Utilizzo elevato della CPU dello switch Catalyst 6500/6000

Sommario

Introduzione

In questo documento vengono descritte le cause dell'elevato utilizzo della CPU sugli switch Cisco Catalyst serie 6500/6000 e sui sistemi basati su Virtual Switching System (VSS) 1440. Come i router Cisco, gli switch usano il comando **show processes cpu** per visualizzare l'utilizzo della CPU da parte del processore del supervisor engine dello switch. Tuttavia, a causa delle differenze nell'architettura e nei meccanismi di inoltro tra i router e gli switch Cisco, l'output tipico del comando **show PROCESSES cpu** differisce in modo significativo. Anche il significato dell'output è diverso. Questo documento chiarisce queste differenze e descrive l'utilizzo della CPU sugli switch e come interpretare l'output del comando **show PROCESSES cpu**.

Nota: in questo documento, i termini "switch" e "switch" si riferiscono agli switch Catalyst 6500/6000.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, sono state usate le versioni software e hardware degli switch Catalyst 6500/6000 e dei sistemi basati su Virtual Switching System (VSS) 1440.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nota: il software supportato dai sistemi basati su Virtual Switching System (VSS) 1440 è il software Cisco IOS® versione 12.2(33)SXH1 o successive.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Differenza tra i software di sistema CatOS e Cisco IOS

Catalyst OS (CatOs) su Supervisor Engine e software Cisco IOS® su modulo Multilayer Switch

Feature Card (MSFC) (ibrido): È possibile usare un'immagine CatOS come software di sistema per eseguire supervisor engine sugli switch Catalyst 6500/6000. Se è installato l'MSFC opzionale, usare un'immagine del software Cisco IOS separata.

Software Cisco IOS su Supervisor Engine e su MSFC (nativo): È possibile usare un'unica immagine software Cisco IOS come software di sistema per eseguire sia il supervisor engine sia l'MSFC sugli switch Catalyst 6500/6000.

Nota: per ulteriori informazioni, fare riferimento a Confronto tra i sistemi operativi Cisco Catalyst e Cisco IOS per gli switch Cisco Catalyst serie 6500.

Comprensione dell'utilizzo della CPU sugli switch Catalyst 6500/6000

I router basati su software Cisco utilizzano il software per elaborare e instradare i pacchetti. L'utilizzo della CPU su un router Cisco tende ad aumentare quando il router esegue una maggiore elaborazione e routing dei pacchetti. Di conseguenza, il comando **show processes cpu** può fornire un'indicazione abbastanza precisa del carico di elaborazione del traffico sul router.

Gli switch Catalyst 6500/6000 non usano la CPU allo stesso modo. Questi switch prendono le decisioni relative all'inoltro nell'hardware, non nel software. Pertanto, quando gli switch prendono la decisione di inoltro o commutazione per la maggior parte dei frame che passano attraverso lo switch, il processo non coinvolge la CPU del supervisor engine.

Sugli switch Catalyst 6500/6000, sono disponibili due CPU. Una CPU è la CPU del Supervisor Engine, denominata NMP (Network Management Processor) o SP (Switch Processor). L'altra CPU è la CPU del motore di routing di layer 3, denominata MSFC o Route Processor (RP).

La CPU dello Storage Processor esegue le seguenti funzioni:

- Assistenza nell'apprendimento e nell'invecchiamento degli indirizzi MAC**Nota:** l'apprendimento dell'indirizzo MAC è anche chiamato impostazione del percorso.
- Esegue protocolli e processi che forniscono il controllo della reteGli esempi includono Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP) e Port Aggregation Protocol (PAgP).
- Gestisce il traffico di gestione della rete destinato alla CPU dello switchGli esempi includono il traffico Telnet, HTTP e SNMP (Simple Network Management Protocol).

La CPU RP esegue le seguenti funzioni:

- Crea e aggiorna le tabelle ARP (Address Resolution Protocol) e routing di layer 3
- Genera il file FIB (Forwarding Information Base) e le tabelle adiacenti di Cisco Express Forwarding (CEF) e le scarica nella Policy Feature Card (PFC)
- Gestisce il traffico di gestione della rete destinato all'RPGli esempi includono il traffico Telnet, HTTP e SNMP.

Situazioni e funzionalità che attivano il traffico per il software

Pacchetti destinati allo switch

Tutti i pacchetti destinati allo switch vengono inviati al software. Tali pacchetti includono:

- Pacchetti di controllol pacchetti di controllo vengono ricevuti per STP, CDP, VTP, HSRP (Hot Standby Router Protocol), PAgP, LACP (Link Aggregation Control Protocol) e UDLD (UniDirectional Link Detection).
- Aggiornamenti del protocollo di routingEsempi di questi protocolli sono il Routing Information Protocol (RIP), il Enhanced Interior Gateway Routing Protocol (EIGRP), il Border Gateway Protocol (BGP) e il Open Shortest Path First Protocol (protocollo OSPF).
- Traffico SNMP destinato allo switch
- Traffico Telnet e Secure Shell Protocol (SSH) verso lo switch.L'elevata utilizzazione della CPU dovuta a SSH è considerata come segue:

```
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
```

  Includere questi comandi nello script EEM per verificare il numero di sessioni SSH stabilite quando la CPU diventa alta:mostra utentimostra riga
- Risposte ARP a richieste ARP

Pacchetti e condizioni che richiedono un'elaborazione speciale

L'elenco fornisce tipi di pacchetti specifici e condizioni che forzano la gestione dei pacchetti nel software:

- Pacchetti con opzioni IP, TTL (Time to Live) scaduto o incapsulamento ARPA (non Advanced Research Projects Agency)
- Pacchetti con gestione speciale, come il tunneling
- Frammentazione IP
- Pacchetti che richiedono messaggi ICMP (Internet Control Message Protocol) dall'RP o dall'SP
- Controllo MTU (Maximum Transmission Unit) non riuscito
- Pacchetti con errori IP, che includono errori di lunghezza e checksum IP
- Se i pacchetti di input restituiscono un errore di bit (ad esempio, l'errore di bit singolo (SBE)), i pacchetti vengono inviati alla CPU per l'elaborazione del software e corretti. Il sistema alloca un buffer e utilizza la risorsa CPU per correggerlo.
- Quando il PBR e l'elenco degli accessi riflessivi si trovano nel percorso di un flusso di traffico, il pacchetto viene commutato dal software, il che richiede un ciclo di CPU aggiuntivo.
- Adiacente stessa interfaccia
- Pacchetti che non superano il controllo Reverse Path Forwarding (RPF) - **rpf-failure**
- Glean/receiveIl termine "glean" si riferisce ai pacchetti che richiedono la risoluzione ARP, mentre il termine "receive" si riferisce ai pacchetti che rientrano nella richiesta di ricezione.
- Traffico Internetwork Packet Exchange (IPX) commutato tramite software sul Supervisor Engine 720 sia nel software Cisco IOS che in CatOSIl traffico IPX viene anche commutato via software sul software Supervisor Engine 2/Cisco IOS, ma il traffico viene commutato via hardware sul Supervisor Engine 2/CatOS. Il traffico IPX viene commutato hardware sul Supervisor Engine 1A per entrambi i sistemi operativi.

- Traffico AppleTalk
- Condizioni complete delle risorse hardwareQueste risorse includono FIB, Content-Addressable Memory (CAM) e Ternary CAM (TCAM).

Funzioni basate sugli ACL

- Traffico negato tramite ACL (Access Control List) con la funzionalità ICMP "destinazione irraggiungibile" attivata**Nota:** questa è l'impostazione predefinita.Se sono abilitati i pacchetti IP non raggiungibili, alcuni pacchetti ACL negati vengono trasmessi all'MSFC. I pacchetti che richiedono pacchetti ICMP non raggiungibili vengono persi a una velocità configurabile dall'utente. Per impostazione predefinita, la velocità è di 500 pacchetti al secondo (pps).
- Filtraggio IPX sulla base di parametri non supportati, ad esempio l'host di origineSul Supervisor Engine 720, il processo del traffico IPX di layer 3 è sempre nel software.
- Voci di controllo di accesso (ACE) che richiedono la registrazione, con la parola chiave **log**Ciò è valido per le funzionalità di registro degli ACL e degli ACL VLAN (VACL). Le voci di controllo di accesso nello stesso ACL che non richiedono la registrazione vengono comunque elaborate nell'hardware. Supervisor Engine 720 con PFC3 supporta il limite di velocità dei pacchetti reindirizzati all'MSFC per la registrazione di ACL e VACL. Supervisor Engine 2 supporta il limite di velocità dei pacchetti reindirizzati all'MSFC per la registrazione dei pacchetti VACL. Il supporto della registrazione ACL sul Supervisor Engine 2 è pianificato per la versione software Cisco IOS 12.2S.
- Traffico instradato tramite criteri, con **lunghezza** della **corrispondenza**, **impostazione della precedenza IP** o altri parametri non supportatiIl parametro **set interface** è supportato nel software. Tuttavia, il parametro **set interface null 0** è un'eccezione. Questo traffico viene gestito nell'hardware sul Supervisor Engine 2 con PFC2 e sul Supervisor Engine 720 con PFC3.
- ACL (RACL) router non IP e non IPXGli ACL non IP si applicano a tutti i supervisor engine. Gli ACL non IPX si applicano solo al Supervisor Engine 1a con PFC e al Supervisor Engine 2 con PFC2.
- Traffico broadcast negato in un RACL
- Traffico negato in un controllo unicast RPF (uRPF), ACL ACEQuesto controllo uRPF si applica al Supervisor Engine 2 con PFC2 e al Supervisor Engine 720 con PFC3.
- Proxy di autenticazioneIl traffico soggetto al proxy di autenticazione può essere limitato alla velocità sul Supervisor Engine 720.
- Software Cisco IOS IP Security (IPsec)Il traffico soggetto alla crittografia Cisco IOS può essere limitato alla velocità sul Supervisor Engine 720.

Funzioni basate su NetFlow

Le funzionalità basate su NetFlow descritte in questa sezione si applicano solo al Supervisor Engine 2 e al Supervisor Engine 720.

- Le funzionalità basate su NetFlow richiedono sempre la visualizzazione del primo pacchetto di un flusso nel software. Quando il primo pacchetto del flusso raggiunge il software, i pacchetti successivi per lo stesso flusso vengono commutati sull'hardware.Questa disposizione del flusso si applica agli ACL riflessivi, al protocollo WCCP (Web Cache Communication Protocol) e al bilanciamento del carico del server Cisco IOS (SLB).**Nota:** sul Supervisor Engine 1, gli ACL riflessivi si basano sulle voci TCAM dinamiche per creare collegamenti hardware per un

particolare flusso. Il principio è lo stesso: il primo pacchetto di un flusso viene inviato al software. I pacchetti successivi per quel flusso vengono commutati dall'hardware.
- Con la funzione TCP Intercept, l'handshake a tre vie e la chiusura della sessione vengono gestiti tramite software. Il resto del traffico viene gestito tramite hardware.**Nota:** i pacchetti SYN (Synchronize (SYN), SYN acknowledledge (SYN ACK) e ACK comprendono l'handshake a tre vie. La sessione viene chiusa quando viene terminata (FIN) o reimpostata (RST).
- Con Network Address Translation (NAT), il traffico viene gestito nel modo seguente:Sul Supervisor Engine 720:Il traffico che richiede NAT viene gestito nell'hardware dopo la traduzione iniziale. La traduzione del primo pacchetto di un flusso viene eseguita nel software e i pacchetti successivi per tale flusso vengono commutati a livello di hardware. Per i pacchetti TCP, viene creato un collegamento hardware nella tabella NetFlow dopo il completamento dell'handshake a tre vie TCP.Sul Supervisor Engine 2 e sul Supervisor Engine 1:Tutto il traffico che richiede NAT è commutato dal software.
- Il controllo degli accessi basato sul contesto (CBAC) utilizza i tasti di scelta rapida di NetFlow per classificare il traffico che richiede un'ispezione. La funzione CBAC invia quindi solo questo traffico al software. La funzione CBAC è disponibile solo tramite software. il traffico soggetto a ispezione non è a commutazione di hardware.**Nota:** il traffico soggetto a ispezione può essere limitato alla velocità sul Supervisor Engine 720.

Traffico Multicast

- Snooping PIM (Protocol Independent Multicast)
- Snooping IGMP (Internet Group Management Protocol) (TTL = 1)Il traffico è infatti destinato al router.
- Snooping Multicast Listener Discovery (MLD) (TTL = 1)Il traffico è infatti destinato al router.
- Errore FIB
- Pacchetti multicast per la registrazione con connessione diretta all'origine multicastQuesti pacchetti multicast vengono tunneling al punto di rendering.
- Multicast IP versione 6 (IPv6)

Altre funzioni

- Riconoscimento applicazioni basato su rete (NBAR)
- Ispezione ARP, solo con CatOS
- Sicurezza porta, solo con CatOS
- snooping DHCP

Situazioni relative all'IPv6

- Pacchetti con intestazione opzione hop-by-hop
- Pacchetti con lo stesso indirizzo IPv6 di destinazione dei router
- Pacchetti che non superano il controllo di imposizione dell'ambito
- Pacchetti che superano l'MTU del collegamento di output
- Pacchetti con un valore TTL inferiore o uguale a 1
- Pacchetti con una VLAN di input uguale alla VLAN di output
- uRPF IPv6Il software esegue questo uRPF per tutti i pacchetti.
- ACL riflessivi IPv6Il software gestisce questi ACL riflessivi.

- Prefissi 6to4 per tunnel ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) IPv6II software gestisce questo tunneling. Tutto il resto del traffico che entra in un tunnel ISATAP è a commutazione di hardware.

LCP Schedulare e modulo DFC

In una scheda DFC (Distributed Forwarding Card), il processo `lcp pianificato` eseguito su una CPU alta non rappresenta un problema e non rappresenta alcun problema per l'operazione. La pianificazione LCP fa parte del codice firmware. Su tutti i moduli che non richiedono un DFC, il firmware viene eseguito su un processore specifico chiamato Line Card Processor (LCP). Questo processore viene utilizzato per programmare l'hardware ASIC e per comunicare con il modulo supervisor centrale.

All'avvio della `pianificazione lcp`, viene utilizzato tutto il tempo di elaborazione disponibile. Tuttavia, quando un nuovo processo richiede tempo di elaborazione, la `pianificazione lcp` riduce il tempo di elaborazione per il nuovo processo. Non vi è alcun impatto sulle prestazioni del sistema in relazione a questo elevato utilizzo della CPU. Il processo acquisisce semplicemente tutti i cicli della CPU inutilizzati, a condizione che non siano richiesti da processi con priorità più alta.

```
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
```

Cause comuni e soluzioni per problemi di utilizzo elevato della CPU

IP non raggiungibile

Quando un gruppo di accesso rifiuta un pacchetto, l'MSFC invia messaggi ICMP "destinazione irraggiungibile". Questa azione viene eseguita per impostazione predefinita.

Con l'abilitazione predefinita del comando **ip unreachables**, il supervisor engine scarta la maggior parte dei pacchetti negati dall'hardware. Quindi, il supervisor engine invia solo un piccolo numero di pacchetti, un massimo di 10 bps, all'MSFC per il rilascio. Questa azione genera messaggi ICMP "destinazione irraggiungibile".

La perdita di pacchetti negati e la generazione di messaggi ICMP "destinazione irraggiungibile" impongono un carico sulla CPU dell'MSFC. Per eliminare il carico, è possibile usare il comando di configurazione dell'interfaccia **no ip unreachables**. Questo comando disabilita i messaggi ICMP "destinazione irraggiungibile", che consentono il drop in hardware di tutti i pacchetti con accesso negato al gruppo.

I messaggi ICMP "destinazione irraggiungibile" non vengono inviati se un VACL rifiuta un pacchetto.

Traduzioni NAT

NAT utilizza l'inoltro hardware e software. L'installazione iniziale delle traduzioni NAT deve essere eseguita tramite software, mentre l'inoltro successivo viene eseguito tramite hardware. NAT utilizza anche la tabella Netflow (massimo 128 KB). Pertanto, se la tabella Netflow è piena, lo switch inizierà anche ad applicare l'inoltro NAT tramite software. Ciò si verifica in genere in caso di picchi di traffico elevati e causerà un aumento della CPU pari a 6500.

Uso di CEF FIB Table Space nella tabella Flow Cache

Il Supervisor Engine 1 ha una tabella della cache di flusso che supporta 128.000 voci. Tuttavia, sulla base dell'efficienza dell'algoritmo di hashing, queste voci vanno da 32.000 a 120.000. Sul Supervisor Engine 2, la tabella FIB viene generata e programmata nel PFC. La tabella contiene fino a 256.000 voci. Supervisor Engine 720 con PFC3-BXL supporta fino a 1.000.000 di voci. Una volta superato questo spazio, i pacchetti diventano commutabili nel software. Ciò può causare un elevato utilizzo della CPU nell'RP. Per controllare il numero di route nella tabella CEF FIB, utilizzare i seguenti comandi:

```
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
```

Sul Supervisor Engine 2, il numero di voci FIB si riduce alla metà se è stato configurato il controllo RPF sulle interfacce. Questa configurazione può portare allo switch software di più pacchetti e, di conseguenza, a un elevato utilizzo della CPU.

Per risolvere il problema di utilizzo elevato della CPU, abilitare il riepilogo route. Il riepilogo delle route può ridurre al minimo la latenza in una rete complessa riducendo i carichi di lavoro del processore, i requisiti di memoria e la richiesta di larghezza di banda.

Per ulteriori informazioni sull'uso e sull'ottimizzazione del TCAM, fare riferimento a Descrizione dell'ACL sugli switch Catalyst serie 6500.

Registrazione ACL ottimizzata

La registrazione OAL (Optimized ACL Logging) fornisce il supporto hardware per la registrazione ACL. A meno che non si configuri OAL, il processo dei pacchetti che richiedono la registrazione avviene completamente nel software dell'MSFC3. OAL consente o scarta i pacchetti nell'hardware dell'MSFC3. OAL utilizza una routine ottimizzata per inviare informazioni all'MSFC3 in modo da generare i messaggi di registrazione.

Nota: per informazioni su OAL, fare riferimento alla sezione *Registrazione ACL ottimizzata con PFC3* nel documento Informazioni sul supporto degli ACL Cisco IOS.

Limite di velocità dei pacchetti per la CPU

Sul Supervisor Engine 720, i limitatori di velocità possono controllare la velocità con cui i pacchetti possono essere inviati al software. Questo controllo della velocità consente di prevenire gli attacchi Denial of Service. È possibile anche utilizzare alcuni di questi limitatori di velocità sul 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      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
```

Di seguito è riportato un esempio:

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

Per limitare la velocità di tutti i pacchetti CEF-punted all'MSFC, usare il comando riportato nell'esempio:

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

Per ridurre il numero di pacchetti indirizzati alla CPU a causa di TTL=1, eseguire questo comando:

```
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.
```

Ad esempio, questo è l'output dell'**acquisizione netdr**, da cui si deduce che il valore TTL dell'IPv4 è 1:

```
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
```

Un elevato livello di CPU può essere dovuto anche a pacchetti con TTL=1 che vengono persi alla CPU. Per limitare il numero di pacchetti persi alla CPU, configurare un limitatore di velocità hardware. I limitatori di velocità possono limitare la velocità dei pacchetti che vengono persi dal

percorso dati hardware fino al percorso dati software. I limitatori di velocità proteggono il percorso di controllo software dalla congestione eliminando il traffico che supera la velocità configurata. Il limite di velocità è configurato utilizzando il comando **mls rate-limit all ttl-failure**.

Fusione fisica di VLAN a causa di cavi non corretti

L'uso elevato della CPU può inoltre derivare dall'unione di due o più VLAN a causa di cavi non corretti. Inoltre, se l'opzione STP viene disabilitata sulle porte a cui si verifica la fusione della VLAN, può verificarsi un elevato utilizzo della CPU.

Per risolvere il problema, identificare gli errori di cablaggio e correggerli. Se le esigenze lo consentono, è possibile abilitare anche STP su tali porte.

Broadcast Storm

Una rete LAN broadcast storm si verifica quando pacchetti broadcast o multicast inondano la LAN, creando traffico eccessivo e degradando le prestazioni della rete. Errori nell'implementazione dello stack del protocollo o nella configurazione della rete possono causare un broadcast storm.

A causa del design architettonico della piattaforma Catalyst serie 6500, i pacchetti broadcast vengono scartati solo a livello software.

La soppressione del broadcast previene l'interruzione delle interfacce LAN a causa di un broadcast. La soppressione della trasmissione utilizza un filtro che misura l'attività di trasmissione su una LAN in un periodo di tempo di 1 secondo e confronta la misurazione con una soglia predefinita. Se la soglia viene raggiunta, l'ulteriore attività di trasmissione viene soppressa per la durata di un periodo di tempo specificato. L'eliminazione della trasmissione è disabilitata per impostazione predefinita.

Nota: il flapping del VRRP dal backup al master causato da problemi di trasmissione potrebbe causare un elevato utilizzo della CPU.

Per comprendere come funziona la soppressione del broadcast e per abilitare la funzione, fare riferimento a:

- Configurazione di Broadcast Suppression (software di sistema Cisco IOS)
- Configurazione di Broadcast Suppression (software di sistema CatOS)

Tracciamento indirizzo BGP Next-Hop (processo scanner BGP)

Il processo dello scanner BGP esamina la tabella BGP e conferma la raggiungibilità degli hop successivi. Questo processo controlla inoltre l'annuncio condizionale per determinare se BGP deve annunciare i prefissi delle condizioni e/o eseguire lo smorzamento delle route. Per impostazione predefinita, il processo esegue la scansione ogni 60 secondi.

Èpossibile prevedere un elevato utilizzo della CPU per brevi periodi a causa del processo dello scanner BGP su un router che dispone di una tabella di routing Internet di grandi dimensioni. Una volta al minuto, lo scanner BGP esamina la tabella RIB (Routing Information Base) BGP ed esegue importanti attività di manutenzione. Tali attività includono:

- Controllo dell'hop successivo a cui viene fatto riferimento nella tabella BGP del router

- Verifica della possibilità di raggiungere i dispositivi dell'hop successivo

Pertanto, una tabella BGP di grandi dimensioni richiede un tempo equivalente per essere spostata e convalidata. Il processo dello scanner BGP analizza la tabella BGP per aggiornare le strutture dei dati e la tabella di routing per la ridistribuzione delle route. Entrambe le tabelle vengono memorizzate separatamente nella memoria del router. Entrambe le tabelle possono avere dimensioni molto grandi e quindi consumare cicli della CPU.

Per ulteriori informazioni sull'utilizzo della CPU da parte del processo dello scanner BGP, fare riferimento alla sezione *High CPU due to BGP Scanner* in Troubleshooting High CPU Cause by the BGP Scanner or BGP Router Process.

Per ulteriori informazioni sulla funzione BGP Next-Hop Address Tracking e sulla procedura per abilitare/disabilitare o regolare l'intervallo di scansione, fare riferimento al supporto BGP per la funzione Next-Hop Address Tracking.

Traffico multicast non RPF

Il routing multicast (a differenza del routing unicast) riguarda solo l'origine di un determinato flusso di dati multicast. Ovvero l'indirizzo IP del dispositivo da cui proviene il traffico multicast. Il principio di base è che il dispositivo sorgente "spinge" il flusso verso un numero indefinito di ricevitori (all'interno del suo gruppo multicast). Tutti i router multicast creano strutture di distribuzione che controllano il percorso del traffico multicast attraverso la rete per consegnare il traffico a tutti i ricevitori. I due tipi di alberi di distribuzione multicast sono alberi di origine e alberi condivisi. RPF è un concetto chiave nell'inoltro multicast. Consente ai router di inoltrare correttamente il traffico multicast lungo la struttura di distribuzione. RPF utilizza la tabella di routing unicast esistente per determinare i router adiacenti a monte e a valle. Un router inoltra un pacchetto multicast solo se viene ricevuto sull'interfaccia upstream. Questo controllo di RPF aiuta a garantire che l'albero di distribuzione sia privo di loop.

Il traffico multicast è sempre visibile da ogni router su una LAN con bridging (layer 2), in base alla specifica CSMA/CD IEEE 802.3. Nello standard 802.3, il bit 0 del primo ottetto viene usato per indicare un frame broadcast e/o multicast, e qualsiasi frame di layer 2 con questo indirizzo viene inondato. Ciò vale anche se sono configurati CGMP o IGMP Snooping. Infatti, se si prevede che i router multicast prendano una decisione di inoltro appropriata, è necessario che vedano il traffico multicast. Se più router multicast dispongono ciascuno di interfacce su una LAN comune, solo un router inoltra i dati (scelti mediante un processo di selezione). A causa della natura a scorrimento delle LAN, il router ridondante (il router che non inoltra il traffico multicast) riceve questi dati sull'interfaccia in uscita per tale LAN. Il router ridondante in genere interrompe il traffico, in quanto è arrivato all'interfaccia errata e non riesce a eseguire il controllo RPF. Questo traffico che non supera il controllo RPF viene definito traffico non RPF o pacchetti di errore RPF, in quanto sono stati trasmessi al contrario rispetto al flusso proveniente dall'origine.

Catalyst 6500 con MSFC installato, può essere configurato per funzionare come router multicast completo. Utilizzando MLS (Multicast Multi-Layer Switching), il traffico RPF viene in genere inoltrato dall'hardware dello switch. ASIC riceve informazioni dallo stato di routing multicast, ad esempio (*,G) e (S,G), in modo da poter programmare un collegamento hardware nella tabella Netflow e/o FIB. Questo traffico non RPF è ancora necessario in alcuni casi ed è richiesto dalla CPU MSFC (a livello di processo) per il meccanismo PIM Assert. In caso contrario, viene scartato dal percorso di commutazione rapida del software (si presume che la commutazione rapida del software non sia disabilitata sull'interfaccia RPF).

In alcune topologie, lo switch Catalyst 6500 con ridondanza potrebbe non gestire in modo

efficiente il traffico non RPF. Per il traffico non RPF, in genere lo stato (*,G) o (S,G) non è presente nel router ridondante, quindi non è possibile creare collegamenti hardware o software per rilasciare il pacchetto. Ogni pacchetto multicast deve essere esaminato singolarmente dal processore di routing MSFC, operazione spesso definita traffico di interrupt della CPU. Con la commutazione hardware di layer 3 e le diverse interfacce/VLAN che connettono lo stesso gruppo di router, il traffico non RPF che colpisce la CPU dell'MSFC ridondante viene amplificato "N" volte la velocità di origine originale (dove "N" è il numero di LAN a cui il router è connesso in modo ridondante). Se la velocità del traffico non RPF supera la capacità di rilascio dei pacchetti del sistema, potrebbe causare un elevato utilizzo della CPU, overflow del buffer e instabilità generale della rete.

Con Catalyst 6500, è disponibile un motore delle liste di accesso che consente di filtrare gli accessi alla velocità wire-rate. Questa funzione può essere utilizzata per gestire in modo efficiente il traffico non RPF per i gruppi in modalità sparsa, in determinate situazioni. È possibile utilizzare il metodo basato su ACL solo nelle 'reti stub' in modalità sparse, in cui non sono presenti router multicast downstream (e ricevitori corrispondenti). Inoltre, a causa della progettazione dell'inoltro di pacchetti di Catalyst 6500, gli MSFC ridondanti internamente non possono utilizzare questa implementazione. Per una descrizione dettagliata, consultare l'ID bug Cisco CSCdr74908 (solo utenti registrati). Per i gruppi in modalità densa, i pacchetti non RPF devono essere visti sul router per permettere al meccanismo PIM Assert di funzionare correttamente. Soluzioni diverse, come la limitazione della velocità basata su CEF o NetFlow e la QoS, vengono usate per controllare gli errori RPF nelle reti in modalità densa e nelle reti di transito in modalità sparsa.

Sullo switch Catalyst 6500 è disponibile un motore delle liste di accesso che consente di filtrare i dati alla velocità wire-rate. Questa funzione può essere utilizzata per gestire in modo efficiente il traffico non RPF per i gruppi in modalità sparsa. Per implementare questa soluzione, posizionare un elenco degli accessi sull'interfaccia in ingresso della 'rete stub' per filtrare il traffico multicast che non proviene dalla 'rete stub'. e viene inoltrato all'hardware nello switch. Questo elenco degli accessi impedisce alla CPU di vedere il pacchetto e consente all'hardware di bloccare il traffico non RPF.

Nota: non posizionare l'elenco degli accessi su un'interfaccia di transito. È destinato solo alle reti stub (reti solo con host).

Per ulteriori informazioni, fare riferimento a questi documenti:

- Problemi dei router ridondanti con multicast IP nelle reti stub
- Elaborazione del traffico non RPF

Comandi show

L'utilizzo della CPU quando si esegue un comando **show** è sempre quasi del 100%. È normale avere un elevato utilizzo della CPU quando si esegue un comando **show** e in genere rimane solo per alcuni secondi.

Ad esempio, è normale che il processo Virtual Exec diventi elevato quando si esegue un comando **show tech-support** in quanto questo output è guidato da un interrupt. L'unica preoccupazione è disporre di un'elevata CPU in processi diversi dai comandi **show**.

Il comando **show cef not-cef-switched** mostra il motivo per cui i pacchetti vengono inviati all'MSFC (ricezione, opzione ip, nessuna adiacenza, ecc.) e il numero. Ad esempio:

```
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
```

I comandi **show ibc** e **show ibc brief** mostrano la coda della CPU e possono essere utilizzati quando si controlla lo stato della CPU.

Processi di esecuzione

Il processo Exec nel software Cisco IOS è responsabile della comunicazione sulle linee TTY (console, ausiliarie, asincrone) del router. Il processo Virtual Exec è responsabile delle linee VTY (sessioni Telnet). I processi Exec e Virtual Exec hanno priorità media, quindi se esistono altri processi con priorità più alta (Alta o Critica), i processi con priorità più alta ottengono le risorse CPU.

Se durante queste sessioni vengono trasferiti molti dati, l'utilizzo della CPU per il processo Exec aumenta. Infatti, quando il router desidera inviare un carattere semplice attraverso queste righe, usa alcune risorse CPU:

- Per la console (Exec), il router utilizza un interrupt per carattere.
- Per la linea VTY (Virtual Exec), la sessione Telnet deve compilare un pacchetto TCP per carattere.

In questo elenco vengono illustrati in dettaglio alcuni dei possibili motivi dell'utilizzo elevato della CPU nel processo di esecuzione:

- **Troppi dati inviati tramite la porta della console.**Verificare se sono stati avviati debug sul router con il comando show debugging.Disabilitare la registrazione sulla console sul router usando il comando **no** form della console di registrazione.Verificare se sulla console è stampato un output lungo. Ad esempio, un comando show tech-support o show memory.
- **Il comando exec è configurato per le linee asincrone e ausiliarie.**Se una linea presenta solo traffico in uscita, disattivare il processo di esecuzione per questa linea. Infatti, se la periferica (ad esempio un modem) collegata a questa linea invia dati non richiesti, il processo di esecuzione inizierà su questa linea.Se il router viene utilizzato come terminal server (per il reverse Telnet su altre console di dispositivi), si consiglia di configurare il comando **no exec** sulle righe connesse alla console delle altre periferiche. In caso contrario, i dati restituiti dalla console potrebbero avviare un processo Exec che utilizza risorse CPU.

Un possibile motivo per un elevato utilizzo della CPU nel processo Virtual Exec è:

- **Troppi dati inviati tramite le sessioni Telnet.**Il motivo più comune per un utilizzo elevato della CPU nel processo Virtual Exec è il trasferimento di una quantità eccessiva di dati dal router alla sessione Telnet. Questo problema può verificarsi quando si eseguono comandi con output lunghi, ad esempio **show tech-support**, **show memory** e così via, dalla sessione Telnet. La quantità di dati trasferiti tramite ciascuna sessione VTY può essere verificata con il comando **show tcp vty** *<numero riga>* .

Processo di aging L3

Quando il processo di misurazione durata L3 esporta un numero elevato di valori *ifindex* utilizzando il protocollo NDE (NetFlow Data Export), l'utilizzo della CPU potrebbe raggiungere il 100%.

Se si verifica questo problema, verificare se i due comandi seguenti sono abilitati:

```
set mls nde destination-ifindex enable

set mls nde source-ifindex enable
```

Se si attivano questi comandi, il processo deve esportare tutti i valori ifindex di destinazione e di origine utilizzando NDE. L'utilizzo del processo di misurazione durata L3 diventa elevato in quanto deve eseguire la ricerca FIB per tutti i valori *ifindex di* origine e destinazione. Per questo motivo, la tabella diventa piena, il processo di invecchiamento L3 diventa elevato e l'utilizzo della CPU raggiunge il 100%.

Per risolvere il problema, disabilitare i seguenti comandi:

```
set mls nde destination-ifindex disable

set mls nde source-ifindex disable
```

Utilizzare questi comandi per verificare i valori:

- mostra riepilogo cef mls
- show mls cef maximum-route

BPDU Storm

Lo Spanning Tree mantiene un ambiente Layer 2 privo di loop in reti bridge e commutate ridondanti. Senza STP, i fotogrammi vengono ripetuti e/o moltiplicati per un tempo indefinito. Questa circostanza causa un blocco della rete in quanto un traffico elevato interrompe tutti i dispositivi nel dominio di trasmissione.

Per alcuni aspetti, il protocollo STP è stato inizialmente sviluppato per le specifiche bridge basate su software lento (IEEE 802.1D), ma può essere complicato implementarlo con successo in reti a commutazione di grandi dimensioni con le seguenti caratteristiche:

- Molte VLAN
- Molti switch in un dominio STP
- Supporto multi-vendor
- Nuovi miglioramenti IEEE

Se la rete deve affrontare frequenti calcoli dello Spanning Tree o lo switch deve elaborare più BPDU, può verificarsi un elevato numero di CPU e di BPDU.

Per risolvere questi problemi, eseguire una o più delle seguenti operazioni:

1. Eliminare le VLAN dagli switch.
2. Utilizzare una versione avanzata di STP, ad esempio MST.
3. Aggiornare l'hardware dello switch.

Fare riferimento anche alle best practice per implementare Spanning Tree Protocol nella rete.

- Best practice per gli switch Catalyst serie 4500/4000, 5500/5000 e 6500/6000 con configurazione e gestione CatOS
- Best practice per gli switch Catalyst serie 6500/6000 e Catalyst serie 4500/4000 con software Cisco IOS

Sessioni SPAN

Basate sull'architettura degli switch Catalyst serie 6000/6500, le sessioni SPAN non influiscono sulle prestazioni dello switch, ma se la sessione SPAN include una porta uplink o ad alto traffico o EtherChannel, può aumentare il carico sul processore. Se poi individua una VLAN specifica, il carico di lavoro aumenta ulteriormente. Se il traffico sul collegamento è danneggiato, è possibile che il carico di lavoro aumenti ulteriormente.

In alcuni scenari, la funzione RSPAN può causare loop e il carico sul processore aumenta. Per ulteriori informazioni, consultare il documento sui motivi per cui la sessione SPAN crea un loop di bridging?

Lo switch può trasmettere il traffico come di consueto poiché tutto si trova nell'hardware, ma la CPU può prendere una botta se cerca di capire a quale traffico inviare. Si consiglia di configurare le sessioni SPAN solo quando necessario.

%CFIB-SP-STBY-7-CFIB_EXCEPTION: Eccezione FIB TCAM, alcune voci saranno software switched

```
%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
```

Questo messaggio di errore viene ricevuto quando viene superata la quantità di spazio disponibile nel TCAM. Il risultato è una CPU elevata. Questa è una limitazione di FIB TCAM. Quando TCAM è pieno, viene impostato un flag e viene ricevuta l'eccezione FIB TCAM. Ciò impedisce di aggiungere nuovi percorsi al TCAM. Pertanto, tutto sarà commutato dal software. La rimozione delle route non consente di riprendere la commutazione hardware. Una volta che TCAM entra nello stato di eccezione, il sistema deve essere ricaricato per uscire da quello stato. Il numero massimo di route che possono essere installate in TCAM viene aumentato dal comando **mls cef maximum-route**.

Catalyst 6500/6000 con CPU elevata e ACL IPv6 con porte L4

Abilita indirizzo unicast di compressione ACL ipv6 mls . Questo comando è necessario se l'ACL IPv6 corrisponde ai numeri di porta del protocollo L4. Se questo comando non è abilitato, il traffico IPv6 verrà indirizzato alla CPU per l'elaborazione del software. Questo comando non è configurato per impostazione predefinita.

SPF in rame

Sugli switch Ethernet Cisco ME serie 6500, gli SFP in rame richiedono una maggiore interazione con il firmware rispetto ad altri tipi di SFP, che aumenta l'utilizzo della CPU.

Gli algoritmi software che gestiscono gli SFP in rame sono stati migliorati nelle versioni Cisco IOS SXH.

Modular IOS

Sugli switch Cisco Catalyst serie 6500 con software IOS modulare, l'utilizzo normale della CPU è leggermente superiore a quello del software IOS non modulare.

Il software Modular IOS paga un prezzo per attività superiore a quello di un pacchetto. Il software Modular IOS mantiene i processi consumando determinate CPU anche se non ci sono molti pacchetti, quindi il consumo della CPU non è basato sul traffico effettivo. Tuttavia, quando i pacchetti vengono elaborati a una velocità elevata, la CPU utilizzata nel software Modular IOS non deve essere superiore a quella del software IOS non modulare.

Verifica utilizzo CPU

Se l'utilizzo della CPU è elevato, eseguire prima il comando **show processes cpu**. L'output mostra l'utilizzo della CPU sullo switch e l'utilizzo della CPU da parte di ciascun processo.

```
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 questo output, l'utilizzo totale della CPU è del 57% e l'utilizzo della CPU degli interrupt è del 48%. Qui, queste percentuali appaiono in grassetto. Lo switch di interrupt del traffico da parte della CPU causa l'utilizzo della CPU di interrupt. L'output del comando elenca i processi che causano la differenza tra le due utilizzazioni. In questo caso, la causa è il processo SNMP.

Sul Supervisor Engine con CatOS, l'output è il seguente:

```
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 questo output, il primo processo è `Kernel e Idle`, che mostra l'utilizzo inattivo della CPU. Questo processo è in genere elevato, a meno che alcuni altri processi non utilizzino cicli di CPU. In questo esempio, il processo `SptBpduRx` causa un elevato utilizzo della CPU.

Se l'utilizzo della CPU è elevato a causa di uno di questi processi, è possibile risolvere i problemi e determinare il motivo per cui questo processo viene eseguito in modo elevato. Tuttavia, se la CPU è alta a causa del traffico puntato alla CPU, è necessario determinare il motivo per cui il traffico viene punito. Questa determinazione può aiutare a identificare di cosa si tratta il traffico.

Per la risoluzione dei problemi, utilizzare questo script di esempio EEM per raccogliere l'output dallo switch quando si verifica un elevato utilizzo della CPU:

```
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"
!
```

Nota: il comando **debug netdr capture rx** è utile quando la CPU è alta a causa della commutazione dei pacchetti anziché dell'hardware. Acquisisce 4096 pacchetti in entrata nella CPU quando si esegue il comando. Il comando è completamente sicuro ed è lo strumento più comodo per risolvere i problemi di CPU elevati dello switch 6500. Non provoca un sovraccarico per la CPU.

Utilità e strumenti per determinare il traffico indirizzato alla CPU

In questa sezione vengono descritte alcune utilità e strumenti che possono essere utili per analizzare il traffico.

Software di sistema Cisco IOS

Nel software Cisco IOS, il processore dello switch sul supervisor engine è denominato SP e l'MSFC è denominato RP.

Il comando **show interface** fornisce informazioni di base sullo stato dell'interfaccia e sulla velocità del traffico sull'interfaccia. Il comando fornisce anche contatori di errori.

```
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 questo output, il traffico in entrata è commutato sul layer 3 anziché sul layer 2. Ciò indica che il traffico viene indirizzato alla CPU.

Il comando **show PROCESSES cpu** dice se questi pacchetti sono pacchetti di traffico regolare o pacchetti di controllo.

```
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
```

Se i pacchetti sono a commutazione di contesto, si osserverà che il processo di `ingresso IP` è in esecuzione ad alta velocità. Per visualizzare questi pacchetti, usare questo comando:

interfaccia di input show buffer

```
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
```

Se il traffico viene **interrotto**, non è possibile visualizzare i pacchetti con il comando **show buffers input-interface**. Per visualizzare i pacchetti indirizzati all'RP per la commutazione di interrupt, è possibile eseguire un'acquisizione SPAN (Switched Port Analyzer) della porta RP.

Nota: per ulteriori informazioni sull'utilizzo della CPU a commutazione di interrupt rispetto a quella a commutazione di contesto, consultare questo documento:

- Sezione *Utilizzo elevato della CPU dovuto a interrupt* in Risoluzione dei problemi di utilizzo elevato della CPU sui router Cisco

SPAN RP-Inband e SP-Inband

Una porta SPAN per la porta RP o SP nel software Cisco IOS è disponibile a partire da Cisco IOS versione 12.1(19)E.

Questa è la sintassi del comando:

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

Utilizzare questa sintassi per il software Cisco IOS versione 12.2 SX:

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

Nota: in SXH, è necessario usare il comando **monitor session** per configurare una sessione SPAN locale, quindi usare questo comando per associare la sessione SPAN alla 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]
```

Nota: per ulteriori informazioni su questi comandi, consultare il documento sulla configurazione della SPAN locale (modalità di configurazione SPAN) nella *guida alla configurazione del software Catalyst 6500 versione 12.2SX*.

Di seguito è riportato un esempio su una 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
```

Passare alla console SP. Di seguito è riportato un esempio:

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

Nota: nelle versioni Cisco IOS 12.2 SX, il comando è stato modificato in **test monitor 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
```

Nota: nelle versioni Cisco IOS 12.2 SX, il comando è stato modificato in **test monitor show 1**.

Di seguito è riportato un esempio su una console SP:

```
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
```

Software di sistema CatOS

Per gli switch con software di sistema CatOS, il supervisor engine esegue CatOS e il modulo MSFC esegue software Cisco IOS.

Se si usa il comando **show mac**, è possibile vedere il numero di frame puntati sull'MSFC. La porta 15/1 è la connessione del supervisor engine all'MSFC.

Nota: la porta è 16/1 per i supervisor engine nello slot 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
```

Un rapido aumento di questo numero indica che i pacchetti vengono indirizzati all'MSFC, il che provoca un elevato utilizzo della CPU. È quindi possibile esaminare i pacchetti nei modi seguenti:

- Porta SPAN MSFC 15/1 o 16/1
- SPAN sc0

Porta SPAN MSFC 15/1 o 16/1

Configurare una sessione SPAN in cui l'origine è la porta MSFC 15/1 (o 16/1) e la destinazione è una porta Ethernet.

Di seguito è riportato un esempio:

```
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
```

Se si raccoglie una traccia dello sniffer sulla porta 5/10, la traccia dello sniffer mostra i pacchetti che trasmettono da e verso l'MSFC. Configurare la sessione SPAN come **tx** per acquisire i pacchetti che sono destinati solo all'MSFC, e non all'MSFC.

SPAN sc0

Configurare una sessione SPAN con l'interfaccia **sc0** come origine per acquisire i frame che vengono inviati alla CPU del 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
```

Nota: per i moduli OSM (Optical Services Module), non è possibile eseguire un'acquisizione SPAN del traffico.

Raccomandazioni

L'utilizzo della CPU del supervisor engine non riflette le prestazioni di inoltro hardware dello switch. È comunque necessario basare e monitorare l'utilizzo della CPU del Supervisor Engine.

1. Basare l'utilizzo della CPU del supervisor engine per lo switch in una rete in stato stabile con modelli di traffico e carico normali.Prendere nota dei processi che generano il massimo utilizzo della CPU.
2. Per la risoluzione dei problemi relativi all'utilizzo della CPU, considerare le domande seguenti:Quali processi generano il massimo utilizzo? Questi processi sono diversi dalla previsione?La CPU è costantemente elevata rispetto alla linea di base? O ci sono picchi di utilizzo elevato, e poi un ritorno ai livelli di base?Nella rete sono presenti notifiche di modifica della topologia (TCN)?**Nota: lo** svuotamento delle porte o delle porte host con la funzionalità PortFast STP disabilitata causa i TCN.Il traffico broadcast o multicast nelle subnet di gestione/VLAN è eccessivo?Sullo switch è presente un traffico di gestione eccessivo, ad esempio il polling SNMP?
3. Durante il tempo CPU elevato (quando la CPU è pari o superiore al 75%), raccogliere l'output dai seguenti comandi:mostra orologioshow versionmostra processi in base a cpumostra cronologia cpu procshow log
4. Se possibile, isolare la VLAN di gestione dalle VLAN con il traffico di dati dell'utente, in particolare con il traffico di broadcast.Esempi di questo tipo di traffico includono IPX RIP/Service Advertising Protocol (SAP), AppleTalk e altro traffico di broadcast. Tale traffico può influire sull'utilizzo della CPU del supervisor engine e, in casi estremi, può interferire con il normale funzionamento dello switch.
5. Se la CPU è in esecuzione a causa della punt del traffico verso l'RP, determinare di cosa si tratta e perché il traffico viene puntato.Per effettuare questa determinazione, utilizzare le utilità descritte nella sezione Utilità e strumenti per determinare il traffico indirizzato alla CPU.

Informazioni correlate

- Comandi utili per la risoluzione dei problemi relativi alla CPU elevata su Catalyst 6500 con Sup720
- Messaggi di errore comuni di CatOS sugli switch Catalyst serie 6000/6500
- Messaggi di errore comuni sugli switch Catalyst serie 6500/6000 con software Cisco IOS
- Risoluzione dei problemi comuni e hardware sugli switch Catalyst serie 6500/6000 con software di sistema Cisco IOS
- Inondazioni unicast nelle reti a campus commutati
- Switch Cisco Catalyst serie 6500 - Supporto dei prodotti
- Script EEM per la raccolta di dati durante il problema Intermittent High CPU
- Supporto dei prodotti LAN
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems