

Catalyst 6500/6000交換器CPU使用率高

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[CatOS 和 Cisco IOS 系統軟體之間的差異](#)

[瞭解Catalyst 6500/6000交換器上的CPU使用率](#)

[觸發流量進入軟體的情況和功能](#)

[目的地為交換器的封包](#)

[需要特殊處理的資料包和條件](#)

[基於ACL的功能](#)

[基於NetFlow的功能](#)

[多點傳送流量](#)

[其他功能](#)

[IPv6情況](#)

[LCP排程和DFC模組](#)

[高CPU利用率問題的常見原因和解決方案](#)

[IP無法到達](#)

[NAT轉換](#)

[在流快取表中使用CEF FIB表空間](#)

[最佳化ACL記錄](#)

[發往CPU的資料包速率限制](#)

[由於不正確佈線導致VLAN的物理合併](#)

[廣播風暴](#)

[BGP下一躍點位址追蹤 \(BGP掃描器程式 \)](#)

[非RPF多點傳送流量](#)

[show命令](#)

[執行過程](#)

[L3老化過程](#)

[BPDU風暴](#)

[SPAN作業階段](#)

[%CFIB-SP-STBY-7-CFIB EXCEPTION :FIB TCAM異常，某些條目將被軟體交換](#)

[使用高CPU的Catalyst 6500/6000具有使用L4埠的IPv6 ACL](#)

[銅纜SPF](#)

[模組化IOS](#)

[檢查CPU利用率](#)

[用於確定傳送到CPU的流量的實用程式和工具](#)

[Cisco IOS® 系統軟體](#)

[CatOS 系統軟體](#)

[建議](#)

[相關資訊](#)

[簡介](#)

本文說明基於Cisco Catalyst 6500/6000系列交換機和虛擬交換系統(VSS)1440的系統上CPU使用率高的原因。與Cisco路由器一樣，交換機使用**show processes cpu**命令來顯示交換機管理引擎處理器的CPU利用率。但是，由於Cisco路由器和交換機之間的體系結構和轉發機制存在差異，因此**show processes cpu**命令的典型輸出明顯不同。輸出的含義也有所不同。本文檔澄清了這些差異，並說明了交換機上的CPU利用率以及如何解釋**show processes cpu**命令輸出。

註：本檔案中的「switch」和「switches」字樣是指Catalyst 6500/6000交換器。

[必要條件](#)

[需求](#)

本文件沒有特定需求。

[採用元件](#)

本檔案中的資訊是根據基於Catalyst 6500/6000交換器和虛擬交換系統(VSS)1440的系統的軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

注意：虛擬交換系統(VSS)1440系統支援的軟體為Cisco IOS®軟體版本12.2(33)SXH1或更高版本。

[慣例](#)

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

[CatOS 和 Cisco IOS 系統軟體之間的差異](#)

Supervisor Engine上使用Catalyst OS(CatOS)，多層交換器功能卡(MSFC)上則使用Cisco IOS®軟體（混合）：您可以使用CatOS映像作為系統軟體，在Catalyst 6500/6000交換器上執行Supervisor engine。如果安裝了選用的MSFC，則會使用單獨的Cisco IOS軟體映像來執行MSFC。

Supervisor Engine 和 MSFC 上皆使用 Cisco IOS 軟體（原生）：您可以使用單一Cisco IOS軟體映像作為系統軟體，在Catalyst 6500/6000交換器上執行Supervisor engine和MSFC。

註：如需詳細資訊，請參閱[適用於Cisco Catalyst 6500系列交換器的Cisco Catalyst和Cisco IOS作業系統的比較](#)。

瞭解Catalyst 6500/6000交換器上的CPU使用率

思科軟體型路由器使用軟體來處理和路由封包。隨著路由器執行更多資料包處理和路由，Cisco路由器上的CPU利用率會增加。因此，`show processes cpu`命令可以相當準確地指示路由器上的流量處理負載。

Catalyst 6500/6000交換器不以相同方式使用CPU。這些交換機在硬體而非軟體中作出轉發決策。因此，當交換機對通過交換機的大多數幀做出轉發或交換決策時，該過程不會涉及Supervisor引擎CPU。

Catalyst 6500/6000交換器上有兩個CPU。一個CPU是管理引擎CPU，稱為網路管理處理器(NMP)或交換機處理器(SP)。另一個CPU是第3層路由引擎CPU，稱為MSFC或路由處理器(RP)。

SP CPU執行的功能包括：

- 協助學習和老化MAC地址注意：MAC地址學習也稱為路徑設定。
- 運行提供網路控制的協定和進程範例包括跨距樹狀目錄通訊協定(STP)、思科探索通訊協定(CDP)、VLAN中繼線通訊協定(VTP)、動態中繼線通訊協定(DTP)和連線埠彙總通訊協定(PAgP)。
- 處理髮往交換機CPU的網路管理流量示例包括Telnet、HTTP和簡單網路管理協定(SNMP)流量。

RP CPU執行的功能包括：

- 建立並更新第3層路由和地址解析協定(ARP)表
- 生成思科快速轉發(CEF)轉發資訊庫(FIB)和鄰接表，並將這些表下載到策略功能卡(PFC)中
- 處理髮往RP的網路管理流量示例包括Telnet、HTTP和SNMP流量。

觸發流量進入軟體的情況和功能

目的地為交換器的封包

任何目的地為交換器的封包都會轉往軟體。此類資料包包括：

- 控制資料包接收STP、CDP、VTP、熱待命路由器協定(HSRP)、PAgP、鏈路聚合控制協定(LACP)和單向鏈路檢測(UDLD)的控制資料包。
- 路由協定更新這些通訊協定的範例包括路由資訊通訊協定(RIP)、增強型內部閘道路由通訊協定(EIGRP)、邊界閘道通訊協定(BGP)和開放最短路徑優先通訊協定(OSPF通訊協定)。
- 目的地為交換器的SNMP流量
- 到交換機的Telnet和安全殼層協定(SSH)流量。由於SSH導致的CPU使用率較高被視為：

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

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

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
3	6468	8568	754	69.30%	7.90%	1.68%	1	SSH Process

在EEM指令碼中包含以下命令，以驗證CPU使用率較高時建立的SSH會話數：[顯示使用者顯示行](#)

- ARP對ARP請求的響應

需要特殊處理的資料包和條件

此清單提供特定封包型別和條件，強制在軟體中處理封包：

- 具有IP選項、過期生存時間(TTL)或非高級研究專案代理(ARPA)封裝的資料包
- 經過特殊處理的資料包，例如隧道
- IP分段
- 需要來自RP或SP的網際網路控制消息協定(ICMP)消息的資料包
- 最大傳輸單元(MTU)檢查失敗
- 具有IP錯誤的資料包，包括IP校驗和和長度錯誤
- 如果輸入分組返回一個位元錯誤(例如單位元錯誤(SBE))，那麼分組被傳送到CPU進行軟體處理並被校正。系統會為其分配一個緩衝區，並使用CPU資源對其進行修正。
- 當PBR和自反訪問清單在流量流的路徑中時，資料包進行軟體交換，這要求額外的CPU週期。
- 鄰接同一介面
- 無法通過反向路徑轉發(RPF)檢查的資料包- `rpf-failure`
- 收集/接收Glean指需要ARP解析的資料包，`receive`指屬於接收情況的資料包。
- 在Cisco IOS軟體和CatOS中的Supervisor Engine 720上以軟體交換的網際網路封包交換(IPX)流量IPX流量也在Supervisor Engine 2/Cisco IOS軟體上進行軟體交換，但流量在Supervisor Engine 2/CatOS上進行硬體交換。IPX流量在Supervisor引擎1A上針對兩個作業系統進行硬體交換。
- AppleTalk流量
- 硬體資源已滿條件這些資源包括FIB、內容可定址儲存器(CAM)和三元CAM(TCAM)。

基於ACL的功能

- 已開啟ICMP不可達功能之存取控制清單(ACL) — 拒絕流量**注意**：這是預設設定。如果啟用了IP無法連線，則會將某些ACL拒絕的封包洩漏到MSFC。需要ICMP無法到達的資料包以使用者可配置的速率洩漏。預設情況下，速率為每秒500個資料包(pps)。
- 基於不受支援的引數(如源主機)進行IPX過濾在Supervisor Engine 720上，第3層IPX流量的處理過程始終在軟體中。
- 需要記錄的訪問控制條目(ACE)，帶有**log**關鍵字這適用於ACL日誌和VLAN ACL(VACL)日誌功能。同一ACL中不需要記錄的ACE仍在硬體中處理。搭載PFC3的Supervisor引擎720支援重新導向到MSFC進行ACL和VACL記錄的封包的速率限制。Supervisor引擎2支援重新定向到MSFC進行VACL日誌記錄的資料包的速率限制。Cisco IOS軟體版本12.2S分支計畫支援Supervisor Engine 2上的ACL日誌記錄。
- 策略路由流量，使用**match length**、**set ip precedence**或其他不支援的引數**set interface**引數在軟體中具有支援。但是，**set interface null 0**引數是一個例外。此流量在搭載PFC2的Supervisor引擎2和搭載PFC3的Supervisor引擎720上的硬體中處理。
- 非IP和非IPX路由器ACL(RACL)非IP RACL適用於所有管理引擎。非IPX RACL僅適用於具有PFC的Supervisor引擎1a和僅具有PFC2的Supervisor引擎2。
- 在RACL中遭到拒絕的廣播流量
- 在單播RPF(uRPF)檢查中被拒絕的流量，ACL ACE此uRPF檢查適用於搭載PFC2的Supervisor引擎2和搭載PFC3的Supervisor引擎720。
- 驗證代理在Supervisor Engine 720上，受驗證代理控制的流量可以受速率限制。
- Cisco IOS軟體IP安全(IPsec)在Supervisor Engine 720上，受Cisco IOS加密管轄的流量可以受速率限制。

基於NetFlow的功能

本節介紹的基於NetFlow的功能僅適用於管理引擎2和管理引擎720。

- 基於NetFlow的功能始終需要檢視軟體中流量的第一個資料包。一旦流量的第一個封包到達軟體，同一流量的後續封包就會進行硬體交換。此流量安排適用於自反型ACL、網路快取通訊協定(WCCP)和Cisco IOS伺服器負載平衡(SLB)。註：在Supervisor Engine 1上，自反型ACL依靠動態TCAM條目為特定流建立硬體快捷方式。原則是一樣的：流量的第一個封包進入軟體。該流的後續分組是硬體交換的。
- 利用TCP攔截功能，軟體中可處理三次握手和會話關閉。其餘的流量在硬體中處理。註：同步(SYN)、SYN確認(SYN ACK)和ACK資料包構成三次握手。完成時(FIN)或重置時(RST)會關閉會話。
- 使用網路位址轉譯(NAT)時，流量處理方式如下：在Supervisor Engine 720上：在初始轉換後，需要NAT的流量在硬體中處理。流的第一分組的轉換在軟體中發生，該流的後續分組是硬體交換的。對於TCP資料包，在TCP三次握手完成後，在NetFlow表中建立硬體快捷方式。在Supervisor Engine 2和Supervisor Engine 1上：所有需要NAT的流量都採用軟體交換。
- 內容型存取控制(CBAC)使用NetFlow快捷方式對需要檢查的流量進行分類。接著，CBAC僅將此流量傳送到軟體。CBAC是一種純軟體功能；接受檢查的流量不是硬體交換的。注意：Supervisor Engine 720上可以限定需要檢查的流量。

多點傳送流量

- 通訊協定無關多點傳送(PIM)窺探
- 網際網路群組管理協定(IGMP)窺探(TTL = 1)此流量的目的地確實是路由器。
- 多點傳送監聽器探索(MLD)窺探(TTL = 1)此流量的目的地確實是路由器。
- FIB未命中
- 直接連線到組播源的註冊組播資料包這些組播資料包通過隧道傳輸到交匯點。
- IP第6版(IPv6)多點傳送

其他功能

- 網路型應用程式辨識(NBAR)
- ARP檢測，僅使用CatOS
- 埠安全，僅支援CatOS
- DHCP窺探

IPv6情況

- 具有逐跳選項報頭的資料包
- 目的IPv6地址與路由器相同的資料包
- 未能通過範圍強制檢查的資料包
- 超出輸出連結MTU的封包
- TTL小於或等於1的資料包
- 輸入VLAN等於輸出VLAN的資料包
- IPv6 uRPF軟體對所有資料包執行此uRPF。
- IPv6自反型ACL軟體會處理這些自反型ACL。
- IPv6站點內自動隧道定址協定(ISATAP)隧道的6to4字首軟體會處理此通道。所有進入

ISATAP隧道的其它流量均採用硬體交換。

LCP排程和DFC模組

在分散式轉送卡(DFC)中，在高CPU上執行的lcp_scheduler程式不會產生問題，也不會對操作造成任何問題。LCP計畫是韌體代碼的一部分。在不需要DFC的所有模組上，韌體在稱為線卡處理器(LCP)的特定處理器上運行。此處理器用於對ASIC硬體進行程式設計並與中央管理引擎模組通訊。

lcp_scheduler啟動時，它將利用所有可用的處理時間。但是，當新進程需要處理器時間時，lcp_scheduler會為新進程釋放進程時間。這種CPU使用率較高不會影響系統的效能。只要優先順序較高的進程不需要所有未使用的CPU週期，該進程就會佔用這些週期。

DFC#show process cpu

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

高CPU利用率問題的常見原因和解決方案

IP無法到達

當存取組拒絕封包時，MSFC會傳送ICMP無法到達訊息。預設情況下會發生此操作。

在預設啟用ip unreachable命令的情況下，Supervisor引擎將丟棄硬體中的大多數被拒絕的資料包。然後，Supervisor引擎僅將少數資料包（最多10 pps）傳送到MSFC進行丟棄。此操作會生成ICMP無法到達消息。

丟棄拒絕的資料包和生成ICMP不可達消息會給MSFC CPU帶來負載。若要消除負載，您可以發出no ip unreachable介面組態指令。此命令禁用ICMP不可達消息，這允許丟棄所有訪問組拒絕的資料包的硬體。

如果VACL拒絕資料包，則不會傳送ICMP無法到達消息。

NAT轉換

NAT同時利用硬體和軟體轉發。NAT轉換的初始建立必須在軟體中完成，而進一步轉發則通過硬體完成。NAT還利用Netflow表（最大128 KB）。因此，如果Netflow表已滿，交換機也將開始通過軟體應用NAT轉發。這種情況通常發生在高流量突發時，並將導致CPU 6500增加。

在流快取表中使用CEF FIB表空間

Supervisor Engine 1具有支援128,000個條目的流快取表。但是，根據雜湊演算法的效率，這些條目範圍從32,000到120,000。在Supervisor引擎2上，FIB表被生成並程式設計到PFC中。該表包含多達256,000個條目。搭載PFC3-BXL的Supervisor引擎720支援最多1,000,000個專案。一旦超出此空間，便會在軟體中交換資料包。這可能導致RP上的CPU使用率高。要檢查CEF FIB表中的路由數，請使用以下命令：

```
Router#show processes cpu
```

```
CPU utilization for five seconds: 99.26%
                                one minute: 100.00%
                                five minutes: 100.00%
```

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
1	0	0	0	0.74%	0.00%	0.00%	-2	Kernel and Idle
2	2	245	1000	0.00%	0.00%	0.00%	-2	Flash MIB Updat
3	0	1	0	0.00%	0.00%	0.00%	-2	L2L3IntHdlr
4	0	1	0	0.00%	0.00%	0.00%	-2	L2L3PatchRev
5	653	11737	1000	0.00%	0.00%	0.00%	-2	SynDi
<i>!--- Output is suppressed.</i>								
26	10576	615970	1000	0.00%	0.00%	0.00%	0	L3Aging 27 47432 51696 8000
0.02%	0.00%	0.00%	0	NetFlow 28 6758259 1060831 501000 96.62%	96.00%	96.00%	0	Fib
29	0	1	0	0.00%	0.00%	0.00%	-2	Fib_bg_task

```
!--- Output is suppressed. CATOS% show mls cef
```

```
Total L3 packets switched: 124893998234
Total L3 octets switched: 53019378962495
Total route entries: 112579
  IP route entries: 112578
  IPX route entries: 1
  IPM route entries: 0
IP load sharing entries: 295
IPX load sharing entries: 0
Forwarding entries: 112521
Bridge entries: 56
Drop entries: 2
```

```
IOS% show ip cef summary
```

```
IP Distributed CEF with switching (Table Version 86771423), flags=0x0
 112564 routes, 1 reresolve, 0 unresolved (0 old, 0 new)
 112567 leaves, 6888 nodes, 21156688 bytes, 86771426
inserts, 86658859
invalidations
 295 load sharing elements, 96760 bytes, 112359 references
 universal per-destination load sharing algorithm, id 8ADDA64A
 2 CEF resets, 2306608 revisions of existing leaves
refcounts: 1981829 leaf, 1763584 node
```

```
!--- You see these messages if the TCAM space is exceeded: %MLSCEF-SP-7-FIB_EXCEPTION: FIB TCAM
exception, Some entries will be software switched %MLSCEF-SP-7-END_FIB_EXCEPTION: FIB TCAM
exception cleared, all CEF entries will be hardware switched
```

在Supervisor Engine 2上，如果您已在介面上配置RPF檢查，則FIB條目數將減少一半。此配置可能導致軟體交換更多資料包，從而導致CPU使用率高。

要解決CPU使用率高的問題，請啟用路由總結。路由總結可以降低處理器工作負載、記憶體要求和頻寬需求，從而最大限度地減少複雜網路中的延遲。

請參閱[瞭解Catalyst 6500系列交換器上的ACL](#)，以瞭解其他有關TCAM使用率和最佳化的資訊。

最佳化ACL記錄

最佳化ACL記錄(OAL)為ACL記錄提供硬體支援。除非您配置OAL，否則需要日誌記錄的資料包過程完全在MSFC3上的軟體中發生。OAL允許或丟棄PFC3上的硬體中的資料包。OAL使用最佳化常式向MSFC3傳送資訊以生成日誌記錄消息。

注意：有關OAL的資訊，請參閱[瞭解Cisco IOS ACL支援的使用PFC3最佳化ACL日誌記錄部分](#)。

發往CPU的資料包速率限制

在Supervisor Engine 720上，速率限制器可以控制封包進入軟體的速率。此速率控制有助於防止拒絕服務攻擊。您還可以在Supervisor Engine 2上使用以下幾個速率限制器：

```
Router#show mls rate-limit
  Rate Limiter Type           Status      Packets/s   Burst
-----
  MCAST NON RPF              Off         -           -
  MCAST DFLT ADJ             On          100000      100
  MCAST DIRECT CON          Off         -           -
  ACL BRIDGED IN            Off         -           -
  ACL BRIDGED OUT          Off         -           -
  IP FEATURES                Off         -           -
  ACL VAACL LOG              On          2000        1
  CEF RECEIVE                Off         -           -
  CEF GLEAN                  Off         -           -
  MCAST PARTIAL SC          On          100000      100
  IP RPF FAILURE             On          500         10
  TTL FAILURE                Off         -           -
  ICMP UNREAC. NO-ROUTE     On          500         10
  ICMP UNREAC. ACL-DROP     On          500         10
  ICMP REDIRECT              Off         -           -
  MTU FAILURE                Off         -           -
  LAYER_2 PDU                Off         -           -
  LAYER_2 PT                 Off         -           -
  IP ERRORS                  On          500         10
  CAPTURE PKT                Off         -           -
  MCAST IGMP                 Off         -           -
```

```
Router(config)#mls rate-limit ?
  all          Rate Limiting for both Unicast and Multicast packets
  layer2       layer2 protocol cases
  multicast    Rate limiting for Multicast packets
  unicast      Rate limiting for Unicast packets
```

以下是範例：

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

若要將所有CEF傳出的封包速率限制到MSFC，請發出以下範例中的命令：

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

為了減少因TTL = 1而傳送到CPU的資料包數量，請發出以下命令：


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

例如，這是netdr capture的輸出，其中顯示IPv4 TTL為1:

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

L3

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

高CPU也可能是因為洩漏到CPU的TTL = 1的資料包。為了限制洩漏到CPU的資料包數量，請配置硬體速率限制器。速率限制器可以限制從硬體資料路徑洩漏到軟體資料路徑的資料包的速率。速率限制器通過丟棄超過已配置速率的流量來保護軟體控制路徑免受擁塞。速率限制是使用mls rate-limit all ttl-failure命令配置的。

[由於不正確佈線導致VLAN的物理合併](#)

由於纜線連線不當，兩個或多個VLAN合併在一起也可能導致CPU使用率高。此外，如果發生VLAN合併的那些埠上禁用STP，則可能會發生CPU使用率較高的情況。

為了解決此問題，請識別佈線錯誤並予以更正。如果您的需求允許，您還可以在這些埠上啟用STP。

[廣播風暴](#)

當廣播或組播資料包泛洪LAN時，就會發生LAN廣播風暴，從而造成過多的流量並降低網路效能。協定堆疊實施或網路配置中的錯誤可能導致廣播風暴。

由於Catalyst 6500系列平台的架構設計，廣播封包只會且總是會在軟體層級遭捨棄。

廣播抑制可防止LAN介面因廣播風暴而中斷。廣播抑制使用過濾，該過濾可測量LAN在1秒時間段內的廣播活動，並將測量值與預定義閾值進行比較。如果達到該閾值，則在指定的時間段內抑制進一步的廣播活動。預設情況下禁用廣播抑制。

註： 廣播風暴導致的VRRP從備份擺動到主節點可能導致CPU使用率高。

要瞭解廣播抑制如何工作並啟用該功能，請參閱：

- [配置廣播抑制](#) (Cisco IOS系統軟體)
- [配置廣播抑制](#) (CatOS系統軟體)

[BGP下一躍點位址追蹤 \(BGP掃描器程式 \)](#)

BGP掃描程式進程將遍歷BGP表並確認下一跳的可達性。此程式還會檢查條件通告，以確定BGP是否應通告條件字首和/或執行路由抑制。預設情況下，進程每60秒掃描一次。

由於BGP Scanner進程在承載大型Internet路由表的路由器上運行，因此可以預期在較短持續時間內較高的CPU利用率。BGP掃描程式每分鐘掃描1次，遍歷BGP路由資訊庫(RIB)表並執行重要的維護任務。這些任務包括：

- 檢查路由器BGP表中引用的下一跳
- 驗證是否可以到達下一跳裝置

因此，大的BGP表需要相當多的時間進行遍歷和驗證。BGP掃描程式進程遍歷BGP表以更新任何資料結構，並遍歷路由表以重分佈路由。兩個表分別儲存在路由器記憶體中。兩個表可能非常大，因此會消耗CPU週期。

有關BGP掃描程式進程的CPU使用率的詳細資訊，請參閱[對由BGP掃描程式或BGP路由器進程引起的高CPU進行故障排除的由於BGP掃描程式而引起的CPU使用率較高部分](#)。

有關BGP下一跳地址跟蹤功能以及啟用/禁用或調整掃描間隔的過程的詳細資訊，請參閱[支援下一跳地址跟蹤](#)。

[非RPF多點傳送流量](#)

組播路由（與單播路由不同）只與給定組播資料流的源相關。即發起組播流量的裝置的IP地址。基本原理是源裝置「推送」流到未定義數量的接收器（在其組播組內）。所有組播路由器都建立分發樹，分發樹控制組播流量通過網路傳遞的路徑，以便向所有接收方傳遞流量。組播分發樹的兩個基本型別是源樹和共用樹。RPF是組播轉發中的一個關鍵概念。它使路由器能夠正確轉發分佈樹中的組播流量。RPF利用現有的單播路由表來確定上游和下游鄰居。只有在上游介面收到組播資料包時，路由器才會轉發該資料包。此RPF檢查有助於確保分發樹無環路。

根據IEEE 802.3 CSMA/CD規範，橋接（第2層）LAN上的每台路由器始終可以看到組播流量。在802.3標準中，第一個二進位制八位數的位0用於表示廣播和/或組播幀，使用此地址的任何第2層幀都會被泛洪。即使已設定CGMP或IGMP窺探，情況也會如此。這是因為如果組播路由器需要做出正確的轉發決策，它們必須看到組播流量。如果多個組播路由器各自具有到公共LAN的介面，則只有一個路由器轉發資料（由選舉過程選擇）。由於LAN的泛洪性質，備援路由器（不轉送多點傳送流量的路由器）在該LAN的傳出介面上接收此資料。冗餘路由器通常會丟棄此流量，因為它到達的介面錯誤，因此未通過RPF檢查。未通過RPF檢查的流量稱為非RPF流量或RPF故障資料包，因為它們已針對來自源的流反向傳輸。

安裝了MSFC的Catalyst 6500可以配置為充當完整的多播路由器。利用多點傳送多層交換(MMLS),RPF流量通常由交換器內的硬體轉送。ASIC從組播路由狀態獲得資訊(例如, (*,G)和(S, G)), 以便可以將硬體快捷方式程式設計到Netflow和/或FIB表中。某些情況下仍需要此非RPF流量, 且MSFC CPU (在進程級別) 需要PIM斷言機制。否則, 軟體快速交換路徑就會捨棄該軟體 (假設在RPF介面上未停用軟體快速交換)。

在某些拓撲中, 使用冗餘的Catalyst 6500可能無法有效處理非RPF流量。對於非RPF流量, 冗餘路由器中通常沒有(*,G)或(S, G)狀態, 因此無法建立硬體或軟體快捷方式來丟棄資料包。每個組播資料包必須由MSFC路由處理器單獨檢查, 這通常稱為CPU中斷流量。由於第3層硬體交換和連線同一組路由器的多個介面/VLAN, 到達冗餘MSFC的CPU的非RPF流量將被放大「N」倍於原始源速率 (其中「N」是路由器冗餘連線的LAN數量)。如果非RPF流量的速率超過系統的丟包容量, 則可能會導致CPU使用率高、緩衝區溢位和整體網路不穩定。

在Catalyst 6500中，有一個訪問清單引擎，允許以線速進行過濾。在特定情況下，此功能可用於有效處理稀疏模式組的非RPF流量。您只能在稀疏模式「末節網路」中使用基於ACL的方法，其中沒有下游組播路由器（和相應的接收器）。此外，由於Catalyst 6500的資料包轉發設計，內部冗餘MSFC無法使用此實施。思科錯誤ID [CSCdr74908](#)(僅限註冊客戶)中概述了此操作。對於密集模式組，必須在路由器上看到非RPF資料包，PIM斷言機制才能正常工作。不同的解決方案，如基於CEF或Netflow的速率限制和QoS，用於控制密集模式網路和稀疏模式傳輸網路中的RPF故障。

在Catalyst 6500上有一個存取清單引擎，允許以線速進行過濾。此功能可用於有效處理稀疏模式組的非RPF流量。為了實施此解決方案，請在「末節網路」的傳入介面上放置訪問清單，以過濾不來自「末節網路」的多播流量。存取清單會向下推播到交換器中的硬體。此訪問清單可防止CPU看到資料包，並允許硬體丟棄非RPF流量。

注意：不要將此訪問清單放在傳輸介面上。它僅適用於末節網路（僅包含主機的網路）。

請參閱以下文件以瞭解更多資訊：

- [末節網路中IP組播的冗餘路由器問題](#)
- [非RPF流量處理](#)

show命令

發出show命令時，CPU使用率一律接近100%。發出show命令時，CPU使用率通常較高，且通常僅保留幾秒鐘。

例如，當您發出show tech-support命令時，虛擬Exec進程進入高位是正常的，因為此輸出是中斷驅動的輸出。您唯一關心的是show命令以外的其他進程的CPU使用率是否高。

[show cef not-cef-switched](#) 命令會顯示為什麼將封包傳送到MSFC（接收、ip選項、無鄰接等）以及有多少封包。例如：

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

show ibc和show ibc brief命令顯示CPU隊列，可在監視CPU狀態時使用。

執行過程

Cisco IOS軟體中的Exec進程負責路由器的TTY線路（控制檯、輔助、非同步）上的通訊。虛擬Exec進程負責VTY線路（Telnet會話）。Exec和虛擬Exec進程是中等優先順序進程，因此，如果有其他進程具有更高的優先順序（高或關鍵），則高優先順序進程將獲得CPU資源。

如果通過這些會話傳輸了大量資料，則Exec進程的CPU利用率會增加。這是因為當路由器希望透過這些線路傳送簡單字元時，路由器會使用一些CPU資源：

- 對於控制檯(Exec)，路由器每個字元使用一個中斷。
- 對於VTY線路（虛擬Exec），Telnet會話必須為每個字元構建一個TCP資料包。

以下清單詳細列出了Exec進程中CPU使用率較高的一些可能原因：

- 通過控制檯埠傳送的資料過多。使用[show debugging](#) 指令檢查路由器上是否已啟動任何偵錯。使用[logging console](#) 命令的no形式在路由器上禁用控制檯日誌記錄。驗證控制檯上是否顯示較長的輸出。例如，[show tech-support](#)或[show memory](#)命令。
- [exec](#)命令用於非同步線路和輔助線路。如果線路只有傳出流量，請禁用此線路的Exec進程。這是因為如果連線到此線路的裝置（例如數據機）傳送一些未經請求的資料，則執行過程將在此線路上啟動。如果路由器用作終端伺服器（用於反向Telnet到其它裝置控制檯），則建議您在連線到其它裝置控制檯的線路上配置no [exec](#)命令。從控制檯返回的資料可能會啟動使用CPU資源的Exec進程。

虛擬Exec進程中的CPU使用率較高的一個可能原因是：

- 通過Telnet會話傳送的資料過多。在虛擬Exec進程中，CPU使用率較高的最常見原因是從路由器傳輸到Telnet會話的資料過多。從Telnet會話執行輸出較長的命令(例如[show tech-support](#)、[show memory](#)等)時，可能會發生這種情況。通過[show tcp vty <line number>](#) 命令可以驗證每個VTY會話傳輸的資料量。

[L3老化過程](#)

當L3老化進程使用NetFlow資料匯出(NDE)匯出大量ifindex值時，CPU使用率可能會達到100%。

如果遇到此問題，請檢查以下兩個命令是否已啟用：

```
set mls nde destination-ifindex enable
```

```
set mls nde source-ifindex enable
```

如果啟用這些命令，進程必須使用NDE匯出所有目標和源ifindex值。第3層老化進程利用率很高，因為它必須對所有目標和源ifindex值執行FIB查詢。因此，表變滿，第3層老化進程變高，CPU使用率達到了100%。

為了解決此問題，請停用以下命令：

```
set mls nde destination-ifindex disable
```

```
set mls nde source-ifindex disable
```

使用以下命令驗證值：

- [show mls cef summary](#)
- [show mls cef maximum-routes](#)

[BPDU風暴](#)

生成樹在冗餘交換網路和網橋網路中維護無環路的第2層環境。如果沒有STP，幀將無限循環和/或倍增。此事件會導致網路崩潰，因為高流量會中斷廣播域中的所有裝置。

在某些方面，STP是最初為基於軟體的緩慢網橋規範(IEEE 802.1D)開發的早期協定，但是STP可能很複雜，以便在具有以下功能的大型交換網路中成功實施：

- 許多VLAN
- STP域中的許多交換機

- 多供應商支援
- 較新的IEEE增強功能

如果網路面臨頻繁的跨距樹狀目錄計算，或者交換機必須處理更多的BPDU，則可能導致高CPU以及BPDU丟棄。

要解決這些問題，請執行以下任意或所有步驟：

1. 從交換機修剪VLAN。
2. 使用STP的增強版本，例如MST。
3. 升級交換機的硬體。

另請參閱在網路中實作生成樹通訊協定的最佳實踐。

- [運行CatOS配置和管理的Catalyst 4500/4000、5500/5000和6500/6000系列交換機的最佳實踐](#)
- [運行Cisco IOS軟體的Catalyst 6500/6000系列和Catalyst 4500/4000系列交換機的最佳實踐](#)

[SPAN作業階段](#)

根據Catalyst 6000/6500系列交換器的架構，SPAN作業階段不會影響交換器的效能，但如果SPAN作業階段包含高流量/上行鏈路連線埠或EtherChannel，則可能會增加處理器上的負載。如果隨後它找出特定VLAN，則會進一步增加工作負載。如果鏈路上有不良流量，可能會進一步增加工作負載。

在某些情況下，RSPAN功能可能會導致回圈，且處理器上的負載會激增。如需詳細資訊，請參閱[SPAN作業階段為什麼會建立橋接回圈？](#)

交換機可以像往常一樣傳遞流量，因為所有流量都在硬體中，但是CPU在嘗試確定要傳送的流量時可能會受到衝擊。建議僅在需要時才配置SPAN會話。

[%CFIB-SP-STBY-7-CFIB_EXCEPTION :FIB TCAM異常，某些條目將被軟體交換](#)

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

超過TCAM中的可用空間量時，會收到此錯誤消息。這會導致CPU使用率高。這是FIB TCAM的限制。TCAM滿後，將設定標誌並接收FIB TCAM異常。這將阻止向TCAM新增新路由。因此，一切都將進行軟體切換。刪除路由無助於恢復硬體交換。TCAM進入異常狀態後，必須重新載入系統才能退出該狀態。`mls cef maximum-routes`命令可增加TCAM中可安裝的最大路由。

[使用高CPU的Catalyst 6500/6000具有使用L4埠的IPv6 ACL](#)

啟用[mls ipv6 acl壓縮地址單播](#)。如果IPv6 ACL與L4協定埠號匹配，則需要使用此命令。如果未啟用此命令，IPv6流量將被傳送到CPU進行軟體處理。預設情況下未配置此命令。

[銅纜SPF](#)

在Cisco ME 6500系列乙太網交換機中，銅纜SFP比其他型別的SFP需要更多的韌體互動，這提高了CPU利用率。

Cisco IOS SXH版本中改進了管理銅纜SFP的軟體演算法。

模組化IOS

在執行模組化IOS軟體的Cisco Catalyst 6500系列交換器中，一般CPU使用率略高於非模組化IOS軟體。

模組化IOS軟體為每個活動支付的價格高於每個資料包支付的價格。即使沒有太多資料包，模組化IOS軟體也會消耗某些CPU來維護進程，因此CPU消耗不基於實際流量。但是，當資料包處理速度較快時，模組化IOS軟體所消耗的CPU不應超過非模組化IOS軟體所消耗的CPU。

檢查CPU利用率

如果CPU使用率高，請首先發出**show processes cpu**命令。輸出會顯示交換機上的CPU使用率以及每個進程的CPU消耗量。

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

在此輸出中，總CPU使用率為57%，中斷CPU使用率為48%。此處，這些百分比以粗體文本顯示。CPU對流量的中斷交換會導致中斷CPU利用率。命令輸出列出導致兩種使用率之間差異的進程。在這種情況下，原因就是SNMP程式。

在執行CatOS的Supervisor引擎上，輸出如下所示：

```
Switch> (enable) show processes cpu

CPU utilization for five seconds: 99.72%
                             one minute: 100.00%
                             five minutes: 100.00%

PID Runtime(ms) Invoked    uSecs   5Sec   1Min   5Min   TTY Process
-----
1 0 0 0 0.28% 0.00% 0.00% -2 Kernel and Idle
2 2 261 1000 0.00% 0.00% 0.00% -2 Flash MIB Updat
3 0 1 0 0.00% 0.00% 0.00% -2 L2L3IntHdlr
4 0 1 0 0.00% 0.00% 0.00% -2 L2L3PatchRev
!--- Output is suppressed. 61 727295 172025 18000 0.82% 0.00% 0.00% -2 SptTimer 62 18185410
3712736 106000 22.22% 21.84% 21.96% -2 SptBpduRx
63 845683 91691 105000 0.92% 0.00% 0.00% -2 SptBpduTx
```

在此輸出中，第一個進程是Kernel and Idle，它顯示空閒CPU利用率。此進程通常較高，除非其他某些進程佔用CPU週期。在本示例中，SptBpduRx進程導致CPU使用率高。

如果其中某個進程導致的CPU使用率高，您可以進行故障排除並確定此進程運行高的原因。但是，如果CPU因流量被傳送到CPU而變高，則需要確定資料流被傳送的原因。此決定可以幫助您識別流量。

要進行故障排除，請使用以下EEM指令碼示例收集交換機在遇到高CPU利用率時的輸出：

```
event manager applet cpu_stats

event snmp oid "1.3.6.1.4.1.9.9.109.1.1.1.3.1" get-type exact entry-op gt entry-val "70"

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

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

action 1.02 cli command "enable"

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

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

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

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

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

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

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

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

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

注意：debug netdr capture rx命令在CPU因資料包而不是硬體的進程交換而處於高位時非常有用。當命令運行時，它會捕獲傳入到CPU的4096個資料包。該命令完全安全，是處理6500上高CPU問題的最便捷工具。不會給CPU造成額外負荷。

[用於確定傳送到CPU的流量的實用程式和工具](#)

本節介紹一些可幫助您檢視此流量的實用程式和工具。

[Cisco IOS® 系統軟體](#)

在Cisco IOS軟體中，Supervisor引擎上的交換機處理器稱為SP，MSFC稱為RP。

show interface命令會提供有關介面狀態和介面流量速率的基本資訊。該命令還提供錯誤計數器。

```
Router#show interface gigabitethernet 4/1
GigabitEthernet4/1 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 000a.42d1.7580 (bia 000a.42d1.7580)
  Internet address is 100.100.100.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  Clock mode is auto
```

```

ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 5/75/1/24075 (size/max/drops/flushes); Total output drops: 2
Queueing strategy: fifo
Output queue: 0/40 (size/max)
30 second input rate 7609000 bits/sec, 14859 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
L2 Switched: ucast: 0 pkt, 184954624 bytes - mcast: 1 pkt, 500 bytes
L3 in Switched: ucast: 2889916 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
2982871 packets input, 190904816 bytes, 0 no buffer
Received 9 broadcasts, 0 runts, 0 giants, 0 throttles
1 input errors, 1 CRC, 0 frame, 28 overrun, 0 ignored
0 input packets with dribble condition detected
1256 packets output, 124317 bytes, 0 underruns
2 output errors, 1 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

```

在此輸出中，您可以看到傳入流量是第3層交換流量，而不是第2層交換流量。這表示流量被傳送到CPU。

show processes cpu命令會告訴您這些資料包是常規流量資料包還是控制資料包。

```

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

```

如果封包是程式交換的，會看到IP Input程式執行率高。核發此命令，以便看到以下封包：

[show buffers input-interface](#)

```

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

Buffer information for Small buffer at 0x437874D4
  data_area 0x8060F04, refcount 1, next 0x5006D400, flags 0x280
  linktype 7 (IP), enctype 1 (ARPA), encsize 14, rxtype 1
  if_input 0x505BC20C (GigabitEthernet4/1), if_output 0x0 (None)
  inputtime 00:00:00.000 (elapsed never)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x8060F7A, datagramsize 60, maximum size 308
  mac_start 0x8060F7A, addr_start 0x8060F7A, info_start 0x0
  network_start 0x8060F88, transport_start 0x8060F9C, caller_pc 0x403519B4

source: 100.100.100.1, destination: 100.100.100.2, id: 0x0000, ttl: 63,
TOS: 0 prot: 17, source port 63, destination port 63

```

```

08060F70:                000A 42D17580                ..BQu.
08060F80: 00000000 11110800 4500002E 00000000  ....E.....
08060F90: 3F11EAF3 64646401 64646402 003F003F  ?.jsddd.ddd..??
08060FA0: 001A261F 00010203 04050607 08090A0B  ..&.....
08060FB0: 0C0D0E0F 101164                .....d

```

如果流量是中斷交換，則無法使用**show buffers input-interface**命令檢視這些封包。若要檢視傳送到RP以進行中斷交換的封包，可以對RP連線埠執行交換連線埠分析器(SPAN)擷取。

註：有關中斷交換與進程交換CPU使用率的詳細資訊，請參閱以下文檔：

- Cisco路由器上高CPU使用率故障排除的 [「由於中斷導致高CPU使用率」部分](#)

[SPAN RP帶內和SP帶內](#)

Cisco IOS軟體版本12.1(19)E和更新版本提供適用於Cisco IOS軟體中RP或SP連線埠的SPAN。

以下是命令語法：

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

對Cisco IOS軟體12.2 SX版本使用以下語法：

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

註：對於SXH版本，必須使用**monitor session**命令來配置本地SPAN會話，然後使用此命令將SPAN會話與CPU相關聯：

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

注意：如需這些命令的詳細資訊，請參閱Catalyst 6500版本12.2SX軟體設定指南中的[設定本地SPAN \(SPAN設定模式\)](#)。

以下是RP控制檯上的示例：

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

現在，轉到SP控制檯。以下是範例：

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

注意：在Cisco IOS 12.2 SX版本中，該命令已更改為測試**monitor add 1 rp-inband rx**。

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

```
Ingress Source Ports: 3/3 15/1
Egress Source Ports: 3/3
Ingress Source Vlans: <empty>
Egress Source Vlans: <empty>
Filter Vlans: <empty>
Destination Ports: 3/2
```

注意：在Cisco IOS 12.2 SX版本中，該命令已更改為測試監控器show 1。

以下是SP控制檯上的示例：

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

[CatOS 系統軟體](#)

對於執行CatOS系統軟體的交換器，Supervisor engine執行CatOS，MSFC執行Cisco IOS軟體。

如果您發出show mac命令，就可以看到傳送到MSFC的幀數。埠15/1是到MSFC的Supervisor引擎連線。

註：插槽2中管理引擎的埠為16/1。

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

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

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

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

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

此數字快速增加表示資料包被傳送到MSFC，這會導致CPU使用率高。然後您可以透過以下方式檢視封包：

- [SPAN MSFC連線埠15/1或16/1](#)
- [SPAN sc0](#)

[SPAN MSFC連線埠15/1或16/1](#)

建立來源為MSFC連線埠15/1（或16/1），且目的地為乙太網路連線埠的SPAN作業階段。

以下是範例：

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

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

如果您在連線埠5/10上收集監聽器追蹤軌跡，則監聽器追蹤軌跡會顯示傳輸至MSFC或從MSFC傳輸的資料包。將SPAN作業階段設定為tx，以擷取僅目的地為MSFC、而不是來源於MSFC的封包。

[SPAN sc0](#)

建立以sc0介面為來源的SPAN作業階段，以便擷取前往Supervisor Engine CPU的訊框。

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

注意：對於光纖服務模組(OSM)，無法執行流量的SPAN擷取。

[建議](#)

Supervisor引擎CPU利用率並不反映交換機的硬體轉發效能。但是，您必須確定基準並監控Supervisor引擎的CPU利用率。

1. 在具有正常流量模式和負載的穩態網路中，為交換機設定基準Supervisor引擎CPU利用率。請注意哪些進程生成最高的CPU利用率。
2. 排除CPU使用率故障時，請考慮以下問題：哪些流程產生的利用率最高？這些流程與您的基準是否不同？CPU使用率是否一直高於基準？或者是否存在出現高使用率峰值，然後返回基準水準的情況？網路中是否存在拓撲更改通知(TCN)?**註：**因為STP PortFast禁用而擺動埠或主機埠會導致TCN。管理子網/VLAN中是否有過多的廣播或組播流量？交換機上是否有過多的管理流量，例如SNMP輪詢？
3. 在CPU使用時間較長期間（CPU使用率等於或大於75%時），收集以下命令的輸出：[show clock](#)顯示版本[show processes cpu sorted](#)[show proc cpu history](#)顯示日誌
4. 如有可能，將管理VLAN與具有使用者資料流量（尤其是繁重的廣播流量）的VLAN隔離。此類流量的示例包括IPX RIP/服務廣告協定(SAP)、AppleTalk和其他廣播流量。此類流量可能會影響Supervisor引擎CPU利用率，而且在極端情況下可能會干擾交換機的正常操作。
5. 如果CPU因向RP傳送流量而運行較高，請確定該流量是什麼，以及流量被傳送的原因。為了做出判斷，請使用[Utilities and Tools to Determine The Traffic That Punted to the CPU](#)（用於確定CPU流量的實用程式和工具）一節介紹的實用程式。

[相關資訊](#)

- [用於排除使用Sup720的Catalyst 6500上的高CPU故障的有用命令](#)
- [Catalyst 6000/6500系列交換器上的常見CatOS錯誤訊息](#)
- [執行Cisco IOS軟體的Catalyst 6500/6000系列交換器上的常見錯誤訊息](#)
- [疑難排解有關執行Cisco IOS系統軟體的Catalyst 6500/6000系列交換器上的硬體和常見問題](#)
- [交換式園區網中的單點傳播泛濫](#)
- [Cisco Catalyst 6500系列交換器產品支援](#)
- [用於在間歇性高CPU問題期間收集資料的EEM指令碼](#)
- [LAN 產品支援](#)
- [LAN 交換技術支援](#)
- [技術支援與文件 - Cisco Systems](#)