أستكشاف أخطاء عمليات مستوى التحكم وإصلاحها على محولات Catalyst 9000 Switches

المحتويات

- المقدمة
- معلومات أساسية
  - المصطلح
- Catalyst 9000 CoPP
  - تنفيذ CoPP
  - النهج الافتراضي
  - ضبط CoPP
- استكشاف الأخطاء وإصلاحها
  - منهجية
  - أوامر الظهار المفيدة
    - تحديد الاستخدام الحالي والتاريخي
    - التحقق من تنظيم مستوى التحكم
    - جمع المعلومات عن حركة المرور الخادعة
    - فحص حركة مرور وحدة المعالجة المركزية (CPU) المرتبطة
- السيناريوهات الشائعة
  - فقدان ICMP (Ping) المتقطع لبروتوكول التنبت (IP) المحلي
  - عمليات إعادة توجيه ICMP عالية وعملية DHCP بطيئة
- موارد إضافية

المقدمة

يصف هذا المستند كيفية أستكشاف أخطاء مستوى التحكم وإصلاحها والتحقق من صحته على محولات Catalyst 9000-family التي تعمل بنظام التشغيل Cisco IOS® XE.

معلومات أساسية

المهمة الأساسية للمحول هي إعادة توجيه الحزم بأسرع ما يمكن. تتم إعادة توجيه معظم الحزم في الأجهزة، ولكن يجب معالجة أنواع معينة من حركة المرور بواسطة وحدة المعالجة المركزية للنظام. تتم معالجة حركة المرور التي تصل إلى وحدة المعالجة المركزية (CPU) في أسرع وقت ممكن. من المتوقع مالحظة قدر معين من حركة المرور في وحدة المعالجة المركزية، ولكن تؤدي الوفرة الكبيرة إلى حدوث مشاكل تشغيلية. تتضمن مجموعة المحوالت Catalyst 9000 آلية قوية لتنظيم مستوى التحكم (CoPP) بشكل افتراضي لمنع المشاكل التي تتسبب فيها تشبع حركة المرور الزائد لوحدة المعالجة المركزية.

تنشأ مشاكل غير متوقعة في بعض حاالت االستخدام كدالة للتشغيل العادي. إن االرتباط بين السبب والنتيجة ليس واضحا في بعض الأحيان، وهو ما من شأنه أن يجعل التعامل مع

المشكلة صعاب. يوفر لك هذا المستند أدوات للتحقق من صحة مستوى التحكم، ويوفر تحديد مستوى التحكم. يسير عملية معالجة المشاكل التي تتضمن مسار إدخال وأجهزة مجمعة. تم تطوير هذه المشاكل التي شوهدت في العديد من السيناريوهات المشتركة على أساس المشاكل التي تم الإبلاغ عنها في الميدان.

تذكر أن مسار تضمين وحدة المعالجة المركزية (CPU) مورد محدود. يمكن لحركة مرور أكبر بشكل ملحوظ أن تدعم مجموعة المحولات Catalyst الأحدث بسهولة في حجم حركة مرور أكبر بشكل ملحوظ أن تدعم مجموعة المحولات Catalyst الأحدث بسهولة في حجم حركة مرور أكبر بشكل ملحوظ. يمكن لمحولات إعادة توجيه وحدة المعالجة المركزية (CPU) مورد محدود. تذكر أن مسار تضمين وحدة المعالجة المركزية (CPU) مورد محدود. يمكن لمحولات إعادة توجيه الأجهزة الحديثة معالجة حجم حركة مرور أكبر بشكل ملحوظ. تدعم مجموعة المحولات Catalyst الأجهزة الحديثة معالجة حجم حركة مرور أكبر بشكل ملحوظ. تدعم مجموعة المحولات Catalyst 9000 بسهولة في حزمة الثانية (PPS) بشكل إجمالي في وحدة المعالجة المركزية في حزمة 19000 تقريبا 9000 بسهولة في حزمة الثانية (PPS) بشكل إجمالي في وحدة المعالجة المركزية في حزمة 19000 تقريبا بدون فقد. تجاوز هذا الحد، وتبدأ حركة المرور المتأثرة في الإسقاط في أي وقت معين. تجاوز هذا الحد، وتبدأ حركة المرور المتأثرة في الإسقاط في أي وقت معين بدون وزن.

المصطلح

- برنامج تشغيل محرك إعادة التوجيه (FED): هذا هو قلب محول Cisco Catalyst switch وهو مسؤول عن جميع برمجة/إعادة توجيه الأجهزة
- IOS: هذا هو برنامج Cisco IOS الأساسي الذي يعمل على نواة Linux. يتم تشغيله كعملية برمجية داخل عنصر kernel
- نظام توصيل الحزم (PDS): هذه هي بنية عملية كيفية تسليم الحزم من الأنظمة الفرعية المختلفة وإليها. وعلى سبيل المثال، فإنه يتحكم في كيفية تسليم الحزم من FED إلى IOSd والعكس بالعكس
- مستوى التحكم (CP): مستوى التحكم هو مصطلح عام يستخدم لتجميع الوظائف وحركة المرور التي تتضمن وحدة المعالجة المركزية الخاصة بالمحول Catalyst switch. وهذا يتضمن حركة مرور البيانات مثل برتوكول الشجرة المتفرعة (STP) وبروتوكول توجيه الموجهة إلى المحول، أو الرسلة من المحول. ويتضمن ذلك أيضا برتوكولات طبقة التطبيقات مثل طبقة الأمان (SSH)، وبروتوكول إدارة الشبكة البسيط (SNMP) الذي يجب معالجته بواسطة وحدة المعالجة المركزية
- مستوى البيانات (DP): عادة ما يتضمن مستوى البيانات وحدات ASIC الخاصة بالأجهزة مستوى التحكم وحركة مرور البيانات التي يتم إعادة توجيهها دون مساعدة من مستوى التحكم
- Punt:إدخال برتوكول تحكم ربط الذي يعترض على DP يرسل إلى ال cp أن يعالجه
- إدخال:حزمة البرتوكول التي تم إنشاؤها بواسطة برتوكول CP والتي يتم إرسالها إلى DP للخروج على واجهة (واجهات) الإدخال والإخراج
- LSMPI: واجهة وحدة ذاكرة Linux المشتركة

Catalyst 9000 CoPP

أساس حماية وحدة المعالجة المركزية على مجموعة المحولات Catalyst 9000 وهو CoPP. باستخدام CoPP، يتم تطبيق سياسة جودة الخدمة (QoS) التي تم إنشاؤها بواسطة النظام على مسار قاطرة وحدة المعالجة المركزية. يتم تجميع حركة مرور البيانات المرتبطة بوحدة تجميع/إدخال وحدة المعالجة المركزية (CPU) في العديد من الفئات المختلفة، ويتم تعيينها بعد ذلك عبر وحدة المعالجة المركزية (CPU). تمنع الشرطات شبكات الأجهزة الفردية المرتبطة بوحدة المعالجة المركزية (CPU). تمنع الشرطات التشبع الزائد لوحدة المعالجة المركزية بواسطة فئة معينة من حركة المرور.

تنفيذ CoPP

يتم تصنيف حركة المرور المرتبطة بوحدة المعالجة المركزية (CPU) في قوائم الانتظار. تكون قوائم الانتظار/الفئات هذه معرفة بواسطة النظام وليست قابلة للتكوين من قبل

32 ل زاهج مظنم 32 9000 Catalyst ةلئاع معدت .ةزهجألا في تاطرشلما نيوكت متي .مدختسلما
.ةمئاقلا انتظار

ةمئاق انتظار مرعف .ىرخأ ةمئاق 32 كانه ،ماع لكشب .ةددحلما ميقلا نم صنم ىلإ نم فلتخت
.ماظنلا ةطساوب .تاسايسلا عضاوف ةطبترلما ،ةئفلا هذه ىلإ ةمئاقلا هذه انتظار قوف ةمئاقلا قلعتت
.ةيضارتفلاا تاسايسلا عضاوف تاسايسلا عضاوف ةصاخلا CoPP ةسايس ىلع تاريغتلا مغر نم ،مدختسلما نم نيوكتلل لبق نم ةحاتلما لدعلما
.ةرظحلما ريغ ةمدخ ريثأتل ضرعتلا نكامإ نم ديزت ةيضارتفلاا

القيم المعرفة من قبل النظام ل CoPP

أسماء خرائط الفئات	فهرس واضع السياسات (رقم واضع السياسات)	قوائم انتظار وحدة المعالجة المركزية (قائمة الانتظار)
نظام حماية مستوى الإدارة (CPP)-بيانات الشرطة	WK_CPP_POLICE_Data(0)	WK_CPU_Q_ICMP_Gen(3) WK_CPU_Q_BROADCAST(12) WK_CPU_Q_ICMP_Redirect(6)
نظام-cpp-police-l2-التحكم	WK_CPP_POLICE_L2_ Control(1)	WK_CPU_Q_L2_CONTROL(1)
النظام-cpp-police-routing-control	WK_CPP_POLICE_Routing_Control(2)	WK_CPU_Q_ROUTING_CONTROL(4) WK_CPU_Q_LOW_Latency (27)
نظام-cpp-police-control-low-priority	WK_CPP_POLICE_CO NTROL_LOW_PRI(3)	WK_CPU_Q_GENERAL_PUNT(25)
system-cpp-police-punt-webauth	WK_CPP_POLICE_PU NT_WEBAUTH(7)	WK_CPU_Q_PUNT_WEBAUTH(22)
النظام-cpp-police-topology-control	WK_CPP_POLICE_TOPOLOGY_CONTROL(8)	WK_CPU_Q_TOPOLOGY_CONTROL(15)
النظام-cpp-police-multicast	wk_cpp_police_multicast(9)	WK_CPU_Q_TRANSPORT_TRAFFIC(18) WK_CPU_Q_MCAST_DATA(30)
system-cpp-police-sys-البيانات	WK_CPP_POLICE_SYS _DATA(10)	WK_CPU_Q_LEARNING_CACHE_OVFL(13

أسماء خرائط الفئات	فهرس واضع السياسات (رقم واضع السياسات)	قوائم انتظار وحدة المعالجة المركزية (قوائم الانتظار)
		WK_CPU_Q_CRYPTO_CONTROL(23) WK_CPU_Q_EXCEPTION(24) WK_CPU_Q_EGR_Exception(28) WK_CPU_Q_NFL_SAMSAMPLE_DATA(26) WK_CPU_Q_GOLD_PKT(31) WK_CPU_Q_RPF_Failed(19)
system-cpp-police-dot1x-auth	WK_CPP_POLICE_DOT1X(11)	WK_CPU_Q_DOT1X_AUTH(0)
بروتوكول حماية مستوى التحكم (CPP) الخاص بالنظام - الشرطة - التطفل على البروتوكول	WK_CPP_POLICE_PR(12)	WK_CPU_Q_PROTO_SNOOPING(16)
system-cpp-police-sw-forward	WK_CPP_POLICE_SW_FWD (13)	WK_CPU_Q_SW_FORWARDING_Q(14) WK_CPU_Q_LOGGING(21) WK_CPU_Q_L2_LVX_DATA_PACK(11)
حماية النظام مستوى الإدارة - الشرطة - القوات	WK_CPP_POLICE_FORUS(14)	WK_CPU_Q_FORUS_ADDR_RESOLUTION WK_CPU_Q_FORUS_TRAFFIC(2)
النظام-cpp-police-multicast-end-station	wk_cpp_police_multicast_snooping(15)	WK_CPU_Q_MCAST_END_STA TION_SERVICE(20)

أسماء خرائط الفئات	فهرس واضع السياسات (رقم واضع السياسات)	قوائم انتظار وحدة المعالجة المركزية (رقم قائمة الانتظار)
افتراضي النظام-cpp	WK_CPP_POLICE_DEFAULT_POLICE(16)	WK_CPU_Q_DHCP_SNOOPING(17) WK_CPU_Q_NON(7) WK_CPU_Q_EWLC_Control(9) WK_CPU_Q_EWLC_Data(10)
system-cpp-police-stackwise-virt-control	WK_CPP_Stackwise_Virtual_Control(5)	WK_CPU_Q_STACKWISE_VIRTUAL_CON (29)
system-cpp-police-l2lvx-control	WK_CPP_ L2_LVX_CONT_PACK(4)	WK_CPU_Q_L2_LVX_CONT_PACK(8)

ترتبط كل قائمة انتظار بنوع حركة مرور أو مجموعة معينة من الميزات. وهذه ليست قائمة شاملة:

قوائم انتظار وحدة المعالجة المركزية (CPU) والميزة (الميزات) المقترنة

الميزة (الميزات)	قوائم انتظار وحدة المعالجة المركزية (رقم قائمة الانتظار)
مصادقة قائمة على المنافذ وفقا لمعيار IEEE 802.1x	WK_CPU_Q_DOT1X_AUTH(0)
بروتوكول التوصيل الديناميكي (DTP) بروتوكول قناة الاتصال لشبكة VLAN (VTP) بروتوكول تجميع المنفذ (PAgP) بروتوكول إرسال إشارات معلومات العميل (CISP) بروتوكول ترحيل جلسة عمل الرسائل بروتوكول التسجيل لشبكة VLAN	WK_CPU_Q_L2_CONTROL(1)

قوائم انتظار وحدة المعالجة المركزية (رقم قائمة الانتظار)	الميزة (الميزات)
	المتعددة (MVRP) شبكة متروبوليتان المتنقلة (MMN) بروتوكول اكتشاف مستوى الارتباط (LLDP) اكتشاف الرابط أحادي الإتجاه (UDLD) بروتوكول التحكم في تجميع الارتباطات (LACP) بروتوكول أستكشاف Cisco (واخصاره CDP) بروتوكول الشجرة المممتدة (STP)
WK_CPU_Q_FORUS_TRAFFIC(2)	مضيف مثل Telnet و Pingv4 و Pingv6 و SNMP اكتشاف Keepalive / الاسترجاع بروتوكول تبادل مفاتيح الاستهلال-الإنترنت (IKE) (IPSec)
WK_CPU_Q_ICMP_Gen(3)	ICMP - الوجهة التي يتعذر الوصول إليها انتهت صلاحية ICMP-TTL
WK_CPU_Q_ROUTING_CONTROL(4)	بروتوكول معلومات التوجيه الإصدار 1 (RIPv1) RIPv2 بروتوكول توجيه العبارة الداخلية (IGRP) بروتوكول البوابة الحدودية (BGP) PIM-UDP بروتوكول تكرار جهاز التوجيه الظاهري

قوائم انتظار وحدة المعالجة المركزية (رقم قائمة الانتظار)	الميزة (الميزات)
	(VRRP) بروتوكول الموجه الاحتياطي الفعال الإصدار 1 (HSRPv1) HSRPv2 بروتوكول موازنة حمل العبارة (GLBP) بروتوكول توزيع التسمية (LDP) بروتوكول إتصالات ذاكرة التخزين المؤقت للويب (WCCP) الجيل التالي من بروتوكول معلومات التوجيه (RIPng) بروتوكول فتح أقصر مسار أولاً (OSPF) الإصدار الأول من بروتوكول فتح أقصر مسار 3(OSPFv3) بروتوكول توجيه العبارة الداخلي المحسن (EIGRP) بروتوكول توجيه البوابة الداخلية المحسنة الإصدار 6 (EIGRPv6) DHCPv6 البث المتعدد المستقل عن البروتوكول (PIM) البث المتعدد المستقل عن البروتوكول الإصدار 6 (PIMv6) بروتوكول الموجه الاحتياطي الفعال من الجيل التالي (HSRPng) التحكم في IPv6 تضمين التوجيه العام (GRE) keepalive أداة ترجمة عنوان الشبكة (NAT)

قوائم انتظار وحدة المعالجة المركزية (رقم قائمة الانتظار)	الميزة (الميزات)
	بروتوكول النظام الوسيط إلى النظام الوسيط (IS-IS)
WK_CPU_Q_FORUS_ADDR_RESOLUTION(5)	بروتوكول تحليل العنوان (ARP) الإعلان عن IPv6 والتماس الجار
WK_CPU_Q_ICMP_Redirect(6)	إعادة توجيه بروتوكول رسائل التحكم في الإنترنت (ICMP)
WK_CPU_Q_INTER_FED_TRAFFIC(7)	إدخال مجال جسر الطبقة 2 للاتصالات الداخلية.
WK_CPU_Q_L2_LVX_CONT_PACK(8)	حزمة معرف Exchange (XID)
WK_CPU_Q_EWLC_Control(9)	وحدة التحكم اللاسلكية المضمنة (eWLC) [التحكم في نقاط الوصول اللاسلكية (CAPWAP) وإدامتها (UDP 5246)]
WK_CPU_Q_EWLC_Data(10)	حزمة بيانات eWLC (بيانات CAPWAP، UDP 5247)
WK_CPU_Q_L2_LVX_DATA_PACK(11)	حزمة البث الأحادي غير معروفة التي تم اعتراضها للطلب الخريطة.
WK_CPU_Q_BROADCAST(12)	جميع أنواع البث
WK_CPU_Q_OPENFLOW(13)	تجاوز سعة ذاكرة التخزين المؤقت للتعلم (الطبقة 3 + الطبقة 2)
WK_CPU_Q_CONTROLLER_PUNT(14)	البيانات - قائمة التحكم في الوصول الكاملة (ACL) البيانات - خيارات IPv4 البيانات - الخطوة الفرعية IPv6

قوائم انتظار وحدة المعالجة المركزية (رقم قائمة الانتظار)	الميزة (الميزات)
	البيانات - خارج المواد / التقاط الكل البيانات - إعادة توجيه المسار غير مكتملة (RPF) العكسي حزمة Glean
WK_CPU_Q_TOPOLOGY_CONTROL(15)	بروتوكول الشجرة الممتدة (STP) بروتوكول إيثرنت المرن (REP) بروتوكول الشجرة الممتدة المشتركة (SSTP)
WK_CPU_Q_PROTO_SNOOPING(16)	تطفل بروتوكول تحليل العنوان الديناميكي (DAI) لفحص ARP (ARP)
WK_CPU_Q_DHCP_SNOOPING(17)	التطفل على بروتوكول DHCP
WK_CPU_Q_TRANSPORT_TRAFFIC(18)	هذا استعملت للحزم يلكم ب nat، أي يحتاج أن يكون عالجت في البرمجية ممر.
WK_CPU_Q_RPF_Failed(19)	البيانات - فشل إعادة توجيه المسار العكسي (RPF) للبث المتعدد
WK_CPU_Q_MCAST_END_STATION_SERVICE(20)	التحكم في بروتوكول إدارة مجموعات الإنترنت (IGMP) / اكتشاف مستمع البث المتعدد (MLD)
WK_CPU_Q_LOGGING(21)	تسجيل قائمة التحكم في الوصول (ACL)
WK_CPU_Q_PUNT_WEBAUTH(22)	مصادقة الويب
WK_CPU_Q_HIGH_RATE_APP(23)	بث

قوائم انتظار وحدة المعالجة المركزية (رقم قائمة الانتظار)	الميزة (الميزات)
WK_CPU_Q_EXCEPTION(24)	مؤشر IKE IP يعلم انتهاك IP ميناء أمن انتهاك انتهاك عنوان IP الثابت التحقق من نطاق IPv6 إستثناء بروتوكول النسخ عن بعد (RCP) فشل إعادة توجيه المسار العكسي للبث الأحادي (RPF)
WK_CPU_Q_SYSTEM_CRITICAL(25)	إرسال إشارات الوسائط/ ARP للوكيل اللاسلكي
WK_CPU_Q_NFL_SAMSAMPLE_DATA(26)	وكيل خدمات الوسائط والبيانات المنمذجة لـ NetFlow (MSP)
WK_CPU_Q_LOW_LATENCY(27)	اكتشاف إعادة التوجيه ثنائي الإتجاه (BFD)، بروتوكول وقت الدقة (PTP)
WK_CPU_Q_EGR_Exception(28)	إستثناء تحليل المخرج
WK_CPU_Q_STACKWISE_VIRTUAL_CONTROL(29)	بروتوكولات التجميع الأمامية، وخاصة SVL
WK_CPU_Q_MCAST_DATA(30)	إنشاء البيانات - (S،G) البيانات - الوصلات المحلية البيانات - تسجيل PIM البيانات - تحويل SPT البيانات - البث المتعدد

قوائم انتظار وحدة المعالجة المركزية (رقم قائمة الانتظار)	الميزة (الميزات)
WK_CPU_Q_GOLD_PKT(31)	ذهب

النهج الافتراضي

بشكل افتراضي، يتم تطبيق سياسة CoPP التي تم إنشاؤها بواسطة النظام على مسار الإدخال/الإخراج. يمكن عرض النهج الافتراضي باستخدام الأوامر المستندة إلى MQC. كما يمكن عرضها ضمن تكوين المحول. السياسة الوحيدة المسموح بتطبيقها هي السياسة التي يحددها النظام.

أستخدم "show policy-map control-plane" لعرض السياسة المطبقة على مستوى التحكم:

```
<#root>

Catalyst-9600#

show policy-map control-plane


Control Plane

 Service-policy input: system-cpp-policy

   Class-map: system-cpp-police-ios-routing (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: none
      police:
          rate 17000 pps, burst 4150 packets
        conformed 95904305 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop

<snip>

   Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

ضبط CoPP

تعدلات واضع سياسات CoPP قابلة للتكوين من قبل المستخدم. يتمتع المستخدمون أيضا بالقدرة على تعطيل قوائم الانتظار.

يوضح هذا المثال كيفية ضبط قيمة واضع السياسات الفردية. في هذا المثال، تكون

الفئة المعدلة هي "التطفل على بروتوكول بروتوكول بروتوكول شرطة النظام."

```
<#root>
Device>
enable

Device#
configure terminal


Device(config)#
policy-map system-cpp-policy

Device(config-pmap)#
Device(config-pmap)#
class system-cpp-police-protocol-snooping

Device(config-pmap-c)#
Device(config-pmap-c)#
police rate 100 pps

Device(config-pmap-c-police)#
Device(config-pmap-c-police)#
exit

Device(config-pmap-c)#
exit

Device(config-pmap)#
exit

Device(config)#
Device(config)#
control-plane

Device(config-cp)#
Device(config)#
control-plane
```

```
Device(config-cp)#
service-policy input system-cpp-policy

Device(config-cp)#
Device(config-cp)#
end

Device#
show policy-map control-plane
```

يوضح هذا المثال كيفية تعطيل قائمة انتظار بالكامل. توخ الحذر عند تعطيل قوائم الانتظار، لأن ذلك قد يؤدي إلى التشبع الزائد المحتمل لوحدة المعالجة المركزية.

```
<#root>
Device>
enable

Device#
configure terminal

Device(config)#
policy-map system-cpp-policy

Device(config-pmap)#
Device(config-pmap)#
class system-cpp-police-protocol-snooping

Device(config-pmap-c)#

Device(config-pmap-c)#
no police rate 100 pps
Device(config-pmap-c)#
end
```

استكشاف الأخطاء وإصلاحها

ةيجهنم

يتأرث إستخدام وحدة المعالجة المركزية بنشاطين أساسيين - العمليات والانقطاع. يتم إنشاء العمليات لتنشيط وحدة المعالجة المركزية أثناء إشارة المقاطعة إلى الجزء التي عارجإلل (CPU) يتم اعتراضها على مستوى البيانات وإرسالها إلى وحدة المعالجة المركزية (CPU). ونظرا لتمكين CoPP وتشكل هذه الأنشطة معا الاستخدام الكلي لوحدة المعالجة المركزية. بشكل افتراضي، فإن تأثير الخدمة باستخدام وحدة المعالجة المركزية المرتفع لوحدة المعالجة المركزية (CPU) بشكل كبير. من المهم النظر في الاستخدام الكلي لوحدة المعالجة المركزية، ولكن الاستخدام الكلي يوري القصة بأكملها. يتم إستخدام أوامر العرض والأدوات المساعدة في هذا القسم لتقييم صحة وحدة المعالجة المركزية (CPU) بسرعة وتحديد التفاصيل ذات الصلة بحركة المرور المرتبطة بوحدة المعالجة المركزية (CPU).

إرشادات:

- حدد ما إذا كانت المشكلة تتعلق بمستوى التحكم. تتم إعادة توجيه معظم حركة مرور النقل في الأجهزة. تتضمن وحدة المعالجة المركزية (CPU) وظائف التحكم في حركة المرور وبعض السيناريوهات، لذلك تذكر هذه الأمر لفترة التحقيق.
- فهم خطة الاستخدام الأساسي. ومن المهم أن نفهم ما يجب عليه الاستخدام العادي حتى يمكن التعرف على الانحرافات عن القاعدة.
- التحقق من الاستخدام الإجمالي لكل من العمليات وحالات المقاطعة. تحديد أي عمليات تشغل كميات غير متوقعة من موارد وحدة المعالجة المركزية. إذا كان الاستخدام خارج النطاق المتوقع، فمن المحتمل أن يكون هذا سببا للقلق. ومن المهم فهم متوسط استخدام النظام، بحيث يتم التعرف على الانحرافات التي تقع خارج القاعدة. تذكر أن استخدام وحدة المعالجة المركزية لا يشير دائما إلى مشكلة، ولكن إذا تم باستكشاف مشكلة متعلقة بـ CoPP وإطلاق دائما بطء حركة مرور يتم تنظيمها بشكل سيئ، فهذا مؤشر قوي على الصلة.

ةديفم رهاظإ رماوأ

يتيح المحول إمكانية الإشراف السريع على صحة وحدة المعالجة المركزية (CPU) وإحصاءات حركة المرور المتطابقة بوحدة المعالجة المركزية (CPU) بسرعة.

تحديد الاستخدام الإجمالي والتاريخي

- تم إستخدام "إظهار عمليات وحدة المعالجة المركزية التي تم فرزها" لعرض إستخدام الانتظار العملية بشكل عام. توفر وسيطة "مفرز" بفرز إخراج وحدة المعالجة المركزية لمعالجة المزيد من الوقت. تكون العمليات التي تستخدم المزيد من وحدة المعالجة المركزية (CPU) في أعلى المخرجات. كما يتم توفير الاستخدام بسبب المقاطعات النسبة المئوية.

<#root>

Catalyst-9600#

show processes cpu sorted

```
CPU utilization for five seconds: 92%/13%; one minute: 76%; five minutes: 73%
```

<<<--- Utilization is displayed for 5 second (both process and interrupt), 1 minute and 5 minute interva

92% refers to the c

The 13% value refer

```
PID Runtime(ms)    Invoked      uSecs   5Sec   1Min   5Min  TTY  Process
```

<<<--- Runtime statistics, as well as utilization averages are displayed here. The process is also ident

```
344   547030523  607054509        901  38.13% 30.61% 29.32%   0  SISF Switcher Th
345   394700227  615024099        641  31.18% 22.68% 21.66%   0  SISF Main Thread
 98   112308516  119818535        937   4.12%  4.76%  5.09%   0  Crimson flush tr
247    47096761   92250875        510   2.42%  2.21%  2.18%   0  Spanning Tree
123    35303496  679878082         51   1.85%  1.88%  1.84%   0  IOSXE-RP Punt Se
234         955       1758        543   1.61%  0.71%  0.23%   3  SSH Process
547     5360168    5484910        977   1.04%  0.46%  0.44%   0  DHCPD Receive
229    27381066  963726156         28   1.04%  1.34%  1.23%   0 IP Input
 79    13183805  108951712        121   0.48%  0.55%  0.55%   0 IOSD ipc task
  9     1073134     315186       3404   0.40%  0.06%  0.03%   0 Check heaps
 37    11099063  147506419         75   0.40%  0.54%  0.52%   0 ARP Input
312     2986160  240782059         12   0.24%  0.12%  0.14%   0 DAI Packet Proce
<snip>
565           0          1          0   0.00%  0.00%  0.00%   0 LICENSE AGENT
566          14       1210         11   0.00%  0.00%  0.00%   0 DHCPD Timer
567          40         45        888   0.00%  0.00%  0.00%   0 OVLD SPA Backgro
568          12       2342          5   0.00%  0.00%  0.00%   0 DHCPD Database
569           0         12          0   0.00%  0.00%  0.00%   0 SpanTree Flush
571           0          1          0   0.00%  0.00%  0.00%   0 EM Action CNS
572         681     140276          4   0.00%  0.00%  0.00%   0 Inline power inc
```

- يوفر "إظهار محفوظات وحدة المعالجة المركزية (CPU)" رسما بيانيا تاريخيا لاستخدام وحدة المعالجة المركزية (CPU) على مدار 60 ثانية و 5 دقائق و 72 ساعة الماضية.

<#root>

```
Catalyst-9600#
```

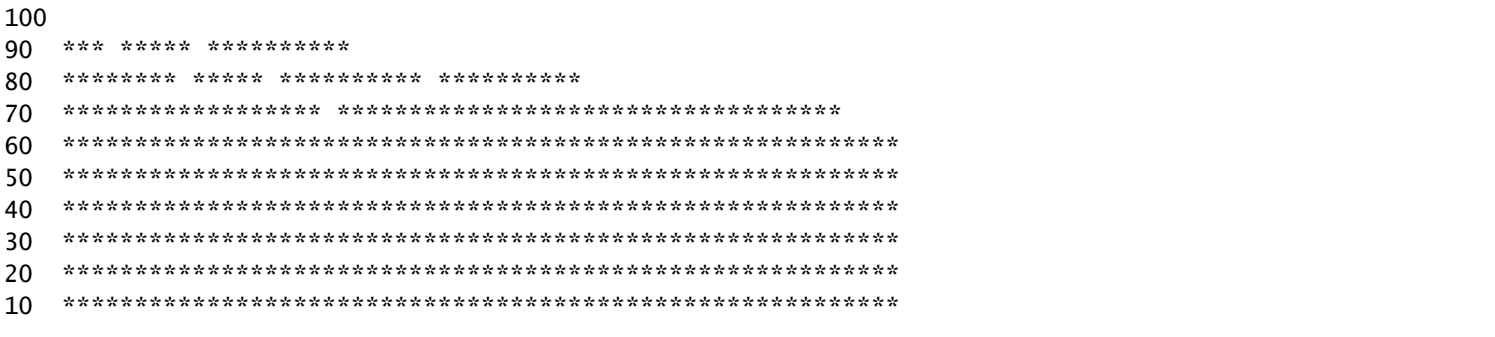
show processes cpu history

```
    999777776666688888666667777777777888887777766666999998888866
```

<<<--- The numbers at the top of each column represent the highest value seen throughout the time period

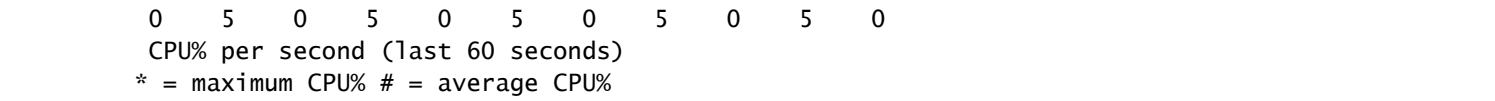
```
    222555559999944444444440000088888888881111177777333335555500
```

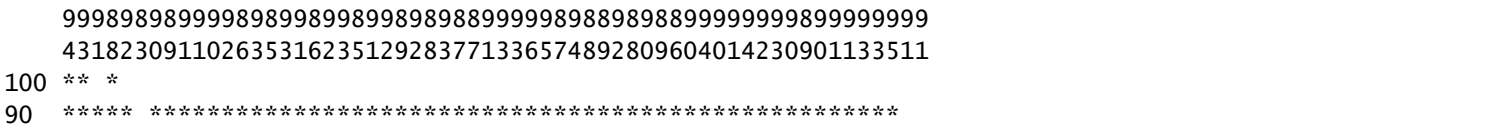
It is read top-down. "9" over "2" in this example means "92%" for example.



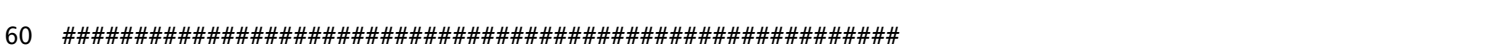
<<<--- The "*" represents the highest value during the given time period. This relates to a momentary sp

In this example, utilization spiked to 92% in the last 5 seconds.

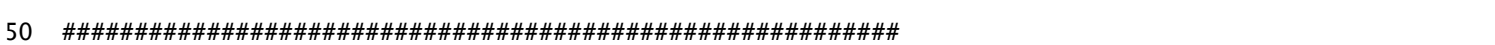




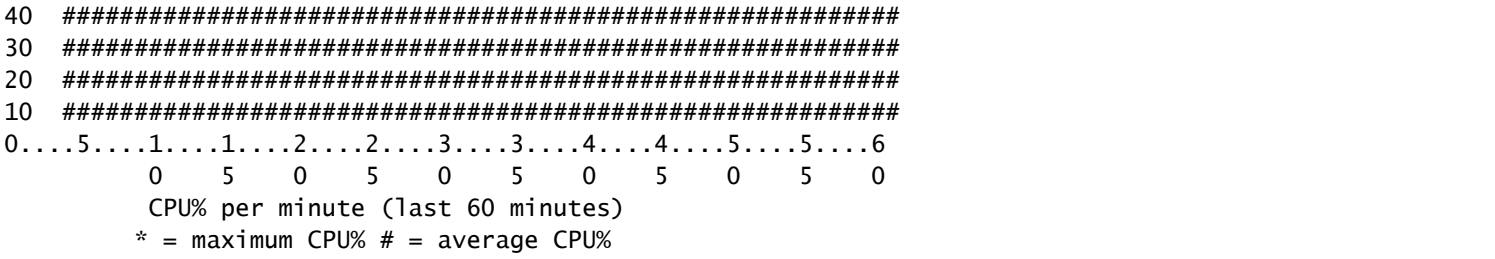
<<<--- The "#" represents the average utilization. This indicates sustained utilization.

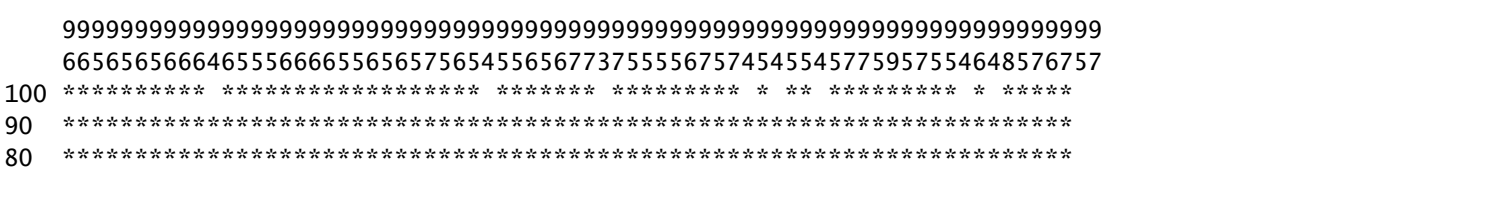


In this example, within the last 5 minutes the average utilization was sustained around 70% while



the maximum utilization spiked to 94%.





```
70  ##########################################################################
60  ##########################################################################
50  ##########################################################################
40  ##########################################################################
30  ##########################################################################
20  ##########################################################################
10  ##########################################################################
0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
          0    5    0    5    0    5    0    5    0    5    0    5    0
               CPU% per hour (last 72 hours)
              * = maximum CPU% # = average CPU%
```

التحقق من تنظيم مستوى التحكم

- أستخدم "show platform hardware fed <switch> حالة قائمة انتظار جودة الخدمة النشطة Active QoS Queue Stats Internal CPU Policy" لعرض إحصائيات CoPP المجمعة والمعلومات الإضافية على بنية قائمة الانتظار/واضع السياسات. يوفر هذا الإخراج طريقة عرض تاريخية لإحصائيات الشرطي منذ آخر إعادة تعيين لمستوى التحكم. هذه العدادات قابلة للمسح يدويا أيضا. وبشكل عام، يشير الدليل على عمليات إسقاط مستوى التحكم بواسطة المنظم إلى مشكلة تتعلق بقائمة الانتظار/الفئة المقترنة، ولكن تأكد من حدوث حالات السقوط بشكل متزايد أثناء حدوث المشكلة. قم بتشغيل الأمر عدة مرات لملاحظة زيادة قيم إسقاط قائمة الانتظار.

<#root>

```
Catalyst9500#

show platform hardware fed active qos queue stats internal cpu policer


                        CPU Queue Statistics
============================================================================================
                                                (default) (set)     Queue         Queue
QId PlcIdx  Queue Name                Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)

<-- The top section of this output gives a historical view of CoPP drops. Run the command several times

--------------------------------------------------------------------------------------------

CPU queues correlate with a Policer Index (PlcIdx) and Queue (QId).

0    11     DOT1X Auth                  Yes     1000      1000     0            0

Note that multiple policer indices map to the same queue for some classes.

1    1      L2 Control                  Yes     2000      2000     0            0
2    14     Forus traffic               Yes     4000      4000     0            0
3    0      ICMP GEN                    Yes     750       750      0            0
4    2      Routing Control             Yes     5500      5500     0            0
5    14     Forus Address resolution    Yes     4000      4000     83027876     1297199
6    0      ICMP Redirect               Yes     750       750      0            0
```

7	16	Inter FED Traffic	Yes	2000	2000	0	0
8	4	L2 LVX Cont Pack	Yes	1000	1000	0	0
9	19	EWLC Control	Yes	13000	13000	0	0
10	16	EWLC Data	Yes	2000	2000	0	0
11	13	L2 LVX Data Pack	Yes	1000	1000	0	0
12	0	BROADCAST	Yes	750	750	0	0
13	10	Openflow	Yes	250	250	0	0
14	13	Sw forwarding	Yes	1000	1000	0	0
15	8	Topology Control	Yes	13000	16000	0	0
16	12	Proto Snooping	Yes	2000	2000	0	0
17	6	DHCP Snooping	Yes	500	500	0	0
18	13	Transit Traffic	Yes	1000	1000	0	0
19	10	RPF Failed	Yes	250	250	0	0
20	15	MCAST END STATION	Yes	2000	2000	0	0
21	13	LOGGING	Yes	1000	1000	769024	12016
22	7	Punt Webauth	Yes	1000	1000	0	0
23	18	High Rate App	Yes	13000	13000	0	0
24	10	Exception	Yes	250	250	0	0
25	3	System Critical	Yes	1000	1000	0	0
26	10	NFL SAMPLED DATA	Yes	250	250	0	0
27	2	Low Latency	Yes	5500	5500	0	0
28	10	EGR Exception	Yes	250	250	0	0
29	5	Stackwise Virtual OOB	Yes	8000	8000	0	0
30	9	MCAST Data	Yes	500	500	0	0
31	3	Gold Pkt	Yes	1000	1000	0	0

* NOTE: CPU queue policer rates are configured to the closest hardware supported value

CPU Queue Policer Statistics

Policer Index	Policer Accept Bytes	Policer Accept Frames	Policer Drop Bytes	Policer Drop Frames
0	59894	613	0	0
1	15701689	57082	0	0
2	5562892	63482	0	0
3	3536	52	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	2347194476	32649666	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	577043	8232	769024	12016
14	719225176	11182355	83027876	1297199
15	132766	1891	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0

Second Level Policer Statistics

<-- Second level policer information begins here. Catalyst CoPP is organized with two policers to allow

20	2368459057	32770230	0	0
21	719994879	11193091	0	0

Policer Index Mapping and Settings

```
-----------------------------------------------------------------
level-2   :   level-1                     (default)   (set)
PlcIndex  :   PlcIndex                      rate      rate
-----------------------------------------------------------------
20        :   1  2  8                       13000     17000
21        :   0 4 7 9 10 11 12 13 14 15      6000      6000
=================================================================

               Second Level Policer Config
=================================================================
    level-1 level-2                             level-2
QId PlcIdx  PlcIdx  Queue Name                  Enabled
-----------------------------------------------------------------
0    11      21      DOT1X Auth                   Yes
1    1       20      L2 Control                   Yes
2    14      21      Forus traffic                Yes
3    0       21      ICMP GEN                     Yes
4    2       20      Routing Control              Yes
5    14      21      Forus Address resolution     Yes
6    0       21      ICMP Redirect                Yes
7    16      -       Inter FED Traffic            No
8    4       21      L2 LVX Cont Pack             Yes
9    19      -       EWLC Control                 No
10   16      -       EWLC Data                    No
11   13      21      L2 LVX Data Pack             Yes
12   0       21      BROADCAST                    Yes
13   10      21      Openflow                     Yes
14   13      21      Sw forwarding                Yes
15   8       20      Topology Control             Yes
16   12      21      Proto Snooping               Yes
17   6       -       DHCP Snooping                No
18   13      21      Transit Traffic              Yes
19   10      21      RPF Failed                   Yes
20   15      21      MCAST END STATION            Yes
21   13      21      LOGGING                      Yes
22   7       21      Punt Webauth                 Yes
23   18      -       High Rate App                No
24   10      21      Exception                    Yes
25   3       -       System Critical              No
26   10      21      NFL SAMPLED DATA             Yes
27   2       20      Low Latency                  Yes
28   10      21      EGR Exception                Yes
29   5       -       Stackwise Virtual OOB        No
30   9       21      MCAST Data                   Yes
31   3       -       Gold Pkt                     No

                        CPP Classes to queue map

<-- Information on how different traffic types map to different queues are found here.
=================================================================================

PlcIdx CPP Class                                 :  Queues
---------------------------------------------------------------------------------
0      system-cpp-police-data                    :  ICMP GEN/ BROADCAST/ ICMP Redirect/
10     system-cpp-police-sys-data                :  Openflow/ Exception/ EGR Exception/ NFL SAMPLED DATA/
13     system-cpp-police-sw-forward              :  Sw forwarding/ LOGGING/ L2 LVX Data Pack/ Transit Tra
9      system-cpp-police-multicast               :  MCAST Data/
15     system-cpp-police-multicast-end-station   :  MCAST END STATION /
7      system-cpp-police-punt-webauth            :  Punt Webauth/
1      system-cpp-police-l2-control              :  L2 Control/
2      system-cpp-police-routing-control         :  Routing Control/ Low Latency/
3      system-cpp-police-system-critical         :  System Critical/ Gold Pkt/
4      system-cpp-police-l2lvx-control           :  L2 LVX Cont Pack/
```

```
8      system-cpp-police-topology-control       :  Topology Control/
11     system-cpp-police-dot1x-auth             :  DOT1X Auth/
12     system-cpp-police-protocol-snooping      :  Proto Snooping/
6      system-cpp-police-dhcp-snooping          :  DHCP Snooping/
14     system-cpp-police-forus                  :  Forus Address resolution/ Forus traffic/
5      system-cpp-police-stackwise-virt-control :  Stackwise Virtual OOB/
16     system-cpp-default                       :  Inter FED Traffic/ EWLC Data/
18     system-cpp-police-high-rate-app          :  High Rate App/
19     system-cpp-police-ewlc-control           :  EWLC Control/
20     system-cpp-police-ios-routing            :  L2 Control/ Topology Control/ Routing Control/ Low La
21     system-cpp-police-ios-feature            :  ICMP GEN/ BROADCAST/ ICMP Redirect/ L2 LVX Cont Pack/
```

جمع المعلومات عن حركة المرور الخادعة

يتم إستخدام هذه الأوامر لتجميع المعلومات حول حركة المرور التي يتم انتقاؤها إلى وحدة المعالجة المركزية، بما في ذلك نوع حركة المرور والنطاق المادية للدخول.

- "يمكن إستخدام show platform software الذي تم تغذيته <switch> نشط cpuq all" أو show platform software الذي تم تغذيته <switch> نشط <0-31> قائمة انتظار "<عرض المعلومات الإحصائية المتعلقة بكل قائمة انتظار وحدة المعالجة المركزية (CPU) أو الخاصة بها.

<#root>

```
C9300#

show platform software fed switch active punt cpuq all

Punt CPU Q Statistics
============================================

CPU Q Id                        : 0
CPU Q Name                      : CPU_Q_DOT1X_AUTH
Packets received from ASIC      : 964
Send to IOSd total attempts     : 964
Send to IOSd failed count       : 0
RX suspend count                : 0
RX unsuspend count              : 0
RX unsuspend send count         : 0
RX unsuspend send failed count  : 0
RX consumed count               : 0
RX dropped count                : 0
RX non-active dropped count     : 0
RX conversion failure dropped   : 0
RX INTACK count                 : 964
RX packets dq'd after intack    : 0
Active RxQ event                : 964
RX spurious interrupt           : 0
RX phy_idb fetch failed: 0
RX table_id fetch failed: 0
RX invalid punt cause: 0

CPU Q Id                        : 1
CPU Q Name                      : CPU_Q_L2_CONTROL
Packets received from ASIC      : 80487
```

```
Send to IOSd total attempts    : 80487
Send to IOSd failed count      : 0
RX suspend count               : 0
RX unsuspend count             : 0
RX unsuspend send count        : 0
RX unsuspend send failed count : 0
RX consumed count              : 0
RX dropped count               : 0
RX non-active dropped count    : 0
RX conversion failure dropped  : 0
RX INTACK count                : 80474
RX packets dq'd after intack   : 16
Active RxQ event               : 80474
RX spurious interrupt          : 9
RX phy_idb fetch failed: 0
RX table_id fetch failed: 0
RX invalid punt cause: 0

CPU Q Id                       : 2
CPU Q Name                     : CPU_Q_FORUS_TRAFFIC
Packets received from ASIC     : 176669
Send to IOSd total attempts    : 176669
Send to IOSd failed count      : 0
RX suspend count               : 0
RX unsuspend count             : 0
RX unsuspend send count        : 0
RX unsuspend send failed count : 0
RX consumed count              : 0
RX dropped count               : 0
RX non-active dropped count    : 0
RX conversion failure dropped  : 0
RX INTACK count                : 165584
RX packets dq'd after intack   : 12601
Active RxQ event               : 165596
RX spurious interrupt          : 11851
RX phy_idb fetch failed: 0
RX table_id fetch failed: 0
RX invalid punt cause: 0
<snip>

C9300#
```

show platform software fed switch active punt cpuq 16 <-- Queue ID 16 correlates with Protocol Snooping.

```
Punt CPU Q Statistics
=============================================

CPU Q Id                       : 16
CPU Q Name                     : CPU_Q_PROTO_SNOOPING
Packets received from ASIC     : 55661
Send to IOSd total attempts    : 55661
Send to IOSd failed count      : 0
RX suspend count               : 0
RX unsuspend count             : 0
RX unsuspend send count        : 0
RX unsuspend send failed count : 0
RX consumed count              : 0
RX dropped count               : 0
RX non-active dropped count    : 0
RX conversion failure dropped  : 0
RX INTACK count                : 55659
RX packets dq'd after intack   : 9
Active RxQ event               : 55659
```

```
RX spurious interrupt          : 23
RX phy_idb fetch failed: 0
RX table_id fetch failed: 0
RX invalid punt cause: 0

Replenish Stats for all rxq:
----------------------------------------
Number of replenish            : 4926842
Number of replenish suspend    : 0
Number of replenish un-suspend : 0
----------------------------------------
```

- أستخدم "show platform software fed <switch> active punt cause summary" للحصول على نظرة سريعة على جميع أنواع حركة المرور المختلفة التي تم رؤيتها في وحدة المعالجة المركزية. لاحظ أنه يتم عرض الأسباب غير الصفر فقط.

<#root>

```
C9300#

show platform software fed switch active punt cause summary

Statistics for all causes

Cause  Cause Info                          Rcvd                 Dropped
--------------------------------------------------------------------------------
7      ARP request or response             142962               0
11     For-us data                         490817               0
21     RP<->QFP keepalive                  448742               0
24     Glean adjacency                     2                    0
55     For-us control                      415222               0
58     Layer2 bridge domain data packe     3654659              0
60     IP subnet or broadcast packet       37167                0
75     EPC                                 17942                0
96     Layer2 control protocols            358614               0
97     Packets to LFTS                     964                  0
109    snoop packets                       48867                0
--------------------------------------------------------------------------------
```

- أستخدم الأمر "show platform software الذي تم تغذيته <switch> واجهات أسعار الحزم النشطة" لعرض حركة مرور البيانات المرتبطة بوحدة المعالجة المركزية (CPU) للواجهات بسرعة فائقة على النظام. يظهر هذا الأمر فقط الواجهات مع قائمة انتظار إدخال غير صفرية.

<#root>

```
C9300#

show platform software fed switch active punt rates interfaces

Punt Rate on Interfaces Statistics

Packets per second averaged over 10 seconds, 1 min and 5 mins
================================================================================
```

```
                              |           |  Recv |  Recv |  Recv |  Drop |  Drop  |  Drop
 Interface Name               |  IF_ID    |  10s  |  1min |  5min |  10s  |  1min  |  5min
==============================================================================================
 TenGigabitEthernet1/0/2       0x0000000a       5       5       5       0       0       0
 TenGigabitEthernet1/0/23      0x0000001f       1       1       1       0       0       0

----------------------------------------------------------------------------------------------
```

- أستخدم "show platform software fed <switch> واجهات <IF-ID> النشطة لمعدلات الخصم" للتنقل لأسفل وعرض قوائم الانتظار الفردية للواجهة. يوضح هذا الأمر إحصائيات التجميع ويمكن إستخدامه لعرض نشاط قائمة انتظار الإدخال التاريخي وإذا تم تنظيم حركة مرور البيانات.

<#root>

```
C9300#

show platform software fed switch active punt rates interfaces 0x1f <-- "0x1f" is the IF_ID of Te1/0/23,

Punt Rate on Single Interfaces Statistics

Interface : TenGigabitEthernet1/0/23 [if_id: 0x1F]

  Received                          Dropped
  --------                          -------
   Total          : 1010652          Total           : 0
   10 sec average : 1                10 sec average  : 0
    1 min average : 1                 1 min average  : 0
    5 min average : 1                 5 min average  : 0

Per CPUQ punt stats on the interface (rate averaged over 10s interval)
=============================================================================
 Q  |         Queue                  |  Recv   |  Recv  |  Drop  |  Drop  |
 no |         Name                   |  Total  |  Rate  |  Total |  Rate  |
=============================================================================
 0   CPU_Q_DOT1X_AUTH                        0        0        0        0
 1   CPU_Q_L2_CONTROL                     9109        0        0        0
 2   CPU_Q_FORUS_TRAFFIC                176659        0        0        0
 3   CPU_Q_ICMP_GEN                          0        0        0        0
 4   CPU_Q_ROUTING_CONTROL              447374        0        0        0
 5   CPU_Q_FORUS_ADDR_RESOLUTION         80693        0        0        0
 6   CPU_Q_ICMP_REDIRECT                     0        0        0        0
 7   CPU_Q_INTER_FED_TRAFFIC                 0        0        0        0
 8   CPU_Q_L2LVX_CONTROL_PKT                 0        0        0        0
 9   CPU_Q_EWLC_CONTROL                      0        0        0        0
 10  CPU_Q_EWLC_DATA                         0        0        0        0
 11  CPU_Q_L2LVX_DATA_PKT                    0        0        0        0
 12  CPU_Q_BROADCAST                     22680        0        0        0
 13  CPU_Q_CONTROLLER_PUNT                   0        0        0        0
 14  CPU_Q_SW_FORWARDING                     0        0        0        0
 15  CPU_Q_TOPOLOGY_CONTROL             271014        0        0        0
 16  CPU_Q_PROTO_SNOOPING                    0        0        0        0
 17  CPU_Q_DHCP_SNOOPING                     0        0        0        0
 18  CPU_Q_TRANSIT_TRAFFIC                   0        0        0        0
 19  CPU_Q_RPF_FAILED                        0        0        0        0
 20  CPU_Q_MCAST_END_STATION_SERVICE      2679        0        0        0
 21  CPU_Q_LOGGING                         444        0        0        0
 22  CPU_Q_PUNT_WEBAUTH                      0        0        0        0
```

```
 23  CPU_Q_HIGH_RATE_APP                0        0        0        0
 24  CPU_Q_EXCEPTION                    0        0        0        0
 25  CPU_Q_SYSTEM_CRITICAL              0        0        0        0
 26  CPU_Q_NFL_SAMPLED_DATA             0        0        0        0
 27  CPU_Q_LOW_LATENCY                  0        0        0        0
 28  CPU_Q_EGR_EXCEPTION                0        0        0        0
 29  CPU_Q_FSS                          0        0        0        0
 30  CPU_Q_MCAST_DATA                   0        0        0        0
 31  CPU_Q_GOLD_PKT                     0        0        0        0

----------------------------------------------------------------------
```

فحص حركة مرور وحدة المعالجة المركزية (CPU) المرتبطة

توفر مجموعة المحولات Catalyst 9000 أدوات مساعدة لمراقبة حركة مرور البيانات المرتبطة بوحدة المعالجة المركزية (CPU) وعرضها. أستخدم هذه الأدوات لفهم حركة المرور التي يتم ضربها إلى وحدة المعالجة المركزية (CPU) بشكل فعال.

التقاط الحزمة المضمنة (EPC)

يمكن عمل EPC على مستوى التحكم في أي من الإتجاهين (أو كليهما). لحركة المرور المرور المضمنة، قم بالتقاط الوارد. يمكن حفظ EPC على مستوى التحكم في المخزن المؤقت أو في الملف.

<#root>

```
C9300#

monitor capture CONTROL control-plane in match any buffer circular size 10


C9300#

show monitor capture CONTROL parameter <-- Check to ensure parameters are as expected.

   monitor capture CONTROL control-plane IN
   monitor capture CONTROL match any
   monitor capture CONTROL buffer size 10 circular
C9300#

monitor capture CONTROL start <-- Starts the capture.

Started capture point : CONTROL
C9300#

monitor capture CONTROL stop <-- Stops the capture.

Capture statistics collected at software:
    Capture duration - 5 seconds
    Packets received - 39
    Packets dropped - 0
    Packets oversized - 0

Bytes dropped in asic - 0

Capture buffer will exists till exported or cleared
```

```
Stopped capture point : CONTROL
```

يمكن عرض نتائج الالتقاط في مخرجات قصيرة أو مفصلة.

<#root>

```
C9300#

show monitor capture CONTROL buffer brief

Starting the packet display ........ Press Ctrl + Shift + 6 to exit

    1   0.000000 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
    2   0.030643 00:00:00:00:00:00 -> 00:06:df:f7:20:01 0x0000 30 Ethernet II
    3   0.200016 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
    4   0.400081 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
    5   0.599962 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
    6   0.800067 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
    7   0.812456 00:1b:0d:a5:e2:a5 -> 01:80:c2:00:00:00 STP 60 RST. Root = 0/10/00:1b:53:bb:91:00  Cost
    8   0.829809 10.122.163.3 -> 224.0.0.2    HSRP 92 Hello (state Active)
    9   0.981313 10.122.163.2 -> 224.0.0.13   PIMv2 72 Hello
   10   1.004747 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
   11   1.200082 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
   12   1.399987 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
   13   1.599944 5c:5a:c7:61:4c:5f -> 00:00:04:00:0e:00 ARP 64 192.168.10.1 is at 5c:5a:c7:61:4c:5f
<snip>

C9300#

show monitor capture CONTROL buffer detail | begin Frame 7

Frame 7: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface /tmp/epc_ws/wif_to_ts_p
    Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe)
        Interface name: /tmp/epc_ws/wif_to_ts_pipe
    Encapsulation type: Ethernet (1)
    Arrival Time: May  3, 2023 23:58:11.727432000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1683158291.727432000 seconds
    [Time delta from previous captured frame: 0.012389000 seconds]
    [Time delta from previous displayed frame: 0.012389000 seconds]
    [Time since reference or first frame: 0.812456000 seconds]
    Frame Number: 7
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:llc:stp]
IEEE 802.3 Ethernet
    Destination: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
        Address: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: 00:1b:0d:a5:e2:a5 (00:1b:0d:a5:e2:a5)
        Address: 00:1b:0d:a5:e2:a5 (00:1b:0d:a5:e2:a5)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Length: 39
    Padding: 00000000000000
Logical-Link Control
```

```
    DSAP: Spanning Tree BPDU (0x42)
        0100 001. = SAP: Spanning Tree BPDU
        .... ...0 = IG Bit: Individual
    SSAP: Spanning Tree BPDU (0x42)
        0100 001. = SAP: Spanning Tree BPDU
        .... ...0 = CR Bit: Command
    Control field: U, func=UI (0x03)
        000. 00.. = Command: Unnumbered Information (0x00)
        .... ..11 = Frame type: Unnumbered frame (0x3)
Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Rapid Spanning Tree (2)
    BPDU Type: Rapid/Multiple Spanning Tree (0x02)
    BPDU flags: 0x3c, Forwarding, Learning, Port Role: Designated
        0... .... = Topology Change Acknowledgment: No
        .0.. .... = Agreement: No
        ..1. .... = Forwarding: Yes
        ...1 .... = Learning: Yes
        .... 11.. = Port Role: Designated (3)
        .... ..0. = Proposal: No
        .... ...0 = Topology Change: No
    Root Identifier: 0 / 10 / 00:1b:53:bb:91:00
        Root Bridge Priority: 0
        Root Bridge System ID Extension: 10
        Root Bridge System ID: 00:1b:53:bb:91:00 (00:1b:53:bb:91:00)
    Root Path Cost: 19
    Bridge Identifier: 32768 / 10 / 00:1b:0d:a5:e2:80
        Bridge Priority: 32768
        Bridge System ID Extension: 10
        Bridge System ID: 00:1b:0d:a5:e2:80 (00:1b:0d:a5:e2:80)
    Port identifier: 0x8025
    Message Age: 1
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
    Version 1 Length: 0

C9300#

monitor capture CONTROL buffer display-filter "frame.number==9" detailed <-- Most Wireshark display filt

Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 9: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface /tmp/epc_ws/wif_to_ts_p
    Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe)
        Interface name: /tmp/epc_ws/wif_to_ts_pipe
    Encapsulation type: Ethernet (1)
    Arrival Time: May  4, 2023 00:07:44.912567000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1683158864.912567000 seconds
    [Time delta from previous captured frame: 0.123942000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.399996000 seconds]
    Frame Number: 9
    Frame Length: 64 bytes (512 bits)
    Capture Length: 64 bytes (512 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:vlan:ethertype:arp]
Ethernet II, Src: 5c:5a:c7:61:4c:5f (5c:5a:c7:61:4c:5f), Dst: 00:00:04:00:0e:00 (00:00:04:00:0e:00)
    Destination: 00:00:04:00:0e:00 (00:00:04:00:0e:00)
        Address: 00:00:04:00:0e:00 (00:00:04:00:0e:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
```

```
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 5c:5a:c7:61:4c:5f (5c:5a:c7:61:4c:5f)
        Address: 5c:5a:c7:61:4c:5f (5c:5a:c7:61:4c:5f)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0000 1010 = ID: 10
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000
    Trailer: 00000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 5c:5a:c7:61:4c:5f (5c:5a:c7:61:4c:5f)
    Sender IP address: 192.168.10.1
    Target MAC address: 00:00:04:00:0e:00 (00:00:04:00:0e:00)
    Target IP address: 192.168.10.25
```

يمكن كتابة نتائج الالتقاط مباشرة إلى الملف، أو تصديرها من المخزن المؤقت.

```
<#root>

C9300#

monitor capture CONTROL export location flash:control.pcap <-- Exports the current buffer to file. Exter

Export Started Successfully

Export completed for capture point CONTROL
C9300#
C9300#

dir flash: | in control.pcap

475231  -rw-             3972   May 4 2023 00:00:38 +00:00  control.pcap
C9300#
```

التقاط حزمة وحدة المعالجة المركزية (CPU) من Fed

تدعم مجموعة المحولات Catalyst 9000 أداة مساعدة لتصحيح الأخطاء تتيح إمكانية رؤية محسنة للحزم إلى وحدة المعالجة المركزية (CPU) ومنها.

```
C9300#debug platform software fed switch active punt packet-capture ?
  buffer        Configure packet capture buffer
  clear-filter  Clear punt PCAP filter
  set-filter    Specify wireshark like filter (Punt PCAP)
  start         Start punt packet capturing
```

```
  stop          Stop punt packet capturing

C9300#$re fed switch active punt packet-capture buffer limit 16384
Punt PCAP buffer configure: one-time with buffer size 16384...done

C9300#show platform software fed switch active punt packet-capture status
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 0 packets. Capture capacity : 16384 packets

C9300#debug platform software fed switch active punt packet-capture start
Punt packet capturing started.

C9300#debug platform software fed switch active punt packet-capture stop
Punt packet capturing stopped. Captured 55 packet(s)
```

تحتوي محتويات المخزن المؤقت على خيارات مختصرة ومفصلة للمخرجات.

```
<#root>

C9300#

show platform software fed switch active punt packet-capture brief

Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 55 packets. Capture capacity : 16384 packets

------ Punt Packet Number: 1, Timestamp: 2023/05/04 00:17:41.709 ------
 interface : physical: TenGigabitEthernet1/0/2[if-id: 0x0000000a], pal: TenGigabitEthernet1/0/2 [if-id:
 metadata  : cause: 109 [snoop packets], sub-cause: 1, q-no: 16, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 0000.0400.0e00, src mac: 5c5a.c761.4c5f
 ether hdr : vlan: 10, ethertype: 0x8100

------ Punt Packet Number: 2, Timestamp: 2023/05/04 00:17:41.909 ------
 interface : physical: TenGigabitEthernet1/0/2[if-id: 0x0000000a], pal: TenGigabitEthernet1/0/2 [if-id:
 metadata  : cause: 109 [snoop packets], sub-cause: 1, q-no: 16, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 0000.0400.0e00, src mac: 5c5a.c761.4c5f
 ether hdr : vlan: 10, ethertype: 0x8100

------ Punt Packet Number: 3, Timestamp: 2023/05/04 00:17:42.109 ------
 interface : physical: TenGigabitEthernet1/0/2[if-id: 0x0000000a], pal: TenGigabitEthernet1/0/2 [if-id:
 metadata  : cause: 109 [snoop packets], sub-cause: 1, q-no: 16, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 0000.0400.0e00, src mac: 5c5a.c761.4c5f
 ether hdr : vlan: 10, ethertype: 0x8100

------ Punt Packet Number: 4, Timestamp: 2023/05/04 00:17:42.309 ------
 interface : physical: TenGigabitEthernet1/0/2[if-id: 0x0000000a], pal: TenGigabitEthernet1/0/2 [if-id:
 metadata  : cause: 109 [snoop packets], sub-cause: 1, q-no: 16, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 0000.0400.0e00, src mac: 5c5a.c761.4c5f
 ether hdr : vlan: 10, ethertype: 0x8100

------ Punt Packet Number: 5, Timestamp: 2023/05/04 00:17:42.509 ------
 interface : physical: TenGigabitEthernet1/0/2[if-id: 0x0000000a], pal: TenGigabitEthernet1/0/2 [if-id:
 metadata  : cause: 109 [snoop packets], sub-cause: 1, q-no: 16, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 0000.0400.0e00, src mac: 5c5a.c761.4c5f
 ether hdr : vlan: 10, ethertype: 0x8100

C9300#

show platform software fed switch active punt packet-capture detailed <-- Detailed provides the same inf
```

```
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 55 packets. Capture capacity : 16384 packets

------ Punt Packet Number: 1, Timestamp: 2023/05/04 00:17:41.709 ------
 interface : physical: TenGigabitEthernet1/0/2[if-id: 0x0000000a], pal: TenGigabitEthernet1/0/2 [if-id:
 metadata  : cause: 109 [snoop packets], sub-cause: 1, q-no: 16, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 0000.0400.0e00, src mac: 5c5a.c761.4c5f
 ether hdr : vlan: 10, ethertype: 0x8100

 Packet Data Hex-Dump (length: 68 bytes) :
   000004000E005C5A  C7614C5F8100000A  0806000108000604  00025C5AC7614C5F
   C0A80A0100000400  0E00C0A80A190000  0000000000000000  0000000000000000
   E9F1C9F3

 Doppler Frame Descriptor :
   fdFormat                  = 0x4           systemTtl                 = 0xe
   loadBalHash1              = 0x20          loadBalHash2              = 0xc
   spanSessionMap            = 0             forwardingMode            = 0
   destModIndex              = 0             skipIdIndex               = 0
   srcGpn                    = 0x2           qosLabel                  = 0x83
   srcCos                    = 0             ingressTranslatedVlan     = 0x7
   bpdu                      = 0             spanHistory               = 0
   sgt                       = 0             fpeFirstHeaderType        = 0
   srcVlan                   = 0xa           rcpServiceId              = 0x1
   wccpSkip                  = 0             srcPortLeIndex            = 0x1
   cryptoProtocol            = 0             debugTagId                = 0
   vrfId                     = 0             saIndex                   = 0
   pendingAfdLabel           = 0             destClient                = 0x1
   appId                     = 0             finalStationIndex         = 0x74
   decryptSuccess            = 0             encryptSuccess            = 0
   rcpMiscResults            = 0             stackedFdPresent          = 0
   spanDirection             = 0             egressRedirect            = 0
   redirectIndex             = 0             exceptionLabel            = 0
   destGpn                   = 0             inlineFd                  = 0x1
   suppressRefPtrUpdate      = 0             suppressRewriteSideEfects = 0
   cmi2                      = 0             currentRi                 = 0x1
   currentDi                 = 0x527b        dropIpUnreachable         = 0
   srcZoneId                 = 0             srcAsicId                 = 0
   originalDi                = 0             originalRi                = 0
   srcL3IfIndex              = 0x27          dstL3IfIndex              = 0
   dstVlan                   = 0             frameLength               = 0x44
   fdCrc                     = 0x97          tunnelSpokeId             = 0
   isPtp                     = 0             ieee1588TimeStampValid    = 0
   ieee1588TimeStamp55_48    = 0             lvxSourceRlocIpAddress    = 0
   sgtCachingNeeded          = 0

 Doppler Frame Descriptor Hex-Dump :
   0000000044004E04  000B40977B520000  0000000000000100  000000070A000000
   0000000001000010  0000000074000100  0000000027830200  0000000000000000
```

العديد من عوامل تصفية العرض متاحة للاستخدام. يتم دعم عوامل تصفية عرض Wireshark الأكثر شيوعا.

<#root>

C9300#

show platform software fed switch active punt packet-capture display-filter-help

```
FED Punject specific filters :
   1. fed.cause              FED punt or inject cause
   2. fed.linktype           FED linktype
   3. fed.pal_if_id          FED platform interface ID
   4. fed.phy_if_id          FED physical interface ID
   5. fed.queue              FED Doppler hardware queue
   6. fed.subcause           FED punt or inject sub cause
Generic filters supported :
   7. arp                    Is this an ARP packet
   8. bootp                  DHCP packets [Macro]
   9. cdp                    Is this a CDP packet
  10. eth                    Does the packet have an Ethernet header
  11. eth.addr               Ethernet source or destination MAC address
  12. eth.dst                Ethernet destination MAC address
  13. eth.ig                 IG bit of ethernet destination address (broadcast/multicast)
  14. eth.src                Ethernet source MAC address
  15. eth.type               Ethernet type
  16. gre                    Is this a GRE packet
  17. icmp                   Is this a ICMP packet
  18. icmp.code              ICMP code
  19. icmp.type              ICMP type
  20. icmpv6                 Is this a ICMPv6 packet
  21. icmpv6.code            ICMPv6 code
  22. icmpv6.type            ICMPv6 type
  23. ip                     Does the packet have an IPv4 header
  24. ip.addr                IPv4 source or destination IP address
  25. ip.dst                 IPv4 destination IP address
  26. ip.flags.df            IPv4 dont fragment flag
  27. ip.flags.mf            IPv4 more fragments flag
  28. ip.frag_offset         IPv4 fragment offset
  29. ip.proto               Protocol used in datagram
  30. ip.src                 IPv4 source IP address
  31. ip.ttl                 IPv4 time to live
  32. ipv6                   Does the packet have an IPv4 header
  33. ipv6.addr              IPv6 source or destination IP address
  34. ipv6.dst               IPv6 destination IP address
  35. ipv6.hlim              IPv6 hop limit
  36. ipv6.nxt               IPv6 next header
  37. ipv6.plen              IPv6 payload length
  38. ipv6.src               IPv6 source IP address
  39. stp                    Is this a STP packet
  40. tcp                    Does the packet have a TCP header
  41. tcp.dstport            TCP destination port
  42. tcp.port               TCP source OR destination port
  43. tcp.srcport            TCP source port
  44. udp                    Does the packet have a UDP header
  45. udp.dstport            UDP destination port
  46. udp.port               UDP source OR destination port
  47. udp.srcport            UDP source port
  48. vlan.id                Vlan ID (dot1q or qinq only)
  49. vxlan                  Is this a VXLAN packet


C9300#
```

show platform software fed switch active punt packet-capture display-filter arp brief

```
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 55 packets. Capture capacity : 16384 packets

------ Punt Packet Number: 1, Timestamp: 2023/05/04 00:17:41.709 ------
 interface : physical: TenGigabitEthernet1/0/2[if-id: 0x0000000a], pal: TenGigabitEthernet1/0/2 [if-id:
 metadata  : cause: 109 [snoop packets], sub-cause: 1, q-no: 16, linktype: MCP_LINK_TYPE_IP [1]
```

```
 ether hdr : dest mac: 0000.0400.0e00, src mac: 5c5a.c761.4c5f
 ether hdr : vlan: 10, ethertype: 0x8100

------ Punt Packet Number: 2, Timestamp: 2023/05/04 00:17:41.909 ------
 interface : physical: TenGigabitEthernet1/0/2[if-id: 0x0000000a], pal: TenGigabitEthernet1/0/2 [if-id:
 metadata  : cause: 109 [snoop packets], sub-cause: 1, q-no: 16, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 0000.0400.0e00, src mac: 5c5a.c761.4c5f
 ether hdr : vlan: 10, ethertype: 0x8100
<snip>
```

يمكن تطبيق المرشحات كمرشحات التقاط، كذلك.

```
<#root>

C9300#

show platform software fed switch active punt packet-capture set-filter arp <-- Most common Wireshark fi

Filter setup successful. Captured packets will be cleared

C9300#$e fed switch active punt packet-capture status
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 0 packets. Capture capacity : 16384 packets
Capture filter : "arp"
```

السيناريوهات الشائعة

فقدان ICMP (Ping) المتقطع لبروتوكول الإنترنت (IP) المحلي

يتم توجيه حركة المرور التي تتم إعادة توجيهها إلى IP محلي على محول ما في قائمة انتظار مزحم Forus CoPP (والتي تعني حرفيا "لان"). ترتبط زيادة في قائمة انتظار Forus CoPP بالحزم المسقطة الموجهة للمحول المحلي. وهذا الأمر مباشر إلى الأمام نسبيا وسهل التصور.

ولكن، في بعض الحالات، يمكن أن تكون هناك خسارة لحركة المرور المحلية التي لا ترتبط إرتباطا وثيقا بحيرات الفورس.

عم تدفق حركة مرور كافي مرتبط بوحدة المعالجة المركزية، يصبح مسار الحزم زائدا عن الحد مما يؤدي إلى قدرة CoPP على تحديد أولوية حركة المرور التي يتم تنظيمها. يتم تنظيم حركة المرور "بصمت" على أساس الإدخال الأول والإخراج الأول.

في هذا السيناريو، يتم مشاهدة الأدلة على تنظيم مستوى التحكم بكميات كبيرة، ولكن عون حركة المرور موضع الاهتمام (Forus في هذا المثال) ال يتزايد بالضرورة.

وباختصار، إذا كان هناك حجم كبير بشكل إستثنائي لحركة مرور البيانات المرتبطة بوحدة المعالجة المركزية (CPU)، والتي يتم إثباتها بواسطة تنظيم CoPP النشط ويتم عرضها باستخدام التقاط الحزمة أو تصحيح أخطاء FED Punt، فقد يكون هناك فقد ال تتم محاذاته إلى قائمة الانتظار التي تقوم باستكشاف الأخطاء وإصلاحها. في هذا السيناريو، حدد سبب وجود كمية مفرطة من حركة المرور المرتبطة بوحدة المعالجة المركزية (CPU) واتخذ التدابير اللازمة لتخفيف العبء على مستوى التحكم.

عمليات إعادة توجيه ICMP عالية وعملية DHCP بطيئة

يتم تنظيم CoPP على المحول Catalyst 9000 series switch في 32 قائمة انتظار أجهزة. وتتوافق قوائم انتظار الأجهزة هذه التي يبلغ عددها 32 قائمة مع 20 فهرس منفرد لمشغل النظام. يتم ربط كل فهرس من فهارس الشرطية بقائمة انتظار أجهزة واحدة أو أكثر.

وبشكل عملي، يعني ذلك أن فئات حركة مرور متعددة تتشارك في فهرس واضع السياسات وتكون خاضعة لقيمة واضع سياسات تجميع عامة.

المشكلة الشائعة التي تظهر على المحولات مع عملاء تحيل DHCP التي تم تمكينها تتضمن إستجابة DHCP البطيئة. يستطيع العملاء الحصول على خدمات بروتوكول الإنترنت (IP) بشكل متقطع، ولكن يلزم إتمام العديد من المحاولات حتى ينتهي بعض العملاء من وقت لآخر.

تشترك قائمة انتظار إعادة توجيه ICMP وقائمة انتظار البث في فهرس واضع السياسات، لذلك يؤثر حجم حركة مرور البيانات الكبير الذي يتم تلقيه على نفس واجهة المحول الظاهرية (SVI) وتوجيهه منها على التطبيقات التي تعتمد على حركة مرور البث. يكون هذا ملحوظا بشكل خاص عندما يعمل المحول كعميل تحيل.

يقدم هذا المستند شرحا متعمقا للمفهوم، وكيفية التخفيف: أستكشاف أخطاء DHCP وإصلاحها على وكلاء تحيل Catalyst 9000 DHCP

موارد إضافية

أستكشاف أخطاء DHCP البطيئة أو المتقطعة وإصلاحها على وكلاء تحيل Catalyst 9000 DHCP

تكوين التقاط حزمة وحدة المعالجة المركزية (CPU) الخاصة بـ Fed على محولات Catalyst 9000 Switches

المحولات Catalyst 9300 switches: تكوين تنظيم مستوى التحكم

تكوين التقاط الحزمة - دليل تكوين إدارة الشبكة، Cisco IOS XE Bengaluru 17.6.x (محولات Catalyst 9300)

تشغيل التطفل على بروتوكول DHCP وإستكشاف أخطاء وإصلاحها على محولات Catalyst 9000 Switches

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).