Hohe CPU-Auslastung bei Cisco IOS Software-basierten Catalyst Switches der Serie 4500

Inhalt

Einführung

Die Catalyst Switches der Serie 4500, zu denen die Catalyst Switches der Serie 4948 gehören, verfügen über ein ausgefeiltes Verfahren zur Paketverwaltung für CPU-gebundenen Datenverkehr. Ein häufig empfundenes Problem ist die hohe CPU-Auslastung dieser Switches. Dieses Dokument enthält Details zur CPU-Paketverwaltungsarchitektur und zeigt, wie Sie die Ursachen für die hohe CPU-Auslastung auf diesen Switches identifizieren können. Das Dokument enthält auch einige allgemeine Netzwerk- oder Konfigurationsszenarien, die eine hohe CPU-Auslastung bei der Catalyst Serie 4500 verursachen.

Hinweis: Wenn Sie Catalyst Switches der Serien 4500/4000 mit Catalyst OS (CatOS) ausführen, lesen Sie das Dokument CPU Utilization on Catalyst 4500/4000, 2948G, 2980G und 4912G Switches. die CatOS-Software ausführen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst Switches der Serie 4500
- Catalyst Switches der Serie 4948

Hinweis: Dieses Dokument gilt nur für Cisco IOS® Software-basierte Switches und nicht für CatOS-basierte Switches.

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.

Konventionen

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

Hintergrundinformationen

Bevor Sie sich die Architektur zur Verarbeitung von CPU-Paketen ansehen und eine Fehlerbehebung für eine hohe CPU-Auslastung durchführen, müssen Sie die verschiedenen Möglichkeiten verstehen, wie hardwarebasierte Weiterleitungs-Switches und Cisco IOS Software-basierte Router die CPU verwenden. Das allgemeine Missverständnis besteht darin, dass eine hohe CPU-Auslastung auf die Erschöpfung der Ressourcen auf einem Gerät und die Gefahr eines Absturzes hinweist. Ein Kapazitätsproblem ist eines der Symptome einer hohen CPU-Auslastung bei Cisco IOS-Routern. Ein Kapazitätsproblem ist jedoch fast nie ein Symptom einer hohen CPU-Auslastung bei hardwarebasierten Weiterleitungs-Switches wie dem Catalyst 4500. Der Catalyst 4500 ist für die Weiterleitung von Paketen in den ASIC (Hardware Application-Specific Integrated Circuit) und die Weiterleitung von Datenverkehr mit Geschwindigkeiten von bis zu 102 Millionen Paketen pro Sekunde (Mpps) konzipiert.

Die Catalyst 4500-CPU erfüllt folgende Funktionen:

- Verwaltung konfigurierter Softwareprotokolle, z. B.:Spanning Tree Protocol (STP)Routing-ProtokollCisco Discovery Protocol (CDP)Port Aggregation Protocol (PAgP)VLAN Trunk Protocol (VTP)Dynamic Trunking Protocol (DTP)
- Programme zur Konfiguration/zu dynamischen Einträgen in die Hardware-ASICs, z. B.:Zugriffskontrolllisten (ACLs)CEF-Einträge
- Interne Verwaltung verschiedener Komponenten, z. B.:Power over Ethernet (PoE) Line CardsNetzteileLüftereinschub

- Verwaltet den Zugriff auf den Switch, z. B.:TelnetKonsoleSimple Network Management Protocol (SNMP)
- Leitet Pakete über den Softwarepfad weiter, z. B.:Über Internetwork Packet Exchange (IPX) geroutete Pakete, die nur im Softwarepfad unterstützt werdenMTU-Fragmentierung (Maximum Transmission Unit)

Laut dieser Liste kann eine hohe CPU-Auslastung durch den Empfang oder die Verarbeitung von Paketen durch die CPU erzielt werden. Einige der Pakete, die für den Prozess gesendet werden, können für den Netzwerkbetrieb wichtig sein. Ein Beispiel für diese grundlegenden Pakete sind BPDUs (Bridge Protocol Data Unit) für Spanning-Tree-Topologiekonfigurationen. Bei anderen Paketen kann es sich jedoch um per Software weitergeleiteten Datenverkehr handeln. In diesen Szenarien müssen Switching-ASICs Pakete zur Verarbeitung an die CPU senden:

- Pakete, die in die CPU kopiert werden, aber die ursprünglichen Pakete in der Hardware gewechselt werdenEin Beispiel hierfür ist das Lernen von Host-MAC-Adressen.
- Pakete, die zur Verarbeitung an die CPU gesendet werdenBeispiele:Routing-Protokoll-UpdatesBPDUsEine beabsichtigte oder unbeabsichtigte Flut von Datenverkehr
- Pakete, die zur Weiterleitung an die CPU gesendet werdenEin Beispiel sind Pakete, die IPX- oder AppleTalk-Routing benötigen.

Kenntnis der Catalyst 4500 CPU-Paketverarbeitungsarchitektur

Der Catalyst 4500 verfügt über einen integrierten QoS-Mechanismus (Quality of Service), um zwischen Datenverkehrstypen zu unterscheiden, die für die CPU bestimmt sind. Der Mechanismus unterscheidet sich anhand der Paketinformationen auf Layer 2 (L2)/Layer 3 (L3)/Layer 4 (L4). Die Supervisor Packet Engine verfügt über 16 Warteschlangen, um verschiedene Arten von Paketen oder Ereignissen zu verarbeiten. Abbildung 1 zeigt diese Warteschlangen. In Tabelle 1 sind die Warteschlangen und die Pakettypen aufgeführt, die jeweils in eine Warteschlange gestellt werden. Die 16 Warteschlangen ermöglichen es dem Catalyst 4500, die Pakete je nach Pakettyp oder -priorität in eine Warteschlange zu stellen.

Abbildung 1: Catalyst 4500 verwendet mehrere CPU-Warteschlangen

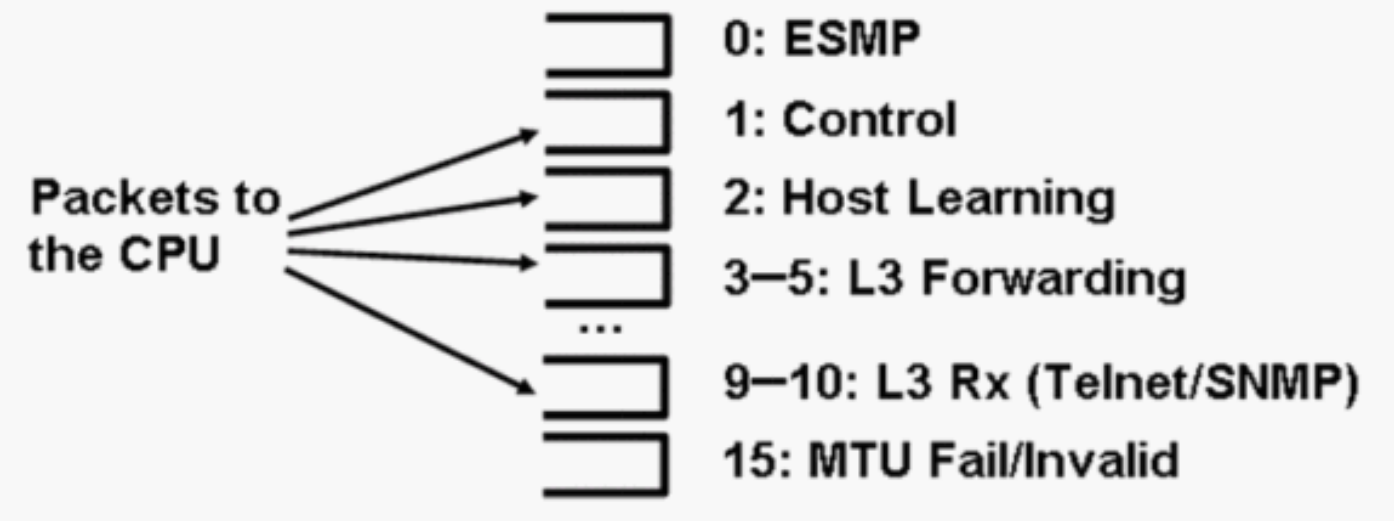


Tabelle 1: Beschreibung der Catalyst 4500-Warteschlange

Warteschlangennummer	Warteschlangenname	Pakete in Warteschlange
0	SMP	ESMP[1]-Pakete (interne

		Managementpakete) für die Linecard-ASICs oder andere Komponentenverwaltung
1	`Kontrolle`	L2-Kontrollebenen-Pakete, z. B. STP, CDP, PAgP, LACP[2] oder UDLD[3]
2	`Host-Learning`	Frames mit unbekannten Quell-MAC-Adressen, die in die CPU kopiert werden, um die L2-Weiterleitungstabelle zu erstellen
3, 4, 5	`L3 Fwd Highest`, `L3 Fwd Hoch/Mittel`, `L3 Fwd Low`	Pakete, die in Software weitergeleitet werden müssen, z. B. GRE[4]-Tunnel Wenn der ARP[5] für die Ziel-IP-Adresse nicht aufgelöst wird, werden Pakete an diese Warteschlange gesendet.
6, 7, 8	`L2 Fwd Highest`, `L2 Fwd Hoch/Mittel`, `L2 Fwd Low`	Pakete, die als Ergebnis von Bridging weitergeleitet werden • Protokolle, die in der Hardware nicht unterstützt werden, wie IPX und über AppleTalk geroutete Pakete, werden an die CPU überbrückt. • ARP-Anfrage und -Antwort • Pakete mit einer MAC-Zieladresse der Switch-SVI[6]/L3-Schnittstelle werden überbrückt, wenn die Pakete aus folgenden Gründen nicht in der Hardware geroutet werden können: IP-HeaderoptionenAbgelaufene TTL[7]Nicht-ARPA-Kapselung
9, 10	`L3 Rx High`, `L3 Rx Low`	L3-Kontrollebenen-Datenverkehr, z. B. Routing-Protokolle, der für CPU-IP-Adressen bestimmt ist Beispiele sind Telnet, SNMP und SSH[8].
11	`RPF-Fehler`	Multicast-Pakete, die die RPF[9]-Prüfung nicht

		bestanden haben
12	`ACL fwd (Snooping)`	Pakete, die mit DHCP[10] Snooping, dynamischer ARP-Inspektion oder IGMP[11]-Snooping verarbeitet werden
13	`ACL-Protokoll, unerreicht`	Pakete, die einen ACE[12] mit dem **log-**Schlüsselwort oder Paketen erreichen, die aufgrund einer Verweigerung in einer Output-ACL oder des Fehlens einer Route zum Ziel verworfen wurden. Diese Pakete erfordern die Generierung von nicht erreichbaren ICMP-Nachrichten.
14	`ACL-Sw-Verarbeitung`	Pakete, die aufgrund fehlender zusätzlicher ACL-Hardware-Ressourcen, wie TCAM[13], für Sicherheits-ACL auf die CPU gestraft werden
15	`MTU-Fehler/Ungültig`	Pakete, die fragmentiert werden müssen, da die MTU-Größe der Ausgangsschnittstelle kleiner als die Größe des Pakets ist

[1] ESMP = Sogar Simple Management Protocol

[2] LACP = Link Aggregation Control Protocol

[3] UDLD = UniDirectional Link Detection.

[4] GRE = Generic Routing Encapsulation.

[5] ARP = Address Resolution Protocol

[6] SVI = Switched Virtual Interface (Switched Virtual Interface)

[7] TTL = Time to Live.

[8] SSH = Secure Shell Protocol

[9] RPF = Reverse Path Forwarding

[10] DHCP = Dynamic Host Configuration Protocol

[11] IGMP = Internet Group Management Protocol

[12] ACE = Zugriffskontrolleintrag.

[13] TCAM = adressierbarer Speicher für ternäre Inhalte.

Diese Warteschlangen sind separate Warteschlangen:

- `L2 Fwd Höchste` oder `L3 Fwd Höchste`
- `L2 Fwd Hoch/Mittel` oder `L3 Fwd Hoch/Mittel`
- `L2 Fwd Low` oder `L3 Fwd Low`
- `L3 Rx High` oder `L3 Rx Low`

Pakete werden auf Basis des QoS-Labels, dem DSCP-Wert (Differentiated Services Code Point) des IP-Diensttyps (ToS), in diese Warteschlangen eingereiht. Beispielsweise werden Pakete mit einem DSCP von 63 in die Warteschlange `L3 Fwd Highest` (`Höchste` Fwd) gestellt. Die Pakete, die für diese 16 Warteschlangen empfangen und verworfen werden, werden in der Ausgabe des Befehls **show platform cpu packet statistics all** angezeigt. Die Ausgabe dieses Befehls ist sehr lang. Geben Sie den Befehl **show platform cpu packet statistics** ein, um nur die Ereignisse anzuzeigen, die nicht null sind. Ein alternativer Befehl ist der Befehl **show platform** cpuport. Verwenden Sie den Befehl **show platform** cpuport nur, wenn Sie die Cisco IOS Software Release 12.1(11)EW oder eine frühere Version ausführen. Dieser Befehl ist inzwischen veraltet. Dieser ältere Befehl war jedoch vor Version 12.2(20)EWA Teil des Befehls **show tech-support** in Cisco IOS-Softwareversionen.

Verwenden Sie den Befehl **show platform cpu packet statistics** für alle Fehlerbehebungsmaßnahmen.

```
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
```

Die Catalyst 4500-CPU weist den verschiedenen Warteschlangen, die in Tabelle 1 aufgeführt sind, Gewichtungen zu. Die CPU weist die Gewichtungen nach Wichtigkeit oder Typ und nach Priorität des Datenverkehrs oder DSCP zu. Die CPU verarbeitet die Warteschlange auf Basis der relativen Gewichte der Warteschlange. Wenn z. B. sowohl ein Steuerungspaket wie eine BPDU als auch eine ICMP-Echoanfrage ausstehen, stellt die CPU zuerst das Steuerungspaket bereit. Ein zu hoher Anteil an Datenverkehr mit niedriger Priorität oder mit geringerer Bedeutung beeinträchtigt die CPU nicht in der Lage, das System zu verarbeiten oder zu verwalten. Dieser Mechanismus garantiert, dass das Netzwerk auch bei hoher CPU-Auslastung stabil ist. Diese Fähigkeit des Netzwerks, stabil zu bleiben, sind wichtige Informationen, die Sie verstehen müssen.

Es gibt noch ein weiteres sehr wichtiges Detail der Implementierung bei der Paketverarbeitung mit der Catalyst 4500 CPU. Wenn die CPU bereits Pakete oder Prozesse mit hoher Priorität bearbeitet hat, aber über mehr freie CPU-Zyklen für einen bestimmten Zeitraum verfügt, verarbeitet die CPU Pakete mit niedriger Priorität oder führt Hintergrundprozesse mit niedrigerer Priorität durch. Eine hohe CPU-Auslastung aufgrund der Paketverarbeitung mit niedriger Priorität oder von Hintergrundprozessen wird als normal angesehen, da die CPU ständig versucht, die

gesamte verfügbare Zeit zu nutzen. Auf diese Weise strebt die CPU eine maximale Leistung des Switches und Netzwerks an, ohne dass die Stabilität des Switches beeinträchtigt wird. Der Catalyst 4500 betrachtet die CPU als nicht ausgelastet, es sei denn, die CPU wird zu 100 Prozent für einen einzelnen Zeitsteckplatz verwendet.

Die Cisco IOS Softwareversion 12.2(25)EWA2 und höher hat den CPU-Paketverarbeitungs- und Prozessverwaltungsmechanismus sowie die Abrechnung verbessert. Verwenden Sie daher diese Versionen für Ihre Catalyst 4500-Bereitstellungen.

Ermitteln Sie den Grund für die hohe CPU-Auslastung beim Catalyst 4500.

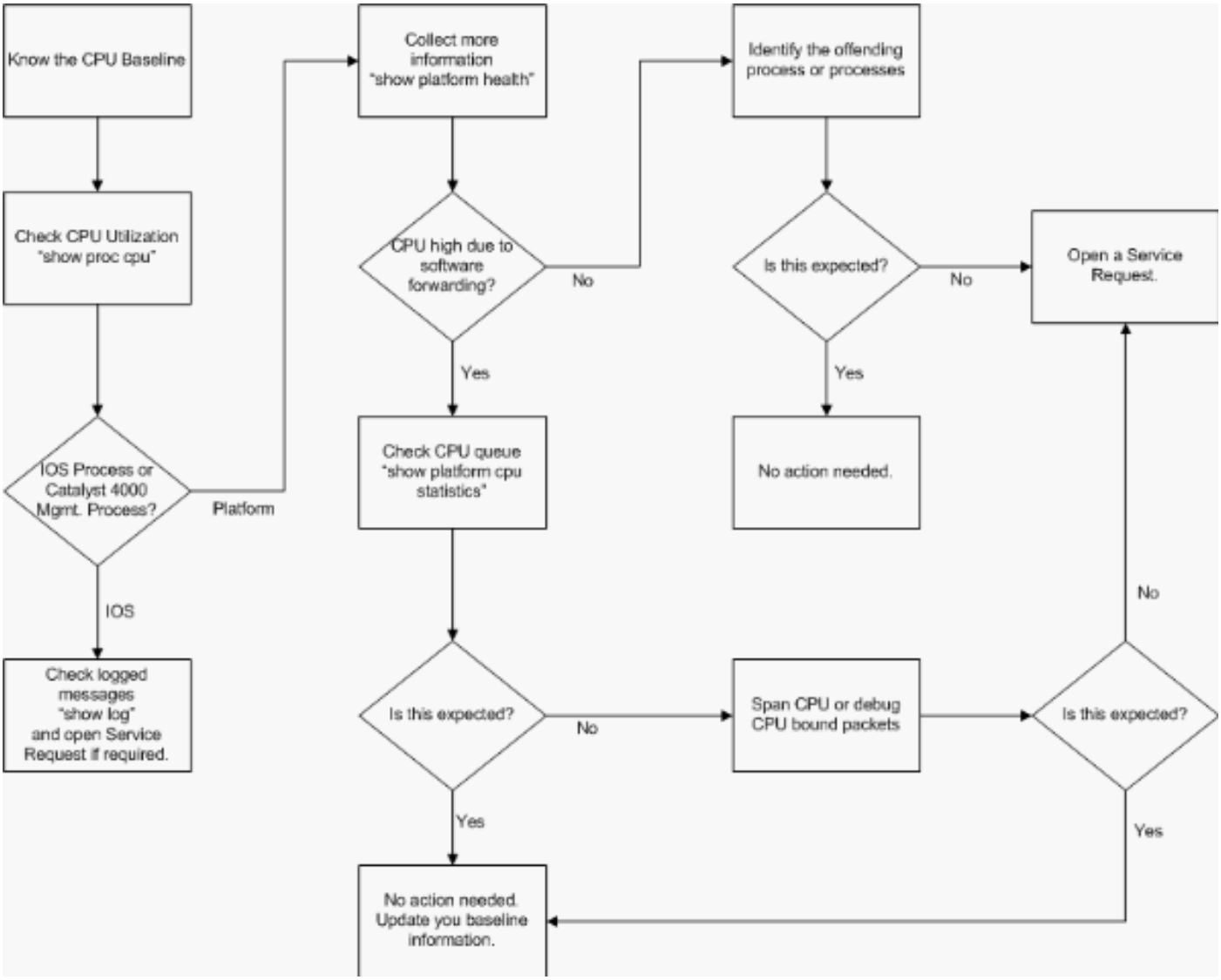
Wenn Sie jetzt die Architektur und das Design der Catalyst 4500 CPU für die Paketverarbeitung kennen, möchten Sie vielleicht trotzdem herausfinden, warum die CPU-Auslastung des Catalyst 4500 hoch ist. Der Catalyst 4500 verfügt über die erforderlichen Befehle und Tools, um die Ursache für die hohe CPU-Auslastung zu ermitteln. Nachdem Sie den Grund ermittelt haben, können die Administratoren eine der folgenden Aktionen durchführen:

- Korrektur - Dies kann Konfigurations- oder Netzwerkänderungen oder die Erstellung einer Anfrage für einen technischen Support von Cisco zur weiteren Analyse umfassen.
- Keine Aktion - Der Catalyst 4500 arbeitet entsprechend der Erwartungen. Die CPU ist sehr CPU-Auslastung, da die Supervisor Engine die CPU-Zyklen maximiert, um alle erforderlichen Aufgaben für die Softwarepaketweiterleitung und die Hintergrundverarbeitung durchzuführen.

Achten Sie darauf, den Grund für eine hohe CPU-Auslastung zu ermitteln, auch wenn keine Korrekturmaßnahmen in allen Fällen erforderlich sind. Eine hohe CPU-Auslastung kann nur ein Symptom für ein Netzwerkproblem sein. Eine Lösung der Ursache dieses Problems kann erforderlich sein, um die CPU-Auslastung zu verringern.

Abbildung 2 zeigt die Methode zur Fehlerbehebung, mit der die Ursache für die hohe CPU-Auslastung des Catalyst 4500 ermittelt werden kann.

Abbildung 2: Verfahren zur Fehlerbehebung bei hoher CPU-Auslastung bei Catalyst Switches der Serie 4500



Die allgemeinen Schritte zur Fehlerbehebung sind:

1. Führen Sie den Befehl **show process cpu** aus, um die Cisco IOS-Prozesse zu identifizieren, die CPU-Zyklen verbrauchen.
2. Führen Sie den Befehl **show platform health** aus, um die plattformspezifischen Prozesse genauer zu identifizieren.
3. Wenn der hochaktive Prozess **K2CpuMan Review** ist**,** geben Sie den Befehl **show platform cpu packet statistics** aus, um die Art des Datenverkehrs zu identifizieren, der die CPU trifft.Wenn die Aktivität nicht auf den **Prozess `K2CpuMan Review`** zurückzuführen ist, überspringen Sie Schritt 4 und fahren Sie mit Schritt 5 fort.
4. Identifizieren Sie die Pakete, die die CPU erreichen, mithilfe der Tools zur Fehlerbehebung, um den an die CPU gerichteten Datenverkehr zu analysieren, falls erforderlich.Ein Beispiel für die zu verwendenden Fehlerbehebungstools ist der CPU Switched Port Analyzer (SPAN).
5. Lesen Sie dieses Dokument und den Abschnitt Fehlerbehebung bei häufigen Problemen mit der CPU-Auslastung für häufige Ursachen.Wenn Sie die Ursache immer noch nicht identifizieren können, wenden Sie sich an den technischen Support von Cisco.

CPU-Auslastung als Basis

Der wichtige erste Schritt besteht darin, die CPU-Auslastung Ihres Switches für die Konfiguration und die Netzwerkeinrichtung zu kennen. Verwenden Sie den Befehl **show process cpu**, um die

CPU-Auslastung auf dem Catalyst 4500 zu ermitteln. Die kontinuierliche Aktualisierung der grundlegenden CPU-Auslastung kann erforderlich sein, wenn Sie der Netzwerkeinrichtung weitere Konfigurationen hinzufügen oder das Netzwerkverkehrsmuster sich ändert. Abbildung 2 zeigt diese Anforderung.

Diese Ausgabe stammt von einem vollständig ausgestatteten Catalyst 4507R. Die Steady-State-CPU beträgt etwa 32 bis 38 Prozent. Dies ist für die Ausführung der Verwaltungsfunktionen für diesen Switch erforderlich:

```
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 IOS ACL Helper
  34           0         2          0  0.00%  0.00%  0.00%   0 NAM Manager
```

Die CPU-Auslastung innerhalb von fünf Sekunden wird wie folgt ausgedrückt:

x%/y%

Der *x* % stellt die gesamte CPU-Auslastung dar, und *y* % stellt die CPU dar, die auf Unterbrechungsebene ausgegeben wird. Bei der Fehlerbehebung für Catalyst 4500-Switches sollten Sie sich nur auf die gesamte CPU-Auslastung konzentrieren.

Verständnis des Befehls show process cpu für die Catalyst 4500-Switches

Diese **Show-Prozesse CPU-**Ausgabe zeigt, dass es zwei Prozesse, die die CPU verwenden - **`Cat4k Mgmt HiPri`** und **`Cat4k Mgmt LoPri`** . Diese beiden Prozesse aggregieren mehrere plattformspezifische Prozesse, die die grundlegenden Verwaltungsfunktionen des Catalyst 4500 ausführen. Diese Prozesse verarbeiten sowohl die Kontrollebene als auch Datenpakete, die softwarevermittelt oder verarbeitet werden müssen.

Um zu sehen, welche der plattformspezifischen Prozesse die CPU im Kontext von **`Cat4k Mgmt HiPri`** und **`Cat4k Mgmt LoPri`** verwenden, führen Sie den **Befehl show platform health aus.**

Jeder plattformspezifische Prozess hat eine Ziel/erwartete Auslastung der CPU. Wenn sich dieser Prozess innerhalb des Ziels befindet, führt die CPU den Prozess im Kontext mit hoher Priorität aus. Die **Ausgabe des Befehls "show prozesse cpu"** zählt unter der **`Cat4k Mgmt HiPri-Mgmt-Funktion für die Nutzung`**. Wenn ein Prozess die Ziel-/erwartete Auslastung überschreitet, wird dieser Prozess im Kontext mit niedriger Priorität ausgeführt. Die Ausgabe des Befehls **show process cpu** zählt für die zusätzliche Nutzung unter **`Cat4k Mgmt LoPri.`** Dieser **`Cat4k Mgmt LoPri`** wird auch zur Ausführung von Hintergrundprozessen und anderen Prozessen mit niedriger Priorität verwendet, z. B. Konsistenzprüfung und Lesen von Schnittstellenzählern. Dieser Mechanismus ermöglicht der CPU, bei Bedarf Prozesse mit hoher Priorität auszuführen, und die verbleibenden CPU-Zyklen im Leerlauf werden für Prozesse mit niedriger Priorität verwendet. Die Überschreitung der Ziel-CPU-Auslastung um eine geringe Menge oder ein kurzzeitiger Anstieg der Auslastung ist kein Hinweis auf ein Problem, das untersucht werden muss.

Switch#**show platform health**

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

Verständnis des Befehls show platform health auf den Catalyst 4500-Switches

Der **show plattform health**-Befehl liefert eine Menge Informationen, die nur für einen Entwicklungsingenieur relevant sind. Um eine Fehlerbehebung für eine hohe CPU-Auslastung zu ermöglichen, suchen Sie in der Ausgabefelder der `%CPU` nach einer höheren Anzahl. Achten Sie außerdem darauf, die CPU-Auslastung des Prozesses in den `durchschnittlichen CPU-`Spalten von 1 Minute und 1 Stunde auf die rechte Seite der Zeile zu überprüfen. Manchmal führen Prozesse kurzzeitig Spitzenwerte aus, halten die CPU aber nicht lange aufrecht. Ein Teil der momentan hohen CPU-Auslastung erfolgt bei der Hardwareprogrammierung oder -optimierung der Programmierung. Beispielsweise ist ein Anstieg der CPU-Auslastung bei der Hardwareprogrammierung einer großen ACL im TCAM normal.

In der **Ausgabe des Befehls show platform health** im Abschnitt Verstehen des Befehls show process cpu für die Catalyst 4500-Switches verwenden die **`Stub-JobEventScheduler`** und die **K2CpuMan Review-Prozesse eine höhere Anzahl an CPU-Zyklen.** Tabelle 2 enthält einige grundlegende Informationen zu den allgemeinen plattformspezifischen Prozessen, die in der Ausgabe des Befehls **show platform health** (Plattformzustand anzeigen) angezeigt werden.

Tabelle 2 - Beschreibung der plattformspezifischen Prozesse mithilfe des Systemstatusbefehls show

Plattformspezifischer Prozessname	Beschreibung
`Überprüfung`	Statusverwaltung für Chassis-/Line Card
`IBM`	Ethernet Bridge-Modul, z. B. für Alterung und Überwachung
`ACL-Flattener /K2ACLman`	ACL-Zusammenführungsprozess
`KxAclPathMan - Pfad TagMan-`	ACL-Statusverwaltung und -Wartung

Review	
K2CpuMan-Review	Der Prozess, der die Weiterleitung von Softwarepaketen ausführt Wenn Sie aufgrund dieses Prozesses eine hohe CPU-Auslastung sehen, untersuchen Sie die Pakete, die die CPU erreichen, mithilfe des Befehls **show platform cpu packet statistics**.
K2AccelPacketMan	Der Treiber, der mit der Paket-Engine interagiert, um Pakete zu senden, die von der CPU bestimmt sind
K2AclCamMan	Verwaltet die Ein- und Ausgabe-TCAM-Hardware für QoS- und Sicherheitsfunktionen
K2AclPolicerTableMan	Verwaltet die Ein- und Ausgabeüberwachungen
K2L2	Stellt das L2-Weiterleitungs-Subsystem der Cisco IOS-Software Catalyst 4500 dar Diese Prozesse sind für die Wartung der verschiedenen L2-Tabellen verantwortlich.
K2PortMan-Review	Verwaltet die verschiedenen portbezogenen Programmierfunktionen
K2Fib	FIB[1]-Management
K2FibFlowCache	PBR[2]-Cache-Verwaltung
K2FibAdjMan	FIB Adjacency Table-Management
K2FibMulticast	Verwaltung von Multicast-FIB-Einträgen
K2MetStatsMan-Review	Verwaltung von MET[3]-Statistiken
K2QosDblMan-Review	Verwaltung von QoS DBL[4]
IrmFibThrottler Thro	IP-Routing-Modul
K2 L2 Aging Table Re	Verwaltet die L2-Alterungsfunktion
GalChassisVP-Überprüfung	Chassis-Zustandsüberwachung
S2w-JobEventSchedule	Verwaltet die S2W[5]-Protokolle, um den Status der Linecards zu überwachen
Stub-JobEventSchema	ASIC-basierte Überwachung und Wartung von Line Cards
RkiosPortManPort-Re	Überwachung und Wartung des Portstatus
Rkios-ModulstatusR	Überwachung und Wartung von Line Cards
EthHoleLinecardMan	Verwaltung von GBICs[6] in jeder Linecard

[1] FIB = Forwarding Information Base

[2] PBR = richtlinienbasiertes Routing

[3] MET = Multicast Expansion Table.

[4] DBL = Dynamic Buffer Limiting.

[5] S2W = Seriell-to-Wire

[6] GBIC = Gigabit Interface Converter

Fehlerbehebung bei häufigen Problemen mit hoher CPU-Auslastung

In diesem Abschnitt werden einige der häufigsten Probleme bei der CPU-Auslastung der Catalyst 4500-Switches behandelt.

Hohe CPU-Auslastung aufgrund prozessgesteuerter Pakete

Einer der häufigen Gründe für eine hohe CPU-Auslastung ist, dass die Catalyst 4500-CPU mit dem Paketprozess für per Software weitergeleitete Pakete oder Kontrollpakete beschäftigt ist. Beispiele für per Software weitergeleitete Pakete sind IPX oder Steuerungspakete, z. B. BPDUs. Eine kleine Anzahl dieser Pakete wird normalerweise an die CPU gesendet. Eine durchgehend große Anzahl von Paketen kann jedoch auf einen Konfigurationsfehler oder ein Netzwerkereignis hinweisen. Sie müssen die Ursache von Ereignissen identifizieren, die zur Weiterleitung von Paketen zur Verarbeitung an die CPU führen. Mit dieser Identifizierung können Sie Probleme bei der hohen CPU-Auslastung debuggen.

Zu den häufigen Gründen für eine hohe CPU-Auslastung aufgrund von prozessgesteuerten Paketen gehören:

- Eine große Anzahl von Spanning-Tree-Port-Instanzen
- ICMP-Umleitungen; Routing-Pakete auf derselben Schnittstelle
- IPX- oder AppleTalk-Routing
- Gastlernen
- Out-of-Hardware-Ressourcen (TCAM) für Sicherheits-ACL
- Das **log**-Schlüsselwort in ACL
- Layer-2-Weiterleitungsschleifen

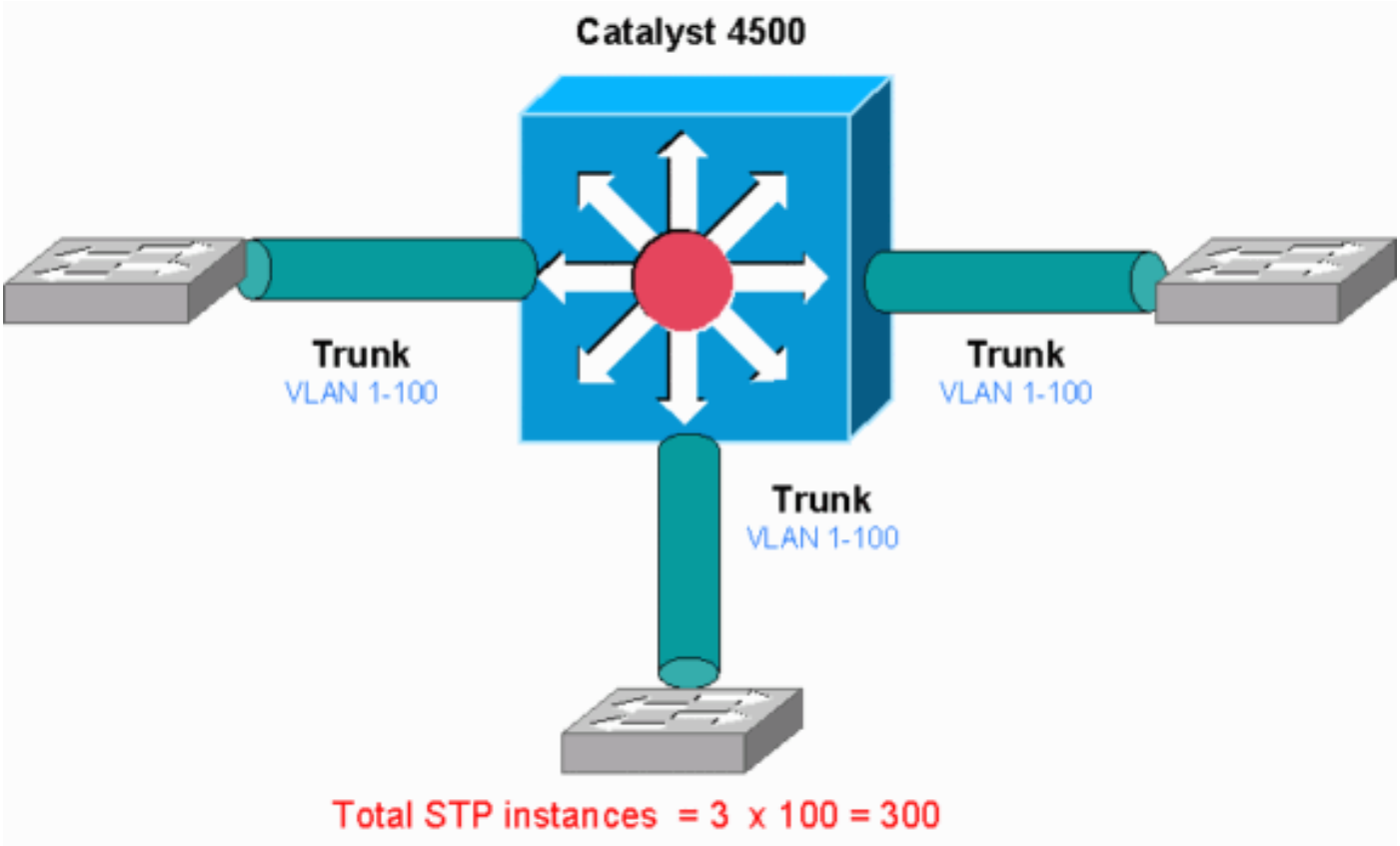
Weitere Gründe für den Wechsel von Paketen zur CPU sind:

- MTU-Fragmentierung - Stellen Sie sicher, dass alle Schnittstellen entlang des Paketpfads die gleiche MTU aufweisen.
- ACL mit anderen TCP-Flags als **etabliert**
- IP-Version 6 (IPv6)-Routing - Dies wird nur über den Software-Switching-Pfad unterstützt.
- GRE - Dies wird nur über den Software-Switching-Pfad unterstützt.
- Verweigerung von Datenverkehr in der Eingangs- oder Ausgangsrouter-ACL (RACL)**Hinweis:** Diese Rate ist in Cisco IOS Software Release 12.1(13)EW1 und höher begrenzt.Geben Sie den Befehl **no ip unreachables** unter der Schnittstelle der ACL aus.
- Übermäßiger ARP- und DHCP-Datenverkehr trifft die CPU für die Verarbeitung, da eine große Anzahl direkt verbundener Hosts vorhanden ist.Wenn Sie einen DHCP-Angriff vermuten,

verwenden Sie DCHP-Snooping, um den DHCP-Datenverkehr von einem bestimmten Host-Port zu begrenzen.
- Übermäßiges SNMP-Polling durch eine legitime oder fehlerhafte Endstation

Eine große Anzahl von Spanning-Tree-Port-Instanzen

Der Catalyst 4500 unterstützt 3.000 Spanning-Tree-Port-Instanzen oder aktive Ports im Per VLAN Spanning Tree+ (PVST+)-Modus. Die Unterstützung gilt für alle Supervisor Engines mit Ausnahme der Supervisor Engines II+ und II+TS und des Catalyst 4948. Die Supervisor Engines II+ und II+TS sowie der Catalyst 4948 unterstützen bis zu 1.500 Port-Instanzen. Wenn Sie diese Empfehlungen für STP-Instanzen übertreffen, weist der Switch eine hohe CPU-Auslastung auf.



Dieses Diagramm zeigt einen Catalyst 4500 mit drei Trunk-Ports, die jeweils die VLANs 1 bis 100 übertragen. Dies entspricht 300 Spanning-Tree-Port-Instanzen. Im Allgemeinen können Sie Spanning-Tree-Port-Instanzen mit der folgenden Formel berechnen:

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

Im Diagramm sind keine Access-Ports vorhanden, aber die drei Trunks übertragen die VLANs 1 bis 100:

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

Schritt 1: Suchen Sie mithilfe des Befehls show process cpu nach dem Cisco IOS-Prozess.

In diesem Abschnitt werden die Befehle erläutert, die ein Administrator verwendet, um das Problem der hohen CPU-Auslastung einzugrenzen. Wenn Sie den Befehl **show process cpu** ausführen, können Sie sehen, dass zwei Hauptprozesse, **`Cat4k Mgmt LoPri`** und **`Spanning Tree,`**

hauptsächlich die CPU verwenden. Nur anhand dieser Informationen wissen Sie, dass der Spanning Tree-Prozess einen beträchtlichen Teil der CPU-Zyklen beansprucht.

```
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
```

Schritt 2: Suchen Sie mithilfe des Befehls show platform health (Plattformstatus anzeigen) nach dem Catalyst 4500-spezifischen Prozess.

Um zu ermitteln, welcher plattformspezifische Prozess die CPU beansprucht, führen Sie den Befehl **show platform health (Plattformzustand anzeigen)** aus. Aus dieser Ausgabe können Sie sehen, dass der **K2CpuMan Review-Prozess**, ein Job zur Verarbeitung von CPU-gebundenen Paketen, die CPU aufruft:

```
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
```

Schritt 3: Überprüfen Sie die CPU-Warteschlange, die Datenverkehr empfängt, um die Art des CPU-gebundenen Datenverkehrs zu identifizieren.

Führen Sie den Befehl **show platform cpu packet statistics** aus, um zu überprüfen, welche CPU-Warteschlange das CPU-gebundene Paket empfängt. Die Ausgabe in diesem Abschnitt zeigt, dass die Steuerwarteschlange viele Pakete empfängt. Verwenden Sie die Informationen in Tabelle 1 und die Schlussfolgerung, die Sie in Schritt 1 gezogen haben. Sie können bestimmen, dass die von der CPU verarbeiteten Pakete und der Grund für die hohe CPU-Auslastung die BPDU-Verarbeitung sind.

```
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
```

Schritt 4: Bestimmen der Ursache

Geben Sie den Befehl **show spanning-tree summary ein**. Sie können überprüfen, ob der Empfang von BPDUs auf eine hohe Anzahl von Spanning-Tree-Port-Instanzen zurückzuführen ist. Die Ausgabe identifiziert eindeutig die Ursache:

```
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
```

Es gibt eine große Anzahl von VLANs mit der Konfiguration des PVST+-Modus. Um das Problem zu beheben, ändern Sie den STP-Modus in Multiple Spanning Tree (MST). In einigen Fällen ist die Anzahl der STP-Instanzen hoch, da eine hohe Anzahl von VLANs auf allen Trunk-Ports weitergeleitet wird. In diesem Fall müssen die nicht erforderlichen VLANs manuell aus dem Trunk entfernt werden, um die Anzahl der aktiven STP-Ports weit unter den empfohlenen Wert zu senken.

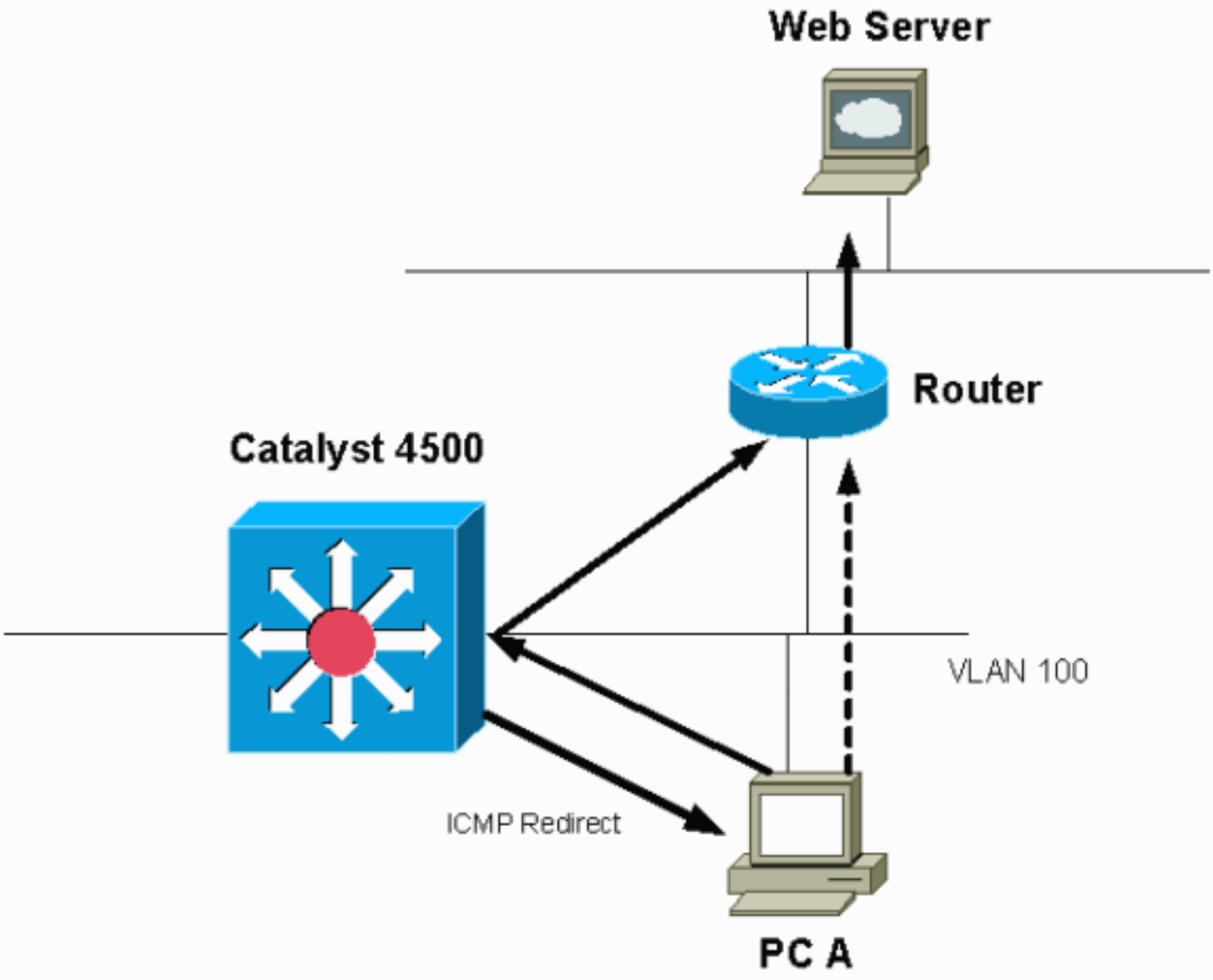
Tipp: Stellen Sie sicher, dass Sie IP-Telefon-Ports nicht als Trunk-Ports konfigurieren. Dies ist eine gängige Fehlkonfiguration. Konfigurieren von IP-Telefon-Ports mit einer Sprach-VLAN-Konfiguration Bei dieser Konfiguration wird ein Pseudo-Trunk erstellt, Sie müssen die nicht benötigten VLANs jedoch nicht manuell bereinigen. Weitere Informationen zum Konfigurieren von Sprachports finden Sie im Softwarekonfigurationsleitfaden Konfigurieren von Sprachschnittstellen. IP-Telefone anderer Anbieter unterstützen diese Sprach-VLAN- oder zusätzliche VLAN-Konfiguration nicht. Sie müssen die Ports manuell mit IP-Telefonen von Drittanbietern bereinigen.

ICMP-Umleitungen; Routing-Pakete auf derselben Schnittstelle

Das Routing von Paketen auf derselben Schnittstelle oder der ein- und ausgehende Datenverkehr auf derselben L3-Schnittstelle kann zu einer ICMP-Umleitung durch den Switch führen. Wenn der Switch weiß, dass sich das nächste Hop-Gerät zum endgültigen Ziel im gleichen Subnetz befindet wie das sendende Gerät, generiert der Switch eine ICMP-Umleitung an die Quelle. Die Umleitungsmeldungen geben an die Quelle an, das Paket direkt an das nächste Hop-Gerät zu senden. Die Meldungen weisen darauf hin, dass das nächste Hop-Gerät eine bessere Route zum Ziel hat, eine Route, die weniger Hop als dieser Switch beträgt.

Im Diagramm in diesem Abschnitt kommuniziert PC A mit dem Webserver. Das Standard-Gateway von PC A verweist auf die IP-Adresse der VLAN 100-Schnittstelle. Der nächste Hop-Router, der es dem Catalyst 4500 ermöglicht, das Ziel zu erreichen, befindet sich jedoch im gleichen Subnetz wie PC A. Der beste Weg in diesem Fall ist, direkt an "Router" zu senden. Catalyst 4500 sendet eine ICMP-Umleitungsmeldung an PC A. Die Meldung weist PC A an, die

Pakete, die zum Webserver bestimmt sind, anstatt über Catalyst 4500 über Router an den Webserver zu senden. In den meisten Fällen antworten die Endgeräte jedoch nicht auf die ICMP-Umleitung. Aufgrund der fehlenden Reaktion verbringt der Catalyst 4500 viel CPU-Zyklen für die Generierung dieser ICMP-Umleitungen für alle Pakete, die der Catalyst über dieselbe Schnittstelle wie die Eingangspakete weiterleitet.



Standardmäßig ist die ICMP-Umleitung aktiviert. Um sie zu deaktivieren, verwenden Sie den Befehl **no ip icmp redirects**. Geben Sie den Befehl unter der entsprechenden SVI- oder L3-Schnittstelle ein.

Hinweis: Da **ip icmp redirects** ein Standardbefehl ist, wird er in der Befehlsausgabe **show running-configuration** nicht angezeigt.

Schritt 1: Suchen Sie mithilfe des Befehls show process cpu nach dem Cisco IOS-Prozess.

Geben Sie den Befehl **show process cpu** ein. Sie sehen, dass zwei Hauptprozesse, **Cat4k Mgmt LoPri** und **IP-Eingang**, hauptsächlich die CPU verwenden. Nur mit diesen Informationen wissen Sie, dass der Prozess der IP-Pakete einen beträchtlichen Teil der CPU ausmacht.

```
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. 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
```

Schritt 2: Suchen Sie mithilfe des Befehls show platform health (Plattformstatus anzeigen) nach dem Catalyst 4500-spezifischen Prozess.

Die Ausgabe des Befehls **show platform health** bestätigt die Verwendung der CPU zur Verarbeitung von Paketen, die an die CPU gebunden sind.

```
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
```

Schritt 3: Überprüfen Sie die CPU-Warteschlange, die Datenverkehr empfängt, um die Art des CPU-gebundenen Datenverkehrs zu identifizieren.

Führen Sie den Befehl **show platform cpu packet statistics** aus, um zu überprüfen, welche CPU-Warteschlange das CPU-gebundene Paket empfängt. Sie sehen, dass die `L3 Fwd Low`-Warteschlange ziemlich viel Datenverkehr empfängt.

```
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
```

Schritt 4: Bestimmen der Ursache

Verwenden Sie in diesem Fall die CPU SPAN, um den Datenverkehr zu bestimmen, der die CPU erreicht. Weitere Informationen zum CPU SPAN finden Sie im Tool 1: Überwachen des CPU-Datenverkehrs mit SPAN - Cisco IOS Software Release 12.1(19)EW und spätere Abschnitte dieses Dokuments. Führen Sie eine Analyse des Datenverkehrs und eine Konfiguration mithilfe des Befehls **show running-configuration aus**. In diesem Fall wird ein Paket über dieselbe Schnittstelle geroutet, was zu einer ICMP-Umleitung für jedes Paket führt. Diese Ursache ist einer der häufigsten Gründe für die hohe CPU-Auslastung beim Catalyst 4500.

Sie können erwarten, dass das Sourcing-Gerät die ICMP-Umleitung übernimmt, die der Catalyst 4500 sendet, und den nächsten Hop für das Ziel ändert. Nicht alle Geräte reagieren jedoch auf

eine ICMP-Umleitung. Wenn das Gerät nicht reagiert, muss der Catalyst 4500 Umleitungen für jedes Paket senden, das der Switch vom Sendegerät empfängt. Diese Umleitungen können eine Menge CPU-Ressourcen verbrauchen. Die Lösung besteht darin, die ICMP-Umleitung zu deaktivieren. Geben Sie den Befehl **no ip redirects** unter den Schnittstellen ein.

Dieses Szenario kann auftreten, wenn Sie auch sekundäre IP-Adressen konfiguriert haben. Wenn Sie die sekundären IP-Adressen aktivieren, wird die IP-Umleitung automatisch deaktiviert. Stellen Sie sicher, dass die IP-Umleitungen nicht manuell aktiviert werden.

wie dieser ICMP umleitet; Routing-Pakete im Abschnitt "Gleiche Schnittstelle" haben gezeigt, dass die meisten Endgeräte nicht auf ICMP-Umleitungen reagieren. Deaktivieren Sie diese Funktion daher generell.

IPX- oder AppleTalk-Routing

Der Catalyst 4500 unterstützt IPX- und AppleTalk-Routing nur über den Pfad für die Software-Weiterleitung. Bei der Konfiguration solcher Protokolle ist eine höhere CPU-Auslastung normal.

Hinweis: Für das Switching von IPX- und AppleTalk-Datenverkehr im selben VLAN ist kein Prozess-Switching erforderlich. Nur Pakete, die geroutet werden müssen, erfordern eine Weiterleitung des Softwarepfads.

Schritt 1: Suchen Sie mithilfe des Befehls show process cpu nach dem Cisco IOS-Prozess.

Geben Sie den Befehl **show process cpu** ein, um zu überprüfen, welcher Cisco IOS-Prozess die CPU beansprucht. Beachten Sie in dieser Befehlsausgabe, dass der oberste Prozess der **Cat4k Mgmt LoPri**:

```
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
```

Schritt 2: Suchen Sie mithilfe des Befehls show platform health (Plattformstatus anzeigen) nach dem Catalyst 4500-spezifischen Prozess.

Die Ausgabe des Befehls **show platform health** bestätigt die Verwendung der CPU zur Verarbeitung von Paketen, die an die CPU gebunden sind.

```
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
```

Schritt 3: Überprüfen Sie die CPU-Warteschlange, die Datenverkehr empfängt, um die Art des CPU-gebundenen Datenverkehrs zu identifizieren.

Um die Art des Datenverkehrs zu bestimmen, der die CPU trifft, führen Sie den Befehl **show platform cpu packet statistics aus**.

```
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
```

Schritt 4: Bestimmen der Ursache

Da der Administrator IPX oder AppleTalk-Routing konfiguriert hat, sollte die Identifizierung der Ursache einfach erfolgen. Um dies zu bestätigen, müssen Sie jedoch den CPU-Datenverkehr über SPAN leiten und sicherstellen, dass der angezeigte Datenverkehr den erwarteten Datenverkehr darstellt. Weitere Informationen zum CPU SPAN finden Sie im Tool 1: Überwachen des CPU-Datenverkehrs mit SPAN - Cisco IOS Software Release 12.1(19)EW und spätere Abschnitte dieses Dokuments.

In diesem Fall muss der Administrator die Basis-CPU auf den aktuellen Wert aktualisieren. Die Catalyst 4500-CPU verhält sich wie erwartet, wenn die CPU Software-Switched-Pakete verarbeitet.

Host-Learning

Der Catalyst 4500 ruft die MAC-Adressen verschiedener Hosts ab, wenn die MAC-Adresse noch nicht in der MAC-Adresstabelle enthalten ist. Die Switching-Engine leitet eine Kopie des Pakets mit der neuen MAC-Adresse an die CPU weiter.

Alle VLAN-Schnittstellen (Layer 3) verwenden die Hardwareadresse der Chassis-Basis als MAC-Adresse. Daher gibt es keinen Eintrag in der MAC-Adresstabelle, und die Pakete, die für diese VLAN-Schnittstellen bestimmt sind, werden nicht zur Verarbeitung an die CPU gesendet.

Wenn der Switch zu viele neue MAC-Adressen erlernen muss, kann dies zu einer hohen CPU-Auslastung führen.

Schritt 1: Suchen Sie mithilfe des Befehls show process cpu nach dem Cisco IOS-Prozess.

Geben Sie den Befehl **show process cpu** ein, um zu überprüfen, welcher Cisco IOS-Prozess die CPU beansprucht. Beachten Sie in dieser Befehlsausgabe, dass der oberste Prozess der **Cat4k Mgmt LoPri**:

```
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
```

Schritt 2: Suchen Sie mithilfe des Befehls show platform health (Plattformstatus anzeigen) nach dem Catalyst 4500-spezifischen Prozess.

Die Ausgabe des Befehls **show platform health** bestätigt die Verwendung der CPU zur Verarbeitung von Paketen, die an die CPU gebunden sind.

```
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
```

Schritt 3: Überprüfen Sie die CPU-Warteschlange, die Datenverkehr empfängt, um die Art des CPU-gebundenen Datenverkehrs zu identifizieren.

Um die Art des Datenverkehrs zu bestimmen, der die CPU trifft, führen Sie den Befehl **show platform cpu packet statistics aus**.

```
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
```

Schritt 4: Bestimmen der Ursache

Die Ausgabe des Befehls **show platform health** zeigt, dass die CPU viele neue MAC-Adressen erkennt. Diese Situation ist häufig auf Instabilität in der Netzwerktopologie zurückzuführen. Wenn sich beispielsweise die Spanning-Tree-Topologie ändert, generiert der Switch Topology Change Notifications (TCNs). Durch das Problem mit TCNs wird die Alterungszeit im PVST+-Modus auf 15 Sekunden reduziert. MAC-Adresseinträge werden geleert, wenn die Adressen innerhalb des Zeitraums nicht zurückgelernt werden. Bei Rapid STP (RSTP) (IEEE 802.1w) oder MST (IEEE 802.1s) werden die Einträge sofort angezeigt, wenn die TCN von einem anderen Switch stammt. Durch diese Alterung werden MAC-Adressen neu erlernt. Dies ist kein großes Problem, wenn die Topologieänderungen selten vorkommen. Es kann jedoch zu viele Topologieänderungen geben, da eine Flapping-Verbindung, ein fehlerhafter Switch oder Host-Ports vorhanden sind, die für PortFast nicht aktiviert sind. Eine große Anzahl von MAC-Tabellen-Flushes und anschließendes erneutes Lernen können dazu führen. Der nächste Schritt bei der Ursachenidentifizierung besteht in der Fehlerbehebung im Netzwerk. Der Switch funktioniert wie erwartet und sendet die Pakete zur Ermittlung der Host-Adresse an die CPU. Identifizieren und beheben Sie das fehlerhafte Gerät, das zu übermäßigen TCNs führt.

In Ihrem Netzwerk können viele Geräte Datenverkehr in Bursts senden, wodurch MAC-Adressen veraltet und anschließend auf dem Switch neu gelernt werden. In diesem Fall sollte die Alterungszeit der MAC-Adresstabelle erhöht werden, um eine gewisse Erleichterung zu erzielen. Mit einer längeren Alterungszeit behalten die Switches die MAC-Adressen des Geräts vor Ablauf des Alters für einen längeren Zeitraum in der Tabelle.

Vorsicht: Nehmen Sie diese Altersvorsorge nur nach sorgfältiger Überlegung vor. Diese Änderung kann zu einem Datenverkehrsloch führen, wenn sich Geräte im Netzwerk befinden, die mobil sind.

Out of Hardware Resources (TCAM) für Security ACL

Der Catalyst 4500 programmiert die konfigurierten ACLs mit dem Cisco TCAM. TCAM ermöglicht die Anwendung der ACLs im Hardware-Weiterleitungspfad. Die Leistung des Switches wird durch oder ohne ACLs im Weiterleitungspfad nicht beeinträchtigt. Trotz der Größe der Zugriffskontrollliste ist die Leistung konstant, da die Zugriffskontrolllisten mit Leitungsgeschwindigkeit ausgeführt werden. TCAM ist jedoch eine begrenzte Ressource. Wenn Sie daher eine übermäßige Anzahl von ACL-Einträgen konfigurieren, überschreiten Sie die TCAM-Kapazität. Tabelle 3 zeigt die Anzahl der für die Catalyst 4500 Supervisor Engines und Switches verfügbaren TCAM-Ressourcen.

Tabelle 3: TCAM-Kapazität für Catalyst 4500 Supervisor Engines/Switches

Produkt	Funktion TCAM (pro Richtung)	QoS-TCAM (pro Richtung)
Supervisor Engine II+/II+TS	8192 Einträge mit 1024 Masken	8192 Einträge mit 1024 Masken
Supervisor Engine III/IV/V und Catalyst 4948	16.384 Einträge mit 2048 Masken	16.384 Einträge mit 2048 Masken
Supervisor Engine V-10GE und Catalyst 4948-10GE	16.384 Einträge mit 16.384 Masken	16.384 Einträge mit 16.384 Masken

Der Switch verwendet die Funktion TCAM, um die Sicherheits-ACL wie RACL und VLAN ACL (VACL) zu programmieren. Der Switch verwendet außerdem die Funktion TCAM für Sicherheitsfunktionen wie IP Source Guard (IPSG) für dynamische Zugriffskontrolllisten. Der Switch verwendet den QoS-TCAM, um Klassifizierungen und Richtlinien-ACLs zu programmieren.

Wenn dem Catalyst 4500 bei der Programmierung einer Sicherheits-ACL keine TCAM-Ressourcen zur Verfügung stehen, erfolgt eine teilweise Anwendung der ACL über den Softwarepfad. Die Pakete, die diese ACEs erreichen, werden in der Software verarbeitet, was zu einer hohen CPU-Auslastung führt. Die ACL wird von oben nach unten programmiert. Anders ausgedrückt: Wenn die ACL nicht in den TCAM passt, wird der ACE am unteren Rand der ACL wahrscheinlich nicht im TCAM programmiert.

Diese Warnmeldung wird angezeigt, wenn ein TCAM-Überlauf auftritt:

```
%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 will be software switched.
```

Diese Fehlermeldung wird in der Ausgabe des Befehls **show logging** angezeigt. Die Meldung weist abschließend darauf hin, dass einige Software-Verarbeitungen stattfinden werden und folglich eine hohe CPU-Auslastung vorliegen kann.

Hinweis: Wenn Sie eine große Zugriffskontrollliste ändern, wird diese Meldung kurz angezeigt, bevor die geänderte Zugriffskontrollliste im TCAM erneut programmiert wird.

Schritt 1: Suchen Sie mithilfe des Befehls show process cpu nach dem Cisco IOS-Prozess.

Geben Sie den Befehl **show process cpu** ein. Sie sehen, dass die CPU-Auslastung hoch ist, da der **Cat4k Mgmt LoPri-Prozess den** Großteil der CPU-Zyklen beansprucht.

```
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
```

Schritt 2: Suchen Sie mithilfe des Befehls show platform health (Plattformstatus anzeigen) nach dem Catalyst 4500-spezifischen Prozess.

Geben Sie den Befehl **show platform health** ein. Sie sehen, dass die **K2CpuMan Review**, ein Auftrag zur Verarbeitung CPU-gebundener Pakete, die CPU verwendet.

```
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
```

Schritt 3: Überprüfen Sie die CPU-Warteschlange, die Datenverkehr empfängt, um die Art des CPU-gebundenen Datenverkehrs zu identifizieren.

Sie müssen genauer verstehen, welche CPU-Warteschlange und daher welche Art von

Datenverkehr die CPU-Warteschlange trifft. Geben Sie den Befehl **show platform cpu packet statistics ein**. Sie sehen, dass die Warteschlange für die `ACL-Sw-Verarbeitung` eine große Anzahl von Paketen empfängt. Aus diesem Grund ist der TCAM-Überlauf die Ursache für dieses Problem mit der hohen CPU-Auslastung.

```
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
```

Schritt 4: Beheben Sie das Problem.

In Schritt 3 haben Sie die Ursache in diesem Szenario ermittelt. Entfernen Sie die ACL, die den Überlauf verursacht hat, oder minimieren Sie die ACL, um einen Überlauf zu vermeiden. Lesen Sie außerdem den Konfigurationsleitfaden zur Konfiguration der Netzwerksicherheit mit ACLs, um die ACL-Konfiguration und -Programmierung in der Hardware zu optimieren.

Das Protokollschlüsselwort in der ACL

Der Catalyst 4500 unterstützt die Protokollierung von Paketdetails, die einen bestimmten ACL-Eintrag erreichen, aber eine übermäßige Protokollierung kann zu einer hohen CPU-Auslastung führen. Vermeiden Sie die Verwendung von **Protokoll-**Schlüsselwörtern, außer während der Datenverkehrserkennungsphase. Während der Datenverkehrserkennungsphase identifizieren Sie den Datenverkehr, der durch Ihr Netzwerk fließt, für den Sie keine expliziten ACEs konfiguriert haben. Verwenden Sie nicht das **log-**Schlüsselwort, um Statistiken zu erstellen. In der Cisco IOS Software-Version 12.1(13)EW und höher sind die **Protokollmeldungen** ratenlimitiert. Wenn Sie **Protokollmeldungen** verwenden, um die Anzahl der Pakete zu zählen, die mit der ACL übereinstimmen, ist die Anzahl nicht korrekt. Verwenden Sie stattdessen den Befehl **show access-list** für genaue Statistiken. Die Identifizierung dieser Ursache ist einfacher, da eine Überprüfung der Konfiguration oder der **Protokollmeldungen** auf die Verwendung der ACL-Protokollierungsfunktion hinweisen kann.

Schritt 1: Suchen Sie mithilfe des Befehls show process cpu nach dem Cisco IOS-Prozess.

Geben Sie die **CPU für Anzeigeprozesse aus**, um zu überprüfen, welcher Cisco IOS-Prozess die CPU beansprucht. In dieser Befehlsausgabe finden Sie den obersten Prozess des **`Cat4k Mgmt LoPri`**:

```
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
```

Schritt 2: Suchen Sie mithilfe des Befehls show platform health (Plattformstatus anzeigen) nach dem Catalyst 4500-spezifischen Prozess.

Überprüfen Sie den plattformspezifischen Prozess, der die CPU verwendet. Geben Sie den Befehl **show platform health** ein. Beachten Sie, dass der **K2CpuMan Review-Prozess** die meisten CPU-Zyklen verwendet. Diese Aktivität weist darauf hin, dass die CPU ausgelastet ist, da sie Pakete verarbeitet, die für sie bestimmt sind.

```
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
```

Schritt 3: Überprüfen Sie die CPU-Warteschlange, die Datenverkehr empfängt, um die Art des CPU-gebundenen Datenverkehrs zu identifizieren.

Um die Art des Datenverkehrs zu bestimmen, der die CPU trifft, führen Sie den Befehl **show platform cpu packet statistics aus**. In dieser Befehlsausgabe sehen Sie, dass der Empfang von Paketen auf das ACL-**Protokoll-**Schlüsselwort zurückzuführen ist:

```
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
```

Schritt 4: Beheben Sie das Problem.

In Schritt 3 haben Sie die Ursache in diesem Szenario ermittelt. Um dieses Problem zu vermeiden, entfernen Sie das **log**-Schlüsselwort aus den ACLs. In der Cisco IOS Software Version 12.1(13)EW1 und höher sind die Pakete ratenlimitiert, sodass die CPU-Auslastung nicht zu hoch wird. Verwenden Sie die Zähler der Zugriffslisten, um ACL-Treffer nachzuverfolgen. Sie können die Zähler der Zugriffslisten in der **Befehlsausgabe show access-list** *acl_id* sehen.

Layer-2-Weiterleitungsschleifen

Layer-2-Weiterleitungsschleifen können durch eine unzureichende Implementierung von Spanning Tree Protocol (STP) und verschiedene Probleme verursacht werden, die sich auf STP auswirken können.

Schritt 1: Suchen Sie mithilfe des Befehls show process cpu nach dem Cisco IOS-Prozess.

In diesem Abschnitt werden die Befehle erläutert, die ein Administrator verwendet, um das Problem der hohen CPU-Auslastung einzugrenzen. Wenn Sie den Befehl **show process cpu** ausführen, können Sie sehen, dass zwei Hauptprozesse, **`Cat4k Mgmt LoPri`** und **`Spanning Tree`**, **hauptsächlich die CPU verwenden.** Nur anhand dieser Informationen wissen Sie, dass der Spanning Tree-Prozess einen beträchtlichen Teil der CPU-Zyklen beansprucht.

```
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
```

Schritt 2: Suchen Sie mithilfe des Befehls show platform health (Plattformstatus anzeigen) nach dem Catalyst 4500-spezifischen Prozess.

Um zu ermitteln, welcher plattformspezifische Prozess die CPU beansprucht, führen Sie den Befehl **show platform health (Plattformzustand anzeigen)** aus. Aus dieser Ausgabe können Sie sehen, dass der **`K2CpuMan Review`-Prozess**, ein Job zur Verarbeitung von CPU-gebundenen Paketen, die CPU aufruft:

```
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
```

Schritt 3: Überprüfen Sie die CPU-Warteschlange, die Datenverkehr empfängt, um die Art des CPU-gebundenen Datenverkehrs zu identifizieren.

Führen Sie den Befehl **show platform cpu packet statistics** aus, um zu überprüfen, welche CPU-Warteschlange das CPU-gebundene Paket empfängt. Die Ausgabe in diesem Abschnitt zeigt, dass die Steuerwarteschlange viele Pakete empfängt. Verwenden Sie die Informationen in Tabelle 1 und die Schlussfolgerung, die Sie in Schritt 1 gezogen haben. Sie können bestimmen, dass die von der CPU verarbeiteten Pakete und der Grund für die hohe CPU-Auslastung die BPDU-Verarbeitung sind.

```
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
```

Schritt 4: Identifizieren der Ursache und Beheben des Problems

Im Allgemeinen können Sie diese Schritte ausführen, um eine Fehlerbehebung durchzuführen (je nach Situation sind einige Schritte nicht erforderlich):

1. Identifizieren der Schleife
2. Entdecken Sie den Umfang der Schleife.
3. Brechen Sie die Schleife.
4. Beheben Sie die Ursache für die Schleife.
5. Stellen Sie die Redundanz wieder her.

Jeder dieser Schritte wird unter Troubleshooting Forwarding Loops - Troubleshooting STP on Catalyst Switches Running Cisco IOS System Software (Fehlerbehebung bei STP auf Catalyst-Switches mit Cisco IOS-Systemsoftware) detailliert erläutert.

Schritt 5: Implementierung erweiterter STP-Funktionen

- **BDPU Guard** - Schützt STP vor nicht autorisierten Netzwerkgeräten, die mit portfast-fähigen Ports verbunden sind. Weitere Informationen finden Sie unter Spanning Tree PortFast BPDU Guard Enhancement.
- **Loop Guard** - Erhöht die Stabilität von Layer-2-Netzwerken. Weitere Informationen finden Sie unter Spanning Tree Protocol Enhancements using Loop Guard and BPDU Skew Detection Features (Spanning-Tree-Protokollerweiterungen mit Loop Guard und BPDU Skew Detection Features.
- **Root Guard** - Erzwingt die Platzierung von Root Bridge im Netzwerk. Weitere Informationen finden Sie unter Spanning Tree Protocol Root Guard Enhancement.
- **UDLD**: Erkennt unidirektionale Verbindungen und verhindert Weiterleitungsschleifen. Weitere Informationen finden Sie unter Verstehen und Konfigurieren der Unidirectional Link Detection Protocol-Funktion.

Weitere Ursachen für die hohe CPU-Auslastung

Dies sind einige andere bekannte Ursachen für die hohe CPU-Auslastung:

- Übermäßige Verbindungslücken
- Spitzenwerte bei der CPU-Auslastung durch FIB-Konsistenzprüfung
- Hohe CPU-Auslastung im **K2FibAdjMan Host Move-**Prozess
- Hohe CPU-Auslastung im **RkiosPortMan Port Review-**Prozess
- Hohe CPU-Auslastung bei Verbindung mit einem IP-Telefon über Trunk-Ports
- Hohe CPU-Auslastung mit RSPAN und Layer-3-Steuerungspaketen
- Spiegelung während der großen ACL-ProgrammierungDie Spitzenauslastung der CPU tritt während der Anwendung oder beim Entfernen einer großen Zugriffskontrollliste von einer Schnittstelle auf.

Übermäßige Link-Flapping

Der Catalyst 4500 weist eine hohe CPU-Auslastung auf, wenn eine oder mehrere der angeschlossenen Verbindungen zu Flapping-Ereignissen führen. Diese Situation tritt bei Cisco IOS Software-Versionen vor Version 12.2(20)EWA der Cisco IOS-Software auf.

Schritt 1: Suchen Sie mithilfe des Befehls show process cpu nach dem Cisco IOS-Prozess.

Geben Sie den Befehl **show process cpu** ein, um zu überprüfen, welcher Cisco IOS-Prozess die CPU beansprucht. Beachten Sie in dieser Befehlsausgabe, dass der oberste Prozess der **Cat4k Mgmt LoPri**:

```
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
```

Schritt 2: Suchen Sie mithilfe des Befehls show platform health (Plattformstatus anzeigen) nach dem Catalyst 4500-spezifischen Prozess.

Die Ausgabe des Befehls **show platform health** gibt an, dass der **Prozess KxAclPathMan erstellt** die CPU aufruft. Dieser Prozess dient der Erstellung interner Pfade.

```
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
```

Schritt 3: Bestimmen der Ursache

Aktivieren Sie die Protokollierung für Nachrichten zum Ein-/Ausschalten von Verbindungen. Diese Protokollierung ist standardmäßig nicht aktiviert. Mit dieser Funktion können Sie die Links, die Sie verletzen, sehr schnell eingrenzen. Geben Sie den Befehl **logging event link-status** unter allen Schnittstellen ein. Sie können den Befehl **interface range** verwenden, um auf einfache Weise für eine Reihe von Schnittstellen zu aktivieren, wie im folgenden Beispiel gezeigt:

```
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
```

```
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
```

Nachdem Sie die fehlerhafte oder Flapping-Schnittstelle identifiziert haben, fahren Sie die Schnittstelle herunter, um das Problem mit der hohen CPU-Auslastung zu beheben. Die Cisco IOS Software-Version 12.2(20)EWA und höher haben das Verhalten von Catalyst 4500 für diese Flapping-Links-Bedingung verbessert. Daher sind die Auswirkungen auf die CPU nicht so groß wie vor der Verbesserung. Denken Sie daran, dass dieser Prozess ein Hintergrundprozess ist. Eine hohe CPU-Auslastung aufgrund dieses Problems hat keine nachteiligen Auswirkungen auf die Catalyst 4500-Switches.

Spitzenwerte bei der CPU-Auslastung durch FIB-Konsistenzprüfung

Der Catalyst 4500 kann während einer Konsistenzprüfung der FIB-Tabelle kurzzeitig Spitzenwerte in der CPU-Auslastung anzeigen. Die FIB-Tabelle ist die L3-Weiterleitungstabelle, die vom CEF-Prozess erstellt wird. Die Konsistenzprüfung gewährleistet die Konsistenz zwischen der FIB-Tabelle der Cisco IOS Software und den Hardwareeinträgen. Diese Konsistenz stellt sicher, dass Pakete nicht falsch geroutet werden. Die Prüfung findet alle 2 Sekunden statt und wird als Hintergrundprozess mit niedriger Priorität ausgeführt. Dieser Prozess ist ein normales Verhalten und beeinträchtigt nicht andere Prozesse oder Pakete mit hoher Priorität.

Die Ausgabe des Befehls **show platform health** zeigt, dass **K2Fib Consistency Ch** den Großteil der CPU beansprucht.

Hinweis: Die durchschnittliche CPU-Auslastung für diesen Prozess ist über eine Minute oder eine Stunde unbedeutend, was bestätigt, dass die Überprüfung eine kurze periodische Überprüfung ist. Dieser Hintergrundprozess verwendet nur die CPU-Zyklen im Leerlauf.

```
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
```

Hohe CPU-Auslastung im K2FibAdjMan-Host-Verschiebungsprozess

Der Catalyst 4500 kann eine hohe CPU-Auslastung im **K2FibAdjMan Host Move-**Prozess anzeigen. Diese hohe Auslastung wird in der Ausgabe des Befehls **show platform health** (Plattformzustand anzeigen) angezeigt. Viele MAC-Adressen laufen häufig ab oder werden an neuen Ports erfasst, was zu dieser hohen CPU-Auslastung führt. Der Standardwert für die Alterungszeit der MAC-Adresstabelle ist 5 Minuten oder 300 Sekunden. Die Lösung für dieses Problem besteht darin, die Alterungszeit der MAC-Adressen zu erhöhen, oder Sie können das Netzwerk so konfigurieren, dass die hohe Anzahl an MAC-Adressverschiebungen vermieden wird. Cisco IOS Software Version 12.2(18)EW und höher haben dieses Prozessverhalten verbessert, um weniger CPU zu verbrauchen. Weitere Informationen finden Sie unter Cisco Bug ID CSCed15021 (nur registrierte Kunden).

```
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
```

Sie können die maximale Alterungszeit einer MAC-Adresse im globalen Konfigurationsmodus ändern. Die Befehlssyntax ist eine **MAC-Adressentabelle für die Alterungszeit** eines Routers und **für die MAC-Adressentabelle in Sekunden [*vlan vlan-id*]** für einen Catalyst Switch. Weitere Informationen finden Sie im Cisco IOS Switching Services Command Reference Guide.

Hohe CPU-Auslastung im RkiosPortMan Port Review Prozess

Der Catalyst 4500 kann eine hohe CPU-Auslastung im **RkiosPortMan Port Review-**Prozess in der Ausgabe des Befehls **show platform health** in Cisco IOS Software Release 12.2(25)EWA und 12.2(25)EWA1 anzeigen. Cisco Bug ID CSCeh08768 (nur registrierte Kunden) verursacht die hohe Auslastung, die durch die Cisco IOS Software Version 12.2(25)EWA2 behoben wird. Dieser Prozess ist ein Hintergrundprozess und beeinträchtigt die Stabilität der Catalyst 4500-Switches nicht.

```
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
```

Hohe CPU-Auslastung bei Verbindung mit einem IP-Telefon über Trunk-Ports

Wenn ein Port sowohl für die Sprach-VLAN-Option als auch für die Zugriffs-VLAN-Option konfiguriert ist, fungiert er als Multi-VLAN-Zugriffsport. Der Vorteil besteht darin, dass nur die VLANs, die für die Sprach- und Zugriffs-VLAN-Optionen konfiguriert sind, gebündelt sind.

Die VLANs, die mit dem Telefon verbunden sind, erhöhen die Anzahl der STP-Instanzen. Der Switch verwaltet die STP-Instanzen. Die Verwaltung der zunehmenden Anzahl von STP-Instanzen erhöht auch die STP-CPU-Auslastung.

Das Trunking aller VLANs führt außerdem dazu, dass der Telefonlink nicht durch unnötige Broadcast-, Multicast- und unbekannten Unicast-Datenverkehr erreicht wird.

```
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
```

Hohe CPU-Auslastung mit RSPAN und Layer-3-Steuerungspaketen

Layer-3-Kontrollpakete, die mit RSPAN erfasst werden, sind für die CPU bestimmt und nicht nur für die RSPAN-Zielschnittstelle, was eine hohe CPU verursacht. Die L3-Steuerungspakete werden von statischen CAM-Einträgen erfasst, wobei die Weiterleitung an die CPU-Aktion erfolgt. Die statischen CAM-Einträge sind für alle VLANs global. Um unnötiges CPU-Flooding zu vermeiden, verwenden Sie die Funktion "Per-VLAN Control Traffic Intercept" (Datenverkehrsabfangen pro VLAN), verfügbar in den Cisco IOS Software-Versionen 12.2(37)SG und höher.

```
Switch(config)# access-list hardware capture mode vlan
```

Statische ACLs werden oben in der TCAM-Funktion für die Eingabefunktion installiert, um Kontrollpakete zu erfassen, die für bekannte IP-Multicast-Adressen im 224.0.0.*-Bereich bestimmt sind. Statische ACLs werden beim Booten installiert und werden vor jeder benutzerdefinierten konfigurierten ACL angezeigt. Statische ACLs werden immer zuerst aufgerufen und Steuerungsdatenverkehr zur CPU in allen VLANs abgefangen.

Die Funktion zum Abfangen von Datenverkehr pro VLAN bietet einen selektiven, auf VLAN-Pfad basierenden Managed-Modus zur Erfassung von Kontrolldatenverkehr. Die entsprechenden statischen CAM-Einträge in der Eingabefunktion TCAM werden im neuen Modus ungültig. Steuerungspakete werden von einer funktionsspezifischen ACL erfasst, die an VLANs angeschlossen ist, auf denen Snooping- oder Routing-Funktionen aktiviert sind. Es ist keine funktionsspezifische ACL mit dem RSPAN-VLAN verbunden. Daher werden nicht alle vom RSPAN-VLAN empfangenen Layer-3-Kontrollpakete an die CPU weitergeleitet.

Tools zur Fehlerbehebung zur Analyse des an die CPU gerichteten Datenverkehrs

Wie dieses Dokument gezeigt hat, ist Datenverkehr, der an die CPU gerichtet ist, eine der Hauptursachen für die hohe CPU-Auslastung auf dem Catalyst 4500. Der CPU-bestimmte Datenverkehr kann entweder vorsätzlich aufgrund der Konfiguration oder unbeabsichtigt aufgrund einer Fehlkonfiguration oder eines Denial-of-Service-Angriffs erfolgen. Die CPU verfügt über einen integrierten QoS-Mechanismus, der schädliche Auswirkungen auf das Netzwerk aufgrund dieses Datenverkehrs verhindert. Identifizieren Sie jedoch die Ursache für CPU-gebundenen Datenverkehr, und beseitigen Sie den Datenverkehr, falls dieser unerwünscht ist.

Tool 1: Überwachen des CPU-Datenverkehrs mit SPAN - Cisco IOS Software Version 12.1(19)EW und höher

Der Catalyst 4500 ermöglicht die Überwachung des ein- oder ausgehenden CPU-Datenverkehrs mithilfe der standardmäßigen SPAN-Funktion. Die Zielschnittstelle stellt eine Verbindung zu einem Paketmonitor oder einem Administrator-Laptop her, auf dem die Software für den Paket-Sniffer ausgeführt wird. Dieses Tool ermöglicht eine schnelle und genaue Analyse des Datenverkehrs, der von der CPU verarbeitet wird. Das Tool ermöglicht die Überwachung einzelner Warteschlangen, die an die CPU-Paket-Engine gebunden sind.

Hinweis: Die Switching-Engine verfügt über 32 Warteschlangen für den CPU-Datenverkehr und die CPU-Paket-Engine über 16 Warteschlangen.

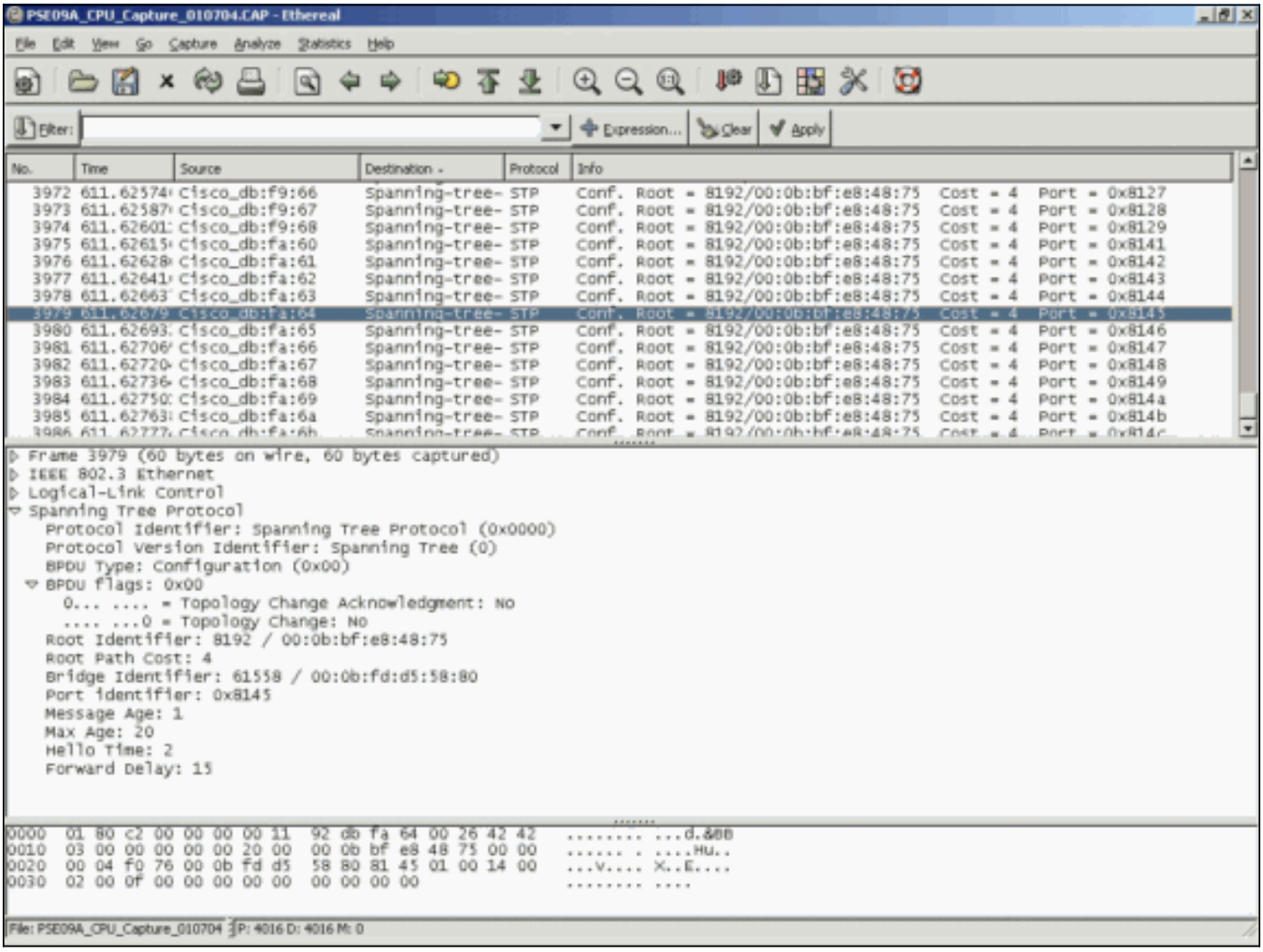
```
Switch(config)#monitor session 1 source cpu ?
  both   Monitor received and transmitted traffic
  queue  SPAN source CPU queue
  rx     Monitor received traffic only
  tx     Monitor transmitted traffic only
  <cr>
Switch(config)#monitor session 1 source cpu queue ?
  <1-32>          SPAN source 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
```

Wenn Sie einen PC anschließen, der ein Sniffer-Programm ausführt, können Sie den Datenverkehr schnell analysieren. In der Ausgabe, die in diesem Abschnitt im Fenster angezeigt wird, sehen Sie, dass die Ursache für die hohe CPU-Auslastung eine übermäßige Anzahl von STP-BPDUs ist.

Hinweis: STP-BPDUs im CPU-Sniffer sind normal. Wenn Sie jedoch mehr sehen, als Sie erwarten, haben Sie möglicherweise die empfohlenen Grenzwerte für Ihre Supervisor Engine überschritten. Weitere Informationen finden Sie im Abschnitt A High Number of Spanning Tree Port Instances (Eine große Anzahl von Spanning-Tree-Port-Instanzen) dieses Dokuments.



Tool 2: Integrierter CPU-Sniffer - Cisco IOS Software Version 12.2(20)EW und höher

Der Catalyst 4500 bietet einen integrierten CPU-Sniffer und -Decoder, um den Datenverkehr, der die CPU erreicht, schnell zu identifizieren. Sie können diese Funktion mit dem Befehl **debug** aktivieren, wie im Beispiel in diesem Abschnitt veranschaulicht wird. Diese Funktion implementiert einen zirkulären Puffer, der 1024 Pakete gleichzeitig speichern kann. Wenn neue Pakete eingehen, überschreiben sie die älteren Pakete. Diese Funktion ist sicher zu verwenden, wenn Sie Probleme mit hoher CPU-Auslastung beheben.

```
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
```

Hinweis: Die CPU-Auslastung bei Ausgabe eines **Debug-**Befehls beträgt immer fast 100 %. Bei der Ausführung eines **Debug-**Befehls ist eine hohe CPU-Auslastung normal.

Tool 3: Identifizieren der Schnittstelle, die Datenverkehr an die CPU sendet - Cisco IOS Software Version 12.2(20)EW und höher

Catalyst 4500 bietet ein weiteres nützliches Tool, um die obersten Schnittstellen zu identifizieren, die Datenverkehr/Pakete zur CPU-Verarbeitung senden. Mit diesem Tool können Sie schnell ein Fehlergerät identifizieren, das eine hohe Anzahl von Broadcast- oder anderen Denial-of-Service-Angriffen an die CPU sendet. Diese Funktion ist auch bei der Fehlerbehebung bei Problemen mit hoher CPU-Auslastung sicher.

```
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
```

Hinweis: Die CPU-Auslastung bei Ausgabe eines **Debug-**Befehls beträgt immer fast 100 %. Bei der Ausführung eines **Debug-**Befehls ist eine hohe CPU-Auslastung normal.

Zusammenfassung

Die Catalyst Switches der Serie 4500 verarbeiten eine hohe IP-Paketweiterleitungsrate der Version 4 (IPv4) in der Hardware. Einige der Funktionen oder Ausnahmen können die Weiterleitung einiger Pakete über den CPU-Prozesspfad verursachen. Der Catalyst 4500 verwendet einen hoch entwickelten QoS-Mechanismus zur Verarbeitung von CPU-gebundenen Paketen. Dieser Mechanismus gewährleistet die Zuverlässigkeit und Stabilität der Switches und maximiert gleichzeitig die CPU für die Software-Weiterleitung von Paketen. Die Cisco IOS Software-Version 12.2(25)EWA2 und höher bietet zusätzliche Verbesserungen bei der Paket-/Prozessverwaltung sowie der Abrechnung. Der Catalyst 4500 verfügt außerdem über ausreichende Befehle und leistungsstarke Tools, um die Ursache für die hohe CPU-Auslastung zu ermitteln. In den meisten Fällen ist die hohe CPU-Auslastung des Catalyst 4500 jedoch weder eine Ursache für Instabilität des Netzwerks noch Anlass zur Sorge.

Zugehörige Informationen

- CPU-Auslastung bei Catalyst Switches der Serien 4500/4000, 2948G, 2980G und 4912G, die CatOS-Software ausführen
- Support-Seiten für LAN-Produkte
- Support-Seite für LAN-Switching
- Technischer Support und Dokumentation - Cisco Systems