وضع سياسة جودة الخدمة على محولات Catalyst 6500/6000 Series Switches

المحتويات

المقدمة

يحدد تنظيم جودة الخدمة على الشبكة ما إذا كانت حركة مرور الشبكة ضمن توصيف محدد (عقد). قد يتسبب ذلك في إسقاط حركة المرور خارج ملف التعريف أو تعليمها لأسفل إلى قيمة رمز خدمات مميزة أخرى (DSCP) لفرض مستوى خدمة تم التعاقد عليه. (DSCP هو قياس لمستوى جودة الخدمة للإطار.)

لا تخلط بين تنظيم حركة المرور وتنظيم حركة المرور. كلا ضمنت أن الحركة مرور يبقى ضمن التشكيل الجانبي (عقد). لا تقوم بتخزين الحزم الخارجة من ملف التعريف مؤقتا عندما تقوم بضبط حركة المرور. لذلك، أنت لا تؤثر على تأخير الإرسال. يمكنك إما إسقاط حركة المرور أو وضع علامة عليها بمستوى جودة خدمة أقل (علامة DSCP). على النقيض، مع تنظيم حركة المرور، يمكنك تخزين حركة المرور خارج ملف التعريف مؤقتا وتلطيف دفعات حركة مرور البيانات. وهذا يؤثر على تباين التأخير والتأخير. يمكنك تطبيق تنظيم حركة البيانات فقط على واجهة صادرة. يمكنك تطبيق التنظيم على كل من الواجهات الواردة والصادرة.

المادة حفازة 6000/6500 سياسة سمة بطاقة (PFC) و PFC2 فقط دعم مدخل تنظيم. يدعم PFC3 تنظيم الدخول والخروج. تنظيم حركة البيانات مدعوم فقط على وحدات WAN معينة للسلسلة Catalyst 6500/7600، مثل الوحدات النمطية للخدمات الضوئية (OSMs) والوحدات النمطية FlexWAN. راجع ملاحظات تكوين الوحدة النمطية للموجه Cisco 7600 Series Router Module للحصول على مزيد من المعلومات

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلمات وضع سياسة جودة الخدمة

لإعداد النهج، قم بتحديد الجهات المسؤولة وتطبيقها على المنافذ (جودة الخدمة المستندة إلى المنافذ) أو على شبكات VLAN (جودة الخدمة المستندة إلى شبكات VLAN). يحدد كل منظم اسم ونوع ومعدل واندفاع وإجراءات لحركة مرور البيانات داخل ملف التعريف وخارج ملف التعريف. كما تدعم الشرطات على Supervisor Engine II معلمات المعدل الزائد. هناك نوعان من المنظمين: Microflow and aggregate.

- **التدفق الدقيق** —حركة مرور بيانات الشرطة لكل منفذ/شبكة محلية ظاهرية (VLAN) يتم تطبيقها بشكل منفصل على أساس كل تدفق.
- **التجميع** — حركة مرور الشرطة عبر جميع المنافذ/شبكات VLAN المطبقة.

يمكن تطبيق كل واضع سياسات على عدة منافذ أو شبكات VLAN. يتم تحديد التدفق باستخدام هذه المعلمات:

- عنوان IP المصدر
- غاية عنوان IP
- بروتوكول الطبقة الرابعة (مثل بروتوكول مخطط بيانات المستخدم [UDP])
- رقم منفذ المصدر
- غاية ميناء رقم

يمكنك القول إن الحزم التي تطابق مجموعة معينة من المعلمات المحددة تنتمي إلى نفس التدفق. (هذا هو أساسا نفس مفهوم التدفق الذي يستخدمه تحويل NetFlow.)

كمثال، إن يشكل أنت Microflow منظم أن يحد ال TFTP حركة مرور إلى 1 Mbps على VLAN 1 و VLAN 3، بعد ذلك 1 Mbps ل كل تدفق في VLAN 1 و 1 Mbps ل كل تدفق في VLAN 3. بمعنى آخر، إذا كان هناك ثلاثة تدفقات في شبكة VLAN رقم 1 وأربعة تدفقات في شبكة VLAN رقم 3، يسمح منظم التدفق الدقيق لكل من هذه التدفقات بسرعة 1 ميجابت في الثانية. إن يشكل أنت تجميع شرطة، هو يحد ال TFTP حركة مرور لكل تدفق إتحاد على VLAN 1 و VLAN 3 إلى 1 ميجابت في الثانية.

إذا قمت بتطبيق كل من منظمي تدفق البيانات المجمعة والجزئية، فإن QoS تتخذ دائما الإجراء الأكثر خطورة الذي تم تحديده من قبل المنظمين. على سبيل المثال، إذا قام أحد المشرفين بتحديد إسقاط الحزمة، بينما يقوم آخر بتحديد لتعليم أسفل الحزمة، يتم إسقاط الحزمة.

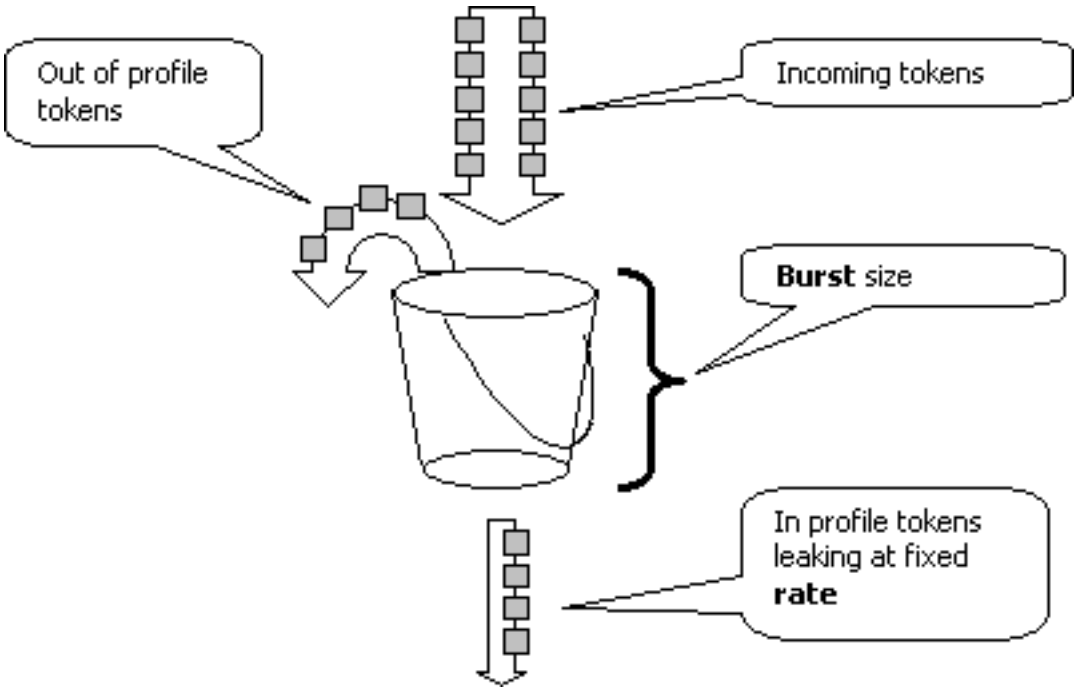
بشكل افتراضي، تعمل شبكات التدفق الصغير فقط مع حركة المرور الموجهة (الطبقة 3 [L3]). لمراقبة حركة المرور التي يتم تقسيمها عبر الجسر (الطبقة 2 [L2]) كذلك، يلزمك تمكين تنظيم تدفق البيانات متناهي الصغر الذي يتم تقسيمه عبر الجسر. في Supervisor Engine II (محرك المشرف)، يلزمك تمكين تنظيم التدفق الصغير المتداخل حتى لتنظيم التدفق الصغير من المستوى الثالث.

وضع الشرطة على دراية بالبروتوكول. تنقسم كل حركة المرور إلى ثلاثة أنواع:

- IP
- تبادل حزم الشبكة البينية (IPX)
- غير ذلك

يتم تنفيذ الشرطة على المادة حفازة 6000/6500 وفقا لمفهوم "دلو متسرب". يتم وضع العلامات المميزة المتوافقة

مع حزم حركة المرور الواردة في دلو. (يمثل كل رمز مميز وحدة بت، لذلك يتم تمثيل الحزمة الكبيرة بمزيد من الرموز المميزة عن الحزمة الصغيرة.) وعلى فترات منتظمة، تتم إزالة عدد محدد من الرموز المميزة من الدلو ويتم إرسالها في طريقها. إذا لم يكن هناك مكان في الدلو لاستيعاب الحزم الواردة، يتم إعتبار الحزم خارج ملف التعريف. يتم إما إسقاطها أو تعليمها لأسفل وفقا لإجراء ضبط الأمن الذي تم تكوينه.



ملاحظة: لا يتم تخزين حركة المرور مؤقتا في الدلو، كما قد تظهر في الصورة أعلاه. لا تمر حركة المرور الفعلية خلال الدلو على الإطلاق، ويتم إستخدام الدلو فقط لتحديد ما إذا كانت الحزمة داخل ملف التعريف أو خارج الملف.

حساب المحددات

تتحكم عدة معلمات في عملية دلو الرمز المميز، كما هو موضح هنا:

- **المعدل**—يحدد عدد الرموز المميزة التي يتم إزالتها في كل فترة زمنية. يعمل هذا على ضبط معدل الشرطة بشكل فعال. يتم إعتبار جميع حركات المرور التي تقل عن المعدل داخل ملف التعريف.
- **الفاصل الزمني**— يحدد عدد مرات إزالة الرموز المميزة من الدلو. تم تحديد الفاصل الزمني عند 0.00025 ثانية، لذلك تتم إزالة الرموز المميزة من الدلو 4000 مرة في الثانية. لا يمكن تغيير الفاصل الزمني.
- **Burst**—يحدد الحد الأقصى لعدد الرموز المميزة التي يمكن أن يستوعبها الدلو في أي وقت. للحفاظ على معدل حركة المرور المحدد، يجب ألا يكون الاندفاع أقل من معدل ضرب الفاصل الزمني. وهناك إعتبار آخر وهو أنه يجب إحتواء الحزمة القصوى في الدلو.

لتحديد معلمة الاندفاع، أستخدم هذه المعادلة:

- اندفاع = (معدل [0.00025 * ([bps [ثانية/فاصل]) *أو* (الحد الأقصى لحجم الحزمة [بت])، أيهما أكبر.

على سبيل المثال، إذا كنت ترغب في حساب الحد الأدنى لقيمة الاندفاع اللازمة لدعم معدل يبلغ 1 ميجابت في الثانية على شبكة إيثرنت، يتم تحديد المعدل على أنه 1 ميجابت في الثانية والحد الأقصى لحجم حزمة الإيثرنت هو 1518 بايت. المعادلة هي:

- الاندفاع = (1،000،000 بت في الثانية * 0.00025) *أو* (1518 بايت * 8 بت/بايت) = 250 *أو* 12144.

أما النتيجة الأكبر فهي 12144 والتي تصل إلى 13 كيلوبت في الثانية.

ملاحظة: في برنامج Cisco IOS®، يتم تحديد معدل التنظيم في وحدات بت في الثانية (BPS)، مقارنة بمعدل كيلوبت في الثانية في نظام التشغيل Catalyst OS (CatOS). أيضا في برنامج Cisco IOS Software، يتم تعريف معدل الاندفاع بالبايت، بدلا من الكيلوبت في CatOS.

ملاحظة: نظرا للدقة في تنظيم الأجهزة، يتم تقريب المعدل الدقيق والدفع إلى أقرب قيمة مدعومة. تأكد من أن قيمة الاندفاع ليست أقل من الحد الأقصى لحجم الحزمة. وإلا، يتم إسقاط جميع الحزم الأكبر من حجم الاندفاع.

على سبيل المثال، إذا حاولت تعيين المحول على 1518 في برنامج Cisco IOS Software، فإنه يتم تقريبه إلى 1000. وهذا يتسبب في إسقاط جميع الإطارات الأكبر من 1000 بايت. الحل هو ترتيب الاندفاع إلى 2000.

عند تكوين معدل الاندفاع، ضع في الاعتبار أن بعض البروتوكولات (مثل TCP) تنفذ آلية التحكم في التدفق التي تتفاعل مع فقدان الحزمة. على سبيل المثال، يقلل بروتوكول TCP تدفق البيانات بمقدار النصف لكل حزمة مفقودة. وبالتالي، عندما يتم وضع السياسات لمعدل معين، يكون إستخدام الارتباط الفعال أقل من المعدل الذي تم تكوينه. يمكنك زيادة الاندفاع لتحقيق إستخدام أفضل. بداية جيدة لهكذا حركة مرور هي مضاعفة حجم الاندفاع. (في هذا المثال، يتم زيادة حجم الاندفاع من 13 كيلوبت في الثانية إلى 26 كيلوبت في الثانية). ثم راقبوا الاداء واجروا تعديلات اضافية إذا لزم الامر.

ولنفس السبب، لا يوصى بإجراء إختبار معياري لعملية المنظم باستخدام حركة مرور موجهة للاتصال. وهذا يظهر عموما أداء أدنى مما يسمح به الشرطي.

إجراءات الشرطة

كما هو مذكور في المقدمة، يمكن أن يقوم الشرطي بأحد أمرين لحزمة خارج الملف الشخصي:

- إسقاط الحزمة (المعلمة `drop` في التكوين)
- وضع علامة على الحزمة إلى DSCP أقل (المعلمة `policed-dscp` في التكوين)

لوضع علامة أسفل الحزمة، يجب عليك تعديل خريطة DSCP ذات السياسات. يتم تعيين DSCP المحدد بشكل افتراضي لمراقبة الحزمة إلى DSCP نفسه. (لا توجد علامة لأسفل.)

ملاحظة: إذا تم وضع علامة "خارج الملف الشخصي" أسفل إلى DSCP تم تعيينه في قائمة انتظار إخراج مختلفة عن DSCP الأصلي، فقد يتم إرسال بعض الحزم خارج الترتيب. ولهذا السبب، إذا كان ترتيب الحزم مهما، فمن المستحسن تمييز الحزم الخارجة من ملف التعريف إلى DSCP التي يتم تعيينها على نفس قائمة انتظار الإخراج كحزم في ملف التعريف.

على Supervisor Engine II (محرك المشرف)، الذي يدعم المعدل الزائد، يمكن أن يكون هناك مشغلان:

- عندما تتجاوز حركة المرور المعدل العادي
- عندما تتجاوز حركة المرور معدل الزيادة

من أمثلة تطبيق معدل الفائض تعليم الحزم التي تتجاوز المعدل العادي وإفلات الحزم التي تتجاوز معدل الفائض.

السياسة سمة يساند بالمادة حفازة 6000/6500

كما هو موضح في المقدمة، فإن PFC1 على المشرف محرك 1a وال PFC2 على المشرف محرك 2 فقط دعم مدخل (قارن داخلي) تنظيم. ال PFC3 على المشرف محرك 720 يساند على حد سواء مدخل ومخرج (قارن خارج) تنظيم.

المادة حفازة 6000/6500 يساند up to 63 microFlow شرطة وما يصل إلى 1023 aggregate policy.

يدعم محرك المشرف 1a تنظيم الدخول، بدءا من CatOS الإصدار 5.3(1) وبرنامج Cisco IOS الإصدار 12.0(7)XE.

ملاحظة: يلزم وجود بطاقة تابعة PFC أو PFC2 لحفظ النظام باستخدام Supervisor Engine (محرك المشرف) 1a.

يدعم محرك المشرف 2 تنظيم الدخول، بدءا من CatOS الإصدار 6.1(1) وبرنامج Cisco IOS الإصدار 12.1(5c)EX.
يدعم Supervisor Engine II معلمة تنظيم المعدل الزائد.

عمليات التهيئة مع بطاقات إعادة التوجيه الموزعة (DFCs) فقط دعم عمليات الشرطة القائمة على المنافذ. كما أن منظم التجميع يقوم بحساب حركة مرور البيانات فقط لكل محرك إعادة توجيه، وليس لكل نظام. تعد كل من DFC و PFC محركات إعادة توجيه؛ وإذا لم تكن الوحدة النمطية (بطاقة الخط) تحتوي على DFC، فإنها تستخدم PFC كمحرك إعادة توجيه.

تحديث ميزات وضع السياسات ل Supervisor Engine 720

ملاحظة: إذا لم تكن على دراية بتنظيم جودة الخدمة Catalyst 6500/6000، فتأكد من قراءة معلمات تنظيم جودة الخدمة وميزات تنظيم العمل التي تدعمها أقسام Catalyst 6500/6000 في هذا المستند.

قدم Supervisor Engine 720 ميزات تنظيم جودة الخدمة الجديدة التالية:

- **وضع سياسات الخروج**. يساند المشرف 720 مدخل تنظيم على ميناء أو VLAN قارن. وهو يدعم تنظيم الخروج على واجهة موجهة إلى L3 أو المنفذ (في حالة برنامج Cisco IOS System). يتم تنظيم جميع المنافذ في شبكة VLAN على المخرج بغض النظر عن وضع جودة الخدمة (سواء جودة الخدمة المستندة إلى المنفذ أو جودة الخدمة المستندة إلى الشبكة المحلية الظاهرية). تنظيم تدفق المايكروسوفت غير مدعوم على المخرج. يتم توفير نموذج للتكوينات في قسم تكوين ومراقبة تنظيم في قسم برنامج CatOS وتكوين ومراقبة تنظيم في قسم برنامج Cisco IOS في هذا المستند.
- **وضع سياسات التدفق الصغير لكل مستخدم**. يدعم Supervisor 720 تحسين تنظيم تدفق الميكروبات المعروف باسم تنظيم تدفق الميكروبات لكل مستخدم. لا يتم دعم هذه الميزة إلا مع برنامج Cisco IOS System. وهو يسمح لك بتوفير نطاق ترددي معين لكل مستخدم (لكل عنوان IP) خلف الواجهات المحددة. ويتم تحقيق ذلك من خلال تحديد قناع تدفق داخل سياسة الخدمة. يحدد قناع التدفق المعلومات التي يتم إستخدامها للتمييز بين التدفقات. على سبيل المثال، إذا قمت بتعيين قناع تدفق مصدر فقط، فإن كل حركة المرور من عنوان IP واحد تعتبر تدفق واحد. باستخدام هذا الأسلوب، يمكنك تنظيم حركة مرور البيانات لكل مستخدم على بعض الواجهات (حيث قمت بتكوين سياسة الخدمة المقابلة)؛ على الواجهات الأخرى، تستمر في إستخدام قناع التدفق الافتراضي. من الممكن أن يكون لديك ما يصل إلى أقنعة تدفق جودة خدمة مختلفة نشطة في النظام في وقت معين. يمكنك ربط فئة واحدة فقط بقناع تدفق واحد. يمكن أن يكون للنهج ما يصل إلى أقنعة تدفق مختلفة.

تغيير آخر مهم في السياسة على المشرف محرك 720 هو أن هو يستطيع عددت حركة مرور ب ال L2 طول الإطار. وهذا يختلف عن Supervisor Engine (محرك المشرف) 2 و Supervisor Engine 1، اللذين يعدان إطارات IP و IPX حسب طول L3 الخاص بهم. مع بعض التطبيقات، قد لا يكون طول L2 و L3 متناسقا. أحد الأمثلة هو حزمة L3 صغيرة داخل إطار كبير من المستوى الثاني. في هذه الحالة، قد يعرض Supervisor Engine (محرك المشرف) 720 معدل حركة مرور بيانات محمية مختلف قليلا مقارنة مع Supervisor Engine (محرك المشرف) 1 و Supervisor Engine 2.

تكوين ومراقبة السياسة في برنامج CatOS

يتكون تكوين السياسة ل CatOS من ثلاث خطوات رئيسية:

1. قم بتعريف واضع السياسات — معدل حركة المرور العادي، معدل الزيادة (إن أمكن)، الاندفاع، والإجراءات الشرطية.
2. قم بإنشاء قائمة تحكم في الوصول (ACL) لجودة الخدمة لتحديد حركة المرور إلى الشرطة، ثم قم بإرفاق منظم بقوائم التحكم في الوصول (ACL) هذه.
3. قم بتطبيق قائمة التحكم في الوصول لجودة الخدمة (QoS) على المنافذ أو شبكات VLAN الضرورية.

يوضح هذا المثال كيفية تنظيم حركة مرور البيانات إلى منفذ UDP 111 على المنفذ 8/2.

Catalyst 6500/6000
`set qos enable`

```
This enables QoS. set qos policer aggregate ---!
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
.switch port
```

المثال التالي هو نفسه؛ ومع ذلك، في هذا المثال، تقوم بإرفاق المنظم بشبكة VLAN. ينتمي المنفذ 8/2 إلى شبكة VLAN 20.

ملاحظة: يجب تغيير جودة الخدمة (QoS) بالمنفذ إلى الوضع VLAN. قم بذلك باستخدام الأمر **set port qos**.

يقوم هذا الشرطي بتقييم حركة مرور البيانات من جميع المنافذ في شبكة VLAN التي تم تكوينها لجودة الخدمة المستندة إلى الشبكة المحلية الظاهرية (VLAN):

Catalyst 6500/6000

```
set qos enable
This enables QoS. set qos policer aggregate ---!
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
.to VLAN 20
```

وبعد ذلك، بدلا من إسقاط الحزم الخارجة من ملف التعريف باستخدام DSCP 32، ضع علامة عليها أسفل إلى DSCP بقيمة 0 (أفضل الجهود).

Catalyst 6500/6000

```
set qos enable
This enables QoS. set qos policer aggregate ---!
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
.ACL

commit qos acl all
This compiles the QoS ACL. set qos policed-dscp-map ---!
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
.map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20
```

يوضح هذا المثال تكوين تنظيم الخروج ل Supervisor Engine 720 فقط. وهو يوضح كيفية تنظيم جميع حركة مرور

IP الصادرة على تجميع VLAN بسرعة 3 إلى 10 ميجابت في الثانية.

Catalyst 6500/6000

```
set qos enable
This enables QoS. set qos policer aggregate ---!
egress_10mbps rate 10000 burst 20 drop !--- This defines
  a policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip egress_pol
    trust-ipprec aggregate egress_10mbps ip any any !---
 This creates the QoS ACL to select traffic and attaches
!--- the policer to the QoS ACL. commit qos acl all !---
 This compiles the QoS ACL. set qos acl map egress_pol 3
      output !--- This maps the QoS ACL to VLAN 3 in the
                                              .output direction
```

أستخدم **show qoS maps runtime policy-dscp-map** لعرض خريطة DSCP المحددة حاليا.

أستخدم **show qos policy runtime {*policer_name* | all}** للتحقق من معلمات الشرطي. كما يمكنك الاطلاع على قائمة التحكم في الوصول لجودة الخدمة (QoS ACL) المرفق بها الشرطي.

ملاحظة: باستخدام Supervisor Engine 1 و 1a، لا يمكن الحصول على إحصائيات تنظيم لأفراد شرطة التجميع. لعرض إحصائيات تنظيم كل نظام، أستخدم هذا الأمر:

```
Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0
```

للتحقق من إحصائيات تنظيم التدفق الجزئي، أستخدم هذا الأمر:

```
Cat6k> (enable) show mls entry qos short
Destination-IP  Source-IP Port  DstPrt SrcPrt Uptime  Age
-------- -------- ------ ------ ----- --------------- ---------------

                                                :IP bridged entries
192.168.10.200UDP   63 6300:22:02 00:00:00 239.77.77.77
                                                  Stat-Pkts : 165360
                                                 Stat-Bytes : 7606560
                                                  Excd-Pkts : 492240
                                                    Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP  888 77700:05:38 00:00:00
                                                  Stat-Pkts : 42372
                                                 Stat-Bytes : 1949112
                                                  Excd-Pkts : 126128
                                                    Stat-Bkts : 1628

Only out of the profile MLS entries are displayed
(Cat6k> (enable
```

باستخدام Supervisor Engine II (محرك المشرف)، يمكنك عرض إحصائيات تنظيم التجميع على أساس كل منظم باستخدام الأمر **show qoS statistics aggregate-policer**.

على سبيل المثال، يتم إرفاق مولد حركة مرور بالمنفذ 8/2. هو يرسل 17 Mbps من حركة مرور UDP مع غاية ميناء 111. تتوقع أن يقوم الشرطي بإسقاط 17/16 من الحركة، بحيث يمكن تنفيذ سرعة 1 ميجابت في الثانية:

```
Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
                                                  :QoS aggregate-policer statistics
                                    Aggregate policerAllowed packet Packets exceed Packets exceed
                                       count        normal rate       excess rate
-------------- -------------- -------------- ------------------------------
                                                  udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
                                                  :QoS aggregate-policer statistics
                                    Aggregate policerAllowed packet Packets exceed Packets exceed
                                       count        normal rate       excess rate
-------------- -------------- -------------- ------------------------------
                                                  udp_1mbps58250497331989733198
```

ملاحظة: إشعار بزيادة الحزم المسموح بها بمقدار 65 وزيادة الحزم الزائدة بمقدار 1090. وهذا يعني أن الشرطي أسقط 1090 حزمة وسمح ل 65 بالمرور. يمكنك حساب أن 65 / (1090 + 65) = 0،056، أو تقريبا 17/1. لذلك، يعمل الشرطي بشكل صحيح.

تكوين وضع السياسة ومراقبتها في برنامج Cisco IOS Software

يتضمن تكوين السياسة في برنامج Cisco IOS الخطوات التالية:

1. قم بتعريف واضع السياسات.
2. قم بإنشاء قائمة تحكم في الوصول (ACL) لتحديد حركة المرور إلى الشرطة.
3. حدد خريطة فئة لتحديد حركة المرور باستخدام قائمة التحكم في الوصول و/أو أسبقية بروتوكول DSCP/IP.
4. قم بتحديد نهج خدمة يستخدم الفئة، وقم بتطبيق المنظم على فئة محددة.
5. تطبيق سياسة الخدمة على منفذ أو شبكة VLAN.

ضع في الاعتبار نفس المثال المتوفر في القسم تكوين تنظيم الشاشة في برنامج CatOS، ولكن الآن مع برنامج Cisco IOS. على سبيل المثال، لديك مولد حركة مرور مرتبط بالمنفذ 8/2. هو يرسل 17 Mbps من حركة مرور UDP مع غاية ميناء 111:

Catalyst 6500/6000

```
                                                                mls qos
      This enables QoS. mls qos aggregate-policer ---!
udp_1mbps 1000000 2000 conform-action transmit exceed-
 action drop !--- Note: The above command should be on
        one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
   Parameters. !--- Note: The burst is 2000 instead of
                                        .1518, due to hardware granularity

                                access-list 111 permit udp any any eq 111
  This defines the ACL to select traffic. class-map ---!
     match-all udp_qos match access-group 111 !--- This
        defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
        the traffic class. interface GigabitEthernet2/8
     switchport service-policy input udp_policy !--- This
                                    .applies the QoS policy to an interface
```

هناك نوعان من واضع السياسات التجميعية في برنامج Cisco IOS Software: **بالاسم** و**لكل واجهة**. يقوم واضع سياسات التجميع المسمى بمعالجة حركة المرور المجمعة من جميع الواجهات التي يتم تطبيقها عليها. هذا هو النوع المستخدم في المثال أعلاه. يقوم واضع السياسات لكل واجهة بمعالجة حركة المرور بشكل منفصل على كل واجهة واردة يتم تطبيقها عليها. يتم تحديد واضع السياسات لكل واجهة ضمن تكوين خريطة السياسة. تأمل في هذا المثال، الذي يحتوي على منظم تجميع لكل واجهة:

Catalyst 6500/6000

```
mls qos
This enables QoS. access-list 111 permit udp any ---!
any eq 111 !--- This defines the ACL to select traffic.
class-map match-all udp_qos match access-group 111 !---
This defines the traffic class to police. policy-map
udp_policy class udp_qos !--- This defines the QoS
policy that attaches the policer to the traffic class.
police 1000000 2000 2000 conform-action transmit exceed-
action drop !--- This creates a per-interface aggregate
!--- policer and applies it to the traffic class.
interface GigabitEthernet2/8 switchport service-policy
input udp_policy !--- This applies the QoS policy to an
.interface
```

يتم تحديد سياسات MicroFlow ضمن تكوين خريطة السياسة، كما هو الحال بالنسبة لشبكات تجميع كل واجهة. في المثال التالي، يتم توجيه كل تدفق من المضيف 192.168.2.2 الذي يأتي إلى شبكة VLAN رقم 2 إلى 100 كيلوبت في الثانية. يتم تنظيم جميع حركات المرور من 192.168.2.2 إلى تجميع 500 كيلوبت في الثانية. VLAN 2 يتضمن قارن FA4/11 و FA4/12:

Catalyst 6500/6000

```
mls qos
This enables QoS. access-list 1 permit 192.168.2.2 ---!
!--- This defines the access list to select traffic from
host 192.168.2.2. class-map match-all host_2_2 match
access-group 1 !--- This defines the traffic class to
police. policy-map host class host_2_2 !--- This defines
the QoS policy. police flow 100000 2000 conform-action
transmit exceed-action drop !--- This defines a
microflow policer. For the calculation of rate and !---
burst, refer to Calculate Parameters. police 500000 2000
2000 conform-action transmit exceed-action drop !---
This defines the aggregate policer to limit !--- traffic
from the host to 500 kbps aggregate. interface fa4/11
mls qos vlan-based interface fa4/12 mls qos vlan-based
!--- This configures interfaces in VLAN 2 for VLAN-based
QoS. interface vlan 2 service-policy input host !---
.This applies the QoS policy to VLAN 2
```

يوضح المثال التالي تكوين لتنظيم الخروج ل Supervisor Engine 720. وهو يضع تنظيم لجميع حركة المرور الصادرة على الواجهة Gigabit Ethernet 8/6 إلى 100 كيلوبت/ثانية:

Catalyst 6500/6000

```
mls qos
This enables QoS. access-list 111 permit ip any any ---!
!--- This defines the ACL to select traffic. All IP
traffic is subject to policing. class-map match-all
cl_out match access-group 111 !--- This defines the
traffic class to police. policy-map pol_out class cl_out
police 100000 3000 3000 conform-action transmit exceed-
action drop !--- This creates a policer and attaches it
to the traffic class. interface GigabitEthernet8/6 ip
address 3.3.3.3 255.255.255.0 service-policy output
.pol_out !--- This attaches the policy to an interface
```

يوضح المثال التالي تكوين تنظيم لكل مستخدم ل Supervisor Engine 720. يتم تنظيم حركة المرور التي تأتي من المستخدمين الذين وراء المنفذ 1/1 تجاه الإنترنت بسرعة 1 ميجابت في الثانية لكل مستخدم. يتم تنظيم حركة المرور التي تأتي من الإنترنت إلى المستخدمين بسرعة 5 ميجابت في الثانية لكل مستخدم:

Catalyst 6500/6000

```
mls qos
This enables QoS. access-list 111 permit ip any any ---!
!--- This defines the ACL to select user traffic. class-
   map match-all cl_out match access-group 111 !--- This
      defines the traffic class for policing. policy-map
  pol_out class cl_out police flow mask src-only 1000000
              32000 conform-act transmit exceed-act drop
  Only the source IP address is considered for flow ---!
  creation !--- on interfaces with this policy attached.
 interface gigabit 1/1 !--- 1/1 is the uplink toward the
  users. service-policy input pol_out !--- Traffic comes
    in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
 dest-only 5000000 32000 conform-act transmit exceed-act
                                                    drop
  Only the destination IP address is considered for ---!
       flow creation !--- on interfaces with this policy
  attached. interface gigabit 1/2 !--- 1/2 is the uplink
              to the Internet. service-policy input pol_in
```

لمراقبة تنظيم، أنت يستطيع استعملت هذا أمر:

```
bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
:QoS global counters
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0

bratan# show mls qos ip gigabitethernet 2/8
.In] Policy map is udp_policy [Out] Default]
(QoS Summary [IP]: (* - shared aggregates, Mod - switch module

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127451  2129602


bratan# show mls qos ip gigabitethernet 2/8
.In] Policy map is udp_policy [Out] Default]
(QoS Summary [IP]: (* - shared aggregates, Mod - switch module

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127755  2134670
```

ملاحظة: زادت الحزم المسموح بها بنسبة 304 وزادت الحزم الزائدة بنسبة 5068. وهذا يعني أن الشرطي أسقط 5068 حزمة وسمح ل 304 بالمرور. بافتراض معدل الإدخال وهو 17 ميجابت في الثانية، يجب أن يمر الشرطي 17/1 من حركة المرور. إذا قمت بمقارنة الحزم التي تم إسقاطها وإعادة توجيهها، فسترى أن هذه هي الحالة: 304 / (304

+ 5068) = 0.057، أو تقريبا 17/1. قد يحدث بعض التباين الطفيف بسبب حساسية تنظيم الأجهزة.

لإحصائيات تنظيم التدفق البالغ الصغر، أستخدم الأمر **show mls ip detail**:

```
                                                Orion# show mls ip detail
 IP Destination IP Source        Protocol L4 Ports     Vlan Xtag L3-protocol
+-----------+----+----+------------+--------+--------------+--------------
                                  192.168.3.33192.168.2.2udp555 / 5550   1ip
                                     192.168.3.3192.168.2.2udp63 / 630   1ip

          IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes]
+-----------+-----------------+-------------+-------+-------------+--------------
                        Fa4/11 - ----ARPA3    0030.7137.1000  0000.3333.3333314548
                        Fa4/11 - ----ARPA3    0030.7137.1000  0000.2222.2222314824

                  Packets     Age   Last SeenQoS      Police Count ThresholdLeak
+-----------+---------+-----------+-----------+---------+-----+------------
                                 18:50:090x80  34619762*2^5 3*2^0   36     6838
                                 18:50:090x80  34669562*2^5 3*2^0   36     6844

                                                Drop Bucket  Use-Tbl Use-Enable
                                               +----------+-------+-------+----
                                                     YES   1968     NONO
                                                     YES   1937     NONO
```

ملاحظة: يظهر حقل عدد الحزم التي تم تنظيمها لكل تدفق.

معلومات ذات صلة

- تكوين جودة الخدمة
- فهم جودة الخدمة على المحولات من مجموعة Catalyst 6000
- دعم منتجات الشبكات المحلية (LAN)
- دعم تقنية تحويل شبكات LAN
- الدعم التقني والمستندات - Cisco Systems

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).