Catalyst 6500/6000-Switch Hohe CPU-Auslastung

Inhalt

Einführung

In diesem Dokument werden die Ursachen für die hohe CPU-Auslastung bei Cisco Catalyst Switches der Serien 6500 und 6000 und Virtual Switching System (VSS) 1440 beschrieben. Wie bei Cisco Routern verwenden Switches den Befehl **show process cpu**, um die CPU-Auslastung für den Switch Supervisor Engine-Prozessor anzuzeigen. Aufgrund der Unterschiede in der Architektur und den Weiterleitungsmechanismen zwischen Cisco Routern und Switches unterscheidet sich die typische Ausgabe des Befehls **show process cpu** erheblich. Die Bedeutung der Ausgabe unterscheidet sich ebenfalls. In diesem Dokument werden diese Unterschiede erläutert und die CPU-Auslastung auf den Switches sowie die Interpretation der Befehlsausgabe **show process cpu** beschrieben.

Hinweis: In diesem Dokument beziehen sich die Wörter "Switch" und "Switches" auf Catalyst 6500/6000-Switches.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Software- und Hardwareversionen für Systeme mit Catalyst 6500/6000-Switches und Virtual Switching System (VSS) 1440.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hinweis: Die unterstützte Software für Virtual Switching System (VSS) 1440-basierte Systeme ist Cisco IOS® Softwareversion 12.2(33)SXH1 oder höher.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Unterschied zwischen CatOS- und Cisco IOS-Systemsoftware

Catalyst OS (CatOS) auf der Supervisor Engine und Cisco IOS® Software auf der Multilayer Switch Feature Card (MSFC) (Hybrid): Sie können ein CatOS-Image als Systemsoftware verwenden, um die Supervisor Engine auf Catalyst 6500/6000-Switches auszuführen. Wenn die optionale MSFC installiert ist, wird für die Ausführung der MSFC ein separates Cisco IOS Software-Image verwendet.

Cisco IOS Software auf der Supervisor Engine und MSFC (nativ): Sie können ein einzelnes Cisco IOS Software-Image als Systemsoftware verwenden, um sowohl die Supervisor Engine als auch MSFC auf Catalyst 6500/6000-Switches auszuführen.

Hinweis: Weitere Informationen finden Sie im Vergleich der Betriebssysteme Cisco Catalyst und Cisco IOS für den Cisco Catalyst Switch der Serie 6500.

CPU-Auslastung bei Catalyst 6500/6000-Switches

Softwarebasierte Router von Cisco verwenden Software, um Pakete zu verarbeiten und weiterzuleiten. Die CPU-Auslastung auf einem Cisco Router steigt tendenziell, da der Router mehr Paketverarbeitung und Routing durchführt. Der Befehl **show process cpu** kann daher eine ziemlich genaue Angabe der Datenverkehrsverarbeitungslast auf dem Router bereitstellen.

Catalyst Switches der Serien 6500/6000 verwenden die CPU nicht auf dieselbe Weise. Diese Switches treffen Weiterleitungsentscheidungen in der Hardware, nicht in der Software. Wenn die Switches daher für die meisten Frames, die den Switch passieren, die Weiterleitungs- oder Switching-Entscheidung treffen, wird die Supervisor Engine-CPU nicht in den Prozess einbezogen.

Auf Catalyst Switches der Serien 6500/6000 sind zwei CPUs vorhanden. Eine CPU ist die Supervisor Engine-CPU, die als Network Management Processor (NMP) oder Switch Processor (SP) bezeichnet wird. Die andere CPU ist die Layer-3-Routing-Engine-CPU, die als MSFC oder Route Processor (RP) bezeichnet wird.

Die SP-CPU führt Funktionen aus, darunter:

- Unterstützung beim Lernen und Altern von MAC-Adressen**Hinweis:** MAC-Adresslernen wird auch als Pfad-Setup bezeichnet.
- Führt Protokolle und Prozesse aus, die Netzwerkkontrolle ermöglichenBeispiele hierfür sind Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP) und Port Aggregation Protocol (PAgP).
- Verarbeitung des Netzwerkmanagementdatenverkehrs, der für die CPU des Switches bestimmt istBeispiele sind Telnet-, HTTP- und SNMP-Verkehr (Simple Network Management Protocol).

Die RP-CPU führt Funktionen aus, darunter:

- Erstellung und Aktualisierung der Tabellen für Layer 3-Routing und ARP (Address Resolution Protocol)
- Generiert die Cisco Express Forwarding (CEF) Forwarding Information Base (FIB) und Adjacency-Tabellen und lädt die Tabellen in die Policy Feature Card (PFC) herunter
- Verarbeitung des Netzwerkmanagement-Datenverkehrs, der für den RP bestimmt istBeispiele sind Telnet-, HTTP- und SNMP-Datenverkehr.

Situationen und Funktionen, die Datenverkehr zu Software auslösen

Pakete, die für den Switch bestimmt sind

Jedes Paket, das für den Switch bestimmt ist, geht an die Software. Zu diesen Paketen gehören:

- KontrollpaketeSteuerungspakete werden für STP, CDP, VTP, Hot Standby Router Protocol (HSRP), PAgP, Link Aggregation Control Protocol (LACP) und UniDirectional Link Detection (UDLD) empfangen.
- Routing-Protokoll-UpdatesBeispiele für diese Protokolle sind Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP) und Open Shortest Path First Protocol (OSPF Protocol).
- SNMP-Datenverkehr, der für den Switch bestimmt ist
- Telnet- und Secure Shell Protocol (SSH)-Datenverkehr zum Switch.Eine hohe CPU-Auslastung aufgrund von SSH wird wie folgt angesehen:

```
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
```

  Integrieren Sie diese Befehle in das EEM-Skript, um die Anzahl der SSH-Sitzungen zu überprüfen, die bei hoher CPU-Belastung eingerichtet wurden:Benutzer anzeigenSchaulinie
- ARP-Antworten auf ARP-Anfragen

Pakete und Bedingungen, die eine Sonderverarbeitung erfordern

Diese Liste enthält spezifische Pakettypen und -bedingungen, die die Verarbeitung von Paketen in der Software erzwingen:

- Pakete mit IP-Optionen, TTL-Kapselung (abgelaufene Lebensdauer) oder ARPA-Kapselung (nicht Advanced Research Projects Agency)
- Pakete mit spezieller Handhabung, z. B. Tunneling
- IP-Fragmentierung
- Pakete, die ICMP-Meldungen (Internet Control Message Protocol) vom RP oder SP erfordern
- Maximum Transmission Unit (MTU)-Prüffehler
- Pakete mit IP-Fehlern, darunter IP-Prüfsummen- und Längenfehler
- Wenn die Eingabepakete einen Bitfehler (z. B. den Single-Bit-Fehler (SBE)) zurückgeben, werden die Pakete zur Softwareverarbeitung an die CPU gesendet und korrigiert. Das System weist ihnen einen Puffer zu und korrigiert diesen mithilfe der CPU-Ressource.
- Wenn sich PBR und reflexive Zugriffslisten im Pfad eines Datenverkehrsflusses befinden, wird das Paket per Software-Switching weitergeleitet, was einen zusätzlichen CPU-Zyklus erfordert.
- Adjacency-Schnittstelle
- Pakete, die die RPF-Prüfung (Reverse Path Forwarding) nicht bestehen - **RPF-Fehler**
- Genießen/EmpfangenGlean bezieht sich auf Pakete, die eine ARP-Auflösung erfordern, und

der Empfang bezieht sich auf Pakete, die im Empfangsfall auftreten.
- Internetwork Packet Exchange (IPX)-Datenverkehr, der in Cisco IOS Software und CatOS auf der Supervisor Engine 720 softwarebasiert istDer IPX-Datenverkehr wird auch über die Supervisor Engine 2/Cisco IOS-Software softwaregeschaltet, der Datenverkehr wird jedoch hardwaregestützt auf die Supervisor Engine 2/CatOS geschaltet. Der IPX-Datenverkehr ist auf der Supervisor Engine 1A für beide Betriebssysteme hardwaregestützt.
- AppleTalk-Datenverkehr
- Vollständige Hardware-RessourcenZu diesen Ressourcen gehören FIB, Content-Addressable Memory (CAM) und ternary CAM (TCAM).

ACL-basierte Funktionen

- Von der Zugriffskontrollliste (ACL) abgelehnter Datenverkehr bei aktivierter ICMP-Funktion "Unreachables"**Hinweis:** Dies ist die Standardeinstellung.Einige Pakete, die von der ACL abgelehnt wurden, werden an die MSFC weitergeleitet, wenn IP-Unreachables aktiviert sind. Pakete, die ICMP-Unreachables erfordern, werden mit einer vom Benutzer konfigurierbaren Geschwindigkeit durchgesickert. Standardmäßig beträgt die Rate 500 Pakete pro Sekunde (pps).
- IPX-Filterung auf Grundlage nicht unterstützter Parameter, z. B. Quell-HostAuf der Supervisor Engine 720 ist der Prozess des Layer-3-IPX-Datenverkehrs immer softwarebasiert.
- Zugriffskontrolleinträge (ACEs), die protokolliert werden müssen, mit dem **log-**SchlüsselwortDies gilt für ACL-Protokollfunktionen und VACL-Protokollfunktionen (VLAN ACL). ACEs in derselben ACL, die keine Protokollierung erfordern, werden in der Hardware trotzdem verarbeitet. Die Supervisor Engine 720 mit PFC3 unterstützt die Ratenbeschränkung von Paketen, die für die ACL- und VACL-Protokollierung an die MSFC umgeleitet werden. Die Supervisor Engine 2 unterstützt die Ratenbeschränkung von Paketen, die zur VACL-Protokollierung an die MSFC umgeleitet werden. Die Unterstützung für die ACL-Protokollierung auf der Supervisor Engine 2 ist für die Zweigstelle Cisco IOS Software Release 12.2S vorgesehen.
- Richtlinienweitergeleiteter Datenverkehr mit Verwendung von **Übereinstimmungslänge**, **festgelegter IP-Rangfolge** oder anderen nicht unterstützten ParameternDer **set interface** Parameter unterstützt Software. Der **set interface null 0**-Parameter ist jedoch eine Ausnahme. Dieser Datenverkehr wird in der Hardware der Supervisor Engine 2 mit PFC2 und der Supervisor Engine 720 mit PFC3 verarbeitet.
- ACLs (RACLs) für Nicht-IP- und Nicht-IPX-RouterNicht-IP-RACLs gelten für alle Supervisor Engines. Die Nicht-IPX-RACLs gelten nur für die Supervisor Engine 1a mit PFC und die Supervisor Engine 2 nur mit PFC2.
- Broadcast-Datenverkehr, der in einem RACL abgelehnt wird
- Datenverkehr, der in einer Unicast-RPF-Prüfung (uRPF) abgelehnt wird, ACL ACEDiese uRPF-Prüfung gilt für die Supervisor Engine 2 mit PFC2 und die Supervisor Engine 720 mit PFC3.
- AuthentifizierungsproxyDer Datenverkehr, der einem Authentifizierungsproxy unterliegt, kann auf der Supervisor Engine 720 auf Ratenlimitierung beschränkt werden.
- Cisco IOS Software IP Security (IPsec)Datenverkehr, der der Cisco IOS-Verschlüsselung unterliegt, kann auf der Supervisor Engine 720 auf Ratenlimitierung beschränkt werden.

NetFlow-basierte Funktionen

Die in diesem Abschnitt beschriebenen NetFlow-basierten Funktionen gelten nur für die Supervisor Engine 2 und die Supervisor Engine 720.

- NetFlow-basierte Funktionen müssen immer das erste Paket eines Softwareflusses anzeigen. Sobald das erste Paket des Datenflusses die Software erreicht hat, werden nachfolgende Pakete für denselben Fluss hardwarevermittelt.Diese Ablaufregelung gilt für reflexive ACLs, Web Cache Communication Protocol (WCCP) und Cisco IOS Server Load Balancing (SLB).**Hinweis:** Auf der Supervisor Engine 1 erstellen reflexive ACLs dynamische TCAM-Einträge, um Hardware-Verknüpfungen für einen bestimmten Datenstrom zu erstellen. Das Prinzip ist dasselbe: das erste Paket eines Datenflusses geht an die Software. Nachfolgende Pakete für diesen Datenfluss sind hardwarebasiert.
- Mit der TCP-Intercept-Funktion werden der Drei-Wege-Handshake und Session Close in der Software behandelt. Der restliche Datenverkehr wird über Hardware abgewickelt.**Hinweis:** Synchronisieren (SYN), SYN-Bestätigung (SYN ACK) und ACK-Pakete umfassen den Drei-Wege-Handshake. Die Sitzung wird mit Finish (FIN) oder Reset (RST) geschlossen.
- Bei Network Address Translation (NAT) wird der Datenverkehr wie folgt behandelt:Auf der Supervisor Engine 720:Datenverkehr, der NAT erfordert, wird nach der Erstübersetzung in der Hardware abgewickelt. Die Übersetzung des ersten Pakets eines Datenflusses erfolgt in der Software, und nachfolgende Pakete für diesen Datenfluss sind hardwarebasiert. Bei TCP-Paketen wird in der NetFlow-Tabelle eine Hardware-Verknüpfung erstellt, nachdem der Drei-Wege-TCP-Handshake abgeschlossen ist.Supervisor Engine 2 und Supervisor Engine 1:Der gesamte Datenverkehr, der NAT erfordert, ist softwarebasiert.
- Die kontextbasierte Zugriffskontrolle (Context-Based Access Control, CBAC) verwendet NetFlow-Verknüpfungen, um den zu überprüfenden Datenverkehr zu klassifizieren. Anschließend sendet CBAC nur diesen Datenverkehr an die Software. CBAC ist eine rein softwarebasierte Funktion. Datenverkehr, der einer Überprüfung unterzogen wird, ist nicht hardwaregestützt.**Hinweis:** Der Datenverkehr, der einer Überprüfung unterzogen wird, kann auf der Supervisor Engine 720 auf Ratenlimitierung beschränkt werden.

Multicast-Datenverkehr

- Protocol Independent Multicast (PIM)-Snooping
- Internet Group Management Protocol (IGMP)-Snooping (TTL = 1)Dieser Datenverkehr ist tatsächlich für den Router bestimmt.
- Multicast Listener Discovery (MLD)-Snooping (TTL = 1)Dieser Datenverkehr ist tatsächlich für den Router bestimmt.
- FIB-Fehler
- Multicast-Pakete für die Registrierung mit direkter Verbindung zur Multicast-QuelleDiese Multicast-Pakete werden bis zum Rendezvous-Punkt getunnelt.
- IP-Version 6 (IPv6) Multicast

Weitere Funktionen

- Network-Based Application Recognition (NBAR)
- ARP-Inspektion, nur mit CatOS
- Port-Sicherheit, nur mit CatOS
- DHCP-Snooping

IPv6-Situationen

- Pakete mit einem Hop-by-Hop-Optionsheader
- Pakete mit derselben IPv6-Zieladresse wie Router
- Pakete, die die Durchsetzungsprüfung nicht bestehen
- Pakete, die die MTU der Ausgangsverbindung überschreiten
- Pakete mit einer TTL kleiner oder gleich 1
- Pakete mit einem Eingabe-VLAN, das dem Output-VLAN entspricht
- IPv6 uRPFDie Software führt diesen uRPF für alle Pakete aus.
- IPv6-reflexive ZugriffskontrolllistenDiese reflexiven Zugriffskontrolllisten werden von der Software verwaltet.
- 6to4-Präfixe für IPv6-ISATAP-Tunnel (Intra-Site Automatic Tunnel Addressing Protocol)Diese Tunneling-Funktion wird von Software übernommen. Der gesamte andere Datenverkehr, der in einen ISATAP-Tunnel gelangt, ist hardwarebasiert.

LCP-Schema und DFC-Modul

Bei einer Distributed Forwarding Card (DFC) ist der Prozess `lcp planular`, der auf einer hohen CPU ausgeführt wird, kein Problem und stellt keine betrieblichen Probleme dar. Das LCP-Modul ist Teil des Firmware-Codes. Auf allen Modulen, die keine DFC-Verbindung erfordern, wird die Firmware auf einem bestimmten Prozessor ausgeführt, der als Line Card Processor (LCP) bezeichnet wird. Dieser Prozessor wird zur Programmierung der ASIC-Hardware und für die Kommunikation mit dem zentralen Supervisor-Modul verwendet.

Wenn die `lcp planular` initiiert wird, nutzt sie die gesamte verfügbare Verarbeitungszeit. Wenn ein neuer Prozess jedoch Prozessorzeit benötigt, `gibt lcp planular` Prozesszeit für den neuen Prozess frei. Diese hohe CPU-Auslastung beeinträchtigt die Leistung des Systems nicht. Der Prozess erfasst einfach alle ungenutzten CPU-Zyklen, solange kein Prozess mit höherer Priorität dies erfordert.

```
DFC#show process cpu

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

Häufige Ursachen und Lösungen für Probleme mit hoher CPU-Auslastung

IP nicht erreichbar

Wenn eine Zugriffsgruppe ein Paket verweigert, sendet die MSFC nicht erreichbare ICMP-Nachrichten. Diese Aktion tritt standardmäßig auf.

Mit der Standardaktivierung des Befehls **ip unreachables** verwirft die Supervisor Engine den Großteil der abgelehnten Pakete in der Hardware. Anschließend sendet die Supervisor Engine nur eine kleine Anzahl von Paketen, maximal 10 pps, zur Weiterleitung an die MSFC. Diese Aktion generiert nicht erreichbare ICMP-Meldungen.

Das Verwerfen von abgelehnten Paketen und die Generierung von nicht erreichbaren ICMP-Nachrichten stellen eine Belastung für die MSFC-CPU dar. Um die Auslastung zu vermeiden, können Sie den Schnittstellenkonfigurationsbefehl **no ip unreachables** ausführen. Mit diesem Befehl werden ICMP-nicht erreichbare Nachrichten deaktiviert, wodurch die Hardware aller Pakete, die aus Zugriffsgruppen abgelehnt wurden, verworfen werden kann.

Nicht erreichbare ICMP-Nachrichten werden nicht gesendet, wenn eine VACL ein Paket ablehnt.

NAT-Übersetzungen

NAT verwendet sowohl Hardware- als auch Software-Weiterleitung. Die Ersteinrichtung der NAT-Übersetzungen muss in der Software erfolgen und die Weiterleitung erfolgt mit der Hardware. NAT verwendet auch die NetFlow-Tabelle (max. 128 KB). Wenn die NetFlow-Tabelle voll ist, wird der Switch daher auch die NAT-Weiterleitung per Software anwenden. Dies geschieht normalerweise bei hohen Datenverkehrsspitzen und führt zu einem Anstieg der CPU auf 6500.

Verwendung des CEF FIB-Tabellenbereichs in der Flow Cache-Tabelle

Die Supervisor Engine 1 verfügt über eine Flow Cache-Tabelle, die 128.000 Einträge unterstützt. Aufgrund der Effizienz des Hashing-Algorithmus liegen diese Einträge jedoch zwischen 32.000 und 120.000. Auf der Supervisor Engine 2 wird die FIB-Tabelle generiert und in die PFC programmiert. Die Tabelle enthält bis zu 256.000 Einträge. Die Supervisor Engine 720 mit PFC3-BXL unterstützt bis zu 1.000.000 Einträge. Sobald dieser Speicherplatz überschritten wird, werden die Pakete in der Software geswitcht. Dies kann zu einer hohen CPU-Auslastung auf dem RP führen. Verwenden Sie folgende Befehle, um die Anzahl der Routen in der CEF FIB-Tabelle zu überprüfen:

```
Router#show processes cpu
CPU utilization for five seconds:  99.26%
                     one minute: 100.00%
                    five minutes: 100.00%

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

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

```
IOS% show ip cef summary
IP Distributed CEF with switching (Table Version 86771423), flags=0x0
  112564 routes, 1 reresolve, 0 unresolved (0 old, 0 new)
  112567 leaves, 6888 nodes, 21156688 bytes, 86771426
inserts, 86658859
invalidations
  295 load sharing elements, 96760 bytes, 112359 references
  universal per-destination load sharing algorithm, id 8ADDA64A
  2 CEF resets, 2306608 revisions of existing leaves
  refcounts:  1981829 leaf, 1763584 node
!--- You see these messages if the TCAM space is exceeded: %MLSCEF-SP-7-FIB_EXCEPTION: FIB TCAM
exception, Some entries will be software switched %MLSCEF-SP-7-END_FIB_EXCEPTION: FIB TCAM
exception cleared, all CEF entries will be hardware switched
```

Auf der Supervisor Engine 2 wird die Anzahl der FIB-Einträge auf die Hälfte reduziert, wenn Sie die RPF-Prüfung für die Schnittstellen konfiguriert haben. Diese Konfiguration kann zum Software-Switch von mehr Paketen und damit zu einer hohen CPU-Auslastung führen.

Um das Problem der hohen CPU-Auslastung zu beheben, aktivieren Sie die Routenzusammenfassung. Die Routenzusammenfassung kann die Latenz in einem komplexen Netzwerk minimieren, indem die Prozessor-Workloads, die Arbeitsspeicheranforderungen und der Bandbreitenbedarf reduziert werden.

Weitere Informationen zur Verwendung und Optimierung von TCAM finden Sie unter Understanding ACL on Catalyst Switches der Serie 6500.

Optimierte ACL-Protokollierung

Optimized ACL Logging (OAL) bietet Hardwareunterstützung für die ACL-Protokollierung. Wenn Sie OAL nicht konfigurieren, erfolgt der Prozess der Pakete, die eine Protokollierung erfordern, vollständig in der Software auf der MSFC3. OAL erlaubt oder verwirft Hardwarepakete auf dem PFC3. OAL verwendet eine optimierte Routine zum Senden von Informationen an MSFC3, um die Protokollierungsmeldungen zu generieren.

Hinweis: Informationen zu OAL finden Sie im Abschnitt *Optimized ACL Logging with a PFC3* of Understanding Cisco IOS ACL Support.

Übertragungsratenlimit für Pakete an die CPU

Auf der Supervisor Engine 720 können Durchsatzratenlimitierungen die Geschwindigkeit steuern, mit der Pakete an die Software gesendet werden können. Diese Ratenkontrolle trägt dazu bei, Denial-of-Service-Angriffe zu verhindern. Sie können auch einige dieser Ratenlimitierungen auf der Supervisor Engine 2 verwenden:

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

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

Hier ein Beispiel:

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

Führen Sie den folgenden Befehl aus, um alle CEF-getesteten Pakete auf die MSFC zu begrenzen:

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

Führen Sie den folgenden Befehl aus, um die Anzahl der Pakete zu reduzieren, die aufgrund von TTL=1 an die CPU gesendet werden:

```
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.
```

Dies ist z. B. die Ausgabe der **Netzwerkerfassung**, die anzeigt, dass die IPv4-TTL 1 ist:

```
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
```

Hohe CPU kann auch durch Pakete mit TTL=1 verursacht werden, die an die CPU übertragen werden. Um die Anzahl der Pakete zu begrenzen, die an die CPU übertragen werden, konfigurieren Sie einen Hardware-Ratenlimitierer. Durchsatzbegrenzer können Pakete begrenzen, die vom Hardwaredatenpfad bis zum Softwaredatenpfad durchgesickert werden. Durchsatzbegrenzer schützen den Softwaresteuerungspfad vor Überlastungen, indem sie den Datenverkehr, der die konfigurierte Rate überschreitet, verwerfen. Die Ratenbeschränkung wird mithilfe des Befehls **mls rate-limit all ttl failure** konfiguriert.

Physische Verschmelzung von VLANs aufgrund falscher Verkabelung

Eine hohe CPU-Auslastung kann auch durch das Zusammenführen von zwei oder mehr VLANs aufgrund einer unsachgemäßen Verkabelung entstehen. Wenn STP auf den Ports deaktiviert ist, an denen die VLAN-Fusion stattfindet, kann es auch zu einer hohen CPU-Auslastung kommen.

Um dieses Problem zu beheben, identifizieren Sie die Verkabelungsfehler und korrigieren Sie sie. Wenn Ihre Anforderung es zulässt, können Sie STP auch auf diesen Ports aktivieren.

Broadcast-Sturm

Ein LAN-Broadcast-Sturm tritt auf, wenn Broadcast- oder Multicast-Pakete das LAN überfluten. Dies führt zu einem übermäßigen Datenverkehr und beeinträchtigt die Netzwerkleistung. Fehler in der Protokoll-Stack-Implementierung oder in der Netzwerkkonfiguration können einen Broadcast-Sturm verursachen.

Aufgrund des architekturbasierten Designs der Catalyst 6500-Plattform werden die Broadcast-Pakete nur auf Softwareebene und immer verworfen.

Die Unterdrückung von Broadcast verhindert die Unterbrechung von LAN-Schnittstellen durch einen Broadcast-Sturm. Bei der Broadcast-Unterdrückung wird eine Filterung verwendet, die die Broadcast-Aktivität in einem LAN über einen Zeitraum von 1 Sekunde misst und den Messwert mit einem vordefinierten Grenzwert vergleicht. Wenn der Schwellenwert erreicht ist, werden während eines bestimmten Zeitraums weitere Broadcast-Aktivitäten unterdrückt. Die Broadcast-Unterdrückung ist standardmäßig deaktiviert.

Hinweis: Durch Broadcast-Stürme verursachte VRRP-Flapping von Backup zu Master kann eine hohe CPU-Auslastung verursachen.

Um zu verstehen, wie die Broadcast-Unterdrückung funktioniert und um die Funktion zu aktivieren, lesen Sie folgende Informationen:

- Konfigurieren der Broadcast-Unterdrückung (Cisco IOS-Systemsoftware)
- Konfigurieren der Broadcast-Unterdrückung (CatOS-Systemsoftware)

BGP Next-Hop Address Tracking (BGP-Scanner-Prozess)

Der BGP Scanner-Prozess durchläuft die BGP-Tabelle und bestätigt die Erreichbarkeit der nächsten Hops. Bei diesem Prozess wird auch bedingtes Advertisement überprüft, um festzustellen, ob das BGP Bedingungspräfixe ankündigen und/oder ein Routen-Dampening durchführen soll. Der Prozess scannt standardmäßig alle 60 Sekunden.

Aufgrund des BGP-Scannerprozesses auf einem Router, der eine große Internet-Routing-Tabelle enthält, ist eine hohe CPU-Auslastung für kurze Zeiträume zu erwarten. Einmal pro Minute durchsucht der BGP Scanner die Tabelle der BGP Routing Information Base (RIB) und führt wichtige Wartungsaufgaben durch. Zu diesen Aufgaben gehören:

- Eine Überprüfung des nächsten Hop, auf den in der Router-BGP-Tabelle verwiesen wird
- Überprüfen, ob die Next-Hop-Geräte erreichbar sind

Daher benötigt eine große BGP-Tabelle eine entsprechend große Zeitspanne, um ausgeführt und validiert zu werden. Der BGP-Scanner-Prozess leitet die BGP-Tabelle, um Datenstrukturen zu aktualisieren, und leitet die Routing-Tabelle zu Weiterleitungszwecken. Beide Tabellen werden separat im Router-Speicher gespeichert. Beide Tabellen können sehr groß sein und daher CPU-Zyklen verbrauchen.

Weitere Informationen zur CPU-Auslastung durch den BGP Scanner-Prozess finden Sie im Abschnitt *BGP Scanner* für *hohe CPU* unter Fehlerbehebung bei hoher CPU, verursacht durch BGP Scanner- oder BGP Router-Prozess.

Weitere Informationen zur Funktion "BGP Next-Hop Address Tracking" und zum Aktivieren/Deaktivieren oder Anpassen des Abtastintervalls finden Sie unter BGP Support für Next-Hop Address Tracking.

Nicht-RPF-Multicast-Datenverkehr

Multicast-Routing (im Gegensatz zu Unicast-Routing) bezieht sich nur auf die Quelle eines bestimmten Multicast-Datenstreams. Das heißt, die IP-Adresse des Geräts, das den Multicast-Datenverkehr generiert. Das Grundprinzip ist, dass das Quellgerät den Stream an eine undefinierte Anzahl von Empfängern (innerhalb der Multicast-Gruppe) "aussendet". Alle Multicast-Router erstellen Distribution Trees, die den Pfad des Multicast-Datenverkehrs durch das Netzwerk steuern, um den Datenverkehr an alle Empfänger weiterzuleiten. Die beiden grundlegenden Typen von Multicast Distribution Trees sind Quellbäume und Shared Trees. RPF ist ein Schlüsselkonzept für die Multicast-Weiterleitung. Router können Multicast-Datenverkehr korrekt über den Distribution Tree weiterleiten. RPF verwendet die vorhandene Unicast-Routing-Tabelle, um die Upstream- und Downstream-Nachbarn zu ermitteln. Ein Router leitet ein Multicast-Paket nur weiter, wenn es auf der Upstream-Schnittstelle empfangen wird. Diese RPF-Prüfung gewährleistet, dass der Distribution Tree schleifenfrei ist.

Der Multicast-Datenverkehr ist für jeden Router in einem überbrückten (Layer-2-) LAN gemäß der CSMA/CD-Spezifikation von IEEE 802.3 immer sichtbar. Im 802.3-Standard wird Bit 0 des ersten Oktetts verwendet, um einen Broadcast- und/oder Multicast-Frame anzugeben, und jeder Layer-2-Frame mit dieser Adresse wird überflutet. Dies ist auch der Fall, wenn CGMP- oder IGMP-Snooping konfiguriert sind. Dies liegt daran, dass Multicast-Router den Multicast-Datenverkehr sehen müssen, wenn sie eine richtige Weiterleitungsentscheidung treffen sollen. Wenn mehrere Multicast-Router über Schnittstellen zu einem gemeinsamen LAN verfügen, leitet nur ein Router die Daten weiter (ausgewählt durch einen Auswahlprozess). Aufgrund der Flutungsart von LANs empfängt der redundante Router (Router, der den Multicast-Datenverkehr nicht weiterleitet) diese

Daten an der ausgehenden Schnittstelle für dieses LAN. Der redundante Router verwirft diesen Datenverkehr normalerweise, da er an der falschen Schnittstelle angekommen ist und daher die RPF-Prüfung nicht bestanden hat. Dieser Datenverkehr, der die RPF-Prüfung nicht besteht, wird als Nicht-RPF-Datenverkehr oder RPF-Fehlerpakete bezeichnet, da sie gegen den Fluss von der Quelle rückwärts übertragen wurden.

Der Catalyst 6500 mit installierter MSFC kann als vollwertiger Multicast-Router konfiguriert werden. Unter Verwendung von Multicast Multi-Layer Switching (MMLS) wird der RPF-Datenverkehr in der Regel von der Hardware innerhalb des Switches weitergeleitet. Die ASICs erhalten Informationen aus dem Multicast-Routing-Status (z. B. (*,G) und (S,G)), sodass eine Hardware-Verknüpfung in die NetFlow- und/oder FIB-Tabelle programmiert werden kann. Dieser Nicht-RPF-Datenverkehr ist in einigen Fällen weiterhin erforderlich und wird von der MSFC-CPU (auf Prozessebene) für den PIM Assert-Mechanismus benötigt. Andernfalls wird es über den Fast-Switching-Pfad der Software verworfen (es wird davon ausgegangen, dass das schnelle Switching der Software auf der RPF-Schnittstelle nicht deaktiviert ist).

Der Catalyst 6500, der Redundanz verwendet, kann in bestimmten Topologien nicht-RPF-Datenverkehr effizient verarbeiten. Für Nicht-RPF-Datenverkehr gibt es im redundanten Router in der Regel keinen (*,G)- oder (S,G)-Status. Aus diesem Grund können keine Hardware- oder Software-Verknüpfungen erstellt werden, um das Paket zu verwerfen. Jedes Multicast-Paket muss vom MSFC-Routingprozessor einzeln geprüft werden. Dies wird häufig als CPU-Interrupt-Datenverkehr bezeichnet. Bei Layer-3-Hardware-Switching und mehreren Schnittstellen/VLANs, die denselben Routersatz verbinden, wird der Nicht-RPF-Datenverkehr, der auf die CPU der redundanten MSFC trifft, "N" größer als die ursprüngliche Quellrate (wobei "N" die Anzahl der LANs ist, mit denen der Router redundant verbunden ist). Wenn die Rate des Nicht-RPF-Datenverkehrs die Paketverwerfungskapazität des Systems übersteigt, kann dies zu einer hohen CPU-Auslastung, Pufferüberläufen und Instabilität des gesamten Netzwerks führen.

Beim Catalyst 6500 gibt es eine Zugriffslisten-Engine, die eine Filterung mit Leitungsgeschwindigkeit ermöglicht. Mit dieser Funktion kann in bestimmten Situationen nicht RPF-basierter Datenverkehr für Sparse-Mode-Gruppen effizient verarbeitet werden. Sie können die ACL-basierte Methode nur in Sparse-Mode-"Stub-Netzwerken" verwenden, in denen es keine Downstream-Multicast-Router (und zugehörigen Empfänger) gibt. Aufgrund des Paketweiterleitungsdesigns des Catalyst 6500 können intern redundante MSFCs diese Implementierung nicht verwenden. Dies ist in der Cisco Bug-ID CSCdr74908 beschrieben (nur registrierte Kunden). Bei Gruppen im Dense-Mode-Modus müssen Nicht-RPF-Pakete auf dem Router sichtbar sein, damit der PIM Assert-Mechanismus ordnungsgemäß funktioniert. Verschiedene Lösungen wie CEF oder NetFlow-basierte Ratenbegrenzung und QoS werden zur Steuerung von RPF-Ausfällen in Netzwerken mit Dense-Mode und Sparse-Mode-Transit verwendet.

Auf dem Catalyst 6500 gibt es eine Zugriffslisten-Engine, die eine Filterung mit Leitungsgeschwindigkeit ermöglicht. Diese Funktion kann verwendet werden, um Nicht-RPF-Datenverkehr für Sparse-Mode-Gruppen effizient zu behandeln. Um diese Lösung zu implementieren, legen Sie eine Zugriffsliste auf die eingehende Schnittstelle des 'Stub-Netzwerks', um Multicast-Datenverkehr zu filtern, der nicht vom 'Stub-Netzwerk' stammt. Die Zugriffsliste wird auf die Hardware im Switch heruntergefahren. Diese Zugriffsliste verhindert, dass die CPU das Paket sieht, und ermöglicht der Hardware, den Nicht-RPF-Datenverkehr zu verwerfen.

Hinweis: Platzieren Sie diese Zugriffsliste nicht auf einer Transit-Schnittstelle. Sie ist nur für Stub-Netzwerke (nur Netzwerke mit Hosts) bestimmt.

Weitere Informationen finden Sie in diesen Dokumenten:

- Probleme mit redundanten Routern bei IP-Multicast in Stub-Netzwerken
- Verarbeitung von Nicht-RPF-Datenverkehr

Befehle anzeigen

Die CPU-Auslastung bei Ausgabe des Befehls **show** beträgt immer fast 100 %. Eine hohe CPU-Auslastung ist bei Ausgabe eines **show-**Befehls normal und bleibt normalerweise nur wenige Sekunden.

Beispielsweise ist es normal, dass der Virtual Exec-Prozess bei der Ausgabe eines **show tech-support-**Befehls hoch wird, da diese Ausgabe eine Interrupt-gesteuerte Ausgabe ist. Es ist Ihre einzige Sorge, dass eine hohe CPU in anderen Prozessen als **show**-Befehlen vorhanden ist.

Der **Befehl** show cef not-cef-switching zeigt, warum Pakete an die MSFC (Receive, ip option, no adjacency, usw.) weitergeleitet werden und wie viele. Beispiel:

```
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
```

Die Befehle **show ibc** und **show ibc brief** zeigen die CPU-Warteschlange an und können verwendet werden, wenn Sie den CPU-Status überwachen.

EXEC-Prozesse

Der Exec-Prozess in der Cisco IOS-Software ist für die Kommunikation auf den TTY-Leitungen (Konsole, Hilfsmittel, asynchron) des Routers verantwortlich. Der Virtual Exec-Prozess ist für die VTY-Leitungen (Telnet-Sitzungen) verantwortlich. Die Exec- und Virtual Exec-Prozesse sind Prozesse mit mittlerer Priorität. Wenn es also andere Prozesse mit höherer Priorität (hoch oder kritisch) gibt, erhalten die Prozesse mit höherer Priorität die CPU-Ressourcen.

Wenn viele Daten durch diese Sitzungen übertragen werden, nimmt die CPU-Auslastung für den Exec-Prozess zu. Wenn der Router ein einfaches Zeichen durch diese Leitungen senden möchte, verwendet der Router einige CPU-Ressourcen:

- Für die Konsole (Exec) verwendet der Router einen Interrupt pro Zeichen.
- Für die VTY-Leitung (Virtual Exec) muss die Telnet-Sitzung ein TCP-Paket pro Zeichen erstellen.

In dieser Liste sind einige mögliche Gründe für eine hohe CPU-Auslastung im Exec-Prozess aufgeführt:

- **Es werden zu viele Daten über den Konsolenport gesendet.**Überprüfen Sie, ob auf dem Router mit dem **Befehl** show debugging (Debuggen **anzeigen)** Debug gestartet wurde.Deaktivieren Sie die Konsolenprotokollierung auf dem Router mit dem **Befehl no** form des Protokollierungskonsolen-**Befehls.**Überprüfen Sie, ob eine lange Ausgabe auf der Konsole ausgegeben wird. Beispielsweise ein Befehl show tech-support oder ein Befehl show memory.

- **Der Befehl exec wird für asynchrone und Hilfslinien konfiguriert.**Wenn eine Leitung nur ausgehenden Datenverkehr hat, deaktivieren Sie den Exec-Prozess für diese Leitung. Dies liegt daran, dass der Exec-Prozess in dieser Zeile gestartet wird, wenn das an diese Leitung angeschlossene Gerät (z. B. ein Modem) unaufgeforderte Daten sendet.Wenn der Router als Terminalserver (für Reverse-Telnet-Verbindungen zu anderen Gerätekonsolen) verwendet wird, wird empfohlen, den Befehl **no exec** auf den mit der Konsole der anderen Geräte verbundenen Leitungen zu konfigurieren. Daten, die von der Konsole zurückgegeben werden, können ansonsten einen Exec-Prozess starten, der CPU-Ressourcen verwendet.

Ein möglicher Grund für eine hohe CPU-Auslastung im Virtual Exec-Prozess ist:

- **Bei den Telnet-Sitzungen werden zu viele Daten gesendet.**Der häufigste Grund für eine hohe CPU-Auslastung im Virtual Exec-Prozess ist, dass zu viele Daten vom Router an die Telnet-Sitzung übertragen werden. Dies kann passieren, wenn Befehle mit langen Ausgaben wie **show tech-support**, **show memory** usw. von der Telnet-Sitzung aus ausgeführt werden. Die Datenmenge, die über jede VTY-Sitzung übertragen wird, kann mithilfe des Befehls **show tcp vty *<line number>*** überprüft werden.

L3-Alterungsprozess

Wenn der L3-Alterungsprozess eine große Anzahl von *Ifindex*-Werten mithilfe von NetFlow Data Export (NDE) exportiert, kann die CPU-Auslastung 100 % erreichen.

Wenn dieses Problem auftritt, prüfen Sie, ob diese beiden Befehle aktiviert sind:

```
set mls nde destination-ifindex enable

set mls nde source-ifindex enable
```

Wenn Sie diese Befehle aktivieren, muss der Prozess alle Ziel- und Quell-Ifindex-Werte mithilfe von NDE exportieren. Die Auslastung des L3-Alterungsprozesses ist hoch, da er FIB-Suchvorgänge für alle Ziel- und Quell-*Ifindex*-Werte durchführen muss. Daher ist die Tabelle voll, der L3-Alterungsprozess hoch und die CPU-Auslastung erreicht 100 %.

Um dieses Problem zu beheben, deaktivieren Sie die folgenden Befehle:

```
set mls nde destination-ifindex disable

set mls nde source-ifindex disable
```

Verwenden Sie diese Befehle, um die Werte zu überprüfen:

- show mls cezusammenfassung
- show mls cef maximum routen

BPDU-Sturm

Spanning Tree erhält eine schleifenfreie Layer-2-Umgebung in redundanten Switching- und Bridges-Netzwerken aufrecht. Ohne STP werden Frames auf unbestimmte Zeit schleifen und/oder multipliziert. Dieses Vorkommen verursacht einen Zusammenbruch des Netzwerks, da der hohe Datenverkehr alle Geräte in der Broadcast-Domäne unterbricht.

In mancher Hinsicht ist STP ein früheres Protokoll, das ursprünglich für langsame, softwarebasierte Bridge-Spezifikationen (IEEE 802.1D) entwickelt wurde. STP kann jedoch kompliziert sein, um es erfolgreich in großen Switch-Netzwerken mit folgenden Funktionen zu implementieren:

- Viele VLANs
- Viele Switches in einer STP-Domäne
- Unterstützung mehrerer Anbieter
- Neuere IEEE-Erweiterungen

Wenn das Netzwerk häufig Spanning Tree-Berechnungen durchlaufen muss oder der Switch mehr BPDUs verarbeiten muss, kann dies zu einer hohen CPU-Belastung und zu BPDU-Verlusten führen.

Um diese Probleme zu umgehen, gehen Sie wie folgt vor:

1. Entfernen Sie die VLANs von den Switches.
2. Verwenden Sie eine erweiterte Version von STP, z. B. MST.
3. Aktualisieren Sie die Hardware des Switches.

Weitere Informationen finden Sie unter Best Practices zur Implementierung des Spanning Tree Protocol im Netzwerk.

- Best Practices für Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000 mit CatOS-Konfiguration und -Verwaltung
- Best Practices für Catalyst Switches der Serien 6500/6000 und 4500/4000 mit Cisco IOS Software

SPAN-Sitzungen

Auf der Grundlage der Architektur von Catalyst Switches der Serien 6000 und 6500 wirken sich SPAN-Sitzungen nicht auf die Switch-Leistung aus. Wenn die SPAN-Sitzung jedoch einen Hochdatenverkehr/Uplink-Port oder einen EtherChannel umfasst, kann dies die Prozessorbelastung erhöhen. Wenn dann ein bestimmtes VLAN einzeln erkannt wird, erhöht sich die Workload sogar noch mehr. Wenn die Verbindung schädlichen Datenverkehr enthält, kann dies die Workload weiter erhöhen.

In einigen Szenarien kann die RSPAN-Funktion Schleifen verursachen, und die Last auf dem Prozessor wird hochgefahren. Weitere Informationen finden Sie unter Warum erstellt die SPAN-Sitzung eine Bridging-Schleife?

Der Switch kann den Datenverkehr wie gewohnt weiterleiten, da alles in der Hardware gespeichert ist. Die CPU kann jedoch einen Schläger durchführen, wenn sie versucht herauszufinden, welcher Datenverkehr durchgestellt werden soll. Es wird empfohlen, SPAN-Sitzungen nur dann zu konfigurieren, wenn dies erforderlich ist.

%CFIB-SP-STBY-7-CFIB_EXCEPTION: FIB TCAM-Ausnahme, einige Einträge werden durch Software-Switching ersetzt

```
%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
```

Diese Fehlermeldung wird angezeigt, wenn der verfügbare Speicherplatz im TCAM überschritten wird. Dies führt zu einer hohen CPU. Dies ist eine FIB-TCAM-Einschränkung. Wenn der TCAM vollständig ist, wird ein Flag festgelegt und die FIB-TCAM-Ausnahme empfangen. Dadurch wird verhindert, dass dem TCAM neue Routen hinzugefügt werden. Aus diesem Grund wird alles durch Software-Switching gesteuert. Das Entfernen von Routen hilft nicht, das Hardware-Switching wieder aufzunehmen. Sobald der TCAM in den Ausnahmezustand wechselt, muss das System neu geladen werden, um diesen Status zu verlassen. Die maximale Anzahl von Routen, die in TCAM installiert werden können, wird durch den Befehl **mls cef maximum-routen** erhöht.

Der Catalyst 6500/600 mit hoher CPU verfügt über eine IPv6-ACL mit L4-Ports.

Aktivieren Sie **mls ipv6 acl compress address unicast**. Dieser Befehl wird benötigt, wenn die IPv6-ACL mit den L4-Protokoll-Portnummern übereinstimmt. Wenn dieser Befehl nicht aktiviert ist, wird der IPv6-Datenverkehr zur Softwareverarbeitung an die CPU geleitet. Dieser Befehl ist nicht standardmäßig konfiguriert.

SPFs für Kupfer

Bei Cisco ME-Ethernet-Switches der Serie 6500 erfordern die Kupfer-SFPs eine stärkere Firmware-Interaktion als andere SFP-Typen, wodurch die CPU-Auslastung erhöht wird.

Die Software-Algorithmen für die Verwaltung von Kupfer-SFPs wurden in den Cisco IOS SXH-Versionen verbessert.

Modulares IOS

Bei Cisco Catalyst Switches der Serie 6500 mit modularer IOS-Software ist die normale CPU-Auslastung etwas größer als die nicht modulare IOS-Software.

Die modulare IOS-Software zahlt pro Aktivität einen höheren Preis als der Preis pro Paket. Die modulare IOS-Software verwaltet die Prozesse, indem sie eine bestimmte CPU belegt, selbst wenn nur wenige Pakete vorhanden sind. Die CPU-Nutzung basiert daher nicht auf dem tatsächlichen Datenverkehr. Wenn Pakete jedoch mit hoher Geschwindigkeit verarbeitet werden, sollte die in der modularen IOS-Software verwendete CPU nicht größer sein als die in der nicht modularen IOS-Software.

CPU-Auslastung prüfen

Wenn die CPU-Auslastung hoch ist, führen Sie den Befehl **show process cpu** zuerst aus. Die Ausgabe zeigt die CPU-Auslastung auf dem Switch sowie den CPU-Verbrauch für jeden Prozess an.

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

```
 174          68       463        146  0.00%  0.00%  0.00%   0 RPC pm-mp
!--- Output is suppressed.
```

In dieser Ausgabe beträgt die CPU-Auslastung insgesamt 57 Prozent, die CPU-Auslastung für Interrupt 48 Prozent. Diese Prozentsätze werden hier als Fettschrift angezeigt. Der Interrupt-Switch des Datenverkehrs durch die CPU verursacht die CPU-Auslastung. Die Befehlsausgabe listet die Prozesse auf, die den Unterschied zwischen den beiden Dienstprogrammen verursachen. In diesem Fall ist der SNMP-Prozess die Ursache.

Auf der Supervisor Engine, die CatOS ausführt, sieht die Ausgabe wie folgt aus:

```
Switch> (enable) show processes cpu


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

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

In dieser Ausgabe ist der erste Prozess `Kernel und Idle`, der die CPU-Auslastung im Leerlauf anzeigt. Dieser Prozess ist normalerweise hoch, es sei denn, einige andere Prozesse verbrauchen CPU-Zyklen. In diesem Beispiel verursacht der `SptBpduRx`-Prozess eine hohe CPU-Auslastung.

Wenn die CPU-Auslastung aufgrund eines dieser Prozesse hoch ist, können Sie eine Fehlerbehebung durchführen und feststellen, warum dieser Prozess hoch ausgeführt wird. Wenn die CPU jedoch aufgrund von Datenverkehr, der an die CPU geleitet wird, hoch ist, müssen Sie ermitteln, warum der Datenverkehr gestohlen wird. Diese Feststellung hilft Ihnen dabei, den Datenverkehr zu identifizieren.

Verwenden Sie zur Fehlerbehebung dieses EEM-Skriptbeispiel, um die Ausgabe des Switches bei hoher CPU-Auslastung zu erfassen:

```
event manager applet cpu_stats

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

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

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

action 1.02 cli command "enable"

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

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

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

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

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

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

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

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

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

Hinweis: Der Befehl **debug netdr capture rx** ist hilfreich, wenn die CPU aufgrund des Prozesswechsels von Paketen statt der Hardware hoch ist. Es erfasst 4096 Pakete, die bei Ausführung des Befehls an die CPU eingehen. Der Befehl ist absolut sicher und das praktischste Werkzeug für hohe CPU-Probleme auf dem 6500. Sie verursacht keine zusätzliche Last für die CPU.

Dienstprogramme und Tools zur Bestimmung des an die CPU gesendeten Datenverkehrs

In diesem Abschnitt werden einige Dienstprogramme und Tools beschrieben, die Ihnen bei der Überprüfung dieses Datenverkehrs helfen können.

Cisco IOS-Systemsoftware

In der Cisco IOS-Software wird der Switch-Prozessor der Supervisor Engine als SP und die MSFC als RP bezeichnet.

Der Befehl **show interface** enthält grundlegende Informationen zum Zustand der Schnittstelle und zur Datenverkehrsrate auf der Schnittstelle. Der Befehl stellt auch Fehlerzähler bereit.

```
Router#show interface gigabitethernet 4/1
GigabitEthernet4/1 is up, line protocol is up (connected)
  Hardware is C6k 1000Mb 802.3, address is 000a.42d1.7580 (bia 000a.42d1.7580)
  Internet address is 100.100.100.2/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  Clock mode is auto
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 5/75/1/24075 (size/max/drops/flushes); Total output drops: 2
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 7609000 bits/sec, 14859 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  L2 Switched: ucast: 0 pkt, 184954624 bytes - mcast: 1 pkt, 500 bytes
  L3 in Switched: ucast: 2889916 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast
  L3 out Switched: ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes
     2982871 packets input, 190904816 bytes, 0 no buffer
     Received 9 broadcasts, 0 runts, 0 giants, 0 throttles
```

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

In dieser Ausgabe können Sie sehen, dass der eingehende Datenverkehr auf Layer 3-Switching statt auf Layer 2-Switched erfolgt. Dies zeigt an, dass der Datenverkehr an die CPU geleitet wird.

Der Befehl **show process cpu** gibt an, ob es sich bei diesen Paketen um reguläre Datenverkehrspakete oder Kontrollpakete handelt.

```
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
```

Wenn die Pakete prozessgesteuert sind, wird der `IP Input`-Prozess auf hohem Niveau ausgeführt. Geben Sie diesen Befehl ein, um die folgenden Pakete anzuzeigen:

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
```

Wenn der Datenverkehr **unterbrochen** wird, können diese Pakete nicht mit dem Befehl **show buffers input-interface** angezeigt werden. Um die Pakete anzuzeigen, die zum Interrupt Switching an den RP weitergeleitet werden, können Sie eine SPAN-Erfassung (Switched Port Analyzer) des RP-Ports durchführen.

Hinweis: Weitere Informationen zur CPU-Auslastung bei Interrupt-Switched und Prozessgesteuerten finden Sie in diesem Dokument:

- *Hohe CPU-Auslastung aufgrund* von *Unterbrechungen* bei der Fehlerbehebung bei hoher CPU-Auslastung bei Cisco Routern

SPAN RP-Inband und SP-Inband

Ein SPAN für den RP- oder SP-Port der Cisco IOS Software ist ab der Cisco IOS Software-Version 12.1(19)E verfügbar.

Dies ist die Befehlssyntax:

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

Verwenden Sie diese Syntax für die Cisco IOS Software 12.2 SX-Versionen:

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

Hinweis: Für die SXH-Version müssen Sie zur Konfiguration einer lokalen SPAN-Sitzung den Befehl **überwachungssitzung** verwenden und dann mit diesem Befehl die SPAN-Sitzung der CPU zuordnen:

```
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]
```

Hinweis: Weitere Informationen zu diesen Befehlen finden Sie unter Konfigurieren des lokalen SPAN-Konfigurationsmodus (SPAN Configuration Mode) im *Catalyst 6500 Release 12.2SX Software Configuration Guide*.

Hier ein Beispiel für eine RP-Konsole:

```
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
```

Wechseln Sie jetzt zur SP-Konsole. Hier ein Beispiel:

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

Hinweis: In Cisco IOS 12.2 SX-Versionen wurde der Befehl in **Test Monitor Add 1 rp-inband rx** geändert.

```
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
```

Hinweis: In Cisco IOS 12.2 SX-Versionen wurde der Befehl in **Testmonitor 1** geändert.

Hier ein Beispiel für eine SP-Konsole:

```
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-Systemsoftware

Bei Switches, auf denen CatOS-Systemsoftware ausgeführt wird, wird CatOS von der Supervisor Engine ausgeführt, und die MSFC führt die Cisco IOS Software aus.

Wenn Sie den Befehl **show mac** ausführen, wird die Anzahl der Frames angezeigt, die auf die MSFC gestrafft werden. Port 15/1 ist die Verbindung der Supervisor Engine zur MSFC.

Hinweis: Der Port ist 16/1 für Supervisor Engines in Steckplatz 2.

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

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

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

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

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

Eine schnelle Erhöhung dieser Anzahl weist darauf hin, dass Pakete an die MSFC gesendet werden, was eine hohe CPU-Auslastung verursacht. Sie können die Pakete dann auf folgende Weise betrachten:

- SPAN MSFC-Port 15/1 oder 16/1
- SPAN sc0

SPAN MSFC-Port 15/1 oder 16/1

Richten Sie eine SPAN-Sitzung ein, bei der die Quelle der MSFC-Port 15/1 (oder 16/1) und das

Ziel ein Ethernet-Port ist.

Hier ein Beispiel:

```
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
```

Wenn Sie eine Sniffer-Ablaufverfolgung auf Port 5/10 sammeln, zeigt die Sniffer-Ablaufverfolgung Pakete an, die an und von der MSFC übertragen werden. Konfigurieren Sie die SPAN-Sitzung als **tx**, um Pakete zu erfassen, die nur für die MSFC und nicht für die MSFC bestimmt sind.

SPAN sc0

Richten Sie eine SPAN-Sitzung mit der **sc0-**Schnittstelle als Quelle ein, um Frames zu erfassen, die zur Supervisor Engine-CPU gehen.

```
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
```

Hinweis: Bei optischen Dienstmodulen (OSMs) können Sie keine SPAN-Erfassung des Datenverkehrs durchführen.

Empfehlungen

Die CPU-Auslastung der Supervisor Engine spiegelt die Hardware-Weiterleitungsleistung des Switches nicht wider. Sie müssen jedoch die CPU-Auslastung der Supervisor Engine auswerten und überwachen.

1. Die CPU-Auslastung der Supervisor Engine für den Switch in einem stationären Netzwerk mit normalen Datenverkehrsmustern und normaler Auslastung wird als Basis dienen.Beachten Sie, welche Prozesse die höchste CPU-Auslastung generieren.
2. Berücksichtigen Sie bei der Fehlerbehebung für die CPU-Auslastung die folgenden Fragen:Welche Prozesse erzeugen die höchste Auslastung? Unterscheiden sich diese Prozesse von Ihrer Ausgangsbasis?Ist die CPU im Vergleich zur Baseline durchgängig erhöht? Oder gibt es Spitzen bei hoher Auslastung und dann eine Rückkehr zu den Ausgangswerten?Gibt es im Netzwerk Topologieänderungsbenachrichtigungen (TCNs)?**Hinweis:** Flapping-Ports oder Host-Ports mit deaktiviertem STP PortFast führen zu TCNs.Gibt es einen übermäßigen Broadcast- oder Multicast-Datenverkehr in den Management-Subnetzen/im VLAN?Gibt es auf dem Switch übermäßigen Verwaltungsdatenverkehr, z. B. SNMP Polling?

3. Erfassen Sie während der hohen CPU-Zeit (wenn die CPU 75 % oder höher beträgt) die Ausgabe dieser Befehle:SchauuhrAnzeigeversionshow prozesse cpu sortiertshow proc cpu historieAnzeigeprotokoll
4. Isolieren Sie das Management-VLAN möglichst von den VLANs mit Benutzerdatenverkehr, insbesondere mit starkem Broadcast-Datenverkehr.Beispiele für diese Art von Datenverkehr sind IPX RIP/Service Advertising Protocol (SAP), AppleTalk und anderer Broadcast-Datenverkehr. Dieser Datenverkehr kann die CPU-Auslastung der Supervisor Engine beeinträchtigen und in Extremfällen den normalen Betrieb des Switches beeinträchtigen.
5. Wenn die CPU aufgrund des Datenverkehrs zum RP hoch läuft, ermitteln Sie, was dieser Datenverkehr ist und warum der Datenverkehr gestohlen wird.Verwenden Sie für diese Bestimmung die Dienstprogramme und Tools, mit denen der an die CPU weitergeleitete Datenverkehr bestimmt wird.

Zugehörige Informationen

- Nützliche Befehle zur Fehlerbehebung bei hoher CPU auf Catalyst 6500-Geräten mit Sup720
- Häufige CatOS-Fehlermeldungen bei Catalyst Switches der Serien 6000 und 6500
- Häufige Fehlermeldungen bei Catalyst Switches der Serien 6500/6000 mit Cisco IOS Software
- Fehlerbehebung bei Hardware- und häufigen Problemen mit Catalyst Switches der Serien 6500/6000 mit Cisco IOS Systemsoftware
- Unicast Flooding in Switched Campus-Netzwerken
- Produktsupport für Cisco Catalyst Switches der Serie 6500
- EEM-Skript zum Erfassen von Daten während eines Intermittent High CPU-Problems
- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems