Catalyst 6500/6000 switchingmodule met hoge CPU's

Inhoud

Inleiding

Dit document beschrijft de oorzaken van gebruik van hoge CPU's op Cisco Catalyst 6500/6000 Series switches en Virtual Switching System (VSS) 1440-gebaseerde systemen. Net zoals Cisco routers, gebruiken de switches de opdracht **om processen cpu** te **tonen** om CPU-gebruik voor de schakelaar Supervisor Engine processor weer te geven. Vanwege de verschillen in architectuur en verzendmechanismen tussen Cisco-routers en switches **verschilt** de **cpu-**opdracht van de **show** echter aanzienlijk van de andere **processen**. De betekenis van de output verschilt ook. Dit document verduidelijkt deze verschillen en beschrijft het gebruik van CPU's op de switches en hoe u de opdrachtoutput van de **showprocessen** interpreteert.

Opmerking: In dit document verwijzen de woorden "schakelaar" en "switches" naar Catalyst 6500/6000 switches.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de software- en hardwareversies voor Catalyst 6500/6000 switches en Virtual Switching System (VSS) 1440-gebaseerde systemen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Opmerking: de ondersteunde software voor het Virtual Switching System (VSS) 1440-gebaseerde systemen is Cisco IOS-softwarerelease 12.2(33)SXH1 of hoger.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Verschil tussen CatOS- en Cisco IOS-systeemsoftware

Catalyst OS (CatOS) op de Supervisor Engine en Cisco IOS® software op de functiekaart voor

meerlaagse switch (MSFC) (hybride): U kunt een CatOS-afbeelding als systeemsoftware gebruiken om de Supervisor Engine op Catalyst 6500/6000 switches te starten. Als de optionele MSFC is geïnstalleerd, wordt een afzonderlijke image van de Cisco IOS-software gebruikt om de MSFC te runnen.

Cisco IOS-software op zowel de Supervisor Engine als de MSFC (native): U kunt één Cisco IOS-softwarebeeld als systeemsoftware gebruiken om zowel de Supervisor Engine als MSFC op Catalyst 6500/6000 switches te starten.

Opmerking: Raadpleeg Vergelijking van Cisco Catalyst en Cisco IOS besturingssystemen voor de Cisco Catalyst 6500 Series switch voor meer informatie.

Verken CPU-gebruik op Catalyst 6500/6000 switches

Cisco software-gebaseerde routers gebruiken software om pakketten te verwerken en te verzenden. CPU-gebruik op een Cisco-router neemt meestal toe naarmate de router meer pakketverwerking en routing uitvoert. Daarom kan de opdracht **om** processen te **tonen cpu** een redelijk nauwkeurige indicatie van de verkeersafwerking op de router geven.

Catalyst 6500/6000 switches gebruiken de CPU niet op dezelfde manier. Deze switches nemen expediteits beslissingen in hardware, niet in software. Daarom, wanneer de switches de expediteits- of switching-beslissing nemen voor de meeste frames die door de switch gaan, is het proces niet van toepassing op de supervisor-motor CPU.

Op Catalyst 6500/6000 switches zijn er twee CPU's. Eén CPU is de supervisor-motor CPU, die wordt aangeduid als de NMP-processor (Network Management Processor) of de switchprocessor (SP). De andere CPU is Layer 3-routeprocessor CPU, die MSFC of de routeprocessor (RP) wordt genoemd.

SP CPU voert functies uit zoals:

- Assistenten in MAC-adressering en -vergrijzing**Opmerking:** MAC-adres learning wordt ook padinstellingen genoemd.
- Voert protocollen en processen uit die netwerkcontrole biedenVoorbeelden hiervan zijn Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP) en Port Aggregation Protocol (PAgP).
- Verkeer netwerkbeheerverkeer dat bestemd is voor de CPU van de switchVoorbeelden zijn telnet, HTTP en Simple Network Management Protocol (SNMP)-verkeer.

De RP CPU voert functies uit zoals:

- Hiermee worden Layer 3 Routing- en adressenprotocol (ARP)-tabellen gebouwd en bijgewerkt
- genereert de Cisco Express Forwarding (CEF) Forwarding Information Base (FIB) en nabijheidstabellen, en downloads de tabellen in de Policy functiekaart (PFC)
- verwerkt netwerkbeheerverkeer dat bestemd is voor de RPVoorbeelden zijn telnet, HTTP, en SNMP verkeer.

Situatie en functies die verkeer naar software stimuleren

Pakketten die aan de switch zijn bestemd

Elk pakket dat bestemd is voor de schakelaar gaat naar de software. Tot deze pakketten behoren:

- BedieningspakkettenEr worden pakketten voor controle ontvangen voor STP, CDP, VTP, Hot Standby Router Protocol (HSRP), PAgP, Link Aggregation Control Protocol (LACP) en UniDirectional Link Detection (UDLD).
- Routing Protocol-updatesVoorbeelden van deze protocollen zijn Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (DHCP), Border Gateway Protocol (BGP) en Open Shortest Path First Protocol (OSPF-protocol).
- SNMP-verkeer dat bestemd is voor de switch
- Telnet- en Secure Shell Protocol (SSH)-verkeer naar de switch.Ultilisering met hoge CPU's door SSH's wordt gezien als:

```
00:30:50.793 SGT Tue Mar 20 2012

CPU utilization for five seconds: 83%/11%; one minute: 15%; five minutes: 8%

 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process

   3        6468      8568        754 69.30%  7.90%  1.68%   1 SSH Process
```

  Voeg deze opdrachten in het EEM-script toe om het aantal SSH-sessies te controleren dat is ingesteld wanneer de CPU hoog is:show-gebruikerstoonlijn
- ARP-antwoorden op ARP-verzoeken

Pakketten en voorwaarden die speciale verwerking vereisen

Deze lijst bevat specifieke pakkettypes en voorwaarden die pakketten dwingen om in software te worden verwerkt:

- Pakketten met IP-opties, een verlopen tijd om te leven (TTL) of niet-geavanceerde Research Projects Agency (ARPA) insluiting
- Pakketten met speciale behandeling, zoals tunneling
- IP-fragmentatie
- Packets die Internet Control Message Protocol (ICMP)-berichten van de RP of SP vereisen
- Max. fout bij controle door transmissieeenheid (MTU)
- Pakketten met IP-fouten, waaronder IP-checksum en lengtefouten
- Als de ingevoerde pakketten een beetje fout teruggeven (zoals de single-bit fout (SBE), worden de pakketten naar de CPU voor softwareverwerking verzonden en gecorrigeerd. Het systeem wijst voor hen een buffer toe en gebruikt de CPU-bron om deze te corrigeren.
- Wanneer PBR- en omgekeerde toegangslijst in het pad van een verkeersstroom staan, wordt de software ingeschakeld en hiervoor is een extra CPU-programma nodig.
- Adjaculatie dezelfde interface
- Pakketten die niet voldoen aan de controle **RPF-doorsturen van** het omgekeerde pad
- Glein/ontvangenGlein verwijst naar pakketten die ARP resolutie vereisen en ontvangt verwijst naar pakketten die in de ontvangstcase vallen.
- Internetwork Packet Exchange (IPX)-verkeer dat via software-switched op de Supervisor Engine 720 in Cisco IOS-software en CatOSIPX-verkeer is ook software-switched op de Supervisor Engine 2/Cisco IOS-software, maar het verkeer is hardware-switched op de Supervisor Engine 2/CatOS. IPX-verkeer is hardware-switched op de Supervisor Engine 1A voor beide besturingssystemen.
- AppleTalk-verkeer

- Hardware resources - volledige voorwaardenDeze middelen omvatten FIB, content-addressable memory (CAM) en ternary CAM (TCAM).

Op ACL gebaseerde functies

- Toegangscontrolelijst (ACL) - ontkend verkeer met de optie ICMP onbereikbaar ingeschakeld**Opmerking:** dit is de standaard.Sommige ACL-ontkende pakketten worden naar de MSFC gelekt als IP onbereikbaar is. Pakketten die onbereikbaar ICMP vereisen worden in een door de gebruiker te configureren tempo uitgelekt. Standaard is de snelheid 500 pakketten per seconde (pps).
- IPX-filtering op basis van niet-ondersteunde parameters, zoals bronhostOp Supervisor Engine 720 is het proces van Layer 3 IPX-verkeer altijd in software.
- Access Control lemma's (ACE's) die loggen, met het **logsleutelwoord** vereisenDit is van toepassing op ACL-logfuncties (ACL's) (VLAN en VLAN ACL's). ACE's in dezelfde ACL's die niet nog in hardware registreren. Supervisor Engine 720 met PFC3 ondersteunt de snelheidslimiet van pakketten die naar de MSFC worden omgeleid voor ACL en VACL-vastlegging. Supervisor Engine 2 ondersteunt de snelheidsbeperking van pakketten die opnieuw naar de MSFC worden gericht voor VACL-vastlegging. Ondersteuning voor ACL-loggen op Supervisor Engine 2 is gepland voor Cisco IOS-softwarerelease 12.2S.
- Op beleid gestuurd verkeer, met gebruik van **overeenkomende lengte**, **stel ip voorrang**, of andere niet ondersteunde parameters inDe **ingestelde interface** parameter ondersteunt de software. Echter, de **set interface ongeldige 0** parameter is een uitzondering. Dit verkeer wordt in hardware op Supervisor Engine 2 met PFC2 en Supervisor Engine 720 met PFC3 verwerkt.
- Niet-IP en niet-IPX router ACL's (RACL's)Niet-IP RACL's zijn van toepassing op alle Supervisor Engine. De niet-IPX RACL's zijn van toepassing op Supervisor Engine 1a met PFC en Supervisor Engine 2 met alleen PFC2.
- Uitgezonden verkeer dat wordt ontkend in een RACL
- Verkeer dat wordt ontkend in een enkelvoudige RPF-controle (uRPF), ACL-ACEDeze uRPF-controle is van toepassing op Supervisor Engine 2 met PFC2 en Supervisor Engine 720 met PFC3.
- VerificatieproxyHet verkeer dat aan authenticatie proxy is onderworpen kan snelheidsbeperkt zijn op Supervisor Engine 720.
- Cisco IOS-software voor IP-beveiliging (IPsec)Het verkeer dat aan Cisco IOS encryptie is kan tarief-beperkt zijn op de Supervisor Engine 720.

Op NetFlow gebaseerde functies

De op NetFlow gebaseerde eigenschappen die deze sectie beschrijft zijn alleen van toepassing op Supervisor Engine 2 en Supervisor Engine 720.

- Op NetFlow gebaseerde functies moeten altijd het eerste pakket van een flow in software zien. Nadat het eerste pakket van de stroom software heeft bereikt, zijn de volgende pakketten voor dezelfde stroom hardware-switched.Deze stroomindeling is van toepassing op flexibele ACL's, Web Cache Communication Protocol (WCCP) en Cisco IOS-servertaakverdeling (SLB).**Opmerking:** Op Supervisor Engine 1 maken reflexive ACL's gebruik van dynamische TCAM-items om hardwaresnelheden te maken voor een bepaalde stroom. Het beginsel is hetzelfde: het eerste stroompakket gaat naar de software . Volgende pakketten voor die stroom zijn hardware-switched.

- Met de functie TCP-onderschepping worden de drie-richtingen handdruk en sessie afgesloten in software verwerkt. De rest van het verkeer wordt in hardware verwerkt.**Opmerking:** Synchronize (SYN), SYN Recognition (SYN ACK) en ACK-pakketten omvatten de drierichtingshanddruk. Sessiesluiting vindt plaats met beëindigen (FIN) of resetten (RST).
- Met Network Address Translation (NAT) wordt het verkeer op deze manier verwerkt:Op Supervisor Engine 720:Verkeer dat NAT nodig heeft, wordt na de eerste vertaling in hardware verwerkt. De omzetting van het eerste pakket van een stroom komt in software voor en de volgende pakketten voor die stroom zijn hardware-switched. Voor TCP-pakketten wordt er een hardware sneltoets gecreëerd in de NetFlow-tabel na voltooiing van de TCP-handdruk.Op Supervisor Engine 2 en Supervisor Engine 1:Al het verkeer dat NAT vereist is software-switched.
- Context-Based Access Control (CBAC) gebruikt NetFlow-sneltoetsen om verkeer te classificeren waarvoor inspectie nodig is. Dan stuurt CBAC alleen dit verkeer naar software. CBAC is een software-only functie; het verkeer dat aan inspectie wordt onderworpen is niet van hardware veranderd.**Opmerking:** verkeer dat aan inspectie is onderworpen, kan snelheidsbeperkt zijn op Supervisor Engine 720.

Multicastverkeer

- Protocol Independent Multicast (PIM)-snooping
- Internet Group Management Protocol (IGMP)-snooping (TTL = 1)Dit verkeer is inderdaad bestemd voor de router.
- Multicast Luistener Discovery (MLD)-snooping (TTL = 1)Dit verkeer is inderdaad bestemd voor de router.
- FIB MIS
- Multicastpakketten voor registratie die een directe verbinding met de multicast bron hebbenDeze multicast pakketten worden naar het renderende punt gekanaliseerd.
- IP, versie 6 (IPv6) multicast

Overige functies

- Network-Based Application Recognition (NBAR)
- ARP-inspectie, alleen met CatOS
- Poortbeveiliging, alleen met CatOS
- DHCP-snooping

IPv6-situaties

- Packet met een hop-by-hopoptie-header
- Packet met hetzelfde IPv6-adres als dat van routers
- Pakketten die niet voldoen aan de controle van het bereik
- Pakketten die de MTU van de uitvoerlink overschrijden
- Pakketten met een TTL dat minder dan of gelijk aan 1 is
- Packet met een input-VLAN dat gelijk is aan het uitvoerVLAN
- IPv6-uRPFSoftware voert deze uRPF uit voor alle pakketten.
- IPv6-reflexieve ACL’sSoftware verwerkt deze reflexive ACL’s.
- 6 tot 4 prefixes voor IPv6 automatische tunneladresseringsprotocol (ISATAP)-tunnelsSoftware

verwerkt deze tunneling. Al het andere verkeer dat een ISATAP-tunnel ingaat is hardware-switched.

LCP schema en DFC-module

In een Distributed Forwarding Card (DFC) is het `planningproces` van `DLP` dat op een hoge CPU wordt uitgevoerd geen probleem en vormt het geen probleem voor de werking. Het LCP-schema maakt deel uit van de firmware-code. Op alle modules die geen DFC vereisen, draait de firmware op een specifieke processor genaamd de LCP-lijnkaartprocessor. Deze processor wordt gebruikt om de ASIC hardware te programmeren en om te communiceren met de centrale toezichthouder module.

Wanneer het `lcp schema` wordt gestart, maakt het gebruik van alle beschikbare procestijd. Maar als een nieuw proces processortijd nodig heeft, bevrijdt `lcp schema` de procestijd voor het nieuwe proces. De prestaties van het systeem met betrekking tot dit hoge CPU-gebruik worden niet beïnvloed. Het proces grijpt simpelweg alle ongebruikte CPU-cycli in, zolang deze niet nodig zijn tijdens een proces met hogere prioriteit.

```
DFC#show process cpu

PID  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
```

Gemeenschappelijke oorzaken en oplossingen voor toepassingsproblemen met hoge CPU's

IP onbereikbaar

Wanneer een toegangsgroep een pakket ontkent, stuurt de MSFC onbereikbare berichten naar ICMP. Deze actie wordt standaard uitgevoerd.

Door standaard de **ip onbereikbare** opdracht in te schakelen, laat de Supervisor Engine de meeste ontkende pakketten in hardware vallen. Vervolgens stuurt de Supervisor Engine slechts een klein aantal pakketten, maximaal 10 pps, naar de MSFC voor een druppel. Deze actie genereert ICMP-onbereikbare berichten.

De daling van ontkende pakketten en de generatie van ICMP-onbereikbare berichten impliceert een lading aan de MSFC CPU. U kunt de **opdracht** voor het configureren van de interface niet

onbereikbaar maken om de lading te elimineren. Deze opdracht schakelt ICMP-onbereikbare berichten uit, waardoor de hardware van alle toegangsgroep-ontkende pakketten kan worden gewijzigd.

ICMP-onbereikbare berichten worden niet verzonden als een VACL een pakket ontkent.

NAT-omzetting

NAT gebruikt zowel hardware- als softwareverzending. De initiële vestiging van de NAT -vertalingen moet in software plaatsvinden en verder doorsturen gebeurt met hardware. NAT gebruikt ook de NetFlow-tabel (maximaal 128 KB). Daarom zal de switch, als de NetFlow-tabel vol is, ook NAT-transport via software gaan toepassen. Dit gebeurt normaal gesproken bij hoge verkeersopstoppingen en leidt tot een stijging van de CPU van 6500.

Gebruik van CEF FIB-tabelruimte in de tabel met Flow Cache

Supervisor Engine 1 heeft een Flow Cache-tabel die 128.000 items ondersteunt. Op basis van de efficiëntie van het hashing-algoritme variëren deze boekingen echter van 32.000 tot 120.000. Op Supervisor Engine 2 wordt de FIB-tabel gegenereerd en geprogrammeerd in de PFC. De tabel bevat niet minder dan 256.000 lemma's. De Supervisor Engine 720 met PFC3-BXL ondersteunt tot 1.000.000 items. Zodra deze ruimte is overschreden, worden de pakketten in de software geschakeld. Dit kan een hoog CPU-gebruik in de RP veroorzaken. Gebruik deze opdrachten om het aantal routes in de tabel van het CEF FIB te controleren:

```
Router#show processes cpu
CPU 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 Idle
2   2           245        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat
3   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 cef
Total L3 packets switched:           124893998234
Total L3 octets switched:          53019378962495
Total route entries:                       112579
  IP route entries:                        112578
  IPX route entries:                            1
  IPM route entries:                            0
IP load sharing entries:                      295
IPX load sharing entries:                       0
Forwarding entries:                        112521
Bridge entries:                                56
Drop entries:                                   2


IOS% show ip cef summary
IP 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, 86771426
inserts, 86658859
invalidations
  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
```

Op Supervisor Engine 2 vermindert het aantal FIB-items tot de helft als u RPF-controles op de interfaces hebt ingesteld. Deze configuratie kan leiden tot de softwareschakelaar van meer pakketten en bijgevolg tot een hoog CPU-gebruik.

Om de kwestie van het hoge gebruik van CPU op te lossen, dient u een routeswitchsamenvatting mogelijk te maken. Routesamenvatting kan de latentie in een complex netwerk minimaliseren door de werkbelasting van de processor, de geheugenvereisten en de vraag naar bandbreedte te verminderen.

Raadpleeg het begrip ACL op Catalyst 6500 Series-switches voor aanvullende informatie over TCAM-gebruik en -optimalisatie.

Geoptimaliseerde ACL-vastlegging

Geoptimaliseerde ACL Logging (OAL) biedt hardwareondersteuning voor ACL-vastlegging. Tenzij u OAL instelt, vindt het proces van pakketten die loggen vereisen volledig in software op MSFC3 plaats. OAL staat of laat pakketten in hardware op PFC3 vallen. OAL gebruikt een geoptimaliseerde routine om informatie naar MSFC3 te verzenden om de houtkap berichten te genereren.

Opmerking: Raadpleeg voor informatie over OAL de *Geoptimaliseerde ACL-vastlegging met een PFC3*-gedeelte van Cisco IOS ACL-ondersteuning.

Snelheidslimiet van pakketten naar de CPU

Op Supervisor Engine 720 kunnen snelheidsbeperkingen het tempo bepalen waarmee pakketten naar software kunnen gaan. Deze snelheidscontrole helpt aanvallen te voorkomen. U kunt ook een paar van deze snelheidslimiters op Supervisor Engine 2 gebruiken:

```
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      10
```

```
ICMP 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
```

Hierna volgt een voorbeeld:

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

Als u alle CEF-geponeerde pakketten naar de MSFC wilt beperken, geeft u de opdracht uit die in dit voorbeeld is:

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

Om het aantal pakketten dat op de CPU is geslagen te verminderen vanwege TTL=1, geeft u deze opdracht uit:

```
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.
```

Dit is bijvoorbeeld de output van de **nettoropname**, wat aantoont dat de IPv4 TTL 1 is:

```
Source mac     00.00.50.02.10.01  3644
Dest mac       AC.A0.16.0A.B0.C0  4092
Protocol       0800               4094
Interface      Gi1/8              3644
Source vlan    0x3FD(1021)        3644
Source index   0x7(7)             3644
Dest index     0x380(896)         3654

L3

ipv4 source    211.204.66.117      762
ipv4 dest      223.175.252.49     3815
ipv4 ttl                1     3656
ipv6 source             -        0
ipv6 dest               -        0
ipv6 hoplt              -        0
ipv6 flow               -        0
ipv6 nexthdr            -        0
```

Een hoge CPU kan ook worden veroorzaakt door pakketten met TTL=1 die naar de CPU worden uitgelekt. Om het aantal pakketten dat naar de CPU is uitgelekt te beperken, moet u een maximale hardwaresnelheid instellen. Snelheidslimiters kunnen pakketjes met een maximale snelheid meten die vanaf het hardwaregegevenspad zijn uitgelekt tot het softwaregegevenspad. Snelheidsbeperkingen beschermen het softwarebeheerpad tegen congestie door het verkeer te

laten vallen dat hoger is dan de ingestelde snelheid. De snelheidslimiet wordt ingesteld met de opdracht **MLS-snelheidslimiet voor** alle **fouten**.

Fysieke samenvoeging van VLAN's door onjuiste bekabeling

Een hoog CPU-gebruik kan ook resulteren uit de samenvoeging van twee of meer VLAN's door onjuiste bekabeling. Als STP ook is uitgeschakeld op die poorten waar de VLAN-fusie plaatsvindt, kan een hoog CPU-gebruik plaatsvinden.

Om dit probleem op te lossen, identificeer de bekabelde fouten en corrigeert u deze. Als uw vereisten dit toestaan, kunt u ook STP op die poorten inschakelen.

Broadcast Storm

Er komt een LAN-uitzendstorm voor wanneer uitzendingen of multicast pakketten het LAN overspoelen, dat excessief verkeer creëert en de netwerkprestaties nadelig beïnvloedt. De fouten in de protocol-stapel implementatie of in de netwerkconfiguratie kunnen een uitzending storm veroorzaken.

Vanwege het architecturale ontwerp van het Catalyst 6500 Series platform, worden de uitgezonden pakketten alleen en altijd op softwarerelease geworpen.

De suppressie van de omroep voorkomt de verstoring van LAN interfaces door een uitzending storm. De omroep gebruikt het filteren dat uitzendactiviteit op een LAN over een periode van 1 seconde meet en de meting met een vooraf bepaalde drempel vergelijkt. Indien de drempel wordt bereikt, wordt verdere uitzendactiviteit gedurende een bepaalde periode onderdrukt. De uitzending wordt standaard uitgeschakeld.

Opmerking: VRRP-flapping van back-up naar master veroorzaakt door uitzendstormen kan een hoog CPU-gebruik veroorzaken.

Raadpleeg voor informatie over hoe televisiesuppressie werkt en om de functie in te schakelen:

- Broadcast suppressie configureren (Cisco IOS-systeemsoftware)
- Broadcast suppressie configureren (CatOS-systeemsoftware)

BGP-scannerproces (Next-hop-Tracking)

Het BGP-scannerproces loopt de BGP-tabel en bevestigt de bereikbaarheid van de volgende hop. In dit proces wordt ook voorwaardelijke reclame gecontroleerd om te bepalen of BGP prefixes moet adverteren en/of routebedaarding moet uitvoeren. Standaard wordt het proces elke 60 seconden gescand.

U kunt een hoog CPU-gebruik verwachten voor korte duur vanwege het BGP-scannerproces op een router die een grote Internet-routingtabel draagt. Eén keer per minuut loopt de BGP-scanner op de BGP-tabel met routinginformatie (RIB) en voert u belangrijke onderhoudstaken uit. Deze taken omvatten:

- Een controle van de volgende hop die in de router BGP tabel van verwijzingen wordt voorzien
- Verificatie dat de volgende hopapparaten kunnen worden bereikt

Een grote BGP-tabel vergt dus evenveel tijd om te lopen en gevalideerd te worden. Het BGP-

scannerproces loopt de BGP-tabel om gegevensstructuren bij te werken en loopt de routingtabel voor routeherdistributie. Beide tabellen worden afzonderlijk in het routergeheugen opgeslagen. Beide tabellen kunnen zeer groot zijn en dus CPU-cycli gebruiken.

Raadpleeg voor meer informatie over het gebruik van CPU's door het BGP-scannerproces het gedeelte *Hoge CPU's door* de *BGP-scanner* van probleemoplossing bij een hoge CPU-functie die wordt veroorzaakt door het BGP-scanner of het BGP-routerproces.

Voor meer informatie over de BGP Next-Hopoptie Tracking en de procedure om het scaninterval in/uit te schakelen of aan te passen, raadpleegt u BGP-ondersteuning voor Next-Hopadrestracering.

Niet-RPF multicast verkeer

Multicast-routing (in tegenstelling tot unicast-routing) is alleen betrokken bij de bron van een bepaalde multicast gegevensstroom. Dat is, het IP adres van het apparaat dat het multicast verkeer voortbrengt. Het basisprincipe is dat het bronapparaat de stroom naar een niet gedefinieerd aantal ontvangers "duwt" (in zijn multicast groep). Alle multicast routers maken distributiebomen, die het pad bepalen dat multicast verkeer door het netwerk neemt om verkeer aan alle ontvangers te leveren. De twee basale types van multicast distributiebomen zijn bronbomen en gedeelde bomen. RPF is een essentieel concept in multicast verzenden. Het stelt routers in staat om multicast verkeer correct door te sturen naar de distributieboom. RPF maakt gebruik van de bestaande éénastroutingtabel om de upstream- en downstreamburen te bepalen. Een router stuurt een multicast pakket alleen door als dit op de upstream interface wordt ontvangen. Deze controle van RPF helpt te waarborgen dat de distributiepomp lus-vrij is.

Multicastverkeer is altijd zichtbaar door elke router op een aangesloten (Layer 2) LAN, volgens de specificatie IEEE 802.3 CSMA/CD. In de 802.3 standaard wordt bit 0 van de eerste octet gebruikt om een uitzending en/of multicast frame aan te geven en wordt elk Layer 2 frame met dit adres overstroomd. Dit is ook het geval, zelfs als CGMP of IGMP Snooping zijn ingesteld. Dit is omdat multicast routers het multicast verkeer moeten zien, als zij van een juiste transportbeslissing worden verwacht. Als meerdere multicast routers elk interfaces op een gemeenschappelijk LAN hebben, stuurt slechts één router de gegevens door (geselecteerd door een verkiezingsproces). Vanwege de overstroomende aard van LAN's ontvangt de redundante router (router die het multicast-verkeer niet verzenden) deze gegevens op de uitgaande interface voor dat LAN. De redundante router daalt normaal dit verkeer omdat het op de verkeerde interface is aangekomen en derhalve de RPF-controle faalt. Dit verkeer dat de controle van RPF faalt wordt genoemd niet-RPF verkeer of de mislukkingspakketten van RPF, omdat zij terug tegen de stroom van de bron zijn verzonden.

Catalyst 6500 met een MSFC geïnstalleerd, kan worden geconfigureerd om als volledige multicast router te fungeren. Gebruikmakend van Multicast Multi-Layer Switching (MMLS) wordt het RPF-verkeer doorgaans door de hardware binnen de schakelaar doorgestuurd. ASIC's krijgen informatie van de multicast routing state (bijvoorbeeld (*,G) en (S,G)), zodat een hardwaresneltoets kan worden geprogrammeerd in de NetFlow- en/of FIB-tabel. Dit niet-RPF-verkeer is in sommige gevallen nog steeds nodig en wordt door de MSFC CPU (op procesniveau) vereist voor het PIM-testmechanisme. Anders wordt deze knop vervolgens laten vallen door de software fast-switching route (ervan wordt uitgegaan dat de software fast-switching niet uitgeschakeld is op de RPF-interface).

Catalyst 6500 dat overtolligheid gebruikt zou niet efficiënt het niet-RPF verkeer in bepaalde topologieën kunnen behandelen. Voor niet-RPF verkeer is er gewoonlijk geen (*,G) of (S,G) staat

in de overtollige router en daarom kunnen geen hardware of software sneltoetsen worden gecreëerd om het pakket te laten vallen. Elk multicast pakket moet afzonderlijk door de MSFC-routeprocessor worden onderzocht en dit wordt vaak CPU-interrupte verkeer genoemd. Dankzij Layer 3 hardware-switching en meerdere interfaces/VLAN's die dezelfde reeks routers verbinden, wordt het niet-RPF-verkeer dat de CPU van de redundante MSFC bereikt, "N" maal de oorspronkelijke bronsnelheid (waarbij "N" het aantal LAN's is waarmee de router redundante verbinding heeft) vergroot. Als het percentage niet-RPF-verkeer de capaciteit van het pakje van het systeem overschrijdt, kan dit een hoog CPU-gebruik, bufferoverstromen en algehele netwerkinstabiliteit veroorzaken.

Met Catalyst 6500, is er een motor van de toegangslijst die het filteren bij draadsnelheid toelaat. Deze functie kan in bepaalde situaties worden gebruikt om niet-PDF-verkeer voor groepen met de spaarstand efficiënt af te handelen. U kunt de op ACL gebaseerde methode alleen gebruiken binnen de "stub netwerken" van de sparse-modus, waar er geen downstreamrouters voor multicast zijn (en bijbehorende ontvangers). Bovendien, wegens het pakket het door verzenden ontwerp van Catalyst 6500, kunnen intern overtollige MSFCs deze implementatie niet gebruiken. Dit wordt geschetst in Cisco bug-ID CSCdr74908 (alleen geregistreerde klanten). Voor dichte-mode groepen, moeten de niet-RPF pakketten op de router worden gezien zodat het mechanisme van de Toewijzing PIM goed functioneert. Verschillende oplossingen, zoals CEF of NetFlow-gebaseerde snelheidsbeperking en QoS worden gebruikt om de tekortkomingen van RPF te beheersen in dichte-mode netwerken en doorvoernetwerken in de spaarstand.

Op Catalyst 6500 is er een toegangslijstmotor die het filteren met draadsnelheid toelaat. Deze functie kan worden gebruikt om niet-RPF-verkeer voor groepen met de spaarstand efficiënt aan te pakken. Om deze oplossing te implementeren plaatst u een toegangslijst op de inkomende interface van het "Stub netwerk" om multicast verkeer te filteren dat niet van het "Stub netwerk" is voortgekomen. De toegangslijst is naar beneden geduwd naar de hardware in de schakelaar. Deze toegangslijst voorkomt dat de CPU het pakket ooit ziet en stelt de hardware in staat het niet-RPF-verkeer te laten vallen.

N.B.: Plaats deze toegangslijst niet op een transitinterface. Het is uitsluitend bedoeld voor staafnetwerken (netwerken met alleen hosts).

Raadpleeg deze documenten voor meer informatie:

- Redundant routerprobleem met IP-multicast in Stub-netwerken
- Niet-RPF traffic shaping

Opdrachten tonen

Het CPU-gebruik bij het uitgeven van een showopdracht is altijd bijna 100%. Het is normaal een hoog CPU-gebruik te hebben wanneer u een toonopdracht geeft en deze meestal slechts enkele seconden blijft gebruiken.

Bijvoorbeeld, het is normaal voor het Virtual Exec-proces om hoog te gaan wanneer u een **show tech-support** opdracht geeft aangezien deze uitvoer een onderbroken gedreven uitvoer is. Uw enige probleem met hoge CPU in andere processen dan **tonen** opdrachten.

De **opdracht Show cef-cef-switched opdracht toont aan waarom pakketten worden gestraft naar MSFC (ontvang, ip optie, geen nabijheid, enz.) en hoeveel.** Bijvoorbeeld:

```
Switch#show cef not-cef-switched
CEF Packets passed on to next switching layer
Slot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     Frag
RP      6222       0         136        0    60122        0        0        0
5          0       0           0        0        0        0        0        0
IPv6 CEF Packets passed on to next switching layer
Slot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTU
RP         0       0           0        0        0        0        0        0
```

De **korte** opdrachten **tonen ibc** en **tonen ibc** de CPU-wachtrij en kunnen worden gebruikt wanneer u de CPU-status controleert.

Exec-processen

Het Exec-proces in Cisco IOS-software is verantwoordelijk voor communicatie op de TTY-lijnen (console, hulpmodule, asynchrone) van de router. Het Virtual Exec-proces is verantwoordelijk voor de VTY-lijnen (Telnet-sessies). De Exec- en Virtual Exec-processen zijn processen met een middelhoge prioriteit, zodat als er andere processen zijn met een hogere prioriteit (Hoog of Kritisch), de hogere prioriteitsprocessen de CPU-middelen krijgen.

Als er veel gegevens door deze sessies worden overgebracht, wordt het CPU-gebruik voor het Exec-proces verhoogd. Dit komt doordat de router wanneer de router een eenvoudig teken door deze lijnen wil verzenden, de router een aantal CPU-bronnen gebruikt:

- Voor de console (EXec) gebruikt de router één interruptie per teken.
- Voor de VTY-lijn (Virtual Exec) moet de Telnet-sessie één TCP-pakket per teken bouwen.

In deze lijst worden enkele redenen genoemd voor een hoog CPU-gebruik in het Exec-proces:

- **Er worden teveel gegevens verzonden door de console poort.**Controleer om of om het even welke details op de router met het **tonen** **het** bevel **van het** **zuiveren zijn begonnen**.Maak console-houtkap op de router **uit zonder** vorm van de **opdracht** van de **logconsole**.Controleer of er een lange uitvoer op de console is afgedrukt. Bijvoorbeeld, een **show tech-support** of een **show memory** **opdracht.**
- **De exec-opdracht is ingesteld voor asynchrone en hulplijnen.**Als een regel alleen uitgaande verkeer heeft, schakelt u het OOG-proces voor deze regel uit. Dit komt doordat als het apparaat (bijvoorbeeld een modem) dat aan deze lijn is gekoppeld ongevraagde gegevens verstuurt, het Exec-proces op deze lijn start.Als de router als eindserver (voor omgekeerd telnet naar andere apparatenconsoles) wordt gebruikt, wordt het aanbevolen dat u de **geen** exec opdracht op de lijnen vormt die op de console van de andere apparaten worden aangesloten. Data dat uit de console komt zou anders een Exec-proces kunnen starten, dat CPU-bronnen gebruikt.

Een mogelijke reden voor gebruik van een hoge CPU in het Virtual Exec-proces is:

- **Er wordt te veel gegevens verzonden over de Telnet-sessies.**De meest algemene reden voor het gebruik van hoge CPU in het Virtual Exec-proces is dat te veel gegevens van de router naar de Telnet-sessie worden overgebracht. Dit kan gebeuren wanneer opdrachten met lange uitgangen, zoals **tonen technologie-ondersteuning**, **het geheugen tonen**, enzovoort, vanaf de Telnet-sessie worden uitgevoerd. De hoeveelheid gegevens die door elke VTY-sessie wordt overgedragen kan met de **show tcp vty** ***<line number>***-opdracht worden geverifieerd.

L3 verouderingsproces

Wanneer het L3-verouderingsproces een groot aantal indexwaarden exporteert met NetFlow Data Export (NDE), kan het CPU-gebruik 100% bereiken.

Als u dit probleem tegenkomt, controleer of deze twee opdrachten zijn ingeschakeld:

```
set mls nde destination-ifindex enable

set mls nde source-ifindex enable
```

Als u deze opdrachten activeert, moet het proces alle doelwaarden en bronindexwaarden exporteren met behulp van NDE. Het L3 verouderingsproces gaat hoog omdat het FIB raadpleging moet uitvoeren voor alle bestemming en bron *ifindex* waarden. Hierdoor wordt de tabel vol, het L3-verouderingsproces is hoog en het CPU-gebruik bereikt 100%.

Schakel deze opdrachten uit om dit probleem op te lossen:

```
set mls nde destination-ifindex disable

set mls nde source-ifindex disable
```

Gebruik deze opdrachten om de waarden te controleren:

- toon mls cef samenvatting
- mls cef-maximumroutes tonen

BPDU Storm

Spanning tree behoudt een lijn-vrije Layer 2-omgeving in redundante geschakelde en bruggen netwerken. Zonder STP vermenigvuldigen frames en/of voor onbepaalde tijd. Dit voorval veroorzaakt een netwerkmeltdown omdat het hoge verkeer alle apparaten in het uitgezonden domein onderbreekt.

In sommige opzichten is STP een vroeg protocol dat aanvankelijk was ontwikkeld voor langzaam software-gebaseerde bridge specificaties (IEEE 802.1D), maar STP kan gecompliceerd zijn om het succesvol te implementeren in grote geschakelde netwerken die deze functies hebben:

- Veel VLAN’s
- Veel switches in een STP-domein
- Ondersteuning voor meerdere leveranciers
- Nieuwe IEEE-verbeteringen

Als het netwerk vaak wordt gescand met boomberekeningen of de switch meer BPDU's moet verwerken, kan dit resulteren in een hoge CPU, evenals BPDU-druppels.

Voer een of alle van deze stappen uit om aan deze problemen te werken:

1. Trek de VLAN's van de switches af.
2. Gebruik een verbeterde versie van STP, zoals MST.
3. Upgradeer de hardware van de switch.

Raadpleeg ook best practices om Spanning Tree Protocol in het netwerk te implementeren.

- Best Practices voor Catalyst 4500/4000, 5500/5000 en 6500/6000 Series-switches met

CatOS-configuratie en -beheer
- Best Practices voor Catalyst 6500/6000 Series en Catalyst 4500/4000 Series-switches die Cisco IOS-software uitvoeren

SPAN-sessies

Op basis van de architectuur van Catalyst 6000/6500 Series switches hebben SPAN-sessies geen invloed op de prestaties van de switch, maar als de SPAN-sessie een hoge verkeers-/uplinks- of EtherChannel-poort bevat, kan deze de lading op de processor verhogen. Als het dan een specifiek VLAN uitdeelt, verhoogt het de werklast zelfs nog meer. Als er slecht verkeer op de link is, kan dat de werklast verder vergroten.

In sommige scenario's kan de functie RSPAN loops veroorzaken, en de lading op de processor schiet omhoog. Raadpleeg voor meer informatie waarom de SPAN-sessie een overbruggingslijn creëert?

De switch kan zoals gebruikelijk verkeer doorgeven aangezien alles in hardware zit, maar de CPU kan een slag maken als zij probeert te achterhalen welk verkeer zij moet doorsturen. Aanbevolen wordt om alleen SPAN-sessies te configureren als dit nodig is.

%CFIB-SP-STBY-7-CFIB_EXCEPTION: FIB TCAM-uitzondering; sommige items worden door software geschakeld

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

Deze foutmelding wordt ontvangen wanneer de hoeveelheid beschikbare ruimte in de TCAM is overschreden. Dit leidt tot een hoge CPU. Dit is een FIB TCAM-beperking. Zodra TCAM vol is, wordt een vlag ingesteld en wordt een FIB TCAM-uitzondering ontvangen. Dit houdt op nieuwe routes aan de TCAM toe te voegen. Daarom zal alles software zijn geschakeld. Het verwijderen van routes helpt niet de hardware-switching te hervatten. Zodra de TCAM de uitzonderingsstaat ingaat moet het systeem opnieuw geladen worden om uit die staat te geraken. De maximum routes die in TCAM kunnen worden geïnstalleerd worden verhoogd door de **maximum-routes** opdracht **van het** cef.

Catalyst 6500/6000 die met een hoge CPU wordt uitgevoerd, heeft een IPv6 ACL met L4-poorten

Laat **mls** ipv6 acl compress unicast**.** Deze opdracht is nodig als IPv6 ACL wordt aangepast op L4 protocol poortnummers. Als deze opdracht niet is ingeschakeld, wordt IPv6-verkeer naar de CPU voor softwareverwerking geleid. Deze opdracht is standaard niet ingesteld.

koper SFP's

In Cisco ME 6500 Series Ethernet-switches vereist koper SFP's meer firmware-interactie dan andere typen SFP's, waardoor het CPU-gebruik wordt verhoogd.

De software algoritmen die koper SFPs beheren zijn verbeterd in de Cisco IOS SXH releases.

modulair IOS

In Cisco Catalyst 6500 Series-switches die modulaire IOS-software gebruiken, is het normale CPU-gebruik iets groter dan niet-modulaire IOS-software.

Modulaire IOS-software betaalt een prijs per activiteit die hoger is dan de prijs per pakket. De modulaire IOS-software onderhoudt de processen door bepaalde CPU's te gebruiken zelfs wanneer er niet veel pakketten zijn, zodat het CPU-verbruik niet op het werkelijke verkeer is gebaseerd. Wanneer pakketten echter met een hoge snelheid worden verwerkt, mag de CPU die in modulaire IOS-software wordt verbruikt, niet hoger zijn dan die in niet-modulaire IOS-software.

Gebruik van CPU's controleren

Als het CPU-gebruik hoog is, geeft u eerst de opdracht **Cpu-processen** tonen. De uitvoer toont u het CPU-gebruik op de switch evenals het CPU-verbruik per proces.

```
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.
```

In deze uitvoer is het totale CPU-gebruik 57% en is het onderbreken van het CPU-gebruik 48%. Hier worden deze percentages weergegeven in de vet-tekst. De onderbreking van de schakelaar van het verkeer door de CPU veroorzaakt het onderbreken van het gebruik van CPU. De opdrachtoutput toont de processen die het verschil tussen de twee toepassingen veroorzaken. In dit geval is de oorzaak het SNMP-proces.

Op de Supervisor Engine die CatOS draait, ziet de output er zo uit:

```
Switch> (enable) show processes cpu


CPU 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 Idle
2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat
3   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
```

In deze uitvoer is het eerste proces `Kernel en Idle`, die het gebruik van inactieve CPU's toont. Dit proces is normaal gesproken hoog, tenzij bepaalde andere processen CPU-cycli gebruiken. In dit voorbeeld veroorzaakt het `SptBPduRx`-proces een hoog CPU-gebruik.

Als het CPU-gebruik hoog is door een van deze processen, kunt u problemen oplossen en bepalen waarom dit proces hoog verloopt. Maar als de CPU hoog is door verkeer dat wordt gestraft naar de CPU, dient u te bepalen waarom het verkeer wordt bestraft. Deze vastberadenheid kan u helpen te identificeren wat het verkeer is.

Gebruik voor het oplossen van problemen dit EEM-script voorbeeld om de uitvoer van de switch te verzamelen wanneer u een hoog CPU-gebruik ervaart:

```
event manager applet cpu_stats

event snmp oid "1.3.6.1.4.1.9.9.109.1.1.1.1.3.1" get-type exact entry-op gt entry-val "70"

exit-op lt exit-val "50" poll-interval 5

action 1.01 syslog msg "------HIGH CPU DETECTED----, CPU:$_snmp_oid_val%"

action 1.02 cli command "enable"

action 1.03 cli command "show clock | append disk0:cpu_stats"

action 1.04 cli command "show proc cpu sort | append disk0:cpu_stats"

action 1.05 cli command "Show proc cpu | exc 0.00% | append disk0:cpu_stats"

action 1.06 cli command "Show proc cpu history | append disk0:cpu_stats"

action 1.07 cli command "show logging | append disk0:cpu_stats "

action 1.08 cli command "show spanning-tree detail | in ieee|occurr|from|is exec | append
disk0:cpu_stats"

action 1.09 cli command "debug netdr cap rx | append disk0:cpu_stats"

action 1.10 cli command "show netdr cap | append disk0:cpu_stats"

action 1.11 cli command "undebug all"
!
```

Opmerking: de opdracht **Opnemen van netwerk** is behulpzaam wanneer de CPU hoog is door verwerkingsoverschakeling van pakketten in plaats van hardware. Hiermee neemt u 4096 pakketten op die naar de CPU zijn binnengebracht wanneer de opdracht wordt uitgevoerd. Deze opdracht is volledig veilig en is het meest handige gereedschap voor hoge CPU-problemen op de 6500. Dit levert geen extra belasting op de CPU's op.

Hulpprogramma's en tools om het verkeer te bepalen dat naar de CPU's wordt gericht

Deze sectie identificeert een aantal hulpprogramma's en tools die u kunnen helpen om naar dit verkeer te kijken.

Cisco IOS-systeemsoftware

In Cisco IOS Software wordt de schakelaar processor op de Supervisor Engine de SP genoemd en MSFC wordt RP genoemd.

De opdracht interface tonen geeft basisinformatie over de status van de interface en de

verkeerssnelheid op de interface. De opdracht biedt ook fouttellers.

```
Router#show interface gigabitethernet 4/1
GigabitEthernet4/1 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
```

In deze uitvoer kunt u zien dat het inkomende verkeer Layer 3-switched is in plaats van Layer 2-switched. Dit geeft aan dat het verkeer naar de CPU is gericht.

De opdracht **Laat** uitvoeren **processen** uitvoeren vertelt u of deze pakketten gewone verkeerspakketten zijn of controlepakketten.

```
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
```

Als de pakketten correct zijn geschakeld, ziet u dat het `IP-ingangsproces` hoog wordt. Geef deze opdracht uit om deze pakketten te zien:

[ingangsinterface voor buffers weergeven]

```
Router#show buffers input-interface gigabitethernet 4/1 packet

Buffer 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 63

08060F70:                       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
```

Als het verkeer **verstopt** is, kunt u die pakketten niet zien met de opdracht **Invoerinterface-**buffers **tonen**. Om de pakketten te zien die aan RP voor interrupte omschakeling worden gestraft kunt u een Switched Port Analyzer (SPAN) vangst van de haven van RP uitvoeren.

N.B.: Raadpleeg dit document voor aanvullende informatie over verstopt-switched versus gebruik van CPU's:

- *Gebruik van hoge CPU's door* onderbreking van het gedeelte Problemen oplossen bij gebruik van hoge CPU's op Cisco-routers

SPAN RP-Inband en SP-band

Een SPAN voor de RP of SP poort in Cisco IOS-software is beschikbaar in Cisco IOS-softwarerelease 12.1(19)E en later.

Dit is de opdrachtsyntaxis:

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

Gebruik deze syntaxis voor de Cisco IOS-softwarereleases 12.2 SX:

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

N.B.: Voor de SXH-release moet u de opdracht **Beeldsessie** gebruiken om een lokale SPAN-sessie te configureren en deze opdracht gebruiken om de SPAN-sessie met de CPU te associëren:

```
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]
```

N.B.: Raadpleeg voor meer informatie over deze opdrachten de installatie van Local SPAN (SPAN Configuration Mode) in de *Catalyst 6500 release 12.2SX-softwareconfiguratiegids*.

Hier is een voorbeeld op een RP-console:

```
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
```

Ga nu naar de SP-console. Hierna volgt een voorbeeld:

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

Opmerking: In Cisco IOS 12.2 SX releases is de opdracht gewijzigd in **testmonitor add 1 rp-inband rx**.

```
Router#show monitor
Session 1
---------
Type : Local Session
Source Ports :
Both : Fa3/3
Destination Ports : Fa3/2
SP console:
Router-sp#test monitor session 1 show
Ingress 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
```

Opmerking: In Cisco IOS 12.2 SX releases is de opdracht gewijzigd in **testmonitor show 1**.

Hier is een voorbeeld op een SP-console:

```
Router-sp#test monitor session 1 show
Ingress 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
```

CatOS-systeemsoftware

Voor switches die CatOS-systeemsoftware gebruiken, voert de Supervisor Engine CatOS in en MSFC voert Cisco IOS-software uit.

Als u de opdracht **show mac** geeft, kunt u het aantal frames zien dat naar de MSFC wordt gestraft. Port 15/1 is de Supervisor Engine verbinding met de MSFC.

Opmerking: de poort is 16/1 voor superieurmotoren in sleuf 2.

```
Console> (enable) show mac 15/1

Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
15/1                  193576                    0                    1
```

```
Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
15/1                       3                    0                    0

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
15/1                18583370                    0

MAC      Dely-Exced MTU-Exced  In-Discard Out-Discard
-------- ---------- ---------- ---------- -----------
15/1              0          -          0           0
```

Een snelle toename van dit nummer duidt erop dat de pakketten worden gestraft naar de MSFC, wat een hoog CPU-gebruik veroorzaakt. U kunt de pakketten vervolgens op de volgende manieren bekijken:

- SPAN MSFC-poort 15/1 of 16/1
- SPAN sc0

SPAN MSFC-poort 15/1 of 16/1

Stel een SPAN-sessie in waarin de bron de MSFC-poort 15/1 (of 16/1) is en de bestemming een Ethernet-poort is.

Hierna volgt een voorbeeld:

```
Console> (enable) set span 15/1 5/10
Console> (enable) show span

Destination     : Port 5/10
Admin Source    : Port 15/1
Oper Source     : None
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active
```

Als u een snuffelspoor op poort 5/10 verzamelt, toont het snuffelspoor pakketten die naar en van de MSFC verzenden. Configureer de SPAN-sessie als **tx** om pakketten op te nemen die alleen bestemd zijn voor de MSFC en niet voor de MSFC.

SPAN sc0

Stel een SPAN-sessie in met de **sc0-**interface als de bron om frames op te nemen die naar de Supervisor Engine CPU gaan.

```
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
```

Opmerking: voor optische servicesmodules (OSM's) kunt u geen SPAN-opname van verkeer uitvoeren.

Aanbevelingen

Het gebruik van de toezichthouder op de cpu-motor geeft niet de hardware-verzendprestaties van de switch weer. Toch moet u de uitgangswaarde van de surveillancemotor en het gebruik van de CPU-motor controleren.

1. Stel het gebruik van de surveillancemotor CPU voor de schakelaar in een"steady-state"-netwerk met normale verkeerspatronen en -belasting in.N.B. welke processen het hoogste CPU-gebruik genereren.
2. Wanneer u CPU-gebruik voor probleemoplossing gebruikt, dient u deze vragen na te denken:Welke processen genereren het hoogste verbruik? Zijn deze processen anders dan uw uitgangssituatie?Is de CPU consequent verhoogd ten opzichte van de uitgangssituatie? Of zijn er pieken van een hoog gebruik, en dan een terugkeer naar de uitgangsniveaus?Zijn er in het netwerk meldingen van wijziging van de topologie (TCN's)?**Opmerking:** Afvlakkende poorten of host-poorten met STP PortFast Disease **TCN**'s.Is er buitensporig uitzending of multicast verkeer in de beheerssubnetten/VLAN?Is er overdreven beheerverkeer, zoals SNMP-opiniepeiling, op de switch?
3. Gedurende de tijd van hoge CPU (wanneer de CPU 75% of hoger is) dient u de uitvoer van deze opdrachten te verzamelen:toonklokshow versiontoon processen gesorteerd cpuproc cpu - geschiedenistoonlogboek
4. Als mogelijk, isoleer het beheer VLAN van VLANs met gebruikersgegevensverkeer, in het bijzonder zwaar uitgezonden verkeer.De voorbeelden van dit type verkeer zijn IPX RIP/Service Advertisation Protocol (SAP), AppleTalk, en ander uitzendverkeer. Dit verkeer kan van invloed zijn op het gebruik van de surveillancemotor CPU en kan in extreme gevallen de normale werking van de schakelaar verstoren.
5. Als de CPU hoog draait vanwege het punt van verkeer naar de RP, bepalen wat dat verkeer is en waarom het verkeer wordt gepunteerd.Om deze bepaling te maken, gebruik de hulpprogramma's die de hulpprogramma's en tools gebruiken om het verkeer te bepalen dat aan het CPU-gedeelte wordt gepunteerd.

Gerelateerde informatie

- Handige opdrachten voor het oplossen van problemen met een hoge CPU op Catalyst 6500's met Sup720
- Common CatOS-foutmeldingen op Catalyst 6000/6500 Series-switches
- Gemeenschappelijke foutmeldingen op Catalyst 6500/6000 Series-switches die Cisco IOS-software uitvoeren
- Probleemoplossing voor hardware en gebruikelijke problemen op Catalyst 6500/6000 Series-switches die Cisco IOS-systeemsoftware uitvoeren
- Unicast overstromingen in Switched Campus Networks
- Cisco Catalyst 6500 Series-switches - productondersteuning
- EEM-scripts voor het verzamelen van gegevens tijdens een intermitterende hoge CPU-emissie
- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems