAST NON RPF   Off                  -       -
MCAST DFLT ADJ   On              100000     100      MCAST DIRECT CON   Off                  -
-        ACL BRIDGED IN   Off                  -       -       ACL BRIDGED OUT   Off
-       -           IP FEATURES   Off                 -       -          ACL VACL LOG   On
2000       1           CEF RECEIVE   Off                   -       -             CEF GLEAN   Off
-       -      MCAST PARTIAL SC   On              100000     100        IP RPF FAILURE   On
500      10           TTL FAILURE   Off                 -       -ICMP UNREAC. NO-ROUTE   On
500      10ICMP UNREAC. ACL-DROP   On                500      10         ICMP REDIRECT   Off
-       -           MTU FAILURE   Off                 -       -           LAYER_2 PDU   Off
-       -            LAYER_2 PT   Off                 -       -             IP ERRORS   On
500      10           CAPTURE PKT   Off                 -       -            MCAST IGMP   Off
-       -Router(config)#mls rate-limit ?  all        Rate Limiting for both Unicast and
Multicast packets  layer2     layer2 protocol cases  multicast  Rate limiting for Multicast
packets  unicast    Rate limiting for Unicast packets
```

Voici un exemple :

```
Router(config)#mls rate-limit layer2 l2pt 3000
```

Afin de limiter le débit de tous les paquets envoyés par CEF au MSFC, lancez la commande de cet exemple :

```
Router(config)#mls ip cef rate-limit 50000
```

Afin de réduire le nombre de paquets envoyés à la CPU en raison de la TTL=1, lancez cette commande :

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```

Par exemple, c'est la sortie de la **capture de netdr**, qui prouve que l'ipv4 TTL est 1 :

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```

Une utilisation élevée de la CPU peut également être due aux paquets avec TTL=1 qui sont intégrés à la CPU. Afin de limiter le nombre de paquets qui sont intégrés à la CPU, configurez un limiteur de débit matériel. Les limiteurs de débit peuvent limiter le débit des paquets qui passent du chemin de données matériel au chemin de données logiciel. Les limiteurs de débit protègent le chemin de contrôle logiciel de l'encombrement en rejetant le trafic qui dépasse le débit configuré. La limite de débit est configurée utilisant la commande mls rate-limit all de ttl-failure.

Fusion physique des VLAN due à un câblage incorrect

L'utilisation élevée de la CPU peut également résulter de la fusion de deux VLAN ou plus en raison d'un câblage inapproprié. En outre, si le protocole STP est désactivé sur ces ports où la fusion de VLAN se produit, une utilisation élevée de la CPU peut se produire.

Afin de résoudre ce problème, identifiez les erreurs de câblage et corrigez-les. Si votre configuration le permet, vous pouvez également activer le protocole STP sur ces ports.

Tempête de diffusion

Une tempête de diffusion de LAN se produit quand la diffusion ou la multidiffusion de paquets inondent le LAN, ce qui crée un trafic excessif et dégrade des performances du réseau. Les erreurs de mise en œuvre de la pile de protocoles ou de la configuration de réseau peuvent entraîner une tempête de diffusion.

En raison de la conception architecturale de la plate-forme de la gamme Catalyst 6500, les paquets de diffusion sont seulement et toujours rejetés au niveau logiciel.

La suppression de diffusion empêche l'interruption des interfaces LAN par une tempête de diffusion. La suppression de diffusion utilise un filtrage qui mesure l'activité de diffusion sur un LAN sur une période d'une seconde et compare la mesure à un seuil prédéfini. Si le seuil est atteint, toute autre activité de diffusion est supprimée pendant la durée d'une période précisée. La suppression de diffusion est désactivée par défaut.

Remarque: Le lien instable VRRP de la sauvegarde à maîtriser entraîné par des saturations de diffusion pourrait entraîner l'utilisation du CPU élevé.

Afin de comprendre comment fonctionne la suppression de diffusion et d'activer la fonctionnalité, consultez :

- Configuration de la suppression de diffusion (logiciel système Cisco IOS)
- Configuration de la suppression de diffusion (logiciel système CatOS)

Suivi d'adresse du prochain saut BGP (processus de scanneur BGP)

Le processus de scanneur BGP parcoure la table BGP et confirme l'accessibilité des prochains sauts. Ce processus vérifie également l'annonce conditionnelle afin de déterminer si le BGP doit annoncer des préfixes de condition ou exécuter l'atténuation de la route. Par défaut, le processus analyse toutes les 60 secondes.

Vous pouvez vous attendre à de courtes durées d'utilisation élevée de la CPU en raison du processus de scanneur BGP sur un routeur qui contient une grande table de routage Internet. Une fois par minute, le scanneur BGP parcoure la table de la base d'informations de routage (RIB) BGP et effectue d'importantes tâches de maintenance. Ces tâches incluent :

- Un contrôle du prochain saut qui est référencé dans la table BGP du routeur
- Vérification que les périphériques de prochain saut peuvent être atteints

Ainsi, une grande table BGP prend une quantité de temps équivalente pour être parcourue et validée. Le processus de scanneur BGP parcoure la table BGP afin de mettre à jour toute structure de données et parcoure la table de routage à des fins de redistribution de routes. Les

deux tables sont stockées séparément dans la mémoire du routeur. Les deux tables peuvent être très grandes et, ainsi, consommer des cycles de CPU.

Pour obtenir plus d'informations sur l'utilisation de la CPU par le processus de scanneur BGP, consultez la section *Utilisation élevée de la CPU en raison du scanneur BGP* de Dépannage de l'utilisation élevée de la CPU en raison du scanneur BGP ou du processus de routeur BGP.

Pour obtenir plus d'informations sur la fonctionnalité de suivi d'adresse du prochain saut BGP et la procédure pour activer/désactive ou ajuster l'intervalle d'analyse, consultez Prise en charge BGP pour le suivi d'adresse du prochain saut.

Trafic multicast non-RPF

Le routage multicast (à la différence du routage unicast) est seulement concerné par la source d'un flux de données multicast donné. C'est-à-dire l'adresse IP du périphérique qui lance le trafic multicast. Le principe de base est que le périphérique source « diffuse » le flux vers un nombre non défini de récepteurs (au sein de son groupe multicast). Tous les routeurs multicast créent les arbres de distribution, qui contrôlent le chemin du trafic multicast à travers le réseau afin de livrer le trafic à tous les récepteurs. Les deux types de base d'arbres de distribution multicast sont les arbres sources et les arbres partagés. Le RPF est un concept clé dans le transfert multicast. Il permet aux routeurs de transférer correctement le trafic multicast vers le bas de l'arbre de distribution. Le RPF se sert de la table de routage unicast existante pour déterminer les voisins à l'amont et à l'aval. Un routeur transfère un paquet multicast seulement s'il est reçu sur l'interface en amont. Ce contrôle RPF aide à garantir que l'arbre de distribution ne comporte pas de boucles.

Le trafic multicast est toujours visible par chaque routeur sur LAN ponté (couche 2), selon la spécification CSMA/CD IEEE 802.3. Dans la norme 802.3, le bit 0 du premier octet est utilisé pour indiquer une trame de diffusion ou de multicast, et toute trame de la couche 2 avec cette adresse est inondée. C'est également le cas même si la surveillance CGMP ou surveillance IGMP est configurée. La raison est que les routeurs multicast doivent consulter le trafic multicast et prendre une décision de transfert appropriée. Si plusieurs routeurs multicast ont chacun des interfaces sur un LAN commun, alors un seul routeur transfère les données (choisi par un processus d'élection). En raison de la nature inondable des LAN, le routeur redondant (routeur qui ne transfère pas le trafic multicast) reçoit ces données sur l'interface de sortie pour ce LAN. Le routeur redondant rejette normalement ce trafic, car il est arrivé sur la mauvaise interface et échoue donc le contrôle RPF. Ce trafic qui échoue le contrôle RPF est appelé le trafic non-RPF ou les paquets d'échec RPF, car ils ont été transmis vers l'arrière contre le flux provenant de la source.

Le Catalyst 6500 avec un MSFC installé, peut être configuré pour agir en tant que véritable routeur multicast. En utilisant la commutation multicouche multicast (MMLS), le trafic RPF est généralement transféré par le matériel à l'intérieur du commutateur. Des informations sont fournies aux ASIC sur l'état du routage multicast (par exemple, (*, G) et (S, G)), de sorte qu'un raccourci matériel puisse être programmé dans la table Netflow ou FIB. Ce trafic non-RPF est encore nécessaire dans certains cas et est requis par la CPU MSFC (au niveau du processus) pour le mécanisme PIM Assert. Autrement, il est alors rejeté par le chemin logiciel à commutation rapide (l'hypothèse est que la commutation rapide par logiciel n'est pas désactivée sur l'interface RPF).

Le Catalyst 6500 qui utilise la redondance pourrait ne pas traiter le trafic non-RPF efficacement dans certaines topologies. Pour le trafic non-RPF, il y a généralement aucun état (*, G) ou (S, G) dans le routeur redondant, et donc aucun raccourcis matériel ou logiciel ne peut être créé pour rejeter le paquet. Chaque paquet multicast doit être examiné par le processeur de routage MSFC

individuellement, et cela est souvent mentionné sous le nom de trafic d'interruption de la CPU. Avec la commutation matériel de la couche 3 et les multiples interfaces/VLAN qui se connectent au même ensemble de routeurs, le trafic non-RPF qui frappe la CPU du MSFC redondant est amplifié « N » fois par rapport au débit source d'origine (où « N » est le nombre de LAN auxquels le routeur est connecté de manière redondante). Si le débit du trafic non-RPF dépasse la capacité de rejet de paquets du système, alors il pourrait entraîner une utilisation élevée de la CPU, des dépassements de mémoire tampon et l'instabilité générale du réseau.

Le Catalyst 6500 est doté d'un moteur de liste d'accès qui active un filtrage ayant lieu au débit câble. Cette fonctionnalité peut être utilisée pour traiter le trafic non-RPF pour les groupes en mode clairsemé efficacement, dans certaines situations. Vous pouvez seulement utiliser la méthode basée sur l'ACL dans des « réseaux de stub » en mode clairsemé , où il n'y a aucun routeur multicast (et récepteur correspondant) en aval. De plus, en raison de la conception de transfert de paquets de Catalyst 6500, les MSFC intérieurement redondants ne peuvent pas utiliser cette mise en œuvre. Cela est présenté dans l'ID de bogue Cisco CSCdr74908 (clients enregistrés seulement). Pour les groupes en mode dense, les paquets non-RPF doivent être consultés sur le routeur pour que le mécanisme PIM Assert fonctionne correctement. Différentes solutions, telles que la limitation de débit basée sur CEF ou Netflow et QoS, sont utilisées pour contrôler les échecs RPF dans des réseaux en mode dense et des réseaux de transit en mode clairsemé.

Le Catalyst 6500 est doté d'un moteur de liste d'accès qui active un filtrage ayant lieu au débit câble. Cette fonctionnalité peut être utilisée pour gérer efficacement le trafic non-RPF pour les groupes en mode clairsemé. Afin de mettre en œuvre cette solution, placez une liste d'accès sur l'interface d'entrée du « réseau de stub » pour filtrer le trafic multicast qui ne provenait pas du « réseau de stub ». La liste d'accès est poussé vers le matériel dans le commutateur. Cette liste d'accès empêche la CPU de consulter le paquet et permet au matériel de rejeter le trafic non-RPF.

Remarque: Ne placez pas cette liste d'accès sur une interface de transit. Elle est uniquement destinée aux réseaux de stub (réseaux avec des hôtes seulement).

Référez-vous à ces documents pour plus d'informations :

- Problèmes de routeur redondant avec Multicast IP dans les réseaux de stub
- Traitement du trafic non-RPF

Commandes show

Lorsque vous lancez une **commande show**, l'utilisation de la CPU est toujours de presque 100 %. Il est normal d'avoir une utilisation élevée de la CPU quand vous lancez une **commande show** et elle ne reste normalement que durant quelques secondes.

Par exemple, il est normal que le processus Virtual Exec soit élevé quand vous lancez une commande **show tech-support**, car ce résultat est un résultat généré par interruption. Votre seule préoccupation est d'avoir une utilisation élevée du la CPU dans d'autres processus que les **commandes show**.

La commande show cef not-cef-switched affiche pourquoi des paquets sont donnés un coup de volée au MSFC (recevez, option d'IP, aucune contiguïté, etc.) et combien. Exemple :

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0         0
```

```
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

Les commandes brief d'ibc d'exposition et d'**ibc d'exposition** affichent la file d'attente CPU et peuvent être utilisées quand vous surveillez l'état CPU.

Processus Exec

Le processus Exec dans le logiciel Cisco IOS est responsable de la transmission sur les lignes TTY (console, auxiliaire, asynchrone) du routeur. Le processus Virtual Exec est responsable des lignes VTY (sessions Telnet). Les processus Exec et Virtual Exec sont des processus de priorité moyenne. Ainsi si d'autres processus ont une priorité plus élevée (élevée ou critique), les processus ayant la priorité la plus élevée obtiennent les ressources de la CPU.

Si beaucoup de données sont transférées par ces sessions, l'utilisation de la CPU pour le processus Exec augmente. La raison est que quand le routeur veut envoyer un caractère simple par ces lignes, le routeur utilise certaines ressources de la CPU :

- Pour la console (Exec), le routeur utilise une interruption par caractère.
- Pour la ligne VTY (Virtual Exec), la session Telnet doit construire un paquet TCP par caractère.

Cette liste détaille certaines des causes possibles d'utilisation élevée de la CPU dans le processus Exec :

- **Il y a trop de données transmises par le port de console.**Vérifiez si des débogages ont commencé sur le routeur avec la commande **show debugging**.Désactivez la journalisation de la console sur le routeur avec la forme **no** de la commande **logging console**.Vérifiez si un long résultat est imprimé sur la console. Par exemple, une commande **show tech-support** ou **show memory**.
- **La commande exec est configurée pour les lignes asynchrones et auxiliaires.**Si une ligne a seulement un trafic sortant, désactivez le processus Exec pour cette ligne. La raison est que si le périphérique (par exemple, un modem) connecté à cette ligne envoie des données non sollicitées, le processus Exec commence sur cette ligne.Si le routeur est utilisé en tant que serveur de terminaux (pour Telnet inverse vers d'autres consoles de périphériques), il est recommandé de configurer la **commande no exec** sur les lignes qui sont connectées à la console des autres périphériques. Sinon, les données qui reviennent de la console pourraient commencer un processus Exec, ce qui utilise des ressources de la CPU.

Une cause possible de l'utilisation élevée de la CPU dans le processus Virtual Exec est :

- **Il y a trop de données transmises à travers les sessions Telnet.**La raison la plus fréquente d'utilisation élevée de la CPU dans le processus Virtual Exec est que trop de données sont transférées du routeur à la session Telnet. Cela peut se produire quand des commandes avec de longs résultats, telles que **show tech-support**, **show memory**, etc., sont exécutées à partir de la session Telnet. La quantité de données transférées par chaque session VTY peut être vérifiée avec la commande **show tcp vty <numéro de ligne>** .

Processus de vieillissement L3

Quand le processus de vieillissement L3 exporte un grand nombre de valeurs *ifindex* en utilisant l'exportation des données Netflow (NDE), l'utilisation de la CPU peut atteindre 100 %.

Si vous rencontrez ce problème, vérifiez si ces deux commandes sont activées :

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

Si vous activez ces commandes, le processus doit exporter toutes les valeurs ifindex de destination et de source en utilisant la NDE. L'utilisation de processus de vieillissement L3 devient élevé puisqu'il doit effectuer une recherche dans la FIB pour toutes les valeurs *ifindex* de destination et de source. Pour cette raison, la table se remplit, le processus de vieillissement L3 devient élevé et l'utilisation de la CPU atteint 100 %.

Afin de résoudre ce problème, désactivez ces commandes :

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

Utilisez ces commandes de vérifier les valeurs :

- show mls cef summary
- show mls cef maximum-routes

Tempête BPDU

Spanning-tree met à jour un environnement sans boucles de la couche 2 sur les réseaux commutés redondants. Sans STP, les trames font une boucle et/ou se multiplient indéfiniment. Cette occurrence entraîne un ralentissement des données sur le réseau parce que le trafic élevé interrompt tous les périphériques du domaine de diffusion.

Àcertains égards, STP est un protocole précoce qui a d'abord été développé pour des spécifications de pont lentes basées sur logiciel (IEEE 802.1D), mais le protocole STP peut être compliqué afin d'être mis en œuvre avec succès dans les grands réseaux commutés qui ont ces fonctionnalités :

- Beaucoup de réseaux VLAN
- Beaucoup de commutateurs dans un domaine STP
- Prise en charge multi-fournisseur
- De nouvelles améliorations IEEE

Si le réseau fait face à des calculs Spanning Tree fréquents ou si le commutateur doit traiter plus de BPDU, cela peut entraîner une utilisation élevée de la CPU, ainsi que des rejets de BPDU.

Afin de contourner ces problèmes, effectuez une ou la totalité de ces étapes :

1. Élaguez les VLAN des commutateurs.
2. Utilisez une version améliorée du protocole STP, tel que MST.
3. Mettez à niveau le matériel du commutateur.

Consultez également les meilleures pratiques de mise en œuvre du protocole Spanning Tree dans le réseau.

- Pratiques recommandées pour la configuration et la gestion des commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000 s'exécutant sous CatOS
- Pratiques recommandées pour les commutateurs des gammes Catalyst 6500/6000 et Catalyst 4500/4000 exécutant le logiciel Cisco IOS

Sessions SPAN

Sur la base de l'architecture des commutateurs de la gamme Catalyst 6000/6500, les sessions SPAN n'ont pas de conséquences sur les performances du commutateur, mais, si la session SPAN inclut un trafic élevé/port de liaison ascendante ou EtherChannel, cela peut augmenter la charge sur le processeur. S'il choisit alors un VLAN spécifique, il augmente la charge encore plus. S'il y a un mauvais trafic sur la liaison, cela peut encore accroître la charge.

Dans certains scénarios, la fonctionnalité RSPAN peut entraîner les boucles et la charge sur le processeur augmente rapidement. Pour obtenir plus d'informations, consultez la page Pourquoi la session SPAN crée une boucle de pontage ?

Le commutateur peut passer le trafic comme d'habitude puisque tout est dans le matériel, mais la CPU peut en voir de toutes les couleurs si elle essaye de comprendre quel trafic envoyer. Il est recommandé de configurer des sessions SPAN seulement lorsque cela est nécessaire.

%CFIB-SP-STBY-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software switched

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0         0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

Ce message d'erreur est reçu quand la quantité d'espace disponible dans la TCAM est dépassée. Cela a comme conséquence une utilisation élevée de la CPU. Il s'agit d'une limitation de la TCAM de la FIB. Lorsque la TCAM est pleine, un indicateur est défini et l'exception de la TCAM du FIB est reçue. Cela arrête l'ajout de nouvelles routes à la TCAM. Par conséquent, tout est commuté par logiciel. La suppression des routes n'aide pas à reprendre la commutation par matériel. Lorsque la TCAM entre dans l'état d'exception, le système doit être rechargé pour sortir de cet état. Le nombre maximum de routes qui peut être installé dans la TCAM est augmenté par la commande **mls cef maximum-routes**.

L'exécution du Catalyst 6500/6000 avec la CPU de haute a un ACL d'IPv6 avec les ports L4

Mls ipv6 acl compress address unicast d'enable. Cette commande est nécessaire si l'ACL d'IPv6

s'assortit sur des nombres du port de protocole L4. Si cette commande n'est pas activée, le trafic d'IPv6 sera donné un coup de volée à la CPU pour le traitement de logiciel. Cette commande n'est pas configurée par défaut.

SPF de cuivre

Dans les commutateurs Ethernet de la gamme Cisco ME 6500, les SFP de cuivre ont besoin de plus d'interaction avec le microprogramme que d'autres types de SFP, ce qui augmente l'utilisation de la CPU.

Les algorithmes logiciels qui gèrent les SFP de cuivre ont été améliorés dans les versions de Cisco IOS SXH.

IOS modulaire

Dans les commutateurs de la gamme Cisco Catalyst 6500 qui exécutent le logiciel IOS modulaire, l'utilisation normale de la CPU est légèrement supérieure à celle d'un logiciel IOS non-modulaire.

Le logiciel IOS modulaire paye un prix par activité plus qu'il paye un prix par paquet. Le logiciel IOS modulaire maintient les processus en consommant une certaine quantité de CPU même s'il y a peu des paquets. Ainsi, la consommation de CPI n'est pas basée sur le trafic réel. Cependant, quand les paquets traités sont importants, la quantité de CPU consommée dans le logiciel IOS modulaire ne devrait pas être supérieure à celle du logiciel IOS non-modulaire.

Contrôle de l'utilisation de la CPU

Si l'utilisation de la CPU est élevée, lancez d'abord la commande **show processes cpu**. Le résultat vous montre l'utilisation de la CPU sur le commutateur, ainsi que la consommation de la CPU par chaque processus.

```
Router#show processes cpu CPU utilization for five seconds: 57%/48%; one minute: 56%; five
minutes: 48% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process    1
0         5          0  0.00%  0.00%  0.00%   0 Chunk Manager       2          12     18062
0  0.00%  0.00%  0.00%   0 Load Meter          4      164532     13717      11994  0.00%  0.21%
0.17%   0 Check heaps         5           0         1          0  0.00%  0.00%  0.00%   0 Pool
Manager      !--- Output is suppressed. 172 0 9 0 0.00% 0.00% 0.00% 0 RPC aapi_rp 173      243912
2171455        112  9.25%  8.11%  7.39%   0 SNMP ENGINE       174          68       463
146  0.00%  0.00%  0.00%   0 RPC pm-mp  !--- Output is suppressed.
```

Dans ce résultat, l'utilisation totale de la CPU est de 57 pour cent et l'utilisation de la CPU au niveau d'interruption est de 48 pour cent. Ici, ces pourcentages apparaissent en caractères gras. Le commutateur d'interruption du trafic par la CPU entraîne l'utilisation de la CPU au niveau d'interruption. Le résultat de la commande liste les processus qui entraînent la différence entre les deux utilisations. Dans ce cas, la cause est le processus SNMP.

Sur le Supervisor Engine qui exécute CatOS, le résultat ressemble à ce qui suit :

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
```

```
0.00% 0.00% -2 SptTimer 62  18185410     3712736     106000     22.22%  21.84%  21.96% -2
SptBpduRx       63  845683       91691       105000      0.92%   0.00%   0.00% -2  SptBpduTx
```

Dans ce résultat, le premier processus est Kernel and Idle, ce qui montre l'utilisation de la CPU inactive. Ce processus est normalement élevé, à moins que d'autres processus consomment des cycles de CPU. Dans cet exemple, le processus de SptBpduRx entraîne une utilisation élevée de la CPU.

Si l'utilisation de la CPU est élevée en raison de l'un de ces processus, vous pouvez dépanner et déterminer pourquoi ce processus s'exécute à un niveau élevé. Mais, si l'utilisation de la CPU est élevée en raison d'un trafic envoyé à la CPU, vous devez déterminer pourquoi le trafic de routage est envoyé. Cette détermination peut vous aider à identifier ce qu'est le trafic.

Pour dépanner, employez cet exemple de script EEM afin de collecter la sortie du commutateur quand vous éprouvez l'utilisation du CPU élevé :

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410     3712736     106000     22.22%  21.84%  21.96% -2
SptBpduRx       63  845683       91691       105000      0.92%   0.00%   0.00% -2  SptBpduTx
```

Remarque: La commande de **rx de capture de netdr de débogage** est utile quand la CPU est haute devant traiter la commutation des paquets au lieu du matériel. Il capture 4096 paquets entrants à la CPU quand la commande est exécutée. La commande est complètement sûre et est l'outil le plus commode pour les questions élevées CPU sur les 6500. Il n'entraîne pas le chargement supplémentaire à la CPU.

Utilitaires et outils pour déterminer le trafic qui est envoyé vers la CPU

Cette section identifie quelques utilitaires et outils qui peuvent vous aider à examiner ce trafic.

Plate-forme logicielle Cisco IOS

Dans le logiciel Cisco IOS, le processeur du commutateur sur le Supervisor Engine est appelé SP, et le MSFC est appelé RP.

La **commande show interface** donne des informations de base sur l'état de l'interface et le débit du trafic sur l'interface. Cette commande fournit également des compteurs d'erreurs.

```
Router#show interface gigabitethernet 4/1GigabitEthernet4/1 is up, line protocol is up
(connected)  Hardware is C6k 1000Mb 802.3, address is 000a.42d1.7580 (bia 000a.42d1.7580)
Internet address is 100.100.100.2/24  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255  Encapsulation ARPA, loopback not set  Keepalive
set (10 sec)  Half-duplex, 100Mb/s  input flow-control is off, output flow-control is off  Clock
mode is auto  ARP type: ARPA, ARP Timeout 04:00:00  Last input 00:00:00, output 00:00:00, output
hang never  Last clearing of "show interface" counters never  Input queue: 5/75/1/24075
(size/max/drops/flushes); Total output drops: 2  Queueing strategy: fifo  Output queue: 0/40
(size/max)  30 second input rate 7609000 bits/sec, 14859 packets/sec  30 second output rate 0
bits/sec, 0 packets/sec  L2 Switched: ucast: 0 pkt, 184954624 bytes - mcast: 1 pkt, 500 bytes
L3 in Switched: ucast: 2889916 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast  L3 out Switched:
ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes     2982871 packets input, 190904816 bytes, 0 no
```

```
buffer     Received 9 broadcasts, 0 runts, 0 giants, 0 throttles     1 input errors, 1 CRC, 0
frame, 28 overrun, 0 ignored     0 input packets with dribble condition detected     1256
packets output, 124317 bytes, 0 underruns     2 output errors, 1 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred     0 lost carrier, 0 no carrier     0 output buffer
failures, 0 output buffers swapped out
```

Dans ce résultat, vous pouvez voir que le trafic entrant commuté par la couche 3 au lieu de la couche 2. Cela indique que le trafic est envoyé à la CPU.

La commande **show processes cpu** vous indique si ces paquets sont des paquets de trafic réguliers ou des paquets de contrôle.

```
Router#show processes cpu | exclude 0.00              CPU utilization for five seconds: 91%/50%;
one minute: 89%; five minutes: 47% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY
Process   5      881160     79142      11133  0.49%  0.19%  0.16%   0 Check heaps       98
121064   3020704         40 40.53% 38.67% 20.59%   0 IP Input         245      209336    894828
233  0.08%  0.05%  0.02%   0 IFCOM Msg Hdlr
```

Si les paquets sont commuté par processus, vous voyez que le IP Input process s'exécute à un niveau élevé. Lancez cette commande afin de voir ces paquets :

show buffers input-interface

```
Router#show buffers input-interface gigabitethernet 4/1 packetBuffer information for Small
buffer at 0x437874D4  data_area 0x8060F04, refcount 1, next 0x5006D400, flags 0x280  linktype 7
(IP), enctype 1 (ARPA), encsize 14, rxtype 1  if_input 0x505BC20C (GigabitEthernet4/1),
if_output 0x0 (None)  inputtime 00:00:00.000 (elapsed never)  outputtime 00:00:00.000 (elapsed
never), oqnumber 65535  datagramstart 0x8060F7A, datagramsize 60, maximum size 308  mac_start
0x8060F7A, addr_start 0x8060F7A, info_start 0x0  network_start 0x8060F88, transport_start
0x8060F9C, caller_pc 0x403519B4  source: 100.100.100.1, destination: 100.100.100.2, id: 0x0000,
ttl: 63,  TOS: 0 prot: 17, source port 63, destination port 6308060F70:
000A 42D17580            ..BQu.08060F80: 00000000 11110800 4500002E 00000000
........E.......08060F90: 3F11EAF3 64646401 64646402 003F003F  ?.jsddd.ddd..?.?08060FA0:
001A261F 00010203 04050607 08090A0B  ..&.............08060FB0: 0C0D0E0F 101164
......d
```

Si le trafic est **commuté par interruption**, vous ne pouvez pas voir ces paquets avec la commande **show buffers input-interface**. Afin de voir les paquets qui sont envoyés au RP pour la commutation par interruption, vous pouvez exécuter une capture SPAN (Switched Port Analyzer) du port RP.

Remarque: Consultez ce document pour obtenir des informations supplémentaires sur l'utilisation de la CPU commutée par interruption par rapport à commuté par processus :

- Section *Utilisation élevée de la CPU en raison d'interruptions* de Dépannage de l'utilisation élevée de la CPU sur des routeurs Cisco

Intrabande RP et intrabande SP du SPAN

Un SPAN pour le port RP ou SP dans le logiciel Cisco IOS est disponible dans le logiciel Cisco IOS version 12.1(19)E et ultérieure.

Voici la syntaxe de commande :

test monitor session *1-66* **add {rp-inband | sp-inband} [rx | tx | both]**

Utilisez cette syntaxe pour le logiciel Cisco IOS versions 12.2 SX :

test monitor add *{1..66}* **{rp-inband | sp-inband} {rx | tx | both}**

Remarque: Pour la version SXH, vous devez utiliser la commande **monitor session** afin de

configurer une session de SPAN local, puis utilisez cette commande pour associer la session de SPAN à la CPU :

source {cpu {rp | sp}} | *single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list***} [rx | tx | both]**

Remarque: Pour obtenir plus d'informations sur ces commandes, consultez Configuration du SPAN local (mode de configuration de SPAN) du *Guide de configuration logicielle de Catalyst 6500 version 12.2SX*.

Voici un exemple sur une console RP :

```
Router#monitor session 1 source interface fast 3/3!--- Use any interface that is
administratively shut down.Router#monitor session 1 destination interface 3/2
```

Maintenant, accédez à la console SP. Voici un exemple :

```
Router-sp#test monitor session 1 add rp-inband rx
```

Remarque: Dans le logiciel Cisco IOS version 12,2 SX, la commande a été remplacée par **test monitor add 1 rp-inband rx**.

```
Router#show monitor Session 1---------Type : Local SessionSource Ports :Both : Fa3/3Destination
Ports : Fa3/2SP console:Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1
Egress Source Ports: 3/3 Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans:
<empty>Destination Ports: 3/2
```

Remarque: Dans le logiciel Cisco IOS version 12.2 SX, la commande a été remplacée par **test monitor show 1**.

Voici un exemple sur une console SP :

```
Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1 Egress Source Ports: 3/3
Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans: <empty>Destination Ports:
3/2
```

Plate-forme logicielle CatOS

Pour les commutateurs qui exécutent le logiciel système CatOS, le Supervisor Engine exécute CatOS et le MSFC exécute le logiciel Cisco IOS.

Si vous lancez la commande **show mac**, vous pouvez voir le nombre de trames qui sont envoyées au MSFC. Le port 15/1 est la connexion du Supervisor Engine au MSFC.

Remarque: Le port est 16/1 pour les Supervisor Engines dans l'emplacement 2.

```
Console> (enable) show mac 15/1Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast-
------- -------------------- -------------------- --------------------15/1
193576                     0                    1Port     Xmit-Unicast         Xmit-Multicast
Xmit-Broadcast-------- -------------------- -------------------- --------------------15/1
3                    0                    0Port     Rcv-Octet            Xmit-Octet-------- ----
---------------- --------------------15/1                 18583370                    0MAC
Dely-Exced MTU-Exced  In-Discard Out-Discard-------- ---------- ---------- ---------- ----------
-15/1              0          -          0           0
```

Une augmentation rapide de ce chiffre indique que des paquets sont envoyés au MSFC, ce qui entraîne une utilisation élevée de la CPU. Vous pouvez alors regarder les paquets de ces façons :

- SPAN avec port MSFC 15/1 ou 16/1
- SPAN avec sc0

SPAN avec port MSFC 15/1 ou 16/1

Configurez une session de SPAN dans laquelle la source est le port MSFC 15/1 (ou 16/1) et la destination est un port Ethernet.

Voici un exemple :

```
Console> (enable) set span 15/1 5/10Console> (enable) show spanDestination      : Port 5/10Admin Source     : Port 15/1Oper Source      : NoneDirection       : transmit/receiveIncoming Packets: disabledLearning        : enabledMulticast       : enabledFilter          : -Status           : active
```

Si vous collectez un tracé de l'analyseur sur le port 5/10, le tracé de l'analyseur montre les paquets qui transmettent vers et depuis le MSFC. Configurez la session de SPAN en tant que **tx** afin de capturer les paquets qui sont seulement destinés au MSFC, pas au MSFC.

SPAN avec sc0

Installez une session de SPAN avec l'interface **sc0** en tant que source afin de capturer les trames qui vont à la CPU du Supervisor Engine.

```
Console> (enable) set span ?  disable                    Disable port monitoring  sc0                  Set span on interface sc0  <mod/port>                Source module and port numbers  <vlan>               Source VLAN numbers
```

Remarque: Pour les modules de services optiques (OSM), vous ne pouvez pas exécuter une capture SPAN du trafic.

Recommandations

L'utilisation de la CPU par le Supervisor Engine ne reflète pas les performances de transfert matériel du commutateur. Cependant, vous devez établir une référence et contrôler l'utilisation de la CPU par le Supervisor Engine.

1. Établissez la référence de l'utilisation de la CPU par le Supervisor Engine pour le commutateur dans un réseau équilibré avec des structures de trafic et une charge normales.Notez quel processus génère l'utilisation de la CPU la plus élevée.
2. Quand vous dépannez l'utilisation de la CPU, prenez en compte ces questions :Quel processus génère l'utilisation de la CPU la plus élevée ? Ces processus sont-ils différents de votre référence ?La CPU est-elle toujours élevée, au-dessus de la référence ? Ou existe-il des pointes d'utilisation élevée, puis un retour au niveau de référence ?Y a-t-il des notifications de modification de topologie (TCN) dans le réseau ?**Remarque:** L'instabilité de ports ou de ports hôte avec STP PortFast désactivé entraîne des TCN.Le trafic de diffusion ou multicast est-il excessif dans le VLAN/sous-réseau de gestion ?Le trafic de gestion (par exemple interrogation SNMP) est-il excessif sur le commutateur ?
3. Pendant le temps- CPU élevé (quand la CPU est 75% ou ci-dessus), collectez la sortie de ces commandes :*show clock*show versionshow processes cpu triéhistorique CPU de show procshow log
4. Si possible, isolez le VLAN de gestion des VLAN avec trafic de données utilisateur, en particulier le trafic de diffusion lourd.Des exemples de ce type de trafic incluent IPX RIP/protocole d'annonce de service (SAP), AppleTalk et tout autre trafic de diffusion. Un tel trafic peut avoir un impact sur l'utilisation de la CPU du Supervisor Engine et, dans des cas

extrêmes, peut gêner le fonctionnement normal du commutateur.

5. Si la CPU s'exécute à un niveau élevé en raison de l'envoi de trafic au RP, déterminez ce qu'est ce trafic et pourquoi le trafic est envoyé.Afin de faire cette détermination, utilisez les utilitaires décrits dans la section Utilitaires et outils pour déterminer le trafic qui est envoyé vers la CPU.

Informations connexes

- Commandes utiles pour dépannage de la CPU de haute sur le Catalyst 6500's avec Sup720
- Messages d'erreur CatOS courants sur les commutateurs de la gamme Catalyst 6000/6500
- Messages d'erreur courants sur les commutateurs des gammes Catalyst 6000/6500 exécutant le logiciel Cisco IOS
- Résolution des problèmes matériels et courants sur les commutateurs des gammes Catalyst 6500/6000 exécutant le logiciel système Cisco IOS
- Propagation monodiffusion dans les réseaux campus commutés
- Assistance sur les commutateurs de la gamme Cisco Catalyst 6500
- Le script EEM pour collecter des données pendant la CPU intermittente de haute émettent
- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems