تنظيم جودة الخدمة ووضع العلامات مع محركات المشرف Catalyst 4000/4500 IOS-based Supervisor Engines

المحتويات

المقدمة

تحدد وظيفة وضع السياسات ما إذا كان مستوى حركة المرور داخل ملف التعريف المحدد (العقد). تسمح وظيفة التخطيط إما بإسقاط حركة مرور البيانات خارج ملف التعريف أو وضع علامة على حركة المرور وصولا إلى قيمة مختلفة لنقطة كود الخدمات التفاضلية (DSCP) لفرض مستوى الخدمة المتعاقد عليه. DSCP هو قياس مستوى جودة الخدمة (QoS) للحزمة. وبالإضافة إلى بروتوكول DSCP، يتم إستخدام أسبقية IP وفئة الخدمة (CoS) أيضا لنقل مستوى جودة الخدمة (QoS) للحزمة.

لا يجب الخلط بين تنظيم تنظيم حركة البيانات، على الرغم من أن كلا منهما يضمن بقاء حركة المرور داخل ملف التعريف (العقد). لا يقوم النظام بتخزين حركة المرور، لذلك لا يتأثر تأخير الإرسال. وبدلا من تخزين الحزم مؤقتا خارج ملف التعريف، ستقوم السياسة بإفلاتها أو تعليمها بمستوى جودة خدمة مختلف (علامة DSCP لأسفل). يخزن تنظيم حركة مرور البيانات المؤقت خارج ملف التعريف ويلين دفعات حركة المرور، لكنه يؤثر على تباين التأخير والتأخير. يمكن تطبيق التشكيل فقط على الواجهة الصادرة، بينما يمكن تطبيق التنظيم على كل من الواجهات الواردة والصادرة.

مادة حفازة 4500/4000 مع مشرف محرك 3، 4 و 2+ (SE2+، SE4، SE3 من الآن فصاعدا في هذا وثيقة) يدعم السياسة في إتجاه الصادر والوارد. تنظيم حركة البيانات مدعوم أيضا، ومع ذلك، سيعالج هذا المستند وضع السياسات ووضع العلامات فقط. التمييز هي عملية لتغيير مستوى جودة خدمة الحزمة وفقا لسياسة ما.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

وضع سياسة جودة الخدمة ومعلمات التمييز

يتم إعداد تنظيم النهج من خلال تحديد خرائط سياسة جودة الخدمة وتطبيقها على المنافذ (جودة الخدمة المستندة إلى المنافذ) أو على شبكات VLAN (جودة الخدمة المستندة إلى شبكة VLAN). يتم تعريف الشرطي بواسطة معلمات المعدل والتفجر، بالإضافة إلى الإجراءات الخاصة بحركة مرور البيانات داخل ملف التعريف وخارج ملف التعريف.

هناك نوعان من المنظمين المدعومين: التجميع وكل واجهة. يمكن تطبيق كل واضع سياسات على عدة منافذ أو شبكات VLAN.

يعمل منظم التجميع على حركة المرور عبر جميع المنافذ/شبكات VLAN المطبقة. على سبيل المثال، نقوم بتطبيق واضع السياسات المجمعة لتحديد حركة مرور بروتوكول نقل الملفات المبسط (TFTP) إلى 1 ميجابت في الثانية على شبكات VLAN أرقام 1 و 3. سيتيح هذا واضع السياسات ل 1 Mbps من حركة مرور TFTP في 1 VLANs و 3 معا. إذا طبقنا منظم لكل واجهة، فسيعمل على الحد من حركة مرور TFTP على شبكات VLAN أرقام 1 و 3 إلى 1 ميجابت في الثانية لكل شبكة.

ملاحظة: إذا تم تطبيق تنظيم الدخول والخروج على حزمة، فإنه سيتم إتخاذ القرار الأكثر صرامة. ذلك، إن المدخل يحدد شرطة أن يسقط الربط ويعين المخرج شرطة أن يضع علامة إلى أسفل الربط، الربط سيتم إسقاطه. يلخص الجدول 1 الإجراء QoS على الحزمة عندما تتم معالجتها بواسطة كل من سياسات الدخول والخروج.

الجدول 1: إجراء جودة الخدمة حسب سياسة الدخول والخروج

	Ingress policy			
Egress policy	**Transmit**	**Drop**	**Markdown$_i$**	**Mark$_i$**
Transmit	Transmit	Drop	Markdown$_i$	Mark$_i$
Drop	Drop	Drop	Drop	Drop
Markdown$_e$	Markdown$_e$	Drop	Markdown$_e$	Markdown$_e$
Mark$_e$	Mark$_e$	Drop	Mark$_e$	Mark$_e$

يتم تنفيذ أجهزة Catalyst 4000 SE3 و SE4 و QoS SE2+ بطريقة تحدث فيها العلامة الحقيقية للحزمة بعد واضع سياسات الخروج. هذا يعني أنه حتى إذا لاحظت سياسة المدخل الحزمة (بواسطة الشرطي وضع علامة للأسفل أو وضع علامة العادي)، فإن سياسة المخرج ستظل ترى الحزم المعلمة بمستوى جودة الخدمة الأصلي. سترى سياسة الخروج الحزمة كما لو لم يتم وضع علامة عليها بنهج الدخول. وهذا يعني ما يلي:

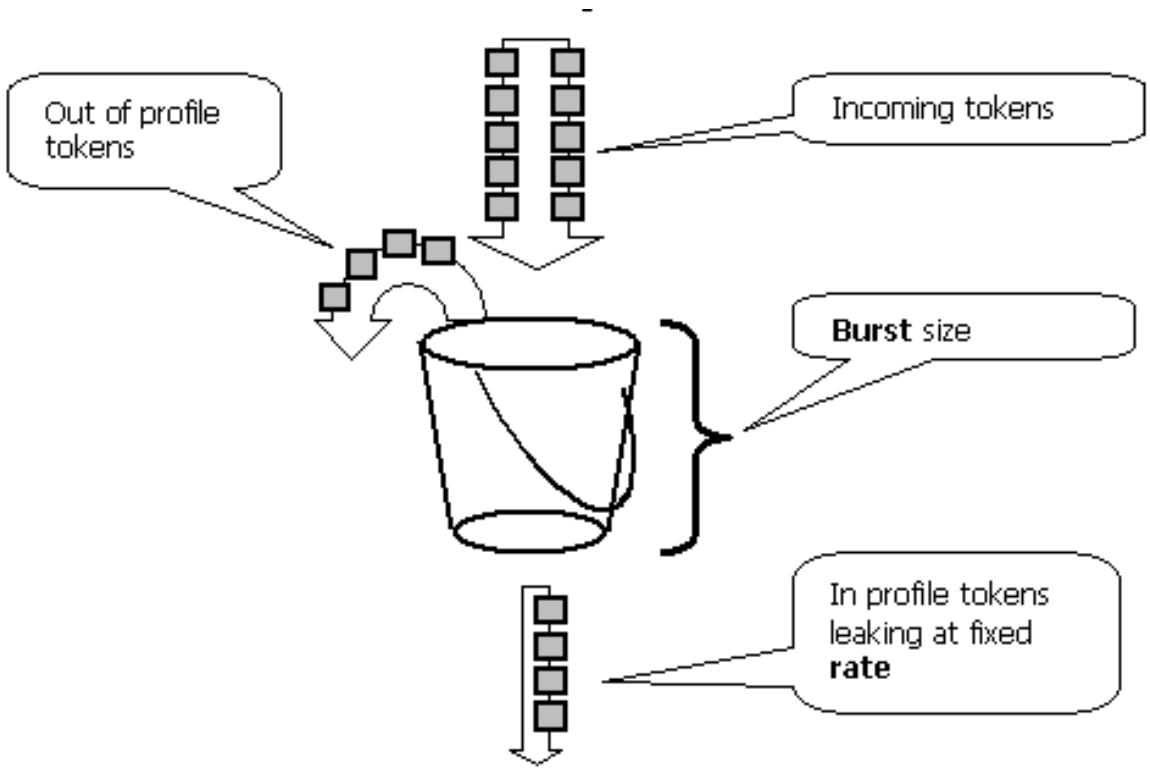
- وضع علامات الخروج يتخطى وضع علامات الدخول.
- لا يمكن لنهج الخروج أن يطابق مستويات جودة الخدمة الجديدة التي تم تغييرها بواسطة تمييز المدخل.

وفيما يلي آثار هامة أخرى:

- لا يمكن وضع علامة وإشارة إلى الأسفل ضمن نفس فئة حركة المرور ضمن نفس النهج.
- تكون منظومات التجميع لكل إتجاه. وهذا يعني أنه إذا تم تطبيق منظم تجميع على كل من المدخل والمخرج، فسيكون هناك شرطيان تجميعيان، أحدهما على الإدخال والآخر على الإخراج.
- عندما يتم تطبيق منظم تجميع ضمن السياسة على شبكات VLAN والواجهة المادية، فسيكون هناك بشكل فعال شرطيان تجميع - أحدهما لواجهات VLAN والآخر للواجهات المادية. حاليا، لا يمكن مراقبة واجهات VLAN والواجهات المادية معا على التجميع.

تتوافق السياسة في Catalyst 4000 SE3 و SE4 و SE2+ مع مفهوم الدلو المتسرب، كما يوضح النموذج أدناه. يتم وضع العلامات المميزة المتوافقة مع حزم حركة المرور الواردة في دلو (# من العلامات المميزة = حجم الحزمة).

على فترات منتظمة، تتم إزالة عدد محدد من الرموز المميزة (المشتقة من المعدل الذي تم تكوينه) من الدلو. إذا لم يكن هناك مكان في الدلو لاستيعاب حزمة واردة، فإن الحزمة تعتبر خارج ملف التعريف ويتم إسقاطها أو تعليمها للأسفل، وفقا لإجراء تنظيم تم تكوينه.



تجدر الإشارة إلى أن حركة المرور لا يتم تخزينها مؤقتا في الدلو، حيث أنها قد تظهر من النموذج أعلاه. حركة المرور الفعلية لا تتدفق عبر الدلو على الإطلاق. يتم إستخدام الدلو فقط لتحديد ما إذا كانت الحزمة داخل ملف التعريف أو خارج ملف التعريف.

لاحظ أن التنفيذ الدقيق للأجهزة أثناء عمل الشرطة يمكن أن يكون مختلفا من الناحية الوظيفية، فهو يمتثل للنموذج المذكور أعلاه.

تتحكم المعلمات التالية في عملية وضع السياسات:

- يحدد المعدل 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.
- يحدد الفاصل الزمني عدد مرات إزالة الرموز المميزة من الدلو. تم تثبيت الفاصل الزمني عند 16 نانو ثانية (16 ثانية *10-9). لا يمكن تغيير الفاصل الزمني.
- يحدد الاندفاع الحد الأقصى لمقدار الرموز المميزة التي يمكن أن يستوعبها الدلو في أي وقت.

راجع قسم مقارنة تنظيم ووضع العلامات على محركات المشرف المستندة إلى Catalyst 6000 و Catalyst IOS 4000/4500 في نهاية هذا المستند بسبب الاختلافات في الاندفاع بين Catalyst 6000 و Catalyst 4000 SE3 و SE4 و +SE2.

يضمن الشرطي أنه إذا فحصت أي فترة من الوقت (من صفر إلى ما لا نهاية) لن يسمح الشرطي بأكثر من

```
rate> * <period> + <burst-bytes> + <1 packet> bytes>
```

من المرور خلال واضع الشرطة خلال تلك الفترة.

تتميز أجهزة Catalyst 4000 SE3 و SE4 و QoS +SE2 ببعض القابلية للتقسيم إلى وحدات أخرى. ووفقا لمعدل التكوين، فإن الحد الأقصى للانحراف عن المعدل هو 1.5٪ من المعدل.

عند تكوين معدل الاندفاع، يلزمك الأخذ في الاعتبار أن بعض البروتوكولات (مثل TCP) تنفذ آليات التحكم في التدفق التي تتفاعل مع فقدان الحزمة. على سبيل المثال، يقلل بروتوكول TCP النافذة بمقدار النصف لكل حزمة مفقودة. عند تحديد المعدل بشكل محدد، سيكون إستخدام الارتباط الفعال أقل من المعدل الذي تم تكوينه. يمكن زيادة الاندفاع لتحقيق إستخدام أفضل. بداية جيدة لمثل هذه الحركة المرور هي أن تجعل الاندفاع يساوي ضعف كمية حركة المرور المرسلة بمعدل المرغوب خلال وقت الذهاب والعودة (RTT). ولنفس السبب، لا يوصى بقياس عملية الشرطي بواسطة حركة المرور الموجهة نحو الاتصال، حيث أنها ستظهر بشكل عام أداء أقل مما يسمح به الشرطي.

ملاحظة: قد تتفاعل حركة المرور غير المتصلة أيضا مع عمليات الشرطة بشكل مختلف. على سبيل المثال، يستخدم نظام ملفات الشبكة (NFS) الكتل، والتي قد تتكون من أكثر من حزمة واحدة لبروتوكول مخطط بيانات المستخدم (UDP). قد يؤدي إسقاط حزمة واحدة إلى تشغيل العديد من الحزم (الكتلة بأكملها) لإعادة إرسالها.

على سبيل المثال، ما يلي هو حساب الاندفاع لجلسة TCP، بمعدل تنظيم يبلغ 64 كيلوبت/ثانية و TCP RTT من 0. 05 ثانية:

```
[burst> = 2* <RTT> * <rate> = 2 * 0.05 [sec] * 64000/8 [bytes/sec] = 800 [bytes>
```

ملاحظة: <burst> هو لجلسة TCP واحدة، لذلك يجب قياسها إلى متوسط عدد الجلسات المتوقع من خلال واضع السياسات. هذا مثال فقط، لذلك في كل حالة، يحتاج المرء إلى تقييم متطلبات حركة المرور/التطبيق والسلوك مقابل الموارد المتاحة لاختيار معلمات تنظيم النظام.

الإجراء الشرطي هو إما أن يسقط الحزمة (إسقاط) أو أن يغير ال DSCP من الربط (وضع علامة أسفل). لوضع علامة أسفل الحزمة، يجب تعديل خريطة DSCP المخططة. يشير التقصير المنظم DSCP إلى الربط إلى ال نفسه DSCP، أي، ما من علامة أسفل يقع.

ملاحظة: قد يتم إرسال الحزم خارج الترتيب عندما يتم وضع علامة أسفل حزمة خارج ملف التعريف إلى DSCP إلى قائمة انتظار إخراج مختلفة عن DSCP الأصلية. ولهذا السبب، إذا كان ترتيب الحزم مهما، فمن المستحسن وضع علامة أسفل الحزم الخارجة من ملف التعريف إلى DSCP المعين إلى نفس قائمة انتظار الإخراج كحزم داخل ملف التعريف.

ميزات وضع السياسات ووضع العلامات المدعومة من قبل محركات المشرف المستندة إلى Catalyst 4000/4500 IOS

يتم دعم كلا من تنظيم المدخل (الواجهة الواردة) والخروج (الواجهة الصادرة) على Catalyst 4000 SE3، SE4، +SE2. يساند المفتاح 1024 مدخل و 1024 مخرج شرطة. يتم إستخدام إثنين من ناظمي الدخول واثنين من ناظمي الخروج من قبل النظام للسلوك الافتراضي بدون تنظيم.

لاحظ أنه عند تطبيق واضع السياسات المجمعة ضمن النهج على شبكة VLAN وواجهة مادية، يتم إستخدام إدخال منظم أجهزة إضافي. حاليا، لا يمكن مراقبة واجهات VLAN والواجهات المادية معا على التجميع. قد يتم تغيير ذلك في إصدارات البرامج المستقبلية.

تتضمن جميع إصدارات البرامج دعم وضع السياسات. يدعم المحول Catalyst 4000 ما يصل إلى 8 عبارات تطابق صالحة لكل فئة، ويتم دعم ما يصل إلى 8 فئات لكل خريطة سياسة. جمل المطابقة الصالحة هي كما يلي:

- مطابقة مجموعة الوصول
- مطابقة ip dscp
- أسبقية IP المطابقة
- مطابقة أي

ملاحظة: بالنسبة لحزم IP v4 غير IP، يكون بيان **IP dscp** هو الطريقة الوحيدة للتصنيف، شريطة أن تكون الحزم واردة إلى منافذ التوصيل الموثوق فيها. لا يتم تضليلك بالكلمة الأساسية ip في الأمر **match ip dscp**، نظرا لمطابقة DSCP الداخلي، فهذا ينطبق على جميع الحزم، وليس IP فقط. عندما شكلت ميناء يكون أن يثق COs، الأخيرة استخرجت من ال 802.1Q) L2 أو ISL tagged) إطار وحولت إلى DSCP داخلي يستعمل CoS إلى DSCP جودة خدمة. يمكن بعد ذلك مطابقة قيمة DSCP الداخلية هذه في النهج باستخدام **تطابق dscp ip**.

إجراءات السياسة الصحيحة هي كما يلي:

- شرطة
- set ip dscp
- ضبط أسبقية IP
- الثقة في DSCP
- تراست كوس

يسمح التمييز بتغيير مستوى جودة الخدمة للحزمة استنادا إلى التصنيف أو السياسة. يقسم التصنيف حركة المرور إلى فئات مختلفة لمعالجة جودة الخدمة بناء على معايير محددة. لمطابقة أسبقية IP أو DSCP، يجب تعيين الواجهة الواردة المطابقة على الوضع الموثوق به. يدعم المحول الثقة في CoS والواجهات غير الموثوق بها و DSCP. تحدد الثقة الحقل الذي سيتم اشتقاق مستوى جودة الخدمة منه للحزمة.

عند الثقة في CoS، سيتم اشتقاق مستوى جودة الخدمة من رأس L2 للحزمة المغلفة ISL أو 802.1Q. عند الاعتماد على DSCP، سيستخرج المحول مستوى جودة الخدمة من حقل DSCP الخاص بالحزمة. تكون الثقة في CoS ذات معنى فقط على واجهات التوصيل، وتكون الثقة في DSCP صالحة لحزم IP V4 فقط.

عندما لا تكون الواجهة موثوق بها (تكون هذه هي الحالة الافتراضية عند تمكين جودة الخدمة)، سيتم اشتقاق DSCP الداخلي من CoS الافتراضية القابلة للتكوين أو DSCP للواجهة المقابلة. في حالة عدم تكوين أي CoS افتراضية أو DSCP، ستكون القيمة الافتراضية صفر (0). بمجرد تحديد مستوى جودة الخدمة الأصلي للحزمة، فإنه يتم تعيينه في DSCP الداخلي. يمكن الاحتفاظ ب DSCP الداخلي أو تغييره عن طريق وضع العلامات أو وضع النهج.

بعد أن تخضع الحزمة لمعالجة جودة الخدمة، سيتم تحديث حقول مستوى جودة الخدمة (داخل حقل IP DSCP ل IP وداخل رأس ISL/802.1Q، إن وجدت) من DSCP الداخلي.

هناك خرائط خاصة تستخدم لتحويل مقاييس جودة الخدمة الموثوق بها للحزمة إلى DSCP داخلي والعكس بالعكس. وفيما يلي هذه الخرائط:

- يستخدم DSCP إلى DSCP المتحكم فيه، لاستخلاص DSCP المتحكم به عند وضع علامة أسفل الحزمة.
- DSCP إلى CoS: يستخدم لاستخلاص مستوى CoS من DSCP الداخلي لتحديث رأس الحزمة الصادرة ISL/802.1Q.
- CoS إلى DSCP: يستخدم لاستخلاص DSCP داخلي من CoS واردة (ISL/802.1Q header) عندما تكون الواجهة في وضع CoS الموثوق.

لاحظ عندما تكون الواجهة في وضع CoS للثقة، فإن CoS الصادرة ستكون دائما هي نفسها CoS الواردة. وهذا خاص بتطبيق جودة الخدمة في Catalyst 4000 SE3، SE4، SE2+.

تكوين النهج ومراقبته

يتضمن تكوين تنظيم في IOS الخطوات التالية:

1. تعريف واضع السياسات.
2. تحديد معايير لتحديد حركة مرور البيانات للتنظيم.
3. تعريف نهج الخدمة باستخدام الفئة وتطبيق واضع السياسات على فئة محددة.
4. تطبيق سياسة الخدمة على منفذ أو شبكة VLAN.

تأملوا في المثال التالي. هناك مولد حركة مرور يربط بالمنفذ 14/5 يرسل حوالي 17 ميجابت في الثانية من حركة مرور UDP مع وجهة المنفذ 111. نريد تنظيم حركة المرور هذه حتى 1 ميجابت في الثانية ويجب إسقاط حركة المرور الزائدة.

```
enable qos !
qos
```

```
define policer, for rate and burst values, see 'policing parameters !
   qos aggregate-policer pol_1mbps 1mbps 1000 conform-action transmit
                                                        exceed-action
                                                                drop
                                          define ACL to select traffic !
                                    access-list 111 permit udp any any eq 111
                                         define traffic class to be policed !
                                                  class-map match-all cl_test
                                                       match access-group 111
                                  define QoS policy, attach policer to traffic class !
                                                          policy-map po_test
                                                               class cl_test
                                                    police aggregate pol_1mbps
                                                apply QoS policy to an interface !
                                                        interface FastEthernet5/14
                                                          switchport access vlan 2
                                    switch qos to vlan-based mode on this port !
                                                                qos vlan-based
                                                apply QoS policy to an interface !
                                                                interface Vlan 2
                                                    service-policy output po_test
                                                                               !
```

لاحظ أنه عندما يكون المنفذ في وضع جودة الخدمة المستندة إلى شبكة VLAN، ولكن لا يتم تطبيق سياسة الخدمة على شبكة VLAN المقابلة، فإن المحول سيتبع سياسة الخدمة (إن وجد) المطبقة على المنفذ الفعلي. وهذا يسمح بمرونة إضافية في دمج جودة الخدمة القائمة على المنافذ والقائمة على الشبكات المحلية الظاهرية (VLAN).

هناك نوعان من أدوات التنظيم المدعومة: تجميع مسمى وكل واجهة. سيقوم شرطي تجميع مسمى بمراقبة حركة المرور المجمعة من جميع الواجهات التي يتم تطبيقها عليها. أستخدم المثال أعلاه واضع السياسات المسمى. سيقوم واضع السياسات لكل واجهة، على عكس واضع السياسات المسمى، بمراقبة حركة المرور بشكل منفصل على كل واجهة حيث يتم تطبيقها. يتم تحديد واضع السياسات لكل واجهة ضمن تكوين خريطة السياسة. تأمل في المثال التالي باستخدام واضع السياسات المجمعة لكل واجهة:

```
                                                              enable qos !
                                                                     qos
                                         define traffic class to be policed !
                                                 class-map match-all cl_test2
                                                      match ip precedence 3 4
                                  define QoS policy, attach policer to traffic class !
                                                         policy-map po_test2
                                                              class cl_test2
                                per-interface policer is defined inside the policy map !
                             police 512k 1000 conform-action transmit exceed-action drop
                                                        interface FastEthernet5/14
                                                                     switchport
                  set port to trust DSCP - need this to be able to match to incoming IP precedence !
                                                                  qos trust dscp
                                               switch to port-based qos mode !
                                                                 no qos vlan-based
                                                apply QoS policy to an interface !
                                                     service-policy input po_test2
```

يتم إستخدام الأمر التالي لمراقبة عملية وضع السياسات:

```
                                                Yoda#show policy-map interface FastEthernet5/14
                                                                  FastEthernet5/14
                                                    service-policy input: po_test2
                                                  (class-map: cl_test2 (match-all
                                                                packets 7400026
```

```
                                    match: ip precedence 3 4
                                      police: Per-interface
                    Conform: 1166067574 bytes Exceed: 5268602114 bytes
                                    (class-map: class-default (match-any
                                                        packets 13312
                                                       match: any
                                                    packets 13312
                                Yoda#show policy-map interface FastEthernet5/14
                                                    FastEthernet5/14
                                  service-policy input: po_test2
                                (class-map: cl_test2 (match-all
                                                  packets 7400138
                                    match: ip precedence 3 4
                                      police: Per-interface
                    Conform: 1166088574 bytes Exceed: 5268693114 bytes
                                    (class-map: class-default (match-any
                                                        packets 13312
                                                       match: any
                                                    packets 13312
```

يقوم العداد الموجود بالقرب من خريطة الفئة بحساب عدد الحزم المطابقة للفئة المطابقة.

يجب أن تكون على علم باعتبارات التنفيذ المحددة التالية:

- عداد الحزم لكل فئة ليس لكل واجهة. وهذا يعني أنها تقوم بحساب جميع الحزم التي تطابق الفئة بين جميع الواجهات حيث يتم تطبيق هذه الفئة داخل نهج الخدمة.
- لا تحتفظ الشرطة بعدادات الحزم، يتم دعم عدادات البايت فقط.
- لا يوجد أمر محدد للتحقق من معدل حركة المرور المقدمة أو الصادرة لكل منظم.
- يتم تحديث العدادات على أساس دوري. إذا تم تنفيذ الأمر أعلاه بشكل متكرر في تسلسل سريع، فقد تستمر العدادات في الظهور في بعض الوقت.

تهيئة ومراقبة وضع العلامات

يتضمن تكوين وضع العلامات الخطوات التالية:

1. حدد معايير تصنيف حركة المرور - قائمة الوصول، DSCP، أسبقية IP، وما إلى ذلك.
2. قم بتحديد فئات حركة المرور التي سيتم تصنيفها باستخدام المعايير التي تم تعريفها مسبقا.
3. قم بإنشاء إجراءات تمييز تمييز و/أو إجراءات تنظيم لمخطط سياسة للفئات المعرفة.
4. تكوين وضع الثقة على الواجهة (الواجهات) المطابقة.
5. تطبيق خريطة السياسة على واجهة.

ضع في الاعتبار المثال التالي حيث نريد حركة مرور واردة ذات أسبقية IP 3 لاستضافة منفذ UDP 192.168.196.3 777 المعين إلى أسبقية IP 6. يتم تنظيم جميع حركات مرور IP الأخرى ذات الأولوية 3 إلى 1 ميجابت في الثانية، ويجب وضع علامة على حركة المرور الزائدة إلى أسبقية IP 2.

```
                                                enable QoS globally !
                                                                 qos
                    define ACL to select UDP traffic to 192.168.196.3 port 777 !
                                                ip access-list extended acl_test4
                                        permit udp any host 192.168.196.3 eq 777
                define class of traffic using ACL and ip precedence matching !
                                                class-map match-all cl_test10
                                                        match ip precedence 3
                                                match access-group name acl_test4
        all the remaining ip precedence 3 traffic will match this class !
```

```
class-map match-all cl_test11
        match ip precedence 3
define policy with above classes !
        policy-map po_test10
             class cl_test10
mark traffic belonging to class with ip precedence 6 !
            set ip precedence 6
             class cl_test11
police and mark down all other ip precedence 3 traffic !
  police 1 mbps 1000 exceed-action policed-dscp-transmit
                                                        !
adjust DSCP to policed DSCP map so to map DSCP 24 to DSCP 16 !
                qos map dscp policed 24 to dscp 16
                                                        !
           interface FastEthernet5/14
set interface to trust IP DSCP !
                 qos trust dscp
      apply policy to interface !
service-policy input po_test10
                                                        !
```

يتم إستخدام أمر **واجهة سياسة sh** لمراقبة العلامات. وتوثق عينة النواتج والآثار في تكوين أعمال الشرطة أعلاه.

مقارنة تنظيم ووضع العلامات على محركات المشرف المستندة إلى Catalyst 6000 و Catalyst 4000/4500 IOS

Feature	Catalyst6000	Catalyst4000 SE3
Egress QoS policies	Not supported by Supervisor 1A and Superviso r2 hardware.	Supported.
Burst policing parameter calculation	Burst should be at least the same size as maximum frame supposed to pass via policer and no less then rate/interval, with the interval being 250 microseconds	No such restriction.
QoS policing L2 & L3	By default, microflow policing is only enabled for L3 on the sup1a and is not enabled at all for Supervisor 2. A CLI command is available to enable it for L2 on sup1a and L2 & L3 for sup2. Aggregate policing for sup1a & Supervisor 2 is enabled by default for L2 & L3.	Always.
Egress CoS	Always derived from internal DSCP using DSCP to CoS QoS map.	If the ingress port is in trust CoS mode, the egress CoS will be the same as the ingress CoS. Otherwise, it will be derived from the internal DSCP.
Microflow policing	Supported.	Not supported.
QoS behavior when port is in VLAN-based QoS mode, but no policy is applied to the VLAN.	No policy applied.	Fallback to port-based QoS. Will apply policy attached to port.

معلومات ذات صلة

- فهم جودة الخدمة وتكوينها
- الدعم الفني - 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).