Risoluzione dei problemi di utilizzo elevato della CPU sugli switch Catalyst 4500

Sommario

Introduzione

Questo documento descrive l'architettura di gestione dei pacchetti CPU e mostra come identificare le cause di un uso elevato della CPU sugli switch Catalyst 4500.

Prerequisiti

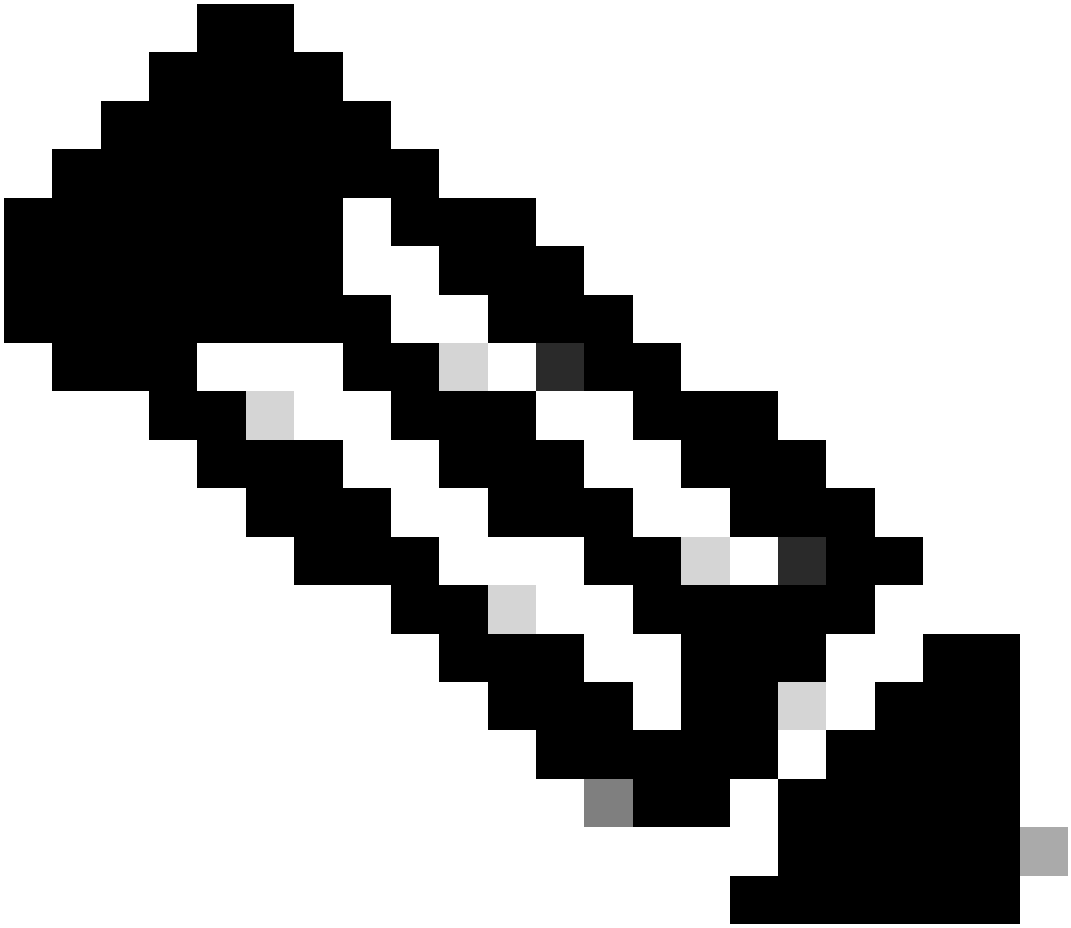
Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Catalyst serie 4500
- Switch Catalyst serie 4948



Nota: questo documento si applica solo agli switch con software Cisco IOS®.

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.

Convenzioni

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

Premesse

Gli switch Catalyst serie 4500, che includono gli switch Catalyst 4948, dispongono di una sofisticata metodologia di gestione dei pacchetti per il traffico basato sulla CPU. Un problema comunemente percepito è l'elevato utilizzo della CPU su questi switch. Questo documento fornisce dettagli sull'architettura di gestione dei pacchetti CPU e mostra come identificare le cause di un elevato utilizzo della CPU su questi switch. Il documento elenca anche alcuni scenari comuni di rete o configurazione che causano un elevato utilizzo della CPU sugli switch Catalyst serie 4500

Prima di esaminare l'architettura di gestione dei pacchetti CPU e risolvere i problemi relativi all'utilizzo elevato della CPU, è necessario comprendere le diverse modalità in cui gli switch di inoltro basati su hardware e i router basati su software Cisco IOS utilizzano la CPU. L'idea sbagliata comune è che un elevato utilizzo della CPU indica l'esaurimento delle risorse su un dispositivo e la minaccia di un arresto anomalo. Un problema di capacità è uno dei sintomi di un elevato utilizzo della CPU sui router Cisco IOS. Tuttavia, un problema di capacità non è quasi mai un sintomo di un elevato utilizzo della CPU con switch di inoltro basati su hardware come Catalyst 4500. Catalyst 4500 è progettato per inoltrare pacchetti nel circuito ASIC (Application-Specific Integrated Circuit) specifico dell'applicazione hardware e raggiungere velocità di inoltro del traffico fino a 102 milioni di pacchetti al secondo (Mpps).

La CPU Catalyst 4500 svolge le seguenti funzioni:

- Gestisce i protocolli software configurati, ad esempio:
    - STP (Spanning Tree Protocol)
    - Protocollo di routing
    - Protocollo CDP (Cisco Discovery Protocol)
    - Protocollo PAgP (Port Aggregation Protocol)
    - VLAN Trunk Protocol (VTP)
    - Protocollo DTP (Dynamic Trunking Protocol)
- Voci dinamiche/di configurazione dei programmi negli ASIC hardware, ad esempio:
    - Access Control List (ACL)
    - Voci CEF
- Gestisce internamente vari componenti, ad esempio:
    - Schede di linea Power over Ethernet (PoE)
    - Alimentatori
    - Cassetto ventola

- Gestisce l'accesso allo switch, ad esempio:
    - Telnet
    - Console
    - Protocollo SNMP (Simple Network Management Protocol)
- Inoltra i pacchetti tramite il percorso software, ad esempio:
    - Pacchetti con routing IPX (Internetwork Packet Exchange), supportati solo nel percorso software
    - Frammentazione Maximum Transmission Unit (MTU)

In base a questo elenco, un elevato utilizzo della CPU può derivare dalla ricezione o dal processo di pacchetti da parte della CPU. Alcuni dei pacchetti inviati per il processo possono essere essenziali per il funzionamento della rete. Un esempio di questi pacchetti essenziali sono le BDPU (Bridge Protocol Data Unit) per le configurazioni della topologia dello spanning-tree. Tuttavia, altri pacchetti possono essere traffico di dati inoltrati dal software. In questi scenari, gli ASIC di switching devono inviare i pacchetti alla CPU per l'elaborazione:

- I pacchetti che vengono copiati sulla CPU, ma i pacchetti originali vengono scambiati in hardware.

  Un esempio è l'apprendimento dell'indirizzo MAC dell'host.
- Pacchetti inviati alla CPU per l'elaborazione

  Alcuni esempi:
    - Aggiornamenti del protocollo di routing
    - BPDU
    - Inondazioni di traffico intenzionali o involontarie
- Pacchetti inviati alla CPU per l'inoltro

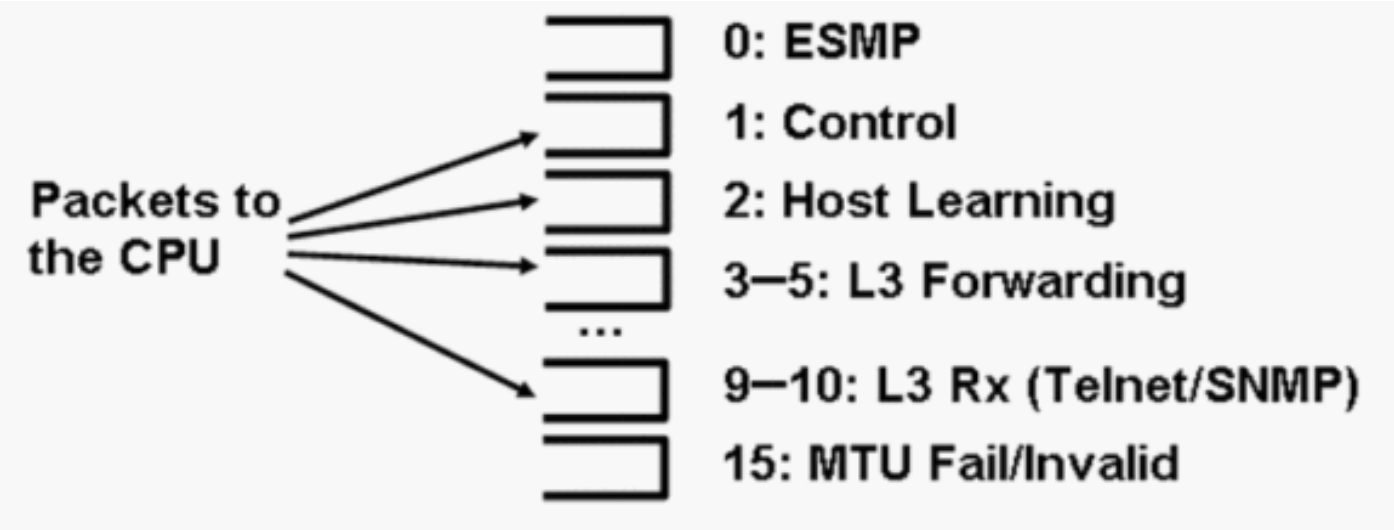
  Ad esempio, i pacchetti che richiedono il routing IPX o AppleTalk.

Conoscenza dell'architettura di gestione dei pacchetti della CPU Catalyst 4500

Catalyst 4500 è dotato di un meccanismo QoS (Quality of Service) incorporato che consente di distinguere tra i tipi di traffico destinati alla CPU. Il meccanismo opera la differenziazione sulla base delle informazioni sui pacchetti di layer 2 (L2)/layer 3 (L3)/layer 4 (L4). Il Supervisor Packet Engine ha 16 code per gestire vari tipi di pacchetti o eventi. Nella Figura 1 sono illustrate queste code. La tabella 1 elenca le code e i tipi di pacchetto che vi si trovano. Le 16 code permettono allo

switch Catalyst 4500 di mettere in coda i pacchetti in base al tipo o alla priorità.

Figura 1 - Catalyst 4500 utilizza più code CPU



Catalyst 4500 utilizza più code CPU

Tabella 1 - Descrizione della coda Catalyst 4500

Numero coda	Nome coda	Pacchetti in coda
0	Esmp	Pacchetti ESMP[1] (pacchetti di gestione interna) per gli ASIC delle schede di linea o per la gestione di altri componenti
1	Controllo	Pacchetti del control plane L2, ad esempio STP, CDP, PAgP, LACP[2] o UDLD[3]
2	Formazione host	Frame con indirizzi MAC di origine sconosciuti copiati nella CPU per compilare la tabella di inoltro L2
3, 4, 5	L3 Fwd Massimo, L3 Fwd Alto/Medio,L3 Fwd Basso	Pacchetti che devono essere inoltrati nel software, ad esempio nei tunnel GRE[4]Se l'ARP[5]non è risolto per l'indirizzo IP di destinazione, i pacchetti vengono inviati a questa coda.
6, 7, 8	L2 Fwd Massimo,L2 Fwd Alto/Medio,L2 Fwd Basso	Pacchetti inoltrati come risultato del bridging • I protocolli non supportati nell'hardware, ad esempio i pacchetti di routing IPX e AppleTalk, vengono collegati tramite bridging alla CPU • Richiesta e risposta ARP • I pacchetti con indirizzo MAC di destinazione dell'interfaccia SVI[6]/L3 dello switch vengono collegati tramite bridge se non è possibile

		instradare i pacchetti nell'hardware a causa di: ◦ Opzioni dell'intestazione IP ◦ TTL[7] scaduto ◦ Incapsulamento non ARPA
11, 10	L3 Rx Alta, L3 Rx Bassa	L3 controlla il traffico del piano, ad esempio i protocolli di routing, destinato agli indirizzi IP della CPU. Alcuni esempi includono Telnet, SNMP e SSH[8].
11	Errore RPF	Pacchetti multicast che non hanno superato il controllo di RPF[9]
12	ACL fwd(snooping)	Pacchetti elaborati dalle funzioni di snooping DHCP[10], ispezione ARP dinamica o snooping IGMP[11]
13	log ACL, non raggiungibile	Pacchetti che hanno raggiunto un ACE[12] con la parola chiave log o pacchetti che sono stati scartati a causa del rifiuto in un ACL di output o della mancanza di un percorso alla destinazione. Questi pacchetti richiedono la generazione di messaggi ICMP "destinazione irraggiungibile".
14	Elaborazione del software ACL	Pacchetti puntati alla CPU per mancanza di risorse hardware ACL aggiuntive, ad esempio TCAM[13], per ACL di sicurezza
15	MTU non riuscita/non valida	Pacchetti da frammentare perché le dimensioni MTU dell'interfaccia di output sono inferiori alle dimensioni del pacchetto

[1]ESMP = Protocollo di gestione semplice e uniforme.

[2]LACP = Link Aggregation Control Protocol.

[3]UDLD = Rilevamento collegamenti unidirezionali.

[4]GRE = incapsulamento del routing generico.

[5]ARP = Address Resolution Protocol (Protocollo di risoluzione indirizzi).

[6]SVI = interfaccia virtuale commutata.

[7]TTL = Time to Live.

[8]SSH = Protocollo Secure Shell.

[9]RPF = Reverse Path Forwarding

[10]DHCP = Protocollo di configurazione host dinamico.

[11]IGMP = Internet Group Management Protocol.

[12]ACE = voce di controllo di accesso.

[13]TCAM = memoria indirizzabile del contenuto ternario.

Queste code sono code separate:

- `L2 Fwd HighestorL3 Fwd Highest`
- `Fwd L2 Alto/MedioL3 Fwd Alto/Medio`
- `L2 Fwd inferioreL3 Fwd inferiore`
- `L3 Rx SuperioreL3 Rx Bassa`

I pacchetti vengono accodati in queste code sulla base dell'etichetta QoS, ossia il valore del punto di codice dei servizi differenziati (DSCP) dal tipo di servizio (ToS) IP. Ad esempio, i pacchetti con un DSCP di 63 vengono accodati `nella` coda `L3 Fwd` Highestqueue. I pacchetti ricevuti e scartati per queste 16 code sono riportati nell'output del comando show platform cpu packet statistics all. L'output di questo comando è molto lungo. Usare il comando show platform cpu packet statistics per visualizzare solo gli eventi diversi da zero. Un comando alternativo è il comando show platform cpuport. Usare il comando show platform cpuport solo se si esegue il software Cisco IOS versione 12.1(11)EW o precedenti. Questo comando è obsoleto. Tuttavia, questo precedente comando faceva parte del comando show tech-support delle versioni del software Cisco IOS precedenti alla versione 12.2(20)EWA.

Usare il comando show platform cpu packet statistics per tutte le procedure di risoluzione dei problemi.

<#root>

```
Switch#
show platform cpu packet statistics all

!--- Output suppressed.

Total packet queues 16

Packets Received by Packet Queue

Queue                  Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- --------------- --------- --------- --------- ----------
Esmp                               0         0         0         0          0
Control                           48         0         0         0          0
Host Learning                      0         0         0         0          0
L3 Fwd High                        0         0         0         0          0
L3 Fwd Medium                      0         0         0         0          0
L3 Fwd Low                         0         0         0         0          0
L2 Fwd High                        0         0         0         0          0
L2 Fwd Medium                      0         0         0         0          0
L2 Fwd Low                         0         0         0         0          0
```

```
L3 Rx High                          0         0         0         0         0
L3 Rx Low                           0         0         0         0         0
RPF Failure                         0         0         0         0         0
ACL fwd(snooping)                   0         0         0         0         0
ACL log, unreach                    0         0         0         0         0
ACL sw processing                   0         0         0         0         0
MTU Fail/Invalid                    0         0         0         0         0

Packets Dropped by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- --------------- --------- --------- --------- ----------
Esmp                                0         0         0         0          0
Control                             0         0         0         0          0
Host Learning                       0         0         0         0          0
L3 Fwd High                         0         0         0         0          0
L3 Fwd Medium                       0         0         0         0          0
L3 Fwd Low                          0         0         0         0          0
L2 Fwd High                         0         0         0         0          0
L2 Fwd Medium                       0         0         0         0          0
L2 Fwd Low                          0         0         0         0          0
L3 Rx High                          0         0         0         0          0
L3 Rx Low                           0         0         0         0          0
RPF Failure                         0         0         0         0          0
ACL fwd(snooping)                   0         0         0         0          0
ACL log, unreach                    0         0         0         0          0
ACL sw processing                   0         0         0         0          0
MTU Fail/Invalid                    0         0         0         0          0
```

La CPU Catalyst 4500 assegna dei pesi alle varie code elencate nella tabella 1. La CPU assegna i pesi in base all'importanza o al tipo e in base alla priorità del traffico o DSCP. La CPU serve la coda in base al peso relativo della coda. Ad esempio, se sono in sospeso sia un pacchetto di controllo, come un BPDU, sia una richiesta echo ICMP, la CPU serve prima il pacchetto di controllo. Una quantità eccessiva di traffico a bassa priorità o meno importante non priva la CPU della capacità di elaborare o gestire il sistema. Questo meccanismo garantisce che la rete sia stabile anche in caso di elevato utilizzo della CPU. Questa capacità della rete di mantenere la stabilità è un'informazione critica che è necessario comprendere.

Un altro dettaglio molto importante riguarda la gestione dei pacchetti della CPU Catalyst 4500. Se la CPU ha già servito pacchetti o processi ad alta priorità ma dispone di più cicli CPU di riserva per un determinato periodo di tempo, la CPU servirà i pacchetti della coda a bassa priorità o eseguirà processi in background di priorità inferiore. L'elevato utilizzo della CPU risultante dall'elaborazione di pacchetti a bassa priorità o da processi in background è considerato normale in quanto la CPU tenta costantemente di utilizzare tutto il tempo disponibile. In questo modo, la CPU si sforza di ottenere le massime prestazioni dello switch e della rete senza compromettere la stabilità dello switch. Catalyst 4500 considera la CPU sottoutilizzata a meno che non venga utilizzata al 100% per un singolo intervallo di tempo.

Il software Cisco IOS versione 12.2(25)EWA2 e successive ha migliorato il meccanismo di gestione e l'accounting dei pacchetti e dei processi della CPU. Pertanto, è possibile usare queste versioni sulle implementazioni Catalyst 4500.

Identificazione del motivo di un elevato utilizzo della CPU su Catalyst 4500

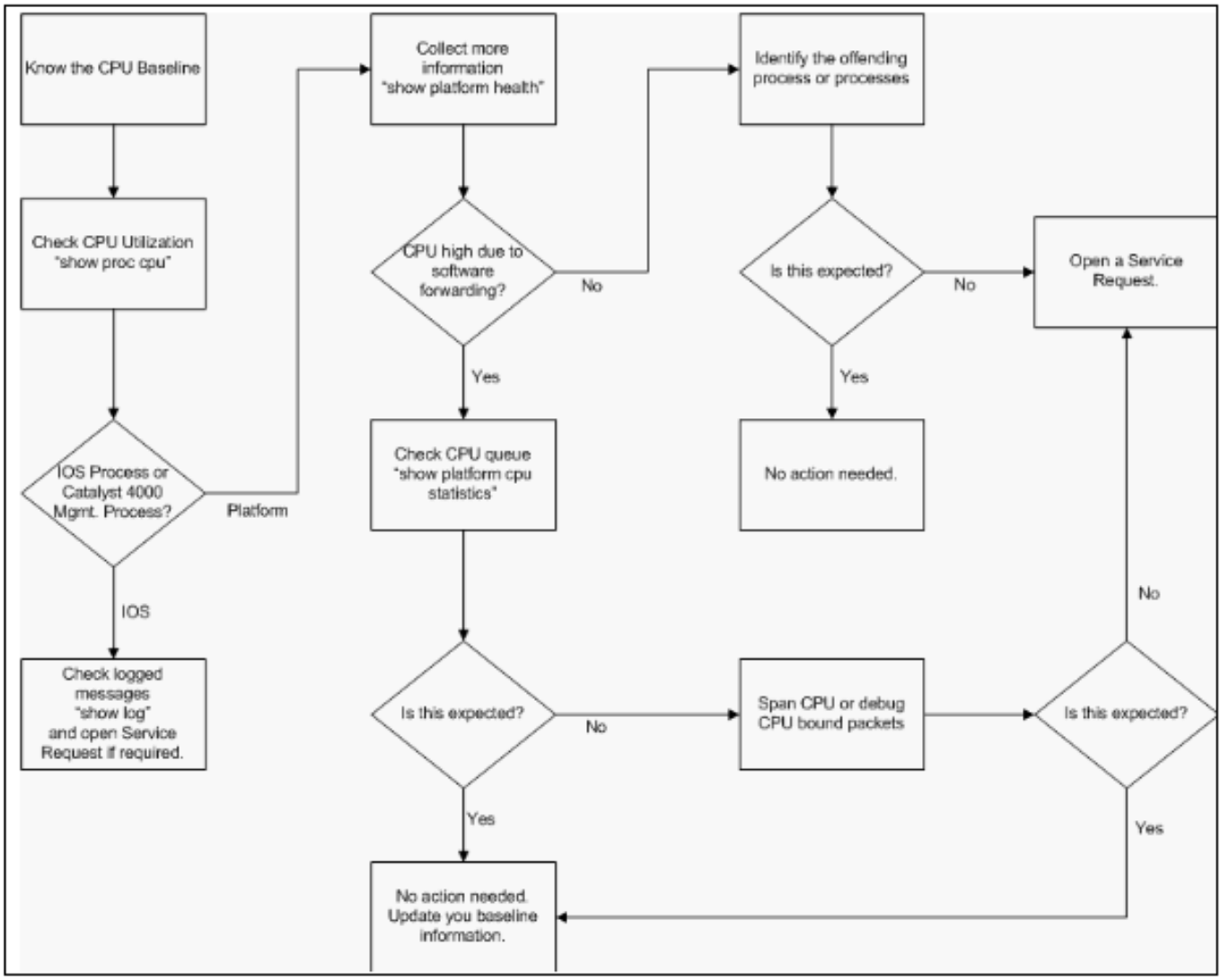
Dopo aver compreso l'architettura e il design per la gestione dei pacchetti della CPU Catalyst 4500, è possibile identificare i motivi per cui l'utilizzo della CPU Catalyst 4500 è elevato. Catalyst 4500 dispone dei comandi e degli strumenti necessari per identificare la causa principale dell'elevato utilizzo della CPU. Dopo aver identificato il motivo, gli amministratori possono eseguire una delle azioni seguenti:

- Azioni correttive: possono includere modifiche alla configurazione o alla rete o la creazione di una richiesta di assistenza tecnica Cisco per un'ulteriore analisi.
- Nessuna azione: le prestazioni di Catalyst 4500 sono conformi alle aspettative. La CPU mostra un elevato utilizzo della CPU perché il Supervisor Engine massimizza i cicli della CPU in modo da eseguire tutti i processi necessari di inoltro e in background dei pacchetti software.

Accertarsi di identificare il motivo dell'elevato utilizzo della CPU anche se non è sempre necessario intraprendere azioni correttive. L'utilizzo elevato della CPU può essere solo un sintomo di un problema nella rete. Per ridurre l'utilizzo della CPU può essere necessaria una risoluzione della causa principale del problema.

Nella Figura 2 viene illustrata la metodologia di risoluzione dei problemi da utilizzare per identificare la causa principale dell'elevato utilizzo della CPU da parte di Catalyst 4500.

Figura 2 - Metodologia di risoluzione dei problemi di utilizzo elevato della CPU sugli switch Catalyst 4500



Metodologia di risoluzione dei problemi di utilizzo elevato della CPU sugli switch Catalyst 4500

Le operazioni generali per la risoluzione dei problemi sono:

1. Utilizzare il comando show processes cpu per identificare i processi Cisco IOS che utilizzano i cicli della CPU.
2. Utilizzare il comando show platform health per identificare ulteriormente i processi specifici della piattaforma.
3. Se il processo altamente attivo è `K2CpuMan Review`, usare il comando show platform cpu packet statistics per identificare il tipo di traffico che colpisce la CPU.

   Se l'attività non è dovuta al processo `di` revisione di `K2CpuMan`, saltare il passaggio 4 e andare al passaggio 5.
4. Se necessario, identificare i pacchetti che raggiungono la CPU utilizzando gli strumenti di risoluzione dei problemi per analizzare il traffico destinato alla CPU.

   Un esempio degli strumenti di risoluzione dei problemi da utilizzare è lo SPAN (CPU

Switched Port Analyzer).

5. Per le cause più comuni, consultare il documento e la sezione Risoluzione dei problemi comuni di utilizzo elevato della CPU.

   Se non è ancora possibile identificare la causa principale, contattare il supporto tecnico Cisco.

Previsione dell'utilizzo CPU

Il primo passaggio importante è conoscere l'utilizzo della CPU dello switch per la configurazione e la configurazione della rete. Per identificare l'utilizzo della CPU sullo switch Catalyst 4500, usare il comando show processes . L'aggiornamento continuo dell'utilizzo della CPU di base può essere necessario quando si aggiunge una maggiore configurazione all'installazione della rete o quando cambia il modello di traffico di rete.La Figura 2 indica questo requisito.

Questo output viene generato da un Catalyst 4507R a pieno carico. La CPU allo stato stazionario è pari a circa il 32-38%, condizione necessaria per eseguire le funzioni di gestione dello switch:

<#root>

```
Switch#
show processes cpu


CPU utilization for five seconds: 38%/1%; one minute: 32%; five minutes: 32%

 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0        63          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2          60     50074          1  0.00%  0.00%  0.00%   0 Load Meter
   3           0         1          0  0.00%  0.00%  0.00%   0 Deferred Events

!--- Output suppressed.

  27         524    250268          2  0.00%  0.00%  0.00%   0 TTY Background
  28         816    254843          3  0.00%  0.00%  0.00%   0 Per-Second Jobs
  29      101100      5053      20007  0.00%  0.01%  0.00%   0 Per-minute Jobs


30    26057260  26720902        975 12.07% 11.41% 11.36%   0 Cat4k Mgmt HiPri
  31    19482908  29413060        662 24.07% 19.32% 19.20%   0 Cat4k Mgmt LoPri

  32        4468    162748         27  0.00%  0.00%  0.00%   0 Galios Reschedul
  33           0         1          0  0.00%  0.00%  0.00%   0 Cisco IOS ACL Helper
  34           0         2          0  0.00%  0.00%  0.00%   0 NAM Manager
```

L'utilizzo della CPU per cinque secondi viene espresso come segue:

x%/y%

Thex% rappresenta l'utilizzo totale della CPU, andy% rappresenta la CPU spesa a livello di interrupt. per la risoluzione dei problemi relativi agli switch Catalyst 4500, considerare solo l'utilizzo totale della CPU.

Comprendere il comando show processes cpu sugli switch Catalyst 4500

In questo modo i processi cpuoutput mostrano che la CPU è utilizzata da due processi: **Cat4k Mgmt HiPriandCat4k Mgmt LoPri**. Questi due processi aggregano più processi specifici della piattaforma che eseguono le principali funzioni di gestione su Catalyst 4500. Questi processi elaborano il control plane e i pacchetti di dati che devono essere commutati o elaborati dal software.

Per vedere quale dei processi specifici della piattaforma usa la CPU nel contesto **di Cat4k Mgmt HiPriandCat4k Mgmt LoPri**, usare il comando show platform health.

Ciascun processo specifico della piattaforma ha un utilizzo previsto/di destinazione della CPU. Quando il processo si trova all'interno della destinazione, la CPU lo esegue nel contesto ad alta priorità. L'output del comando cpushow PROCESSES conta l'utilizzo **in Cat4k Mgmt HiPri**. Se un processo supera l'utilizzo previsto/di destinazione, viene eseguito nel contesto a bassa priorità. L'output di cpucommand di questi processi conta l'utilizzo aggiuntivo **inCat4k Mgmt LoPri**. **QuestoCat4k Mgmt** LoPriis viene utilizzato anche per eseguire processi in background e altri processi a bassa priorità, come la verifica della coerenza e la lettura dei contatori dell'interfaccia. Questo meccanismo consente alla CPU di eseguire processi ad alta priorità quando necessario e i cicli di CPU inattivi rimanenti vengono utilizzati per i processi a bassa priorità. Il superamento dell'utilizzo della CPU di destinazione di una piccola quantità, o di un picco momentaneo nell'utilizzo, non è un'indicazione di un problema che richiede un'analisi.

<#root>

```
Switch#

show platform health


                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                1.00

0.02

      2      1  100  500    0

0    0

  1:09
GalChassisVp-review    3.00

0.29

     10      3  100  500    0

0    0

  11:15
S2w-JobEventSchedule  10.00

0.32
```

```
     10      7  100  500    0
0    0
  10:14
Stub-JobEventSchedul  10.00
12.09
     10      6  100  500   14
13    9
  396:35
StatValueMan Update    1.00
0.22
      1      0  100  500    0
0    0
  6:28
Pim-review             0.10
0.00
      1      0  100  500    0
0    0
  0:22
Ebm-host-review        1.00
0.00
      8      0  100  500    0
0    0
  0:05
Ebm-port-review        0.10
0.00
      1      0  100  500    0
0    0
  0:01
Protocol-aging-revie   0.20
0.00
      2      0  100  500    0
0    0
  0:00
Acl-Flattener  e       1.00
0.00
     10      0  100  500    0
0    0
  0:00
KxAclPathMan create/   1.00
```

0.00

     10   5 100 500   0

0   0

  0:39
KxAclPathMan update   2.00

0.00

     10   0 100 500   0

0   0

  0:00
KxAclPathMan reprogr   1.00

0.00

      2   0 100 500   0

0   0

  0:00
TagMan-RecreateMtegR   1.00

0.00

     10   0 100 500   0

0   0

  0:00
K2CpuMan Review   30.00

10.19

     30   28 100 500   14

13   9

  397:11
K2AccelPacketMan: Tx 10.00

2.20

     20   0 100 500   2

2   1

  82:06
K2AccelPacketMan: Au   0.10

0.00

      0   0 100 500   0

0   0

  0:00
K2AclMan-taggedFlatA   1.00

0.00

     10   0 100 500   0

0   0

  0:00

K2AclCamMan stale en   1.00

0.00

     10   0 100 500   0

0   0

  0:00
K2AclCamMan hw stats   3.00

1.04

     10   5 100 500   1

1   0

  39:36
K2AclCamMan kx stats   1.00

0.00

     10   5 100 500   0

0   0

  13:40
K2AclCamMan Audit re   1.00

0.00

     10   5 100 500   0

0   0

  13:10
K2AclPolicerTableMan   1.00

0.00

     10   1 100 500   0

0   0

  0:38
K2L2 Address Table R   2.00

0.00

     12   5 100 500   0

0   0

  0:00
K2L2 New Static Addr   2.00

0.00

     10   1 100 500   0

0   0

  0:00
K2L2 New Multicast A   2.00

0.00

     10   5 100 500   0

0   0

  0:01
K2L2 Dynamic Address   2.00

0.00

     10   0 100 500   0

0   0

  0:00
K2L2 Vlan Table Revi   2.00

0.00

     12   9 100 500   0

0   0

  0:01
K2 L2 Destination Ca   2.00

0.00

     10   0 100 500   0

0   0

  0:00
K2PortMan Review   2.00

0.72

     15   11 100 500   1

1   0

  37:22
Gigaport65535 Review   0.40

0.07

      4   2 100 500   0

0   0

  3:38
Gigaport65535 Review   0.40

0.08

      4   2 100 500   0

0   0

  3:39
K2Fib cam usage revi   2.00

0.00

     15   0 100 500   0

0   0

  0:00
K2Fib IrmFib Review   2.00

0.00

     15   0 100 500   0

0 0

0:00
K2Fib Vrf Default Ro 2.00

0.00

15 0 100 500 0

0 0

0:00
K2Fib AdjRepop Revie 2.00

0.00

15 0 100 500 0

0 0

0:00
K2Fib Vrf Unpunt Rev 2.00

0.01

15 0 100 500 0

0 0

0:23
K2Fib Consistency Ch 1.00

0.00

5 2 100 500 0

0 0

29:25
K2FibAdjMan Stats Re 2.00

0.30

10 4 100 500 0

0 0

6:21
K2FibAdjMan Host Mov 2.00

0.00

10 4 100 500 0

0 0

0:00
K2FibAdjMan Adj Chan 2.00

0.00

10 0 100 500 0

0 0

0:00
K2FibMulticast Signa 2.00

0.01

```
     10      2  100  500    0
0    0
  2:04
K2FibMulticast Entry   2.00
0.00
     10      7  100  500    0
0    0
  0:00
K2FibMulticast Irm M   2.00
0.00
     10      7  100  500    0
0    0
  0:00
K2FibFastDropMan Rev   2.00
0.00
      7      0  100  500    0
0    0
  0:00
K2FibPbr route map r   2.00
0.06
     20      5  100  500    0
0    0
  16:42
K2FibPbr flat acl pr   2.00
0.07
     20      2  100  500    0
0    0
  3:24
K2FibPbr consolidati   2.00
0.01
     10      0  100  500    0
0    0
  0:24
K2FibPerVlanPuntMan    2.00
0.00
     15      4  100  500    0
0    0
  0:00
K2FibFlowCache flow    2.00
```

0.01

     10   0 100 500   0

0   0

  0:23
K2FibFlowCache flow   2.00

0.00

     10   0 100 500   0

0   0

  0:00
K2FibFlowCache adj r   2.00

0.01

     10   0 100 500   0

0   0

  0:20
K2FibFlowCache flow   2.00

0.00

     10   0 100 500   0

0   0

  0:06
K2MetStatsMan Review   2.00

0.14

      5   2 100 500   0

0   0

  23:40
K2FibMulticast MET S   2.00

0.00

     10   0 100 500   0

0   0

  0:00
K2QosDblMan Rate DBL   2.00

0.12

      7   0 100 500   0

0   0

  4:52
IrmFibThrottler Thro   2.00

0.01

      7   0 100 500   0

0   0

  0:21

K2 VlanStatsMan Revi   2.00

1.46

     15   7 100 500   2

2   1

  64:44
K2 Packet Memory Dia   2.00

0.00

     15   8 100 500   0

1   1

  45:46
K2 L2 Aging Table Re   2.00

0.12

     20   3 100 500   0

0   0

  7:22
RkiosPortMan Port Re   2.00

0.73

     12   7 100 500   1

1   1

  52:36
Rkios Module State R   4.00

0.02

     40   1 100 500   0

0   0

  1:28
Rkios Online Diag Re   4.00

0.02

     40   0 100 500   0

0   0

  1:15
RkiosIpPbr IrmPort R   2.00

0.02

     10   3 100 500   0

0   0

  2:44
RkiosAclMan Review   3.00

0.06

     30   0 100 500   0

0   0

  2:35
MatMan Review   0.50

0.00

      4   0 100 500   0

0   0

  0:00
Slot 3 ILC Manager R   3.00

0.00

     10   0 100 500   0

0   0

  0:00
Slot 3 ILC S2wMan Re   3.00

0.00

     10   0 100 500   0

0   0

  0:00
Slot 4 ILC Manager R   3.00

0.00

     10   0 100 500   0

0   0

  0:00
Slot 4 ILC S2wMan Re   3.00

0.00

     10   0 100 500   0

0   0

  0:00
Slot 5 ILC Manager R   3.00

0.00

     10   0 100 500   0

0   0

  0:00
Slot 5 ILC S2wMan Re   3.00

0.00

     10   0 100 500   0

0   0

  0:00
Slot 6 ILC Manager R   3.00

0.00

     10   0 100 500   0

```
0    0

  0:00
Slot 6 ILC S2wMan Re   3.00

0.00

     10      0  100  500    0

0    0

  0:00
Slot 7 ILC Manager R   3.00

0.00

     10      0  100  500    0

0    0

  0:00
Slot 7 ILC S2wMan Re   3.00

0.00

     10      0  100  500    0

0    0

  0:00
EthHoleLinecardMan(1   1.66

0.04

     10      0  100  500    0

0    0

  1:18
EthHoleLinecardMan(2   1.66

0.02

     10      0  100  500    0

0    0

  1:18
EthHoleLinecardMan(6   1.66

0.17

     10      6  100  500    0

0    0

  6:38
                      -------------
%CPU Totals           212.80

35.63
```

Comprendere il comando show platform health sugli switch Catalyst 4500

In questo comando show platform health sono disponibili numerose informazioni utili solo per i

tecnici di sviluppo. Per risolvere i problemi relativi a un utilizzo elevato della CPU, cercare un numero più alto nella colonna %CPU effettivo nell'output. Inoltre, assicurarsi di guardare il lato destro della riga per verificare l'utilizzo della CPU da parte del processo nelle colonne %CPU medie di 1 minuto e 1 ora. A volte i processi raggiungono momentaneamente il picco massimo ma non mantengono la CPU per molto tempo. Parte dell'utilizzo momentaneamente elevato della CPU si verifica durante la programmazione hardware o l'ottimizzazione della programmazione. Ad esempio, un picco di utilizzo della CPU è normale durante la programmazione hardware di un ACL di grandi dimensioni nella TCAM.

Nell'output del comando show platform health nella sezioneInformazioni sul comando show processes cpu sugli switch Catalyst 4500, i processi Stub-JobEventSchedule **K2CpuMan** Reviewprocess utilizzano un numero maggiore di cicli di CPU.La tabella 2 fornisce alcune informazioni di base sui processi comuni specifici della piattaforma che compaiono nell'output del comando show platform health.

Tabella 2 - Descrizione dei processi specifici della piattaforma dal comando show platform health

Nome processo specifico della piattaforma	Descrizione
Pim-review	Gestione stato chassis/scheda di linea
Ebm	Modulo bridge Ethernet, ad esempio monitoraggio e misurazione durata
Acl-Flattener/K2AclMan	Processo di unione ACL
KxAclPathMan - PathTagMan-Review	Gestione e manutenzione dello stato degli ACL
Recensione di K2CpuMan	Processo che esegue l'inoltro dei pacchetti software Se si riscontra un elevato utilizzo della CPU a causa di questo processo, esaminare i pacchetti che raggiungono la CPU con il comando show platform cpu packet statistics.
K2AccelPacketMan	Driver che interagisce con il modulo di gestione pacchetti per inviare pacchetti destinati dalla CPU
UomoCammaK2Acl	Gestisce l'hardware TCAM di input e output per le funzioni QoS e di sicurezza
Oggetto K2AclPolicerTableMan	Gestisce i criteri di input e output
K2L2	Rappresenta il sottosistema di inoltro L2 del software Catalyst 4500 Cisco IOS. Questi processi sono responsabili della manutenzione delle varie tabelle L2.
Recensione di K2PortMan	Gestisce le varie funzioni di programmazione relative alle porte
K2Fib	Gestione FIB[1]
K2FibFlowCache	Gestione cache PBR[2]
AdattatoreK2Fib	Gestione tabelle adiacenti FIB
Multicast K2Fib	Gestisce le voci FIB multicast
Recensione di K2MetStatsMan	Gestisce le statistiche MET[3]

Recensione di K2QosDblMan	Gestisce QoS DBL[4]
IrmFibThrottler Thro	Modulo di routing IP
Re tabella di aging K2 L2	Gestisce la funzione di aging L2
GalChassisVp-review	Monitoraggio dello stato dello chassis
S2w-PianificazioneEventiProcesso	Gestisce i protocolli S2W[5] per monitorare lo stato delle schede di linea
Stub-JobEventScheduled	Monitoraggio e manutenzione delle schede di linea basate su ASIC Stub
RichPortMan Port Re	Monitoraggio e manutenzione dello stato delle porte
R stato modulo Rkios	Monitoraggio e manutenzione della scheda di linea
EthHoleLinecardMan	Gestisce i GBIC[6]in ciascuna scheda di linea

[1]FIB = Base informazioni di inoltro.

[2]PBR = policy-based routing.

[3]MET = Tabella di espansione multicast.

[4]DBL = Limitazione dinamica del buffer.

[5]S2W = da seriale a filo.

[6]GBIC = Gigabit Interface Converter.

Risoluzione dei problemi comuni di utilizzo elevato della CPU

In questa sezione vengono illustrati alcuni dei più comuni problemi di utilizzo elevato della CPU sugli switch Catalyst 4500.

Utilizzo elevato della CPU dovuto a pacchetti con commutazione di contesto

Una delle cause più comuni dell'elevato utilizzo della CPU è che la CPU Catalyst 4500 è occupata dal processo di inoltro di pacchetti software o di pacchetti di controllo. Esempi di pacchetti inoltrati dal software sono i pacchetti IPX o i pacchetti di controllo, come i BPDU. Un piccolo numero di questi pacchetti viene in genere inviato alla CPU. Tuttavia, un numero elevato di pacchetti può indicare un errore di configurazione o un evento di rete. È necessario identificare la causa degli eventi che portano all'inoltro dei pacchetti alla CPU per l'elaborazione. Questa identificazione consente di eseguire il debug dei problemi di utilizzo elevato della CPU.

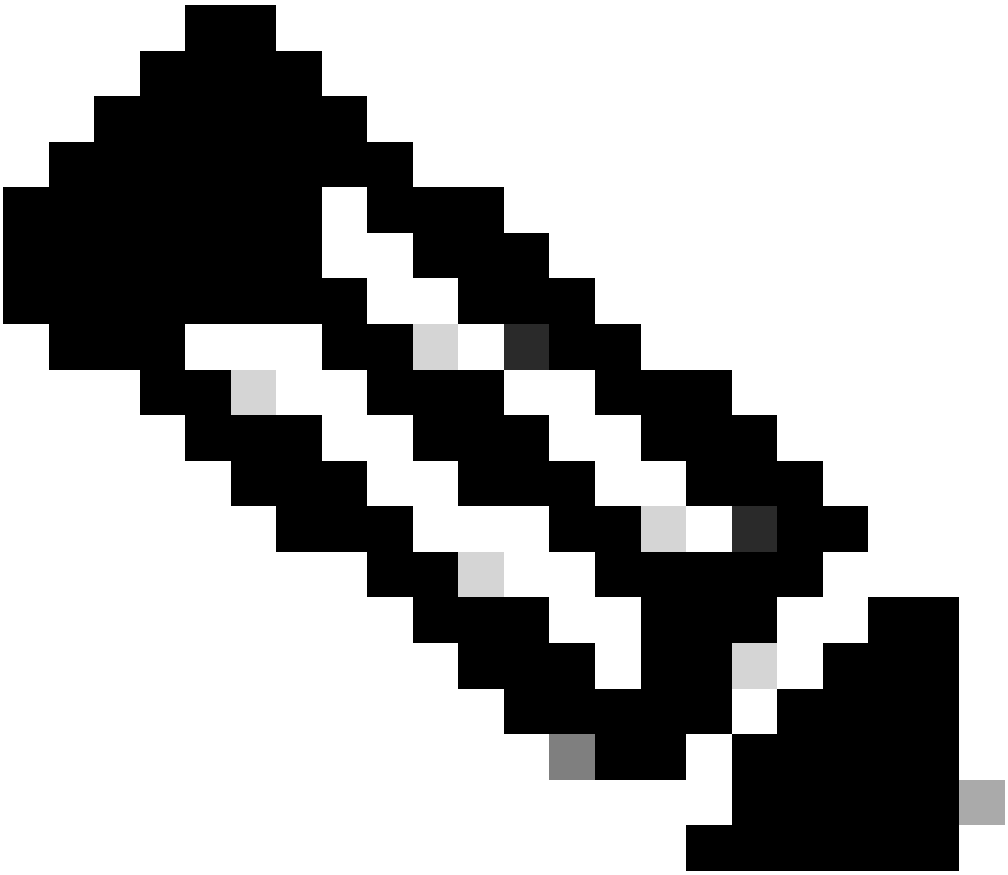
Alcuni dei motivi più comuni dell'elevato utilizzo della CPU dovuto ai pacchetti a commutazione di contesto sono:

- Numero elevato di istanze di porte Spanning-Tree
- Reindirizzamenti ICMP; routing di pacchetti sulla stessa interfaccia

- Routing IPX o AppleTalk
- Apprendimento host
- Risorse hardware (TCAM) esaurite per ACL di sicurezza
- Thelogkeyword in ACL
- Loop di inoltro di livello 2

Altri motivi del passaggio dei pacchetti alla CPU sono:

- Frammentazione MTU: verificare che tutte le interfacce sul percorso del pacchetto abbiano la stessa MTU.
- ACL con flag TCP diversi da quelli stabiliti
- Routing IP versione 6 (IPv6): supportato solo tramite il percorso di commutazione software.
- GRE: questa operazione è supportata solo tramite il percorso di commutazione software.
- Rifiuto del traffico nell'ACL (RACL) del router di input o output



Nota: questa funzionalità è soggetta a limitazioni di velocità nel software Cisco IOS versione 12.1(13)EW1 e successive.

Usare il comando no ip unreachablesnell'interfaccia dell'ACL.

- Traffico ARP e DHCP eccessivo sulla CPU per l'elaborazione a causa di un numero elevato di host connessi direttamente

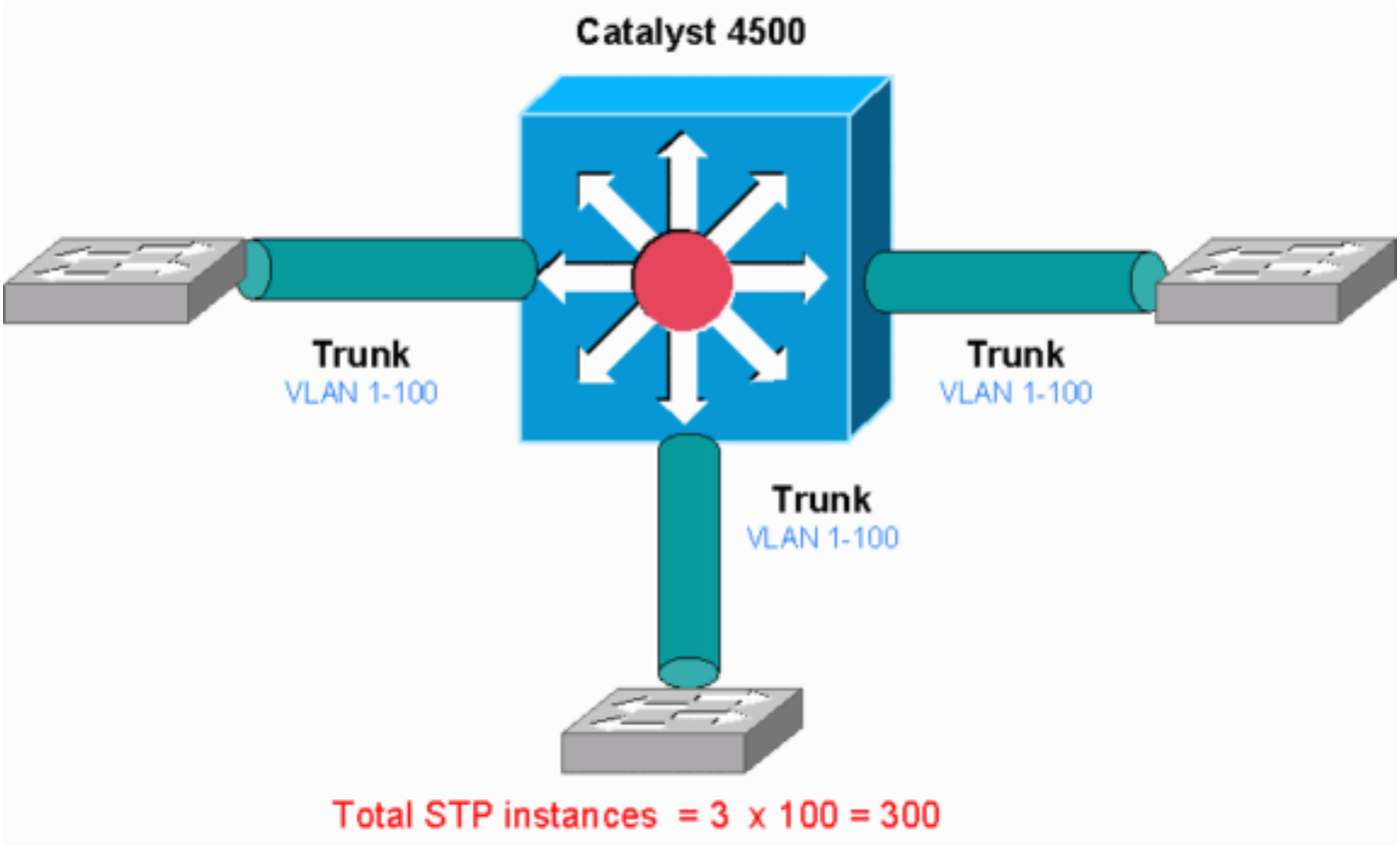
  Se si sospetta la presenza di un attacco DHCP, utilizzare lo snooping DHCP per limitare la velocità del traffico DHCP proveniente da una porta host specifica.

- Polling SNMP eccessivo da parte di una stazione terminale legittima o con comportamento errato

Numero elevato di istanze di porte Spanning-Tree

Catalyst 4500 supporta 3000 istanze di porte Spanning-Tree o porte attive in modalità Per VLAN Spanning Tree+ (PVST+). Il supporto è disponibile su tutti i Supervisor Engine, ad eccezione di Supervisor Engine II+ e II+TS, e Catalyst 4948. Supervisor Engine II+ e II+TS e Catalyst 4948

supportano fino a 1500 istanze di porte. Se si superano i valori consigliati per le istanze STP, lo switch mostra un elevato utilizzo della CPU.



Catalyst 4500

Il diagramma mostra uno switch Catalyst 4500 con tre porte trunk ciascuna con VLAN da 1 a 100. Questo valore equivale a 300 istanze di porta spanning-tree. In generale, è possibile calcolare le istanze della porta Spanning-Tree con questa formula:

```
Total number of STP instances = Number of access ports + Sum of all VLANs
that are carried in each of the trunks
```

Nel diagramma non ci sono porte di accesso, ma i tre trunk trasportano le VLAN da 1 a 100:

```
Total number of STP instances = 0 + 100 + 100 + 100 = 300
```

Passaggio 1: verificare la presenza del processo Cisco IOS con `show processes cpu` il comando.

In questa sezione vengono esaminati i comandi utilizzati dall'amministratore per risolvere il problema dell'utilizzo elevato della CPU. Se si esegue il comando **show processes cpu**, si osserverà che due processi principali, **`Cat4k Mgmt LoPriandSpanning Tree`**, utilizzano principalmente la CPU. Utilizzando solo queste informazioni, lo Spanning Tree utilizza una parte considerevole dei cicli della CPU.

<#root>

Switch#

show processes cpu

```
CPU utilization for five seconds: 74%/1%; one minute: 73%; five minutes: 50%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4       198         20  0.00%  0.00%  0.00%   0 Chunk Manager
   2           4       290         13  0.00%  0.00%  0.00%   0 Load Meter

!--- Output suppressed.

  25         488        33      14787  0.00%  0.02%  0.00%   0 Per-minute Jobs
  26       90656    223674        405  6.79%  6.90%  7.22%   0 Cat4k Mgmt HiPri

 27      158796     59219       2681 32.55% 33.80% 21.43%   0 Cat4k Mgmt LoPri

  28          20      1693         11  0.00%  0.00%  0.00%   0 Galios Reschedul
  29           0         1          0  0.00%  0.00%  0.00%   0 Cisco IOS ACL Helper
  30           0         2          0  0.00%  0.00%  0.00%   0 NAM Manager

!--- Output suppressed.

  41           0         1          0  0.00%  0.00%  0.00%   0 SFF8472
  42           0         2          0  0.00%  0.00%  0.00%   0 AAA Dictionary R

 43       78564     20723       3791 32.63% 30.03% 17.35%   0 Spanning Tree

  44         112       999        112  0.00%  0.00%  0.00%   0 DTP Protocol
  45           0       147          0  0.00%  0.00%  0.00%   0 Ethchnl
```

Passaggio 2: verificare la presenza del processo specifico di Catalyst 4500 con il comando show platform health.

Per comprendere quale processo specifico della piattaforma utilizza la CPU, eseguire **il** comando **show platform** health. Da questo output, è possibile vedere che **`il processo K2CpuMan`** Reviewprocess, un processo per gestire i pacchetti basati sulla CPU, utilizza fino alla CPU:

```
<#root>

Switch#

show platform health

%CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                 Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU

!--- Output suppressed.

TagMan-RecreateMtegR   1.00   0.00     10      0  100  500    0   0    0  0:00

K2CpuMan Review       30.00  37.62     30     53  100  500   41  33    1  2:12

K2AccelPacketMan: Tx  10.00   4.95     20      0  100  500    5   4    0  0:36
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
K2AclMan-taggedFlatA   1.00   0.00     10      0  100  500    0   0    0  0:00
```

Passaggio 3: controllare la coda CPU che riceve il traffico per identificare il tipo di traffico basato sulla CPU.

Utilizzare il show platform cpu packet statisticscomando per verificare quale coda CPU riceve il pacchetto basato sulla CPU. L'output in questa sezione mostra che la coda di controllo riceve molti pacchetti. Utilizzare le informazioni riportate nella Tabella 1 e le conclusioni tratte nel Passaggio 1. È possibile stabilire che i pacchetti elaborati dalla CPU e il motivo dell'utilizzo elevato della CPU siano l'elaborazione BPDU.

```
<#root>
```

```
Switch#
```

show platform cpu packet statistics

```
!--- Output suppressed.

Total packet queues 16
Packets Received by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
----------------------- --------------- --------- --------- --------- ----------
Esmp                           202760       196       173       128         28


Control                        388623      2121      1740       598         16


Packets Dropped by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
----------------------- --------------- --------- --------- --------- ----------
Control                         17918         0        19        24          3
```

Passaggio 4: Identificare la root cause.

Eseguire il show spanning-tree summarycomando. È possibile verificare se la ricezione di BPDU è causata da un numero elevato di istanze di porte Spanning-Tree. L'output identifica chiaramente la causa principale:

```
    <#root>

Switch#
```

show spanning-tree summary

```
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

!--- Output suppressed.

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------



2994 vlans                0         0        0       5999       5999
```

Le VLAN in modalità PVST+ sono numerose. Per risolvere il problema, modificare la modalità STP in Multiple Spanning Tree (MST). In alcuni casi, il numero di istanze STP è elevato perché su tutte le porte trunk viene inoltrato un numero elevato di VLAN. In questo caso, eliminare manualmente le VLAN non necessarie dal trunk per ridurre il numero di porte attive STP al di sotto del valore consigliato.

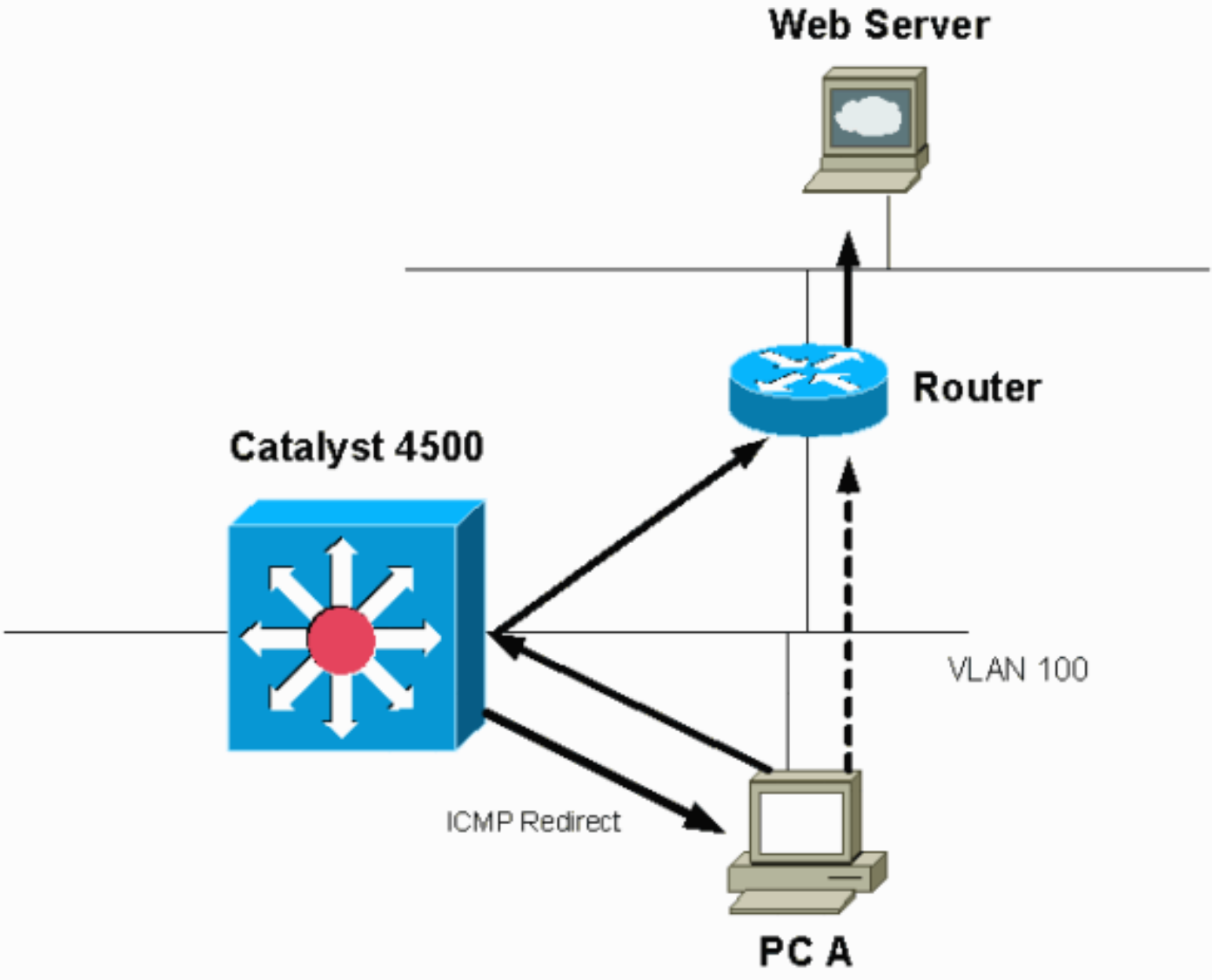
Suggerimento: verificare di non configurare le porte telefoniche IP come porte trunk. Questa è una configurazione errata comune. Configurare le porte telefoniche IP con una configurazione VLAN voce. Questa configurazione crea uno pseudo trunk, ma non richiede l'eliminazione manuale delle VLAN non necessarie. Per ulteriori informazioni su come configurare le porte vocali, consultare la guida alla configurazione delle interfacce vocali. I telefoni IP non Cisco non supportano questa configurazione VLAN voce o VLAN ausiliaria. È necessario eliminare manualmente le porte con telefoni IP non Cisco.

Reindirizzamenti ICMP; routing di pacchetti sulla stessa interfaccia

Il routing di pacchetti sulla stessa interfaccia, o il traffico in entrata e in uscita sulla stessa interfaccia L3, può causare un reindirizzamento ICMP da parte dello switch. se lo switch sa che il dispositivo che si desidera passare alla destinazione finale si trova nella stessa subnet del dispositivo di invio, genera un reindirizzamento ICMP verso l'origine. I messaggi di reindirizzamento indicano all'origine di inviare il pacchetto direttamente al dispositivo dell'hop successivo. I messaggi indicano che il dispositivo dell'hop successivo ha un percorso migliore verso la destinazione, ossia un percorso con un hop in meno rispetto allo switch.

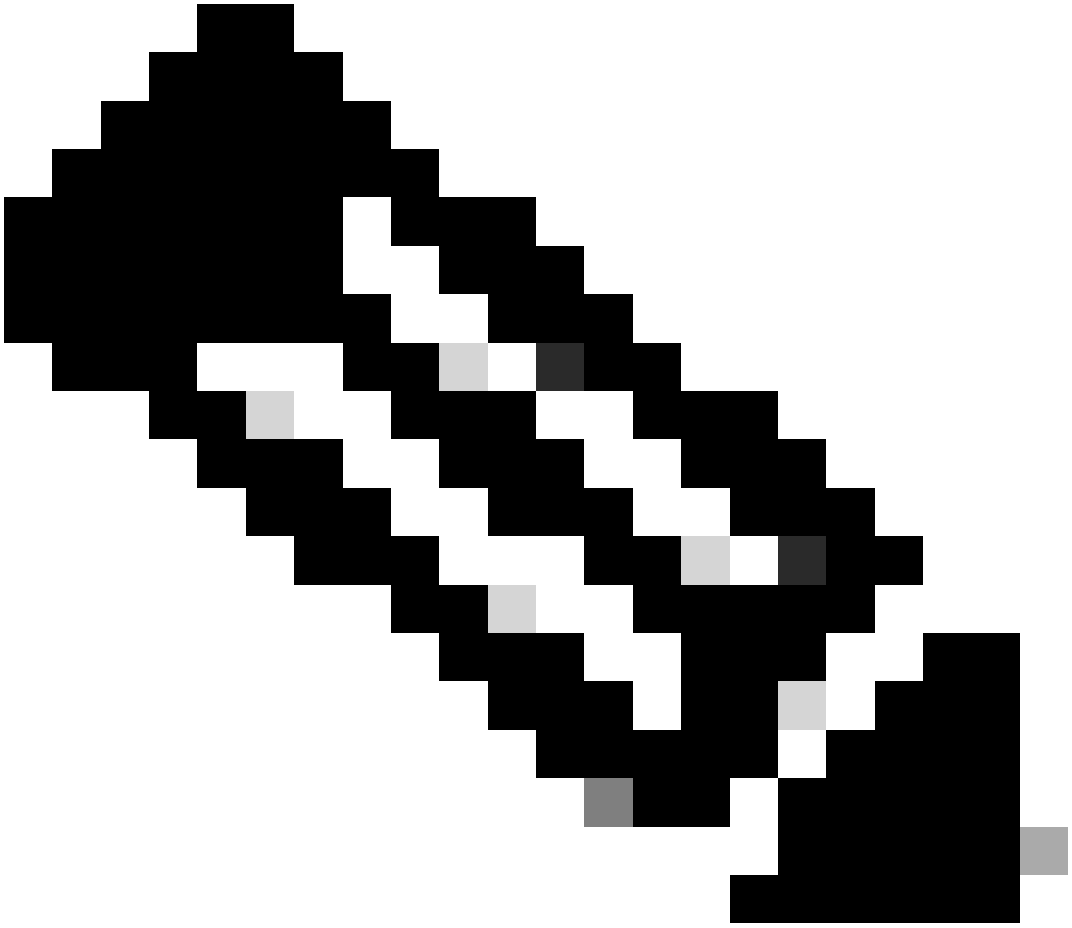
Nello schema di questa sezione, il PC A comunica con il server Web. Il gateway predefinito del PC A punta all'indirizzo IP dell'interfaccia VLAN 100. Tuttavia, il router dell'hop successivo che consente al Catalyst 4500 di raggiungere la destinazione è nella stessa subnet del PC A. Il modo migliore in questo caso è inviare direttamente al router. Catalyst 4500 invia un messaggio di reindirizzamento ICMP al PC A. Il messaggio indica al PC A di inviare i pacchetti destinati al server Web tramite il router, anziché tramite Catalyst 4500. Tuttavia, nella maggior parte dei casi, i dispositivi terminali non rispondono al reindirizzamento ICMP. A causa della mancanza di risposta, Catalyst 4500 impiega molti cicli della CPU nella generazione di questi reindirizzamenti ICMP per tutti i pacchetti che Catalyst inoltra tramite la stessa interfaccia dei

pacchetti in entrata.



Per impostazione predefinita, il reindirizzamento ICMP è abilitato.

Per impostazione predefinita, il reindirizzamento ICMP è abilitato. Per disabilitarla, usare il **ip icmp redirects**comando. Eseguire il comando nell'interfaccia SVI o L3 pertinente.



Nota: poiché **ip icmp redirects** è un comando predefinito, non è visibile nell'output del show running-configuration comando.

Passaggio 1: Controllare il processo Cisco IOS con il show processes cpu comando.

Eseguire il show processes cpu comando. Si può notare che due processi principali, **`Cat4k Mgmt LoPriandIP Input`**, utilizzano principalmente la CPU. Con queste sole informazioni, si sa che il processo dei pacchetti IP spende una parte considerevole della CPU.

<#root>

```
Switch#
```

show processes cpu

CPU utilization for five seconds: 38%/1%; one minute: 32%; five minutes: 32%

```
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0        63          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2          60     50074          1  0.00%  0.00%  0.00%   0 Load Meter
   3           0         1          0  0.00%  0.00%  0.00%   0 Deferred Events

!--- Output suppressed.

  27         524    250268          2  0.00%  0.00%  0.00%   0 TTY Background
  28         816    254843          3  0.00%  0.00%  0.00%   0 Per-Second Jobs
  29      101100      5053      20007  0.00%  0.01%  0.00%   0 Per-minute Jobs
  30    26057260  26720902        975  5.81%  6.78%  5.76%   0 Cat4k Mgmt HiPri
```

31   19482908 29413060   662 19.64% 18.20% 20.48%   0 Cat4k Mgmt LoPri

*!--- Output suppressed.*show platform health 35 60 902 0 0.00% 0.00% 0.00% 0 DHCP Snooping

36 504625304 645491491 781 72.40% 72.63% 73.82% 0 IP Input

Passaggio 2: controllare la presenza del processo specifico di Catalyst 4500 con il show platform health comando.

L'output del **show platform health**comando conferma l'utilizzo della CPU per elaborare i pacchetti basati sulla CPU.

```
<#root>

Switch#

show platform health

%CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU

--- Output suppressed.

TagMan-RecreateMtegR   1.00   0.00     10      0  100  500    0   0    0  0:00
K2CpuMan Review      330.00  19.18    150     79   25  500   20  19   18 5794:08
K2AccelPacketMan: Tx  10.00   4.95     20      0  100  500    5   4    0  0:36
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
K2AclMan-taggedFlatA   1.00   0.00     10      0  100  500    0   0    0  0:00
```

Passaggio 3: controllare la coda CPU che riceve il traffico per identificare il tipo di traffico basato sulla CPU.

Utilizzare il show platform cpu packet statisticscomando per verificare quale coda CPU riceve il pacchetto basato sulla CPU. La coda `L3 Fwd` Lowqueue riceve molto traffico.

```
<#root>

Switch#

show platform cpu packet statistics

!--- Output suppressed.

Packets Received by Packet Queue
```

Queue	Total	5 sec avg	1 min avg	5 min avg	1 hour avg
Esmp	48613268	38	39	38	39
Control	142166648	74	74	73	73
Host Learning	1845568	2	2	2	2
L3 Fwd High	17	0	0	0	0
L3 Fwd Medium	2626	0	0	0	0
L3 Fwd Low	**4717094264**	**3841**	**3879**	**3873**	**3547**
L2 Fwd Medium	1	0	0	0	0
L3 Rx High	257147	0	0	0	0
L3 Rx Low	5325772	10	19	13	7
RPF Failure	155	0	0	0	0
ACL fwd(snooping)	65604591	53	54	54	53
ACL log, unreach	11013420	9	8	8	8

Passaggio 4: Identificare la root cause.

In questo caso, utilizzare l'SPAN della CPU per determinare il traffico che colpisce la CPU. Per informazioni sull'SPAN della CPU, fare riferimento alla sezione Tool 1: Monitor the CPU Traffic with SPAN—Cisco IOS Software release 12.1(19)EW and Latersection di questo documento. Completare un'analisi del traffico e una configurazione con il show running-configurationcomando. In questo caso, il pacchetto viene indirizzato tramite la stessa interfaccia, il che porta al rilascio di un reindirizzamento ICMP per ciascun pacchetto. Questa causa principale è una delle cause più comuni dell'elevato utilizzo della CPU su Catalyst 4500.

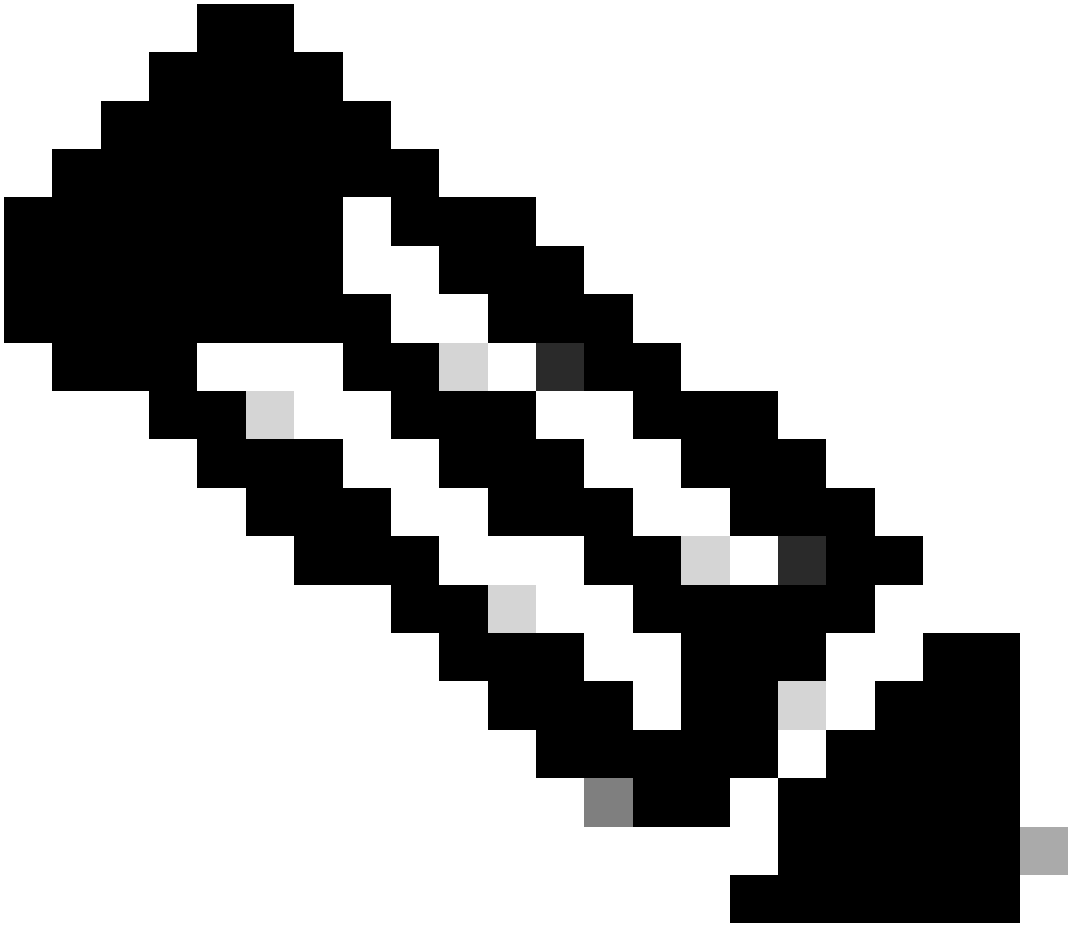
Ci si aspetta che il dispositivo di origine agisca sul reindirizzamento ICMP inviato dallo switch Catalyst 4500 e modifichi l'hop successivo alla destinazione. Tuttavia, non tutti i dispositivi rispondono a un reindirizzamento ICMP. Se il dispositivo non risponde, Catalyst 4500 deve inviare i reindirizzamenti per ogni pacchetto ricevuto dallo switch dal dispositivo di invio. Questi reindirizzamenti possono utilizzare molte risorse della CPU. La soluzione è disabilitare il reindirizzamento ICMP. Eseguire il no ip redirectscomando nelle interfacce.

Questo scenario può verificarsi quando sono stati configurati anche indirizzi IP secondari. Quando si abilitano gli indirizzi IP secondari, il reindirizzamento IP viene disabilitato automaticamente. Accertarsi di non abilitare manualmente i reindirizzamenti IP.

Come indicato da questo reindirizzamento ICMP; Routing Packets on the Same Interface Section, la maggior parte dei dispositivi finali non risponde ai reindirizzamenti ICMP. Di conseguenza, è buona norma disabilitare questa funzione.

Routing IPX o AppleTalk

Catalyst 4500 supporta il routing IPX e AppleTalk solo tramite percorso di inoltro software. Con la configurazione di tali protocolli, un maggiore utilizzo della CPU è normale.



Nota: la commutazione del traffico IPX e AppleTalk sulla stessa VLAN non richiede la commutazione di contesto. Solo i pacchetti che devono essere instradati richiedono l'inoltro del percorso software.

Passaggio 1: verificare la presenza del processo Cisco IOS con il show processes cpu comando.

Utilizzare il **show processes cpu** comando per verificare quale processo Cisco IOS utilizza la CPU. In questo output del comando, il processo principale è **`il processo LoPri di gestione Cat4k`**:

<#root>

```
witch#
```

show processes cpu

```
CPU utilization for five seconds: 87%/10%; one minute: 86%; five minutes: 87%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4        53         75  0.00%  0.00%  0.00%   0 Chunk Manager

!--- Output suppressed.

  25        8008   1329154          6  0.00%  0.00%  0.00%   0 Per-Second Jobs
  26      413128     38493      10732  0.00%  0.02%  0.00%   0 Per-minute Jobs
  27   148288424 354390017        418  2.60%  2.42%  2.77%   0 Cat4k Mgmt HiPri
```

28   285796820 720618753   396 50.15% 59.72% 61.31%   0 Cat4k Mgmt LoPri

Passaggio 2: controllare la presenza del processo specifico di Catalyst 4500 con il show platform health comando.

L'output del show platform healthcomando conferma l'utilizzo della CPU per elaborare i pacchetti collegati alla CPU.

<#root>

```
Switch#
```

show platform health

```
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU

!--- Output suppressed.
```

```
TagMan-RecreateMtegR   1.00   0.00     10      4  100  500    0   0    0  0:00

K2CpuMan Review       30.00  27.39     30     53  100  500   42  47   42  4841:

K2AccelPacketMan: Tx  10.00   8.03     20      0  100  500   21  29   26  270:4
```

Passaggio 3: controllare la coda della CPU che riceve il traffico per identificare il tipo di traffico basato sulla CPU.

Per determinare il tipo di traffico che colpisce la CPU, usare il show platform cpu packet statisticscomando.

```
    <#root>

Switch#

show platform cpu packet statistics

!--- Output suppressed.

Packets Received by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- --------------- --------- --------- --------- ----------
Esmp                         48613268        38        39        38         39
Control                     142166648        74        74        73         73
Host Learning                 1845568         2         2         2          2
L3 Fwd High                        17         0         0         0          0
L3 Fwd Medium                    2626         0         0         0          0
L3 Fwd Low                    1582414         1         1         1          1
L2 Fwd Medium                       1         0         0         0          0

L2 Fwd Low                  576905398      1837      1697      1938       1515
```

```
L3 Rx High                    257147          0          0          0          0
L3 Rx Low                    5325772         10         19         13          7
RPF Failure                      155          0          0          0          0
ACL fwd(snooping)           65604591         53         54         54         53
ACL log, unreach            11013420          9          8          8          8
```

Passaggio 4: Identificare la root cause.

Poiché l'amministratore ha configurato il routing IPX o AppleTalk, l'identificazione della causa principale deve essere semplice. Tuttavia, per conferma, eseguire un'estensione del traffico della CPU e verificare che il traffico visualizzato sia quello previsto. Per informazioni sull'SPAN della CPU, fare riferimento alla sezione Tool 1: Monitor the CPU Traffic with SPAN—Cisco IOS Software release 12.1(19)EW and Latersection di questo documento.

In questo caso, l'amministratore deve aggiornare la CPU di base al valore corrente. Il comportamento della CPU Catalyst 4500 è quello previsto quando la CPU elabora pacchetti a commutazione di software.

Formazione host

Catalyst 4500 apprende gli indirizzi MAC di vari host, se non sono già presenti nella tabella degli indirizzi MAC. Il motore di commutazione inoltra una copia del pacchetto con il nuovo indirizzo MAC alla CPU.

Tutte le interfacce VLAN (livello 3) utilizzano l'indirizzo hardware di base dello chassis come indirizzo MAC. Di conseguenza, non esiste una voce nella tabella degli indirizzi MAC e i pacchetti destinati a queste interfacce VLAN non vengono inviati alla CPU per l'elaborazione.

Se il numero di nuovi indirizzi MAC da conoscere per lo switch è eccessivo, è possibile che la CPU venga utilizzata in modo intensivo.

Passaggio 1: verificare la presenza del processo Cisco IOS con il show processes cpu comando.

Utilizzare **show processes cpu**il comando per verificare quale processo Cisco IOS utilizza la CPU. In questo output del comando, il processo principale è **`il processo LoPri di gestione Cat4k`**:

<#root>

```
Switch#
```

`show processes cpu`

```
CPU utilization for five seconds: 89%/1%; one minute: 74%; five minutes: 71%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
```

```
   1           4        53          75  0.00%  0.00%  0.00%   0 Chunk Manager

!--- Output suppressed.

  25        8008   1329154           6  0.00%  0.00%  0.00%   0 Per-Second Jobs
  26      413128     38493       10732  0.00%  0.02%  0.00%   0 Per-minute Jobs
  27   148288424 354390017         418 26.47% 10.28% 10.11%   0 Cat4k Mgmt HiPri
```

28   285796820 720618753   396 52.71% 56.79% 55.70%   0 Cat4k Mgmt LoPri

Passaggio 2: verificare la presenza del processo specifico di Catalyst 4500 con il comando show platform health.

L'output del comando **show platform** health conferma l'utilizzo della CPU per elaborare i pacchetti collegati alla CPU.

<#root>

```
Switch#
```

show platform health

```
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU

!--- Output suppressed.

TagMan-RecreateMtegR   1.00   0.00     10      4  100  500    0   0    0  0:00
```

K2CpuMan Review   30.00 46.88   30   47 100 500   30 29   21 265:01

```
K2AccelPacketMan: Tx  10.00   8.03     20      0  100  500   21  29   26  270:4
```

Passaggio 3: controllare la coda della CPU che riceve il traffico per identificare il tipo di traffico basato sulla CPU.

Per determinare il tipo di traffico che interessa la CPU, usare **il** comando **show platform cpu packet** statistics.

<#root>

Switch#

show platform cpu packet statistics

!--- Output suppressed.

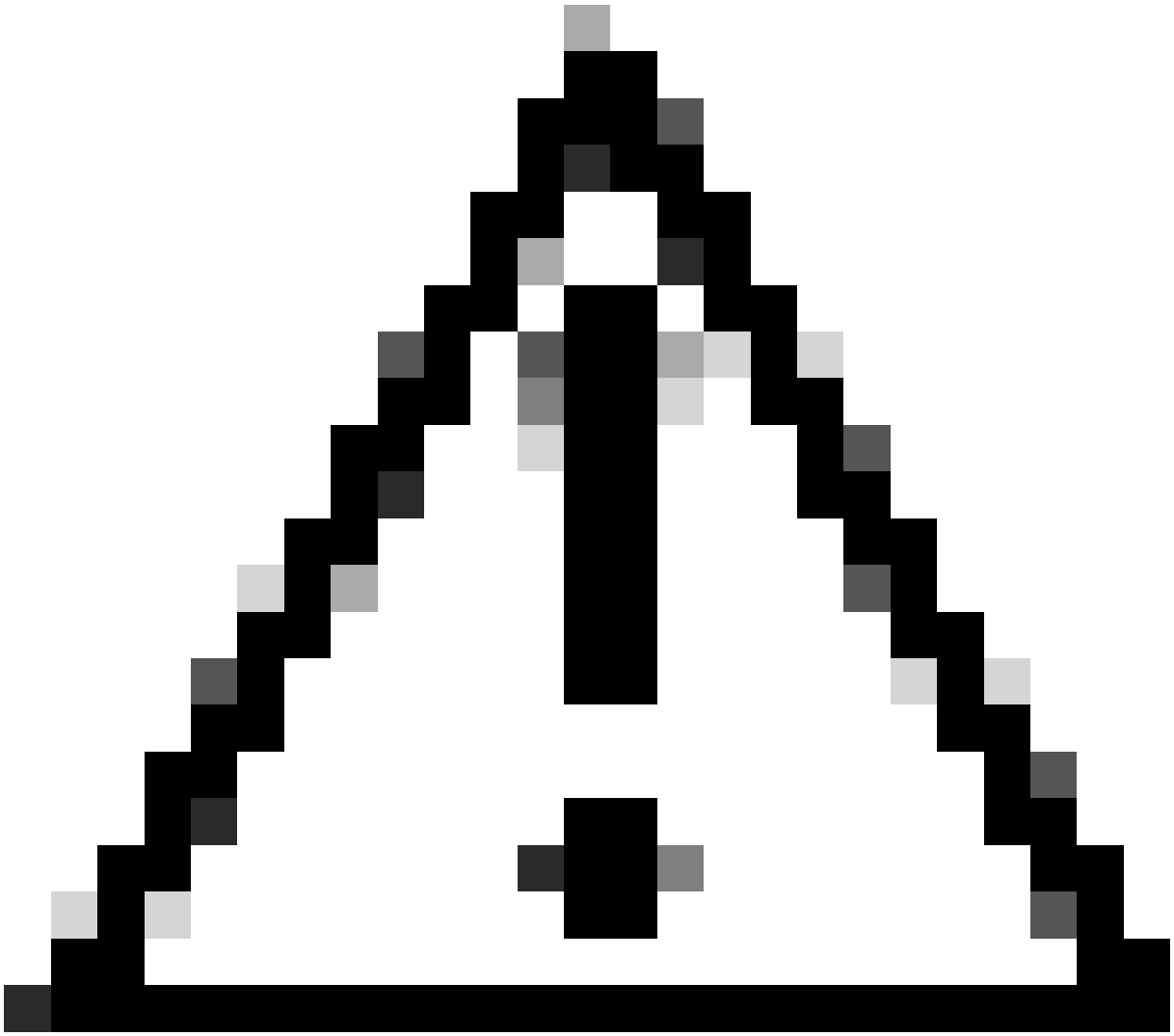
Packets Received by Packet Queue

Queue	Total	5 sec avg	1 min avg	5 min avg	1 hour avg
Esmp	48613268	38	39	38	39
Control	142166648	74	74	73	73
Host Learning	**1845568**	**1328**	**1808**	**1393**	**1309**
L3 Fwd High	17	0	0	0	0
L3 Fwd Medium	2626	0	0	0	0
L3 Fwd Low	1582414	1	1	1	1
L2 Fwd Medium	1	0	0	0	0
L2 Fwd Low	576905398	37	7	8	5
L3 Rx High	257147	0	0	0	0
L3 Rx Low	5325772	10	19	13	7
RPF Failure	155	0	0	0	0
ACL fwd(snooping)	65604591	53	54	54	53
ACL log, unreach	11013420	9	8	8	8

Passaggio 4: Identificare la root cause.

L'output del show platform healthcomando mostra che la CPU vede molti nuovi indirizzi MAC. Questa situazione è spesso il risultato dell'instabilità della topologia di rete. Ad esempio, se la topologia dello spanning-tree cambia, lo switch genera notifiche di modifica della topologia (TCN). Il problema dei TCN riduce il tempo di aging a 15 secondi in modalità PVST+. Le voci degli indirizzi MAC vengono scaricate se gli indirizzi non vengono recuperati entro il periodo di tempo specificato. In caso di RSTP (Rapid STP) (IEEE 802.1w) o MST (IEEE 802.1s), le voci scadono immediatamente se il TCN proviene da un altro switch. In questo caso, gli indirizzi MAC vengono nuovamente appresi. Questo non è un problema grave se le modifiche alla topologia sono rare. Tuttavia, è possibile che vi sia un numero eccessivo di modifiche alla topologia a causa di un collegamento flapping, di uno switch difettoso o di porte host non abilitate per PortFast. È possibile che si verifichi un numero elevato di scaricamenti della tabella MAC e il successivo riapprendimento. Il passaggio successivo per l'identificazione della causa principale è la risoluzione dei problemi della rete. Lo switch funziona come previsto e invia i pacchetti alla CPU per l'apprendimento dell'indirizzo host. Identificare e correggere il dispositivo difettoso che provoca un numero eccessivo di TCN.

La rete può avere molti dispositivi che inviano il traffico in burst, il che fa sì che gli indirizzi MAC siano obsoleti e successivamente riacquisiti sullo switch. In questo caso, aumentare il tempo di permanenza della tabella degli indirizzi MAC in modo da fornire un qualche sollievo. Con un tempo di aging più lungo, gli switch conservano gli indirizzi MAC dei dispositivi nella tabella per un periodo di tempo più lungo prima del timeout.



Attenzione: apportare questa modifica alla durata solo dopo un'attenta considerazione. Se nella rete sono presenti dispositivi mobili, la modifica può generare un buco nero del traffico.

TCAM (Out of Hardware Resources) per ACL di sicurezza

Catalyst 4500 usa gli ACL configurati con Cisco TCAM. TCAM consente l'applicazione degli ACL nel percorso di inoltro hardware. Non vi è alcun impatto sulle prestazioni dello switch, con o senza ACL nel percorso di inoltro. Le prestazioni rimangono costanti nonostante le dimensioni dell'ACL, in quanto le prestazioni delle ricerche ACL avvengono alla velocità della linea. Tuttavia, TCAM è una risorsa limitata. Pertanto, se si configura un numero eccessivo di voci ACL, si supera la capacità TCAM.La tabella 3mostra il numero di risorse TCAM disponibili su ciascuno dei Supervisor Engine e degli switch Catalyst 4500.

Tabella 3 - Capacità TCAM su motori/switch Supervisor Catalyst 4500

Prodotto	Funzione TCAM (per direzione)	QoS TCAM (per direzione)
Supervisor Engine II+/II+TS	8192 voci con 1024 maschere	8192 voci con 1024 maschere
Supervisor Engine III/IV/V e Catalyst 4948	16.384 voci con 2048 maschere	16.384 voci con 2048 maschere
Supervisor Engine V-10GE e Catalyst 4948-10GE	16.384 voci con 16.384 maschere	16.384 voci con 16.384 maschere

Lo switch usa la funzionalità TCAM per programmare l'ACL di sicurezza, ad esempio RACL e VLAN ACL (VACL). Lo switch usa anche la funzione TCAM per funzioni di sicurezza come IP Source Guard (IPSG) per gli ACL dinamici. Lo switch usa il QoS TCAM per programmare gli ACL di classificazione e di controllo.

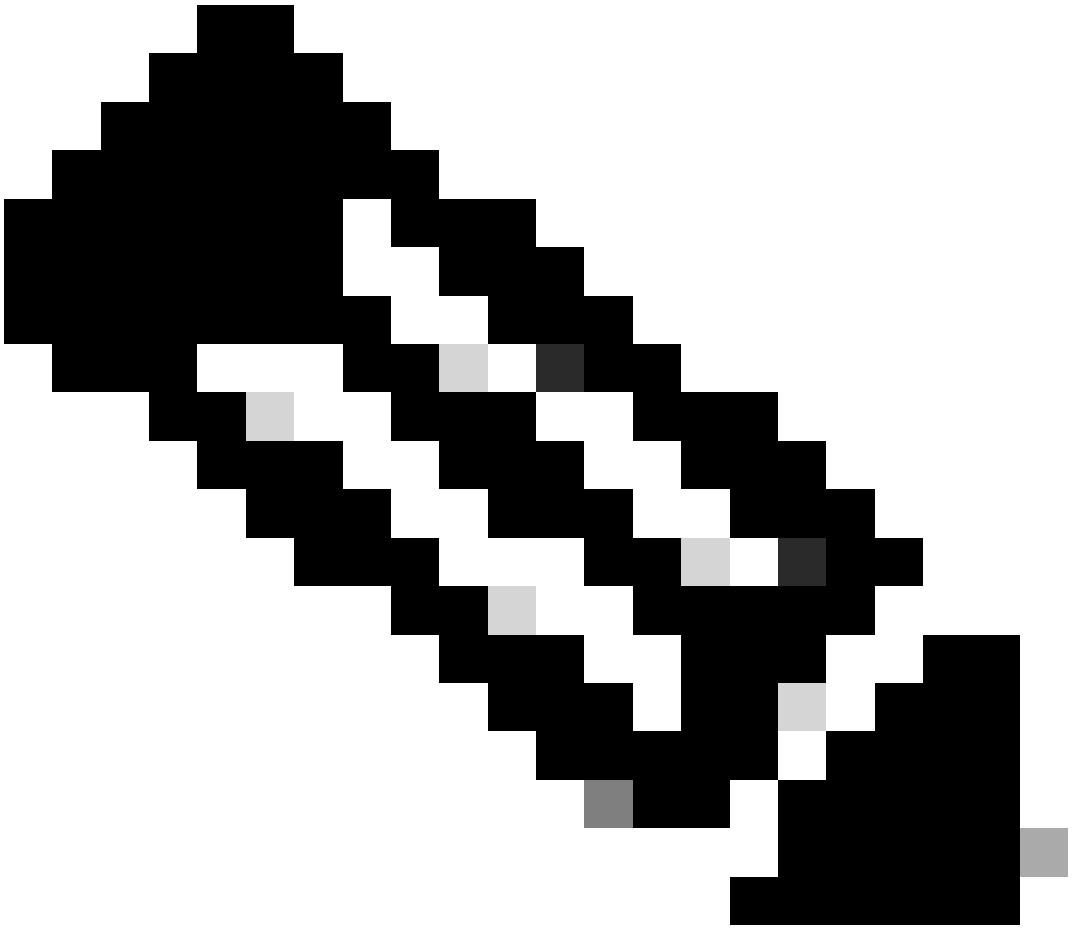
Quando le risorse TCAM dello switch Catalyst 4500 si esauriscono durante la programmazione di un ACL di sicurezza, l'applicazione dell'ACL viene parzialmente eseguita tramite il percorso software. I pacchetti che colpiscono questi ACE vengono elaborati nel software, il che provoca un elevato utilizzo della CPU. L'ACL è programmato dall'alto verso il basso. In altre parole, se l'ACL non può essere contenuto nel TCAM, è probabile che l'ACE nella parte inferiore dell'ACL non sia programmato nel TCAM.

Questo messaggio di avviso viene visualizzato quando si verifica un overflow TCAM:

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing can be software switched.
```

Questo messaggio di errore viene visualizzato nell'output **del** comando show logging. Il messaggio indica in modo definitivo che è possibile

eseguire alcune elaborazioni software e, di conseguenza, che l'utilizzo della CPU è elevato.



Nota: se si modifica un ACL di grandi dimensioni, è possibile visualizzare questo messaggio brevemente prima che l'ACL modificato venga programmato di nuovo nella TCAM.

Passaggio 1: Controllare il processo Cisco IOS con il comando show processes cpu.

Eseguire **il comando show processes** cpucommand. L'utilizzo della CPU è elevato perché **`la gestione Cat4k`** LoPriprocess occupa la maggior parte dei cicli della CPU.

<#root>

```
Switch#
```

show processes cpu

```
CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 99%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0        11          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        9716    632814         15  0.00%  0.00%  0.00%   0 Load Meter
   3         780       302       2582  0.00%  0.00%  0.00%   0 SpanTree Helper

!--- Output suppressed.

  23       18208   3154201          5  0.00%  0.00%  0.00%   0 TTY Background
  24       37208   3942818          9  0.00%  0.00%  0.00%   0 Per-Second Jobs
  25     1046448    110711       9452  0.00%  0.03%  0.00%   0 Per-minute Jobs
  26   175803612 339500656        517  4.12%  4.31%  4.48%   0 Cat4k Mgmt HiPri

  27   835809548 339138782       2464 86.81% 89.20% 89.76%   0 Cat4k Mgmt LoPri

  28       28668   2058810         13  0.00%  0.00%  0.00%   0 Galios Reschedul
```

Passaggio 2: controllare la presenza del processo specifico di Catalyst 4500 con il show platform health comando.

Eseguire il show platform healthcomando. Come si può notare, **K2CpuMan Review**, un job per gestire pacchetti basati sulla CPU, utilizza la CPU.

```
    <#root>

Switch#
```

show platform health

```
%CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                   Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll              1.00   0.01      2      0  100  500    0   0    0  13:45
GalChassisVp-review   3.00   0.20     10     16  100  500    0   0    0  88:44
S2w-JobEventSchedule 10.00   0.57     10      7  100  500    1   0    0  404:22
Stub-JobEventSchedul 10.00   0.00     10      0  100  500    0   0    0  0:00
StatValueMan Update   1.00   0.09      1      0  100  500    0   0    0  91:33
Pim-review            0.10   0.00      1      0  100  500    0   0    0  4:46
Ebm-host-review       1.00   0.00      8      4  100  500    0   0    0  14:01
Ebm-port-review       0.10   0.00      1      0  100  500    0   0    0  0:20
Protocol-aging-revie  0.20   0.00      2      0  100  500    0   0    0  0:01
Acl-Flattener         1.00   0.00     10      5  100  500    0   0    0  0:04
KxAclPathMan create/  1.00   0.00     10      5  100  500    0   0    0  0:21
KxAclPathMan update   2.00   0.00     10      6  100  500    0   0    0  0:05
KxAclPathMan reprogr  1.00   0.00      2      1  100  500    0   0    0  0:00
TagMan-InformMtegRev  1.00   0.00      5      0  100  500    0   0    0  0:00
TagMan-RecreateMtegR  1.00   0.00     10     14  100  500    0   0    0  0:18
```

K2CpuMan Review 30.00 91.31 30 92 100 500 128 119 84 13039:02

```
K2AccelPacketMan: Tx  10.00   2.30     20      0  100  500    2   2    2  1345:30
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
```

Passaggio 3: controllare la coda della CPU che riceve il traffico per identificare il tipo di traffico basato sulla CPU.

È necessario comprendere ulteriormente quale coda CPU e, di conseguenza, quale tipo di traffico raggiunge la coda CPU. Eseguire **il** comando **show platform cpu packet** statistics. Si noti che `la` coda di elaborazione del `software ACL` riceve un numero elevato di pacchetti. Pertanto, l'overflow TCAM è la causa di questo problema di utilizzo elevato della CPU.

```
<#root>

Switch#

show platform cpu packet statistics

!--- Output suppressed.
```

Packets Received by Packet Queue

Queue	Total	5 sec avg	1 min avg	5 min avg	1 hour avg
Control	57902635	22	16	12	3
Host Learning	464678	0	0	0	0
L3 Fwd Low	623229	0	0	0	0
L2 Fwd Low	11267182	7	4	6	1
L3 Rx High	508	0	0	0	0
L3 Rx Low	1275695	10	1	0	0
ACL fwd(snooping)	2645752	0	0	0	0
ACL log, unreach	51443268	9	4	5	5
ACL sw processing	**842889240**	**1453**	**1532**	**1267**	**1179**

Packets Dropped by Packet Queue

Queue	Total	5 sec avg	1 min avg	5 min avg	1 hour avg
L2 Fwd Low	3270	0	0	0	0
ACL sw processing	12636	0	0	0	0

Passaggio 4: risolvere il problema.

Nel passaggio 3 è stata determinata la causa principale di questo scenario. Rimuovere l'ACL che ha causato l'overflow o ridurre a icona l'ACL per evitare l'overflow. Inoltre, rivedere le linee guida sulla configurazione della configurazione della sicurezza di rete con ACL per ottimizzare la configurazione e la programmazione degli ACL nell'hardware.

Parola chiave log nell'ACL

Catalyst 4500 supporta la registrazione dei dettagli dei pacchetti che hanno raggiunto una voce ACL specifica, ma una registrazione eccessiva può causare un elevato utilizzo della CPU. Evitare l'uso di parole chiave log, tranne durante la fase di rilevamento del traffico. Durante la fase di rilevamento del traffico è possibile identificare il traffico che attraversa la rete per il quale non sono state configurate le voci di controllo di accesso in modo esplicito. Non utilizzare thelogkeyword per raccogliere statistiche. Nel software Cisco IOS versione 12.1(13)EW e successive, i messaggi logo hanno una velocità limitata. Se si usano i messaggi logper contare il numero di pacchetti che corrispondono all'ACL, il conteggio non è accurato. Per ottenere statistiche accurate, utilizzare il **show access-list**comando. L'identificazione di questa causa principale è più semplice perché un'analisi della configurazione orlogmessages può indicare l'uso della funzione di registrazione ACL.

Passaggio 1: Controllare il processo Cisco IOS con il comando show processes cpu.

Utilizzare il show processes cpucomando per verificare quale processo Cisco IOS utilizza la CPU. In questo output del comando, il processo principale è **il** processo di **gestione Cat4k LoPri:**

<#root>

Switch#

show processes cpu

```
CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 99%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0        11          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        9716    632814         15  0.00%  0.00%  0.00%   0 Load Meter

!--- Output suppressed.

  26   175803612 339500656        517  4.12%  4.31%  4.48%   0 Cat4k Mgmt HiPri

  27   835809548 339138782       2464 86.81% 89.20% 89.76%   0 Cat4k Mgmt LoPri

  28       28668   2058810         13  0.00%  0.00%  0.00%   0 Galios Reschedul
```

Passaggio 2: verificare la presenza del processo specifico di Catalyst 4500 con il comando show platform health.

Controllare il processo specifico della piattaforma che utilizza la CPU. Eseguire il show platform healthcomando. Nell'output, notare che **il** processo di revisione **K2CpuMan** utilizza la maggior parte dei cicli della CPU. Questa attività indica che la CPU è occupata mentre elabora i pacchetti ad essa destinati.

<#root>

Switch#

show platform health

```
                      %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                1.00   0.01      2      0  100  500    0   0    0  13:45
GalChassisVp-review    3.00   0.20     10     16  100  500    0   0    0  88:44
S2w-JobEventSchedule  10.00   0.57     10      7  100  500    1   0    0  404:22
Stub-JobEventSchedul  10.00   0.00     10      0  100  500    0   0    0  0:00
StatValueMan Update    1.00   0.09      1      0  100  500    0   0    0  91:33
Pim-review             0.10   0.00      1      0  100  500    0   0    0  4:46
Ebm-host-review        1.00   0.00      8      4  100  500    0   0    0  14:01
Ebm-port-review        0.10   0.00      1      0  100  500    0   0    0  0:20
Protocol-aging-revie   0.20   0.00      2      0  100  500    0   0    0  0:01
Acl-Flattener          1.00   0.00     10      5  100  500    0   0    0  0:04
KxAclPathMan create/   1.00   0.00     10      5  100  500    0   0    0  0:21
KxAclPathMan update    2.00   0.00     10      6  100  500    0   0    0  0:05
KxAclPathMan reprogr   1.00   0.00      2      1  100  500    0   0    0  0:00
TagMan-InformMtegRev   1.00   0.00      5      0  100  500    0   0    0  0:00
TagMan-RecreateMtegR   1.00   0.00     10     14  100  500    0   0    0  0:18



K2CpuMan Review       30.00  91.31     30     92  100  500  128 119   84  13039:02



K2AccelPacketMan: Tx  10.00   2.30     20      0  100  500    2   2    2  1345:30
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
```

Passaggio 3: controllare la coda della CPU che riceve il traffico per identificare il tipo di traffico basato sulla CPU.

Per determinare il tipo di traffico che colpisce la CPU, eseguire **show platform cpu packet statistics**il comando. In questo output del comando, è possibile vedere che la ricezione dei pacchetti è dovuta alla parola chiave ACLlog:

```
<#root>

Switch#

show platform cpu packet statistics

!--- Output suppressed.

Total packet queues 16
Packets Received by Packet Queue
```

```
Queue              Total                 5 sec avg 1 min avg 5 min avg 1 hour avg
------------------ -------------------- --------- --------- --------- ----------
Control                      1198701435        35        35        34         35
Host Learning                    874391         0         0         0          0
L3 Fwd High                         428         0         0         0          0
L3 Fwd Medium                     12745         0         0         0          0
L3 Fwd Low                      2420401         0         0         0          0
L2 Fwd High                       26855         0         0         0          0
L2 Fwd Medium                    116587         0         0         0          0
L2 Fwd Low                    317829151        53        41        31         31
L3 Rx High                        2371         0         0         0          0
L3 Rx Low                     32333361         7         1         2          0
RPF Failure                       4127         0         0         0          0
ACL fwd (snooping)           107743299         4         4         4          4
```

```
ACL log, unreach            1209056404      1987      2125      2139       2089
```

```
Packets Dropped by Packet Queue

Queue              Total                 5 sec avg 1 min avg 5 min avg 1 hour avg
------------------ -------------------- --------- --------- --------- ----------
ACL log, unreach             193094788       509       362       437        394
```

Passaggio 4: risolvere il problema.

Nel passaggio 3 è stata determinata la causa principale di questo scenario. Per evitare il problema, rimuovere la parola chiave ogdagli ACL. Nel software Cisco IOS versione 12.1(13)EW1 e successive, la velocità dei pacchetti è limitata in modo che l'utilizzo della CPU non diventi troppo elevato. Usare i contatori dell'elenco degli accessi per tenere traccia dei riscontri ACL. I contatori dell'elenco degli accessi sono visibili nell'output **show access-list acl_id**del comando.

Loop di inoltro di livello 2

I loop di inoltro di livello 2 possono essere causati da una scarsa implementazione del protocollo Spanning Tree Protocol (STP) e da vari problemi che possono influire su STP.

Passaggio 1: Controllare il processo Cisco IOS con il show processes cpu comando

In questa sezione vengono esaminati i comandi utilizzati dall'amministratore per risolvere il problema dell'utilizzo elevato della CPU. Se si usa il **show processes cpu**comando, si osserverà che due processi principali,**`Cat4k Mgmt LoPriand`**`Spanning Tree`, usano principalmente la CPU. Utilizzando solo queste informazioni, lo Spanning Tree utilizza una parte considerevole dei cicli della CPU.

<#root>

Switch#

show processes cpu

```
CPU utilization for five seconds: 74%/1%; one minute: 73%; five minutes: 50%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4       198         20  0.00%  0.00%  0.00%   0 Chunk Manager
   2           4       290         13  0.00%  0.00%  0.00%   0 Load Meter

!--- Output suppressed.

  25         488        33      14787  0.00%  0.02%  0.00%   0 Per-minute Jobs
  26       90656    223674        405  6.79%  6.90%  7.22%   0 Cat4k Mgmt HiPri

 27      158796     59219       2681 32.55% 33.80% 21.43%   0 Cat4k Mgmt LoPri

  28          20      1693         11  0.00%  0.00%  0.00%   0 Galios Reschedul
  29           0         1          0  0.00%  0.00%  0.00%   0 IOS ACL Helper
  30           0         2          0  0.00%  0.00%  0.00%   0 NAM Manager

!--- Output suppressed.

  41           0         1          0  0.00%  0.00%  0.00%   0 SFF8472
  42           0         2          0  0.00%  0.00%  0.00%   0 AAA Dictionary R

 43       78564     20723       3791 32.63% 30.03% 17.35%   0 Spanning Tree

  44         112       999        112  0.00%  0.00%  0.00%   0 DTP Protocol
  45           0       147          0  0.00%  0.00%  0.00%   0 Ethchnl
```

Passaggio 2: Controllare il processo specifico di Catalyst 4500 con il comando show platform health

Per comprendere quale processo specifico della piattaforma utilizza la CPU, eseguire il show platform healthcomando. Da questo output, è possibile vedere che **`il processo K2CpuMan`** Reviewprocess, un processo per gestire i pacchetti basati sulla CPU, utilizza fino alla CPU:

```
<#root>

Switch#

show platform health

%CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                  Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU

!--- Output suppressed.

TagMan-RecreateMtegR   1.00   0.00     10      0  100  500    0   0    0  0:00

K2CpuMan Review       30.00  37.62     30     53  100  500   41  33    1  2:12

K2AccelPacketMan: Tx  10.00   4.95     20      0  100  500    5   4    0  0:36
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
K2AclMan-taggedFlatA   1.00   0.00     10      0  100  500    0   0    0  0:00
```

Passaggio 3: controllare la coda della CPU che riceve il traffico per identificare il tipo di traffico basato sulla CPU

Utilizzare il show platform cpu packet statisticscomando per verificare quale coda CPU riceve il pacchetto basato sulla CPU. L'output in questa sezione mostra che la coda di controllo riceve molti pacchetti. Utilizzare le informazioni riportate nella Tabella 1 e le conclusioni tratte nel Passaggio 1. È possibile stabilire che i pacchetti elaborati dalla CPU e il motivo dell'utilizzo elevato della CPU siano l'elaborazione BPDU.

```
<#root>

Switch#
```

show platform cpu packet statistics

!--- Output suppressed.

```
Total packet queues 16
Packets Received by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- --------------- --------- --------- --------- ----------
Esmp                           202760       196       173       128         28


Control                        388623      2121      1740       598         16


Packets Dropped by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- --------------- --------- --------- --------- ----------
Control                         17918         0        19        24          3
```

Passaggio 4: Identificare la causa principale e risolvere il problema

In genere, è possibile completare questi passaggi per risolvere il problema (a seconda della situazione, alcuni passaggi non sono necessari):

- Identificare il loop.
- Individuare l'ambito del ciclo.
- Rompi il cerchio.
- Correggere la causa del loop.

- Ripristinare la ridondanza.

Ciascuna procedura viene descritta in dettaglio nella sezione Risoluzione dei problemi relativi ai loop di inoltro - Risoluzione dei problemi relativi a STP sugli switch Catalyst con software di sistema Cisco IOS.

Passaggio 5: Implementare le funzionalità STP avanzate

- **BDPU Guard**: protegge il protocollo STP dai dispositivi di rete non autorizzati connessi alle porte abilitate a portfast. per ulteriori informazioni, fare riferimento ai miglioramenti della funzionalità Spanning Tree PortFast BPDU Guard.

- **Protezione loop (Loop Guard**) - Aumenta la stabilità delle reti di livello 2. per ulteriori informazioni, fare riferimento a Miglioramenti del protocollo Spanning-Tree che usano le funzionalità di rilevamento dell'inclinazione del loop e BPDU.

- **Protezione root (Root Guard)** - Attiva il posizionamento del bridge radice nella rete. per ulteriori informazioni, fare riferimento a Miglioramenti della protezione radice dello Spanning Tree Protocol.

- **UDLD** - Rileva i collegamenti unidirezionali e impedisce l'inoltro dei loop. per ulteriori informazioni, fare riferimento a Descrizione e configurazione della funzionalità protocollo di rilevamento dei collegamenti unidirezionale.

Altre cause di un elevato utilizzo della CPU

Di seguito sono riportate altre cause note dell'elevato utilizzo della CPU:

- Numero eccessivo di link flap

- Picchi nell'utilizzo della CPU dovuti alla verifica di coerenza FIB

- Utilizzo elevato della CPU nel processo di spostamento **dell'host K2FibAdjMan**

- Utilizzo CPU elevato nel processo **di** revisione **della porta RkiosPortMan**

- Utilizzo elevato della CPU quando collegato a un telefono IP tramite porte trunk

- Utilizzo elevato della CPU con RSPAN e pacchetti di controllo di livello 3

- Picco durante la programmazione ACL di grandi dimensioni

Il picco nell'utilizzo della CPU si verifica durante l'applicazione o la rimozione di un ACL di grandi dimensioni da un'interfaccia.

Numero eccessivo di link flap

Lo switch Catalyst 4500 mostra un elevato utilizzo della CPU quando uno o più collegamenti collegati iniziano a lampeggiare eccessivamente. Questa situazione si verifica nelle versioni del software Cisco IOS precedenti alla versione 12.2(20)EWA.

Passaggio 1: Controllare il processo Cisco IOS con il comando show processes cpu.

Utilizzare **il comando** show **processes** cp per verificare quale processo Cisco IOS utilizza la CPU. In questo output del comando, il processo principale è **`il processo LoPri di gestione Cat4k`**:

<#root>

```
Switch#
```

`show processes cpu`

```
CPU utilization for five seconds: 96%/0%; one minute: 76%; five minutes: 68%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         4          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        9840    463370         21  0.00%  0.00%  0.00%   0 Load Meter
   3           0         2          0  0.00%  0.00%  0.00%   0 SNMP Timers

!--- Output suppressed.

  27   232385144 530644966        437 13.98% 12.65% 12.16%   0 Cat4k Mgmt HiPri




  28   564756724 156627753       3605 64.74% 60.71% 54.75%   0 Cat4k Mgmt LoPri




  29        9716   1806301          5  0.00%  0.00%  0.00%   0 Galios Reschedul
```

Passaggio 2: verificare la presenza del processo specifico di Catalyst 4500 con il comando show platform health.

L'output del comando **show platform** health indica che **il processo di creazione di KxAclPathMan** utilizza l'intera CPU. Questo processo è per la creazione di percorsi interni.

```
    <#root>

Switch#
```

show platform health

```
                    %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                    Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll               1.00   0.03      2      0  100  500    0   0    0  9:49
GalChassisVp-review    3.00   1.11     10     62  100  500    0   0    0  37:39
S2w-JobEventSchedule  10.00   2.85     10      8  100  500    2   2    2  90:00
Stub-JobEventSchedul  10.00   5.27     10      9  100  500    4   4    4  186:2
Pim-review             0.10   0.00      1      0  100  500    0   0    0  2:51
Ebm-host-review        1.00   0.00      8      4  100  500    0   0    0  8:06
Ebm-port-review        0.10   0.00      1      0  100  500    0   0    0  0:14
Protocol-aging-revie   0.20   0.00      2      0  100  500    0   0    0  0:00
Acl-Flattener          1.00   0.00     10      5  100  500    0   0    0  0:00
```

```
KxAclPathMan create/   1.00  69.11     10      5  100  500   42  53   22  715:0
```

```
KxAclPathMan update    2.00   0.76     10      6  100  500    0   0    0  86:00
KxAclPathMan reprogr   1.00   0.00      2      1  100  500    0   0    0  0:00
TagMan-InformMtegRev   1.00   0.00      5      0  100  500    0   0    0  0:00
TagMan-RecreateMtegR   1.00   0.00     10    227  100  500    0   0    0  0:00
K2CpuMan Review       30.00   8.05     30     57  100  500    6   5    5  215:0
K2AccelPacketMan: Tx  10.00   6.86     20      0  100  500    5   5    4  78:42
```

Passaggio 3: Identificare la root cause.

Abilita la registrazione per i messaggi di collegamento attivo/inattivo. Per impostazione predefinita, questa registrazione non è attivata. L'abilitazione consente di restringere i collegamenti che causano problemi molto rapidamente. Eseguire **il** comando **link-**status dell'**evento di registrazione** in tutte le interfacce. È possibile utilizzare **il comando interface** range per abilitare la funzione su un intervallo di interfacce, come mostrato nell'esempio:

```
    <#root>

Switch#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#

interface range gigabitethernet 5/1 - 48

Switch(config-if-range)#

logging event link-status
```

```
Switch(config--if-range)#
```

end

<#root>

```
Switch#
```

show logging

```
!--- Output suppressed.

3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to down
3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to up
3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to down
3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to up
3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to down
3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to up
```

Dopo aver identificato l'interfaccia difettosa o instabile, arrestare l'interfaccia per risolvere il problema di utilizzo elevato della CPU. Il software Cisco IOS versione 12.2(20)EWA e successive ha migliorato il comportamento di Catalyst 4500 per questa condizione di flapping dei collegamenti. Pertanto, l'impatto sulla CPU non è così grande come prima del miglioramento. Tenere presente che si tratta di un processo in background. L'elevato utilizzo della CPU causato da questo problema non produce effetti negativi sugli switch Catalyst 4500.

Picchi nell'utilizzo della CPU dovuti al controllo di coerenza FIB

Catalyst 4500 può mostrare picchi momentanei nell'utilizzo della CPU durante una verifica di coerenza della tabella FIB. La tabella FIB è la tabella di inoltro L3 creata dal processo CEF. La verifica della coerenza mantiene la coerenza tra la tabella FIB del software Cisco IOS e le voci hardware. Questa coerenza garantisce che i pacchetti non vengano instradati in modo errato. Il controllo viene eseguito ogni 2 secondi come processo in background a bassa priorità. Si tratta di un comportamento normale che non interferisce con altri processi o pacchetti ad alta priorità.

L'output del comando **show platform** health mostra **che la coerenza K2Fib** consuma la maggior parte della CPU.

Nota: l'utilizzo medio della CPU per questo processo è insignificante in un minuto o un'ora, a conferma del fatto che il controllo è una breve revisione periodica. Questo processo in background utilizza solo i cicli di CPU inattivi.

<#root>

Switch#

show platform health

```
                    %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                    Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll               1.00   0.02      2      1  100  500    0   0    0  1:09
GalChassisVp-review   3.00   0.29     10      3  100  500    0   0    0  11:15

!--- Output suppressed.

K2Fib cam usage revi   2.00   0.00     15      0  100  500    0   0    0  0:00
K2Fib IrmFib Review    2.00   0.00     15      0  100  500    0   0    0  0:00
K2Fib Vrf Default Ro   2.00   0.00     15      0  100  500    0   0    0  0:00
K2Fib AdjRepop Revie   2.00   0.00     15      0  100  500    0   0    0  0:00
K2Fib Vrf Unpunt Rev   2.00   0.01     15      0  100  500    0   0    0  0:23
K2Fib Consistency Ch   1.00  60.40      5      2  100  500
```

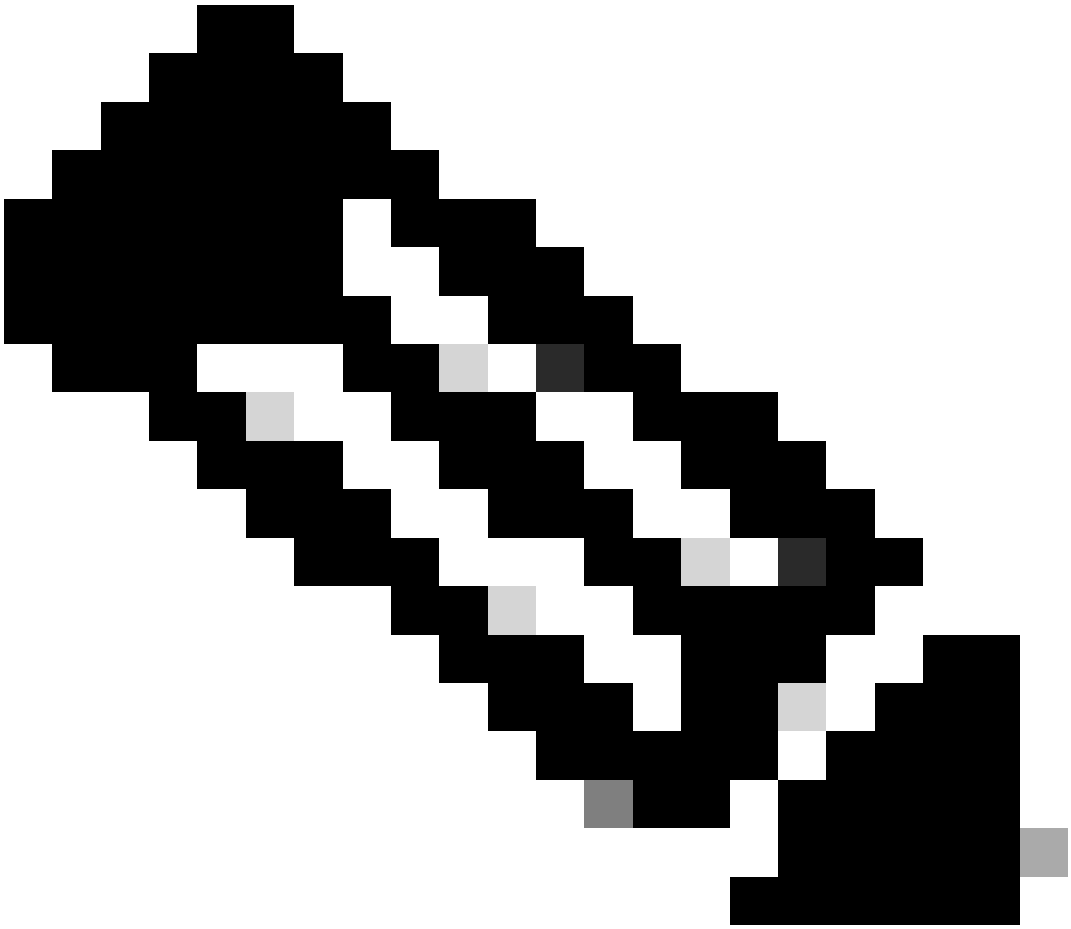
0 0 0

```
 100:23
K2FibAdjMan Stats Re   2.00   0.30     10      4  100  500    0   0    0  6:21
K2FibAdjMan Host Mov   2.00   0.00     10      4  100  500    0   0    0  0:00
K2FibAdjMan Adj Chan   2.00   0.00     10      0  100  500    0   0    0  0:00
K2FibMulticast Signa   2.00   0.01     10      2  100  500    0   0    0  2:04
```

Utilizzo elevato della CPU nel processo di spostamento dell'host K2FibAdjMan

Catalyst 4500 può visualizzare un elevato utilizzo **della** CPU nel processo di spostamento **host K2FibAdjMan**. Questo utilizzo elevato viene visualizzato nell'output del comando **show platform** health. Molti indirizzi MAC scadono spesso o vengono appresi su nuove porte, il che

provoca un elevato utilizzo della CPU. Il valore predefinito di tempo di aging tabella indirizzi MAC è 5 minuti o 300 secondi. Per risolvere questo problema, è possibile aumentare il tempo di aging dell'indirizzo MAC oppure configurare la rete in modo da evitare il numero elevato di spostamenti dell'indirizzo MAC. Il software Cisco IOS versione 12.2(18)EW e successive ha migliorato il comportamento di questo processo per ridurre il consumo di CPU. Fare riferimento al bug Cisco IDCSCed15021.



Nota: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti Cisco interni.

<#root>

```
Switch#
```

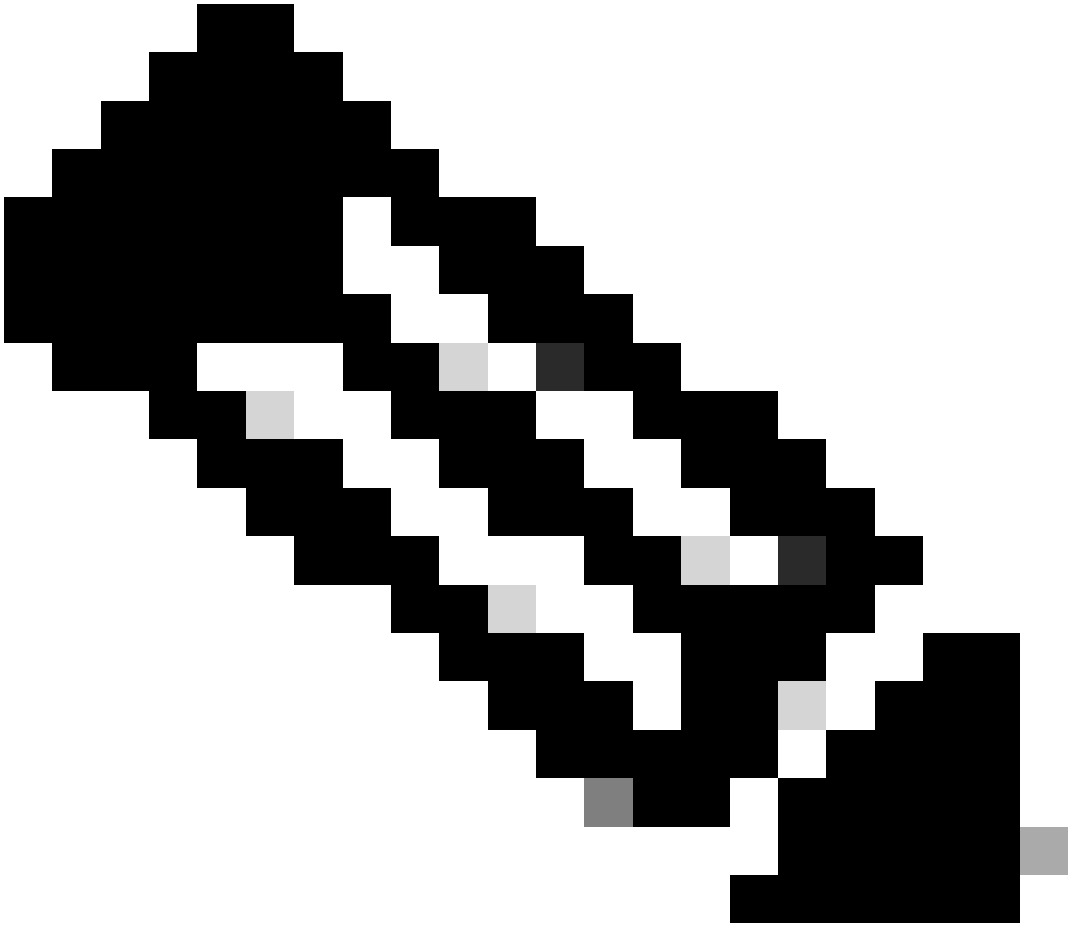
show platform health

```
                      %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                      Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                 1.00   0.02      2      1  100  500    0   0    0  1:09
GalChassisVp-review     3.00   0.29     10      3  100  500    0   0    0  11:15
S2w-JobEventSchedule   10.00   0.32     10      7  100  500    0   0    0  10:14

!--- Output suppressed.

K2FibAdjMan Stats Re    2.00   0.30     10      4  100  500    0   0    0  6:21



K2FibAdjMan Host Mov    2.00  18.68     10      4  100  500   25  29   28  2134:39



K2FibAdjMan Adj Chan    2.00   0.00     10      0  100  500    0   0    0  0:00
K2FibMulticast Signa    2.00   0.01     10      2  100  500    0   0    0  2:04
K2FibMulticast Entry    2.00   0.00     10      7  100  500    0   0    0  0:00
```

È possibile modificare il tempo di permanenza massimo di un indirizzo MAC nella modalità di configurazione globale. La sintassi del comando **ismac-address-table-aging-time** seconds per un router **e mac-address-table-aging-time seconds [vlan-vlan-id]**per uno switch Catalyst. Per ulteriori informazioni, consultare la guida di riferimento dei comandi di Cisco IOS Switching Services.

Elevato utilizzo della CPU nel processo di revisione della porta RkiosPortMan

Catalyst 4500 può visualizzare un elevato utilizzo **della** CPU nel processo **RkiosPortMan Port** Review nei risultati del comando **show platform** health del software Cisco IOS versione 12.2(25)EWA e 12.2(25)EWA1. Il bug Cisco IDCSCeh08768causa un elevato utilizzo del software Cisco IOS versione 12.2(25)EWA2. Questo processo è in background e non influisce sulla stabilità degli switch Catalyst 4500.



Nota: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti Cisco interni.

<#root>

Switch#

show platform health

```
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                1.00   0.02      2      1  100  500    0   0    0  1:09
GalChassisVp-review    3.00   0.29     10      3  100  500    0   0    0  11:15
S2w-JobEventSchedule  10.00   0.32     10      7  100  500    0   0    0  10:14

!--- Output suppressed.

K2 Packet Memory Dia   2.00   0.00     15      8  100  500    0   1    1  45:46
K2 L2 Aging Table Re   2.00   0.12     20      3  100  500    0   0    0  7:22




RkiosPortMan Port Re   2.00  87.92     12      7  100  500   99  99   89  1052:36




Rkios Module State R   4.00   0.02     40      1  100  500    0   0    0  1:28
Rkios Online Diag Re   4.00   0.02     40      0  100  500    0   0    0  1:15
```

Utilizzo elevato della CPU quando collegato a un telefono IP con porte trunk

Se una porta è configurata sia per l'opzione Voice VLAN sia per l'opzione Access VLAN, la porta funziona come porta di accesso multi VLAN. Il vantaggio è che solo le VLAN configurate per le opzioni VLAN di accesso e voce vengono trunking.

Le VLAN trunking al telefono aumentano il numero di istanze STP. Lo switch gestisce le istanze STP. La gestione dell'aumento delle istanze STP aumenta inoltre l'utilizzo della CPU STP.

Il trunking di tutte le VLAN provoca anche traffico broadcast, multicast e unicast sconosciuto non necessario sul collegamento telefonico.

<#root>

Switch#

show processes cpu

CPU utilization for five seconds: 69%/0%; one minute: 72%; five minutes: 73%

```
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4       165         24  0.00%  0.00%  0.00%   0 Chunk Manager
   2       29012    739091         39  0.00%  0.00%  0.00%   0 Load Meter
   3       67080     13762       4874  0.00%  0.00%  0.00%   0 SpanTree Helper
   4           0         1          0  0.00%  0.00%  0.00%   0 Deferred Events
   5           0         2          0  0.00%  0.00%  0.00%   0 IpSecMibTopN
   6     4980144    570766       8725  0.00%  0.09%  0.11%   0 Check heaps
  26   539173952 530982442       1015 13.09% 13.05% 13.20%   0 Cat4k Mgmt HiPri
  27   716335120 180543127       3967 17.61% 18.19% 18.41%   0 Cat4k Mgmt LoPri
  33     1073728     61623      17424  0.00%  0.03%  0.00%   0 Per-minute Jobs
  34  1366717824 231584970       5901 38.99% 38.90% 38.92%   0 Spanning Tree
  35     2218424  18349158        120  0.00%  0.03%  0.02%   0 DTP Protocol
  36        5160    369525         13  0.00%  0.00%  0.00%   0 Ethchnl
  37      271016   2308022        117  0.00%  0.00%  0.00%   0 VLAN Manager
  38      958084   3965585        241  0.00%  0.01%  0.01%   0 UDLD
  39        1436     51011         28  0.00%  0.00%  0.00%   0 DHCP Snooping
  40         780     61658         12  0.00%  0.00%  0.00%   0 Port-Security
  41     1355308  12210934        110  0.00%  0.01%  0.00%   0 IP Input
```

Utilizzo elevato della CPU con RSPAN e pacchetti di controllo di livello 3

I pacchetti di controllo di layer 3 acquisiti con RSPAN sono destinati alla CPU anziché solo all'interfaccia di destinazione RSPAN, il che provoca un utilizzo elevato della CPU. I pacchetti di controllo L3 vengono acquisiti da voci CAM statiche con azione forward to CPU. Le voci CAM statiche sono globali per tutte le VLAN. Per evitare un sovraccarico della CPU, usare la funzione Per-VLAN Control Traffic Intercept, disponibile nella versione 12.2(37)SG del software Cisco IOS e successive.

<#root>

```
Switch(config)#
```

access-list hardware capture mode vlan

Gli ACL statici vengono installati nella parte superiore della funzionalità di input TCAM per acquisire pacchetti di controllo destinati a indirizzi multicast IP noti nell'intervallo 24.0.0.*. Gli ACL statici vengono installati all'avvio e visualizzati prima di qualsiasi ACL configurato dall'utente. Gli ACL statici vengono sempre premuti per primi e intercettano il traffico di controllo verso la CPU su tutte le VLAN.

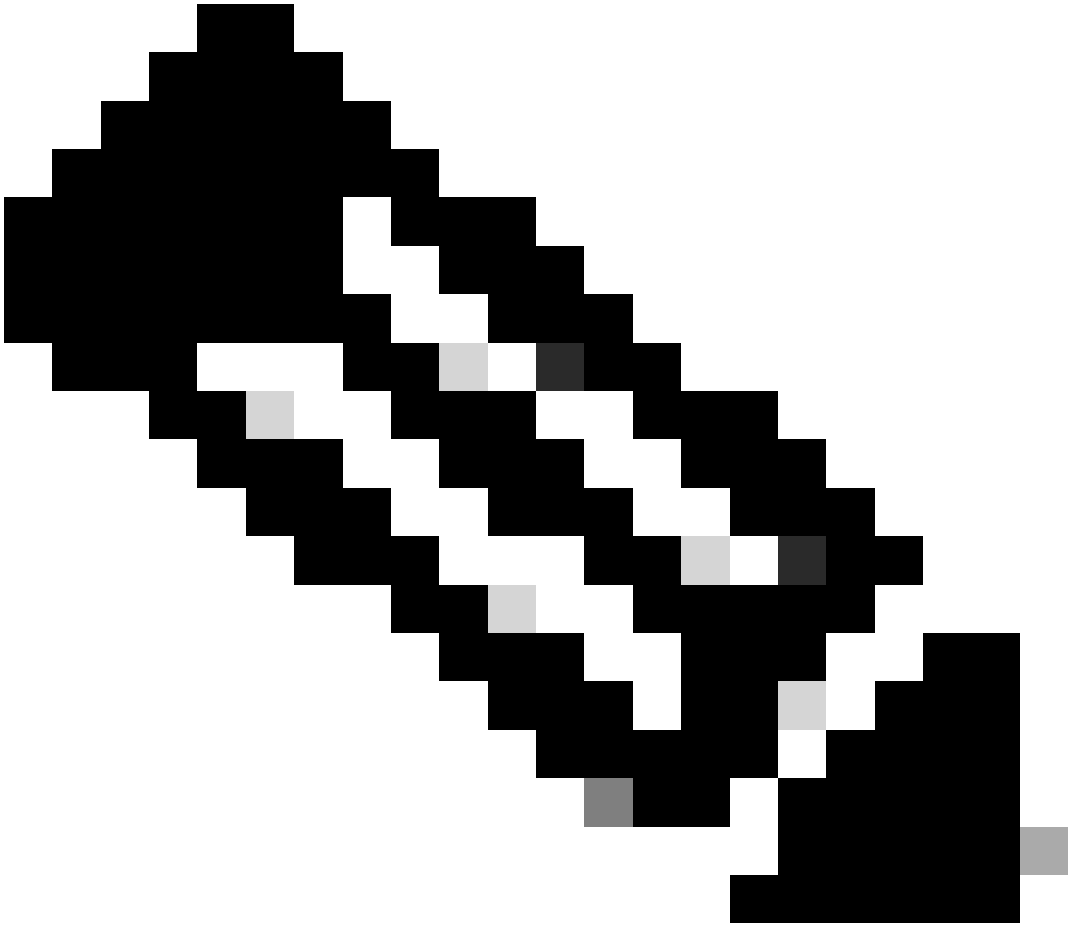
La funzione di intercettazione del traffico di controllo per VLAN fornisce la modalità selettiva gestita dal percorso per VLAN per l'acquisizione del traffico di controllo. Le corrispondenti voci statiche CAM nella funzione di input TCAM vengono invalidate nella nuova modalità. I pacchetti di controllo vengono acquisiti da ACL specifici della funzionalità collegati alle VLAN su cui sono abilitate le funzionalità di snooping o routing. Alla VLAN RSPAN non è associato alcun ACL specifico per la funzionalità. Pertanto, tutti i pacchetti di controllo di layer 3 ricevuti dalla VLAN RSPAN non vengono inoltrati alla CPU.

Strumenti di risoluzione dei problemi per analizzare il traffico destinato alla CPU

Come mostrato nel documento, il traffico destinato alla CPU è una delle cause principali dell'elevato utilizzo della CPU su Catalyst 4500. Il traffico destinato alla CPU può essere intenzionale o a causa della configurazione, o non intenzionale a causa di una configurazione errata o di un attacco di negazione del servizio. La CPU dispone di un meccanismo QoS integrato per prevenire eventuali effetti negativi sulla rete causati da questo traffico. Tuttavia, identificare la causa principale del traffico basato sulla CPU ed eliminare il traffico se non è desiderabile.

Strumento 1: monitoraggio del traffico della CPU con SPAN - Software Cisco IOS versione 12.1(19)EW e successive

Catalyst 4500 consente di monitorare il traffico basato sulla CPU, in entrata o in uscita, con la funzione SPAN standard. L'interfaccia di destinazione si connette a un monitor di pacchetto o a un laptop dell'amministratore con software di sniffer di pacchetto. Questo strumento consente di analizzare in modo rapido e accurato il traffico elaborato dalla CPU. Lo strumento consente di monitorare le singole code associate al motore dei pacchetti della CPU.



Nota: il motore di commutazione ha 32 code per il traffico CPU e il motore dei pacchetti CPU ne ha 16.

<#root>

Switch(config)#

monitor session 1 source cpu ?

```
  both   Monitor received and transmitted traffic
  queue  SPAN source CPU queue
  rx     Monitor received traffic only
  tx     Monitor transmitted traffic only
  <cr>
Switch(config)#
```

monitor session 1 source cpu queue ?

```
  <1-32>          SPAN source CPU queue numbers
  acl             Input and output ACL [13-20]
  adj-same-if     Packets routed to the incoming interface [7]
  all             All queues [1-32]
  bridged         L2/bridged packets [29-32]
  control-packet  Layer 2 Control Packets [5]
  mtu-exceeded    Output interface MTU exceeded [9]
  nfl             Packets sent to CPU by netflow (unused) [8]
  routed          L3/routed packets [21-28]
  rpf-failure     Multicast RPF Failures [6]
  span            SPAN to CPU (unused) [11]
  unknown-sa      Packets with missing source address [10]
Switch(config)#
```

monitor session 1 source cpu queue all rx

```
Switch(config)#
```

monitor session 1 destination interface gigabitethernet 1/3

```
Switch(config)#
```

end

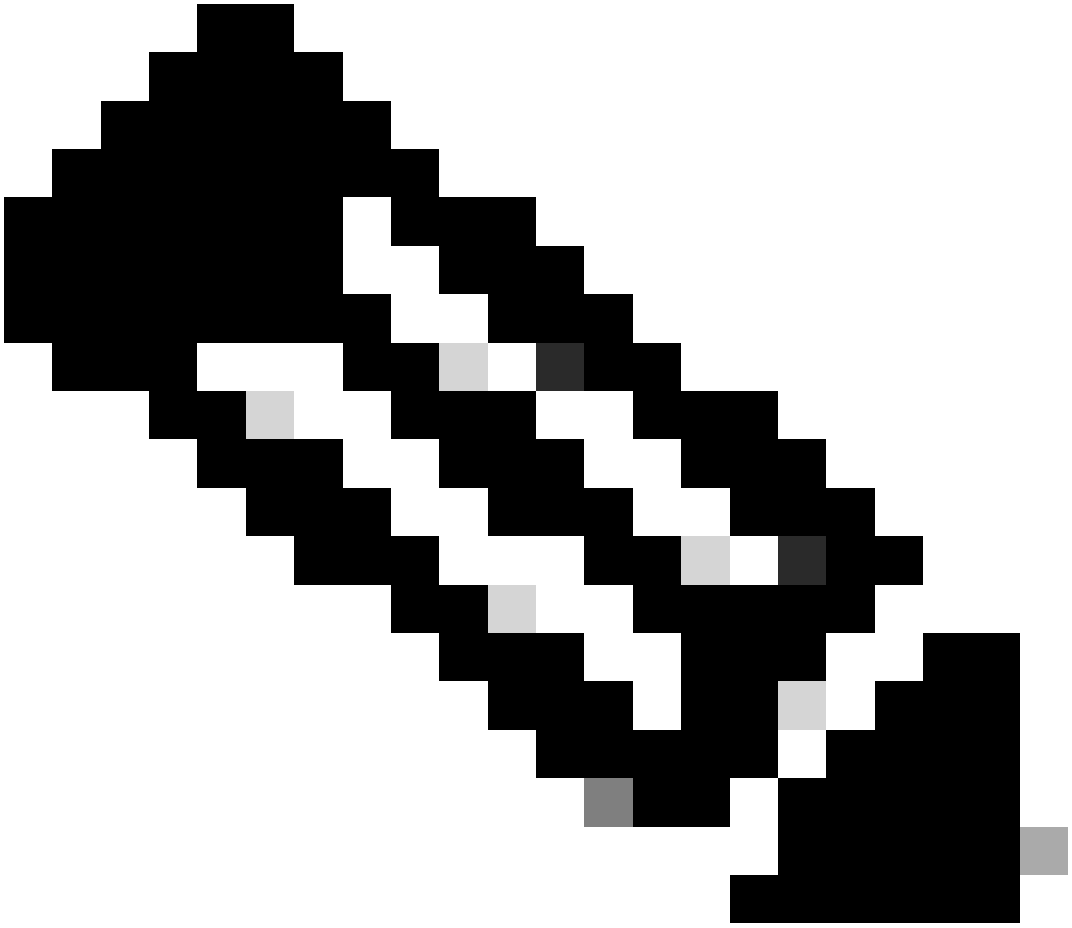
```
4w6d: %SYS-5-CONFIG_I: Configured from console by console
```

```
Switch#
```

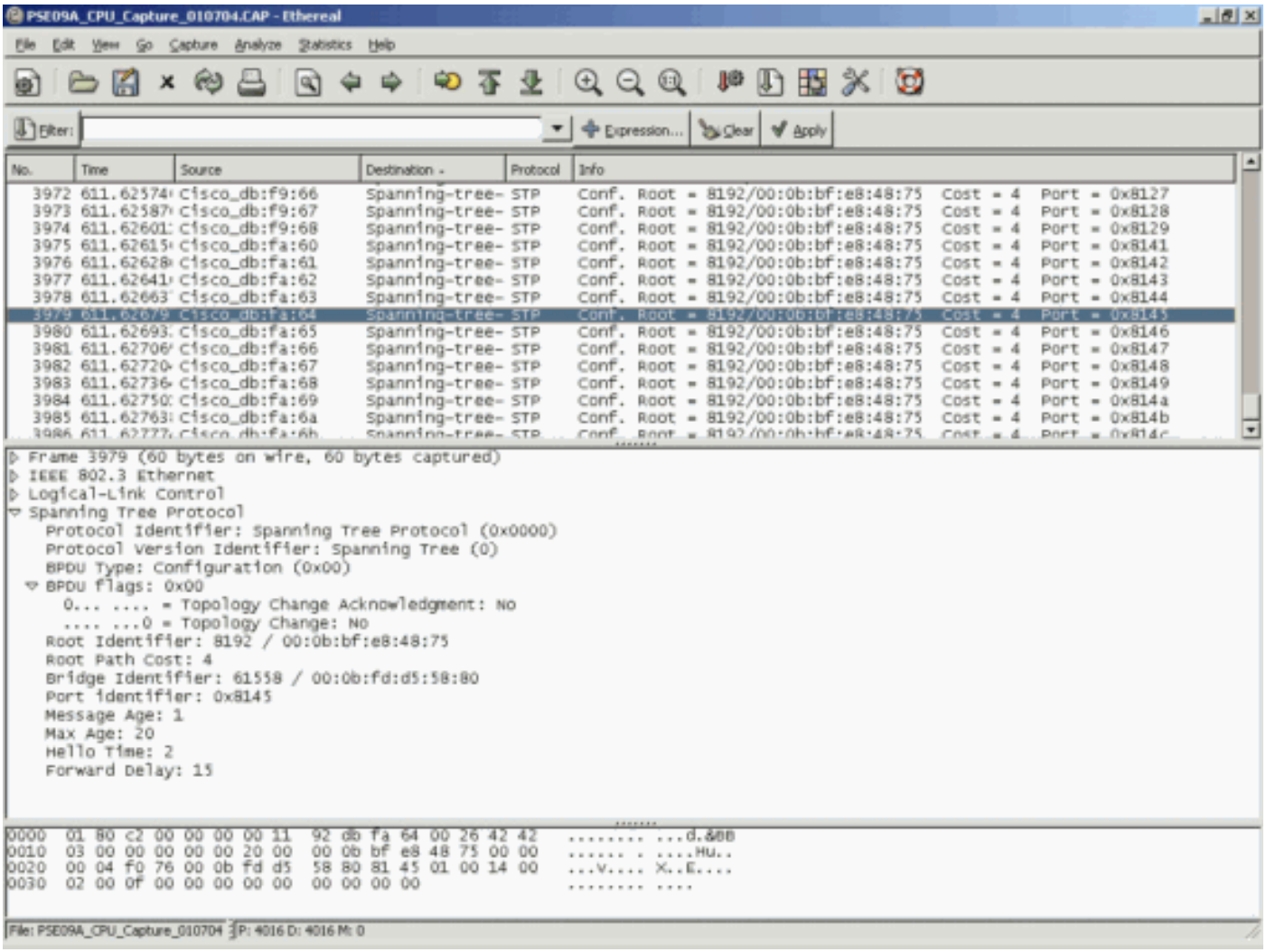
show monitor session 1

```
Session 1
---------
Type              : Local Session
Source Ports      :
    RX Only       : CPU
Destination Ports : Gi1/3
    Encapsulation : Native
          Ingress : Disabled
         Learning : Disabled
```

Se si collega un PC che esegue un programma di rilevamento, è possibile analizzare rapidamente il traffico. Nell'output visualizzato nella finestra di questa sezione, si osserverà che la causa dell'elevato utilizzo della CPU è un numero eccessivo di BPDU STP.



Nota: le BPDU STP nello sniffer della CPU sono normali. Tuttavia, se il risultato supera le aspettative, significa che sono stati superati i limiti consigliati per il Supervisor Engine. Per ulteriori informazioni, vedere la sezione **Numero elevato di istanze della porta Spanning-Tree** in questo documento.



L'elevato utilizzo della CPU è un numero eccessivo di BPDU STP

Strumento 2: Sniffer CPU incorporato—Software Cisco IOS versione 12.2(20)EW e successive

Catalyst 4500 fornisce uno sniffer e un decoder CPU integrati per identificare rapidamente il traffico che colpisce la CPU. È possibile attivare questa funzionalità con il debug comando, come illustrato nell'esempio riportato in questa sezione. Questa funzione implementa un buffer circolare in grado di conservare 1024 pacchetti alla volta. All'arrivo di nuovi pacchetti, quelli precedenti vengono sovrascritti. Questa funzione è sicura da utilizzare quando si risolvono problemi di utilizzo elevato della CPU.

<#root>

Switch#

debug platform packet all receive buffer

platform packet debugging is on

```
Switch#
```

show platform cpu packet buffered

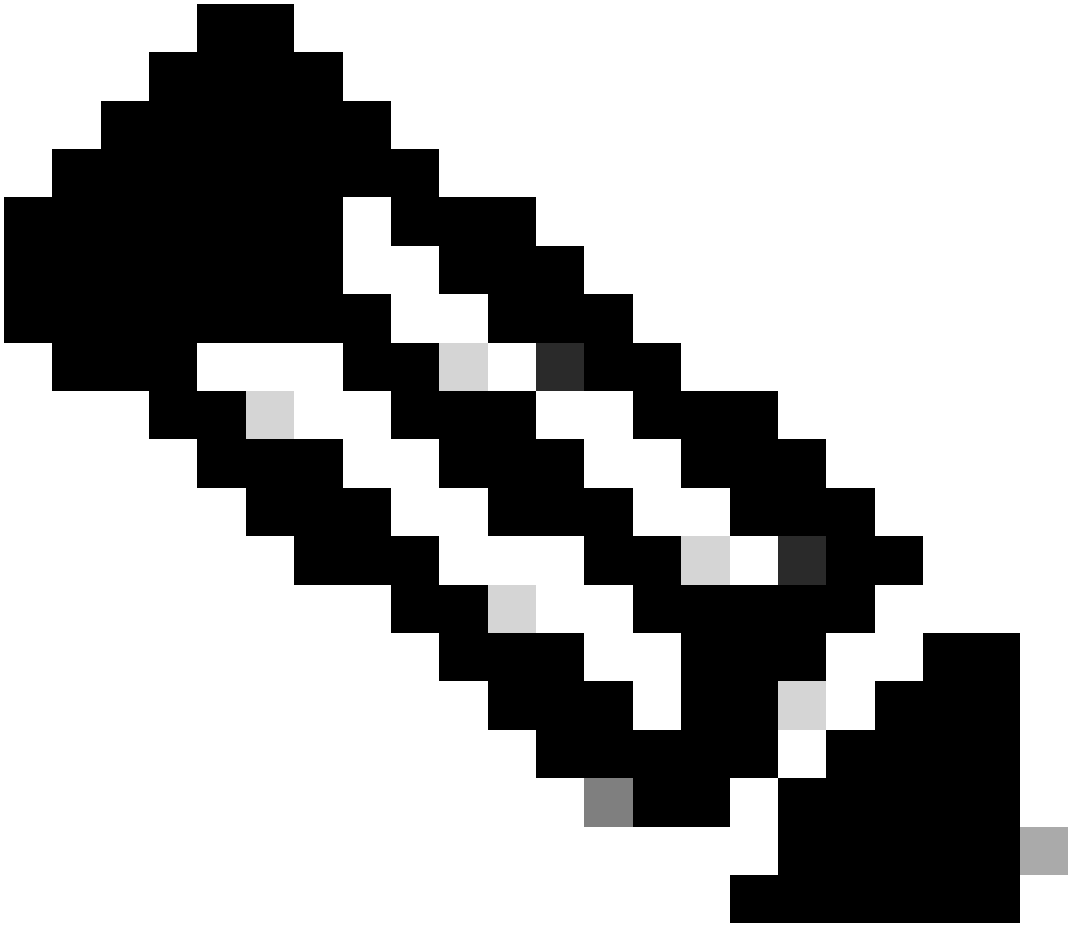
```
Total Received Packets Buffered: 36
-----------------------------------
Index 0:
7 days 23:6:32:37214 - RxVlan: 99,
```

RxPort: Gi4/48

```
Priority: Crucial, Tag: Dot1Q Tag, Event: Control Packet, Flags: 0x40, Size: 68
Eth:
```

Src 00-0F-F7-AC-EE-4F

```
 Dst 01-00-0C-CC-CC-CD Type/Len 0x0032
Remaining data:
 0: 0xAA 0xAA 0x3  0x0  0x0  0xC  0x1  0xB  0x0  0x0
10: 0x0  0x0  0x0  0x80 0x0  0x0  0x2  0x16 0x63 0x28
20: 0x62 0x0  0x0  0x0  0x0  0x80 0x0  0x0  0x2  0x16
30: 0x63 0x28 0x62 0x80 0xF0 0x0  0x0  0x14 0x0  0x2
40: 0x0  0xF  0x0  0x0  0x0  0x0  0x0  0x2  0x0  0x63
Index 1:
7 days 23:6:33:180863 - RxVlan: 1, RxPort: Gi4/48
Priority: Crucial, Tag: Dot1Q Tag, Event: Control Packet, Flags: 0x40, Size: 68
Eth: Src 00-0F-F7-AC-EE-4F Dst 01-00-0C-CC-CC-CD Type/Len 0x0032
Remaining data:
 0: 0xAA 0xAA 0x3  0x0  0x0  0xC  0x1  0xB  0x0  0x0
10: 0x0  0x0  0x0  0x80 0x0  0x0  0x2  0x16 0x63 0x28
20: 0x62 0x0  0x0  0x0  0x0  0x80 0x0  0x0  0x2  0x16
30: 0x63 0x28 0x62 0x80 0xF0 0x0  0x0  0x14 0x0  0x2
40: 0x0  0xF  0x0  0x0  0x0  0x0  0x0  0x2  0x0  0x63
```



Nota: l'utilizzo della CPU quando si esegue un debug comando è sempre quasi del 100%. Quando si usa un debug comando, è normale avere un elevato utilizzo della CPU.

Strumento 3: Identificare l'interfaccia che invia il traffico alla CPU: software Cisco IOS versione 12.2(20)EW e successive

Catalyst 4500 offre un altro utile strumento per identificare le principali interfacce che inviano traffico/pacchetti per l'elaborazione CPU. Questo strumento consente di identificare rapidamente un dispositivo di errore che invia un numero elevato di attacchi broadcast o di negazione del servizio alla CPU. Questa funzione è inoltre sicura quando si risolvono problemi di utilizzo elevato della CPU.

```
Switch#
```

debug platform packet all count

```
platform packet debugging is on
Switch#
```

show platform cpu packet statistics

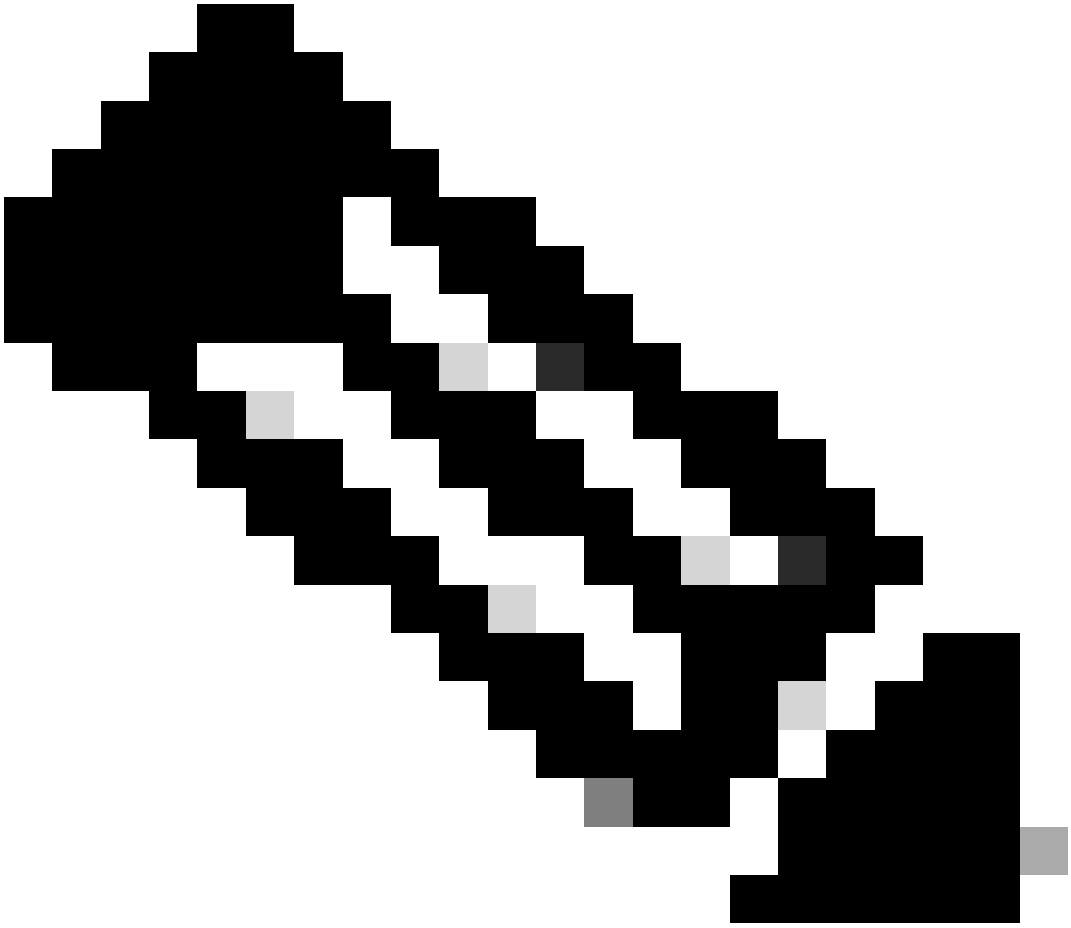
!--- Output suppressed.

Packets Transmitted from CPU per Output Interface

Interface	Total	5 sec avg	1 min avg	5 min avg	1 hour avg
Gi4/47	1150	1	5	10	0
Gi4/48	50	1	0	0	0

Packets Received at CPU per Input Interface

Interface	Total	5 sec avg	1 min avg	5 min avg	1 hour avg
Gi4/47	23130	5	10	50	20
Gi4/48	50	1	0	0	0



Nota: l'utilizzo della CPU quando si esegue un comando debug è sempre quasi del 100%. Quando si usa un comando debug, è normale avere un elevato utilizzo della CPU.

Riepilogo

Gli switch Catalyst 4500 gestiscono una velocità elevata di inoltro di pacchetti IP versione 4 (IPv4) nell'hardware. Alcune funzionalità o eccezioni possono causare l'inoltro di alcuni pacchetti tramite il percorso di processo della CPU. Catalyst 4500 utilizza un sofisticato meccanismo QoS per gestire i pacchetti basati sulla CPU. Questo meccanismo garantisce l'affidabilità e la stabilità degli switch e, allo stesso tempo, massimizza la CPU per l'inoltro software dei pacchetti. Il software Cisco IOS versione 12.2(25)EWA2 e successive offre ulteriori miglioramenti per la gestione di pacchetti/processi e per l'accounting. Catalyst 4500 dispone inoltre di comandi e strumenti potenti sufficienti per identificare la root cause di scenari di elevato utilizzo della CPU. Tuttavia, nella maggior parte dei casi, l'elevato utilizzo della CPU sullo switch

Catalyst 4500 non è una causa di instabilità della rete né un motivo di preoccupazione.

Informazioni correlate

- **Utilizzo della CPU sugli switch Catalyst 4500/4000, 2948G, 2980G e 4912G con CatOS**
- **Pagine di supporto dei prodotti LAN**
- **Pagina di supporto dello switching LAN**
- **Documentazione e supporto tecnico – Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).