فهم QoS ووضعت علامة على المادة حفازة 3550

المحتويات

المقدمة

تحدد وظيفة تنظيم البيانات ما إذا كان مستوى حركة المرور داخل ملف التعريف المحدد أو العقد المحدد، وتسمح لك إما بإنزال حركة المرور خارج ملف التعريف أو تعليمها لأسفل إلى قيمة مختلفة لنقطة رمز الخدمات التفاضلية (DSCP). يؤدي هذا إلى فرض مستوى خدمة تم التعاقد 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 السياسة وتنظيم حركة المرور، على الرغم من أن كليهما تأكد من بقاء حركة المرور ضمن ملف التعريف أو العقد.

لا تقوم السياسة بعمل مخزن مؤقت لحركة المرور، لذلك لا تؤثر السياسة على تأخير الإرسال. بدلا من تخزين الحزم مؤقتا خارج ملف التعريف، تقوم السياسة بإسقاطها أو تعليمها بمستويات جودة الخدمة المختلفة (تمييز DSCP).

يخزن تنظيم حركة مرور البيانات المؤقت خارج ملف التعريف ويلين دفعات حركة المرور، لكن يؤثر على تباين التأخير والتأخير. يمكن تطبيق التشكيل فقط على الواجهة الصادرة، بينما يمكن تطبيق التنظيم على كل من الواجهة الواردة والصادرة.

المادة حفازة 3550 يساند الشرطة لكل من إتجاه قادم أو صادر. تنظيم حركة البيانات غير مدعوم.

يغير التمييز مستوى جودة خدمة الحزمة وفقا لسياسة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

إصدارات الأجهزة والبرامج

يتم دعم وضع السياسات ووضع العلامات على Catalyst 3550 مع جميع إصدارات البرامج. يتم سرد أحدث دليل تكوين هنا. ارجع إلى هذه الوثائق للحصول على جميع الميزات المدعومة.

- تكوين جودة الخدمة

وضع سياسة جودة الخدمة ومعلمات التمييز

من أجل إعداد تنظيم، يجب تحديد خرائط نهج جودة الخدمة وتطبيقها على المنافذ. وهذا يعرف أيضا باسم جودة الخدمة (QoS) المستندة إلى المنفذ.

ملاحظة: جودة الخدمة المستندة إلى شبكات VLAN غير مدعومة حاليا من قبل المحول Catalyst 3550.

يتم تعريف الشرطي بواسطة معلمات المعدل والتفجر بالإضافة إلى الإجراء الخاص بحركة المرور خارج ملف التعريف.

يتم دعم هذين النوعين من المنظمين:

- ركام
- إفراديا

يعمل واضع سياسات التجميع على حركة المرور عبر جميع الحالات التي يتم تطبيقها فيها. يتصرف الشرطي الفرد بشكل منفصل على حركة المرور عبر كل حالة يتم تطبيقها فيها.

ملاحظة: على المادة حفازة 3550، يمكن تطبيق واضع السياسات المجمعة فقط على فئات مختلفة من نفس النهج. لا يتم دعم تنظيم التجميع عبر الواجهات أو السياسات المتعددة.

على سبيل المثال، قم بتطبيق منظم التجميع لتحديد حركة مرور بيانات الفئة Customer1 والفئة Customer2 في نفس مخطط السياسة إلى 1 ميجابت في الثانية. يسمح هذا واضع السياسات بحركة مرور البيانات بسرعة 1 ميجابت في الثانية في الفئة Customer1 و Customer2 معا. إذا قمت بتطبيق المنظم الفردي، فسيحدد المنظم حركة مرور البيانات لعميل الفئة 1 إلى 1 ميجابت في الثانية ولعميل الفئة 2 إلى 1 ميجابت في الثانية. لذلك، يكون كل مثيل للمنظم منفصلا.

يلخص هذا طاولة الإجراء QoS على الربط عندما عالجت ب على حد سواء مدخل ومخرج سياسة:

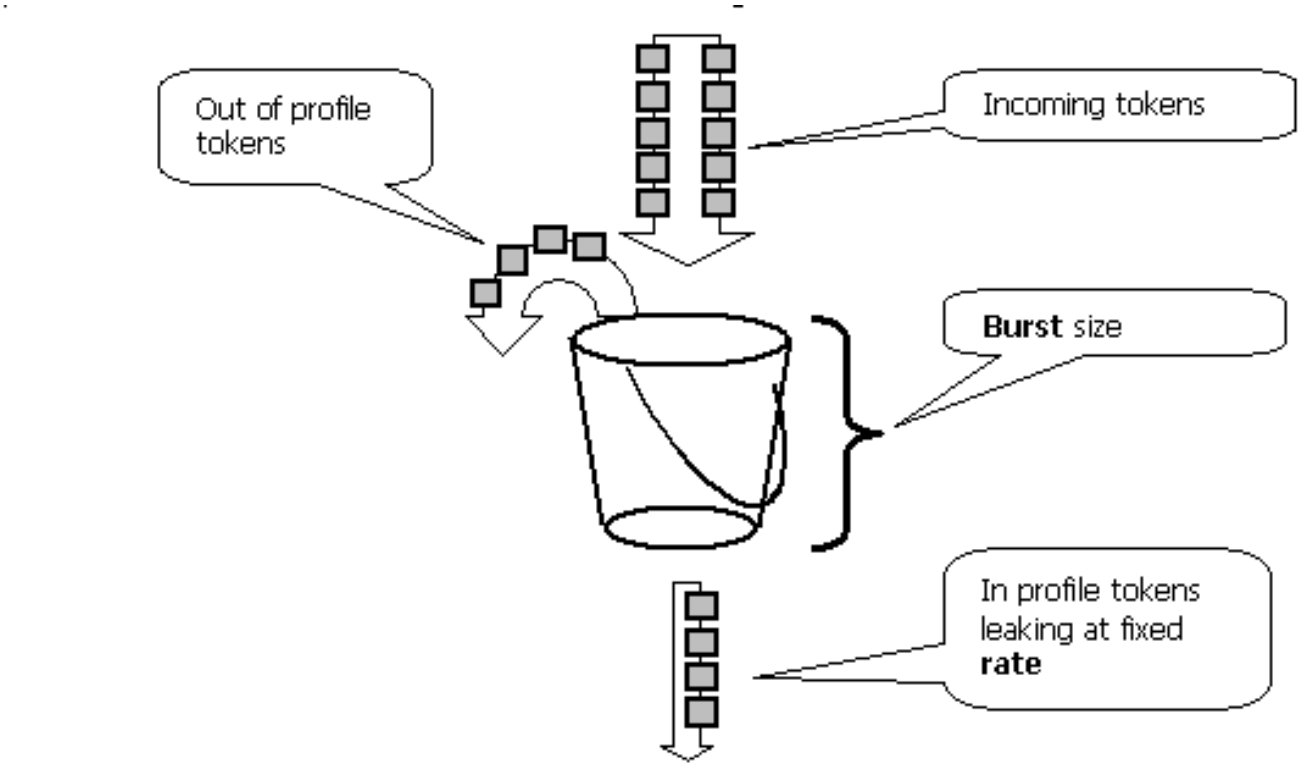
	Ingress policy			
Egress policy	Transmit	Drop	$Markdown_i$	$Mark_i$
Transmit	Transmit	Drop	$Markdown_i$	$Mark_i$
Drop	Drop	Drop	Drop	Drop
$Markdown_e$	$Markdown_e$	Drop	$Markdown_i$ then $Markdown_e$	$Mark_i$ then $Markdown_e$

ملاحظة: من الممكن وضع علامة وترسيم داخل نفس فئة حركة المرور الخاصة بنفس السياسة. وفي هذه الحالة، يتم تمييز جميع حركات مرور الفئة المحددة أولا. تحدث عملية التنظيم والتأشير على حركة المرور التي تم وضع علامة عليها مسبقا.

سياسة جودة الخدمة في المادة حفازة 3550 تتوافق مع هذا مسرب مفهوم:

يتم وضع عدد الرموز المميزة المتناسبة مع أحجام حزمة حركة المرور الواردة في دلو الرمز المميز، ويساوي عدد الرموز المميزة حجم الحزمة. في الفاصل الزمني العادي، 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.

يتم توضيح هذا المفهوم في هذا المثال:



ملاحظة: لا يتم تخزين حركة المرور مؤقتا في الدلو كما يمكن أن تظهر في هذا المثال. لا تتدفق حركة المرور الفعلية عبر الدلو على الإطلاق، ويتم إستخدام الدلو فقط لتحديد ما إذا كانت الحزمة في ملف التعريف أو خارج ملف التعريف.

ملاحظة: يمكن أن يختلف تنفيذ أجهزة الشرطة، ولكنه لا يزال يتوافق من الناحية الوظيفية مع هذا النموذج.

تتحكم هذه المعلمات في عملية وضع السياسات:

- **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 في ملف التعريف. تتراوح المعدلات المدعومة من 8 كيلوبت/ثانية إلى 2 جيجابت/ثانية، والزيادة بمعدل 8 كيلوبت/ثانية.
- **الفاصل الزمني**— يحدد عدد مرات إزالة الرموز المميزة من الدلو. تم تحديد الفاصل الزمني عند 0.125 مللي ثانية

(أو 8000 مرة في الثانية). لا يمكن تغيير هذا الفاصل الزمني.
- **Burst**—يحدد الحد الأقصى لمقدار الرموز التي يمكن أن يستوعبها الدلو في أي وقت. وتتراوح عمليات التفجر المدعومة من 8000 بايت إلى 200000 بايت، والزيادة ب 64 بايت.

ملاحظة: على الرغم من أن سلاسل تعليمات سطر الأوامر تظهر مجموعة كبيرة من القيم، إلا أن خيار rate-bps لا يمكن أن يتجاوز سرعة المنفذ التي تم تكوينها، ولا يمكن أن يتجاوز خيار burst-byte 200000 بايت. إذا قمت بإدخال قيمة أكبر، فإن المحول يرفض خريطة السياسة عندما تقوم بإرفاقها بواجهة.

من أجل الحفاظ على معدل حركة المرور المحدد، يجب أن يكون الاندفاع أقل من مجموع هذه المعادلة:

```
(Burstmin (bits) = Rate (bps) / 8000 (1/sec
```

على سبيل المثال، قم بحساب الحد الأدنى لقيمة الاندفاع للحفاظ على معدل مقداره 1 ميجابت في الثانية. يتم تحديد المعدل بأنها 1000 كيلوبت في الثانية، لذلك فإن الاندفاع الأدنى المطلوب هو مجموع هذه المعادلة:

```
(Kbps) / 8000 (1/sec) =125 (bits) 1000
```

الحد الأدنى لحجم الاندفاع المدعوم هو 8000 بايت، وهو أكثر من الحد الأدنى للاندفاع الذي تم حسابه.

ملاحظة: نظرا للدقة في تنظيم الأجهزة، يتم تقريب المعدل الدقيق والدفع إلى أقرب قيمة مدعومة.

عند تكوين معدل الاندفاع، يجب أن تأخذ في الاعتبار أن بعض البروتوكولات تنفذ آليات تستجيب لفقدان الحزمة. على سبيل المثال، يقلل بروتوكول التحكم في الإرسال (TCP) النافذة بمقدار النصف لكل حزمة مفقودة. وهذا يتسبب في تأثير "السن المنشار" في حركة مرور TCP عندما يحاول TCP التسريع إلى معدل الخط ويتم التحكم فيه بواسطة واضع السياسات. إذا تم حساب متوسط معدل حركة مرور السن المنشار، فإن هذا المعدل أقل بكثير من المعدل المحدد. ومع ذلك، يمكنك زيادة الاندفاع لتحقيق إستخدام أفضل. بداية جيدة هي تعيين الاندفاع الذي يساوي ضعف كمية حركة المرور المرسلة مع المعدل المرغوب أثناء وقت الذهاب والعودة (TCP RTT). إذا لم يكن RTT معروفا، يمكنك مضاعفة قيمة المعلمة burst.

ولنفس السبب، لا يوصى بإجراء إختبار معياري لعملية الشرطي بواسطة حركة المرور الموجهة للاتصال. يظهر هذا السيناريو بشكل عام أداء أقل من الذي يسمح به الشرطي.

كما يمكن لحركة المرور غير المتصلة الاستجابة بشكل مختلف لعمليات ضبط الأمن. على سبيل المثال، يستخدم نظام ملفات الشبكة (NFS) الكتل، والتي يمكن أن تتألف من أكثر من حزمة واحدة لبروتوكول مخطط بيانات المستخدم (UDP). يمكن أن تؤدي حزمة واحدة يتم إسقاطها إلى تشغيل العديد من الحزم، حتى الكتلة بأكملها، لإعادة إرسالها.

يقوم هذا المثال بحساب الاندفاع لجلسة عمل TCP بمعدل تنظيم يبلغ 64 كيلوبت/ثانية ونظرا لأن TCP RTT هو، 0.05 ثانية:

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

في هذا المثال، يكون <burst>لجلسة TCP واحدة. قم بقياس هذا الشكل ليعمل على متوسط عدد الجلسات المتوقع أثناء التنقل عبر واضع السياسات.

ملاحظة: هذا مثال فقط، في كل حالة تحتاج إلى تقييم حركة المرور ومتطلبات التطبيقات والسلوك مقابل الموارد المتاحة لاختيار معلمات تنظيم النظام.

يمكن أن يكون إجراء السياسة إما لإسقاط الحزمة أو تغيير DSCP الخاصة بالحزمة (العلامات). لتحديد الحزمة، يجب تعديل خريطة DSCP المخططة. يلاحظ مخطط DSCP الافتراضي الخاضع للتنظيم الحزمة إلى DSCP نفسه. لذلك، لا تحدث أي علامات تمييز.

يمكن إرسال الحزم بدون ترتيب عندما يتم وضع علامة أسفل حزمة خارج ملف التعريف إلى DSCP معينة في قائمة انتظار إخراج مختلفة عن DSCP الأصلية. إذا كان ترتيب الحزم مهما، قم بتأشير الحزم الخارجة من ملف التعريف إلى DSCP المعين إلى نفس قائمة انتظار الإخراج كحزم داخل ملف التعريف.

السياسة وسمة سمة يساند ب المادة حفازة 3550

يقدم هذا الجدول ملخصا للسمات ذات الصلة بالتنظيم ووضع العلامات التي يدعمها المحول Catalyst 3550، وينقسم حسب الإتجاه:

	Direction	
Feature	Ingress	Egress
Individual policers	Yes, totally 128 for GE and 8 for FE including ingress aggregate policers	Yes, totally 8 including egress aggregate policers
Aggregate policers	Yes, totally 128 for GE and 8 for FE including ingress individual policers	Yes, totally 8 including egress individual policers
Marking	Yes	No
Policer Markdown	Yes	Yes
Match with ACL	Yes	**No**
Match DSCP	Yes	**Yes**
Match IP precedence	Yes	No
Match COS	Yes, for non-IP traffic	No
Trust DSCP	Yes	No
Trust COS	Yes	No
Trust IP precedence	Yes	No

يتم دعم عبارة مطابقة واحدة لكل خريطة فئة. هذه جمل مطابقة صالحة لنهج المدخل:

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

ملاحظة: على المادة حفازة 3550، لا يتم دعم أمر **تطابق الواجهة** ويتم السماح بأمر تطابق واحد فقط في خريطة الفئة. لذلك، من الصعب تصنيف جميع حركة المرور التي تأتي من خلال واجهة والتحكم في جميع حركة المرور باستخدام شرطي واحد. راجع كيفية تصنيف جميع حركة مرور الواجهة باستخدام قسم منظم واحد في هذا المستند.

هذه هي عبارة المطابقة الصالحة لنهج الخروج:

- مطابقة ip dscp

هذه إجراءات نهج صالحة لنهج الدخول:

- شرطة
- مجموعة ip dscp (تمييز)
- ضبط أسبقية IP (التمييز)
- الثقة في DSCP
- أسبقية بروتوكول الإنترنت (IP)
- تراست كوس

يوضح هذا الجدول مصفوفة سياسات جودة الخدمة المعتمدة عند المدخل:

Trust I/F	Match DSCP[1]	Match ACL	Trust Class[2]	Set DSCP[3]	Police	Result
						Traffic is assigned default QOS level of the port (0 by default)
√						QOS level of incoming traffic is preserved, according to what is trusted
	√		√		√	IP Traffic is matched by DSCP and then trusted then policed, excess traffic dropped or marked down
	√		√			IP Traffic is matched by DSCP/IP precedence and its QOS level is preserved
	√			√		IP Traffic is matched by DSCP/IP precedence then marked
	√			√	√	IP Traffic is matched by DSCP/IP precedence then marked then policed
		√	√		√	Traffic is matched by access list, QOS level of the matched traffic is preserved, then traffic is policed
		√	√			Traffic is matched by access list and its QOS level is preserved according to what is trusted
		√		√	√	Traffic is matched by access list then marked and then policed
		√		√		Traffic is matched by ACL then marked with specified DSCP/IP precedence
		MAC ACL w/COS	√			Match non-IP traffic by MAC EtherType and COS and preserve QOS level
		MAC ACL w/COS	√		√	Match non-IP IP traffic by MAC EtherType and COS and preserve QOS level then police
		MAC ACL w/COS		√		Match non-IP IP traffic by MAC EtherType and COS then mark matched traffic
		MAC ACL W/COS		√	√	Match non-IP IP traffic by MAC EtherType and COS then mark and then police

1. يغطي هذا الخيار أيضا أسبقية IP المطابقة.
2. يغطي هذا الخيار بيانات الاعتماد CoS، أسبقية IP، و DSCP.
3. يغطي هذا الخيار أيضا إعداد أسبقية IP.

هذا هو إجراء النهج الصحيح لنهج الخروج:

- شرطة

يوضح هذا الجدول مصفوفة سياسات جودة خدمة الخروج المدعومة:

Match DSCP	Police	Result
		Traffic is sent out with COS and IP precedence according to QOS maps and internal DSCP after ingress QOS processing
√	√	Traffic is matched by DSCP and policed

يسمح العلامات بتغيير مستوى جودة الخدمة للحزمة استنادا إلى التصنيف أو السياسة. يقسم التصنيف حركة المرور إلى فئات مختلفة لمعالجة جودة الخدمة بناء على المعايير المحددة.

تستند معالجة جودة الخدمة إلى DSCP الداخلي، وهو قياس مستوى جودة الخدمة للحزمة. يتم اشتقاق DSCP الداخلي وفقا لتكوين الثقة. يدعم النظام الثقة في CoS و DSCP وأسبقية IP والواجهات غير الموثوق بها. تحدد الثقة الحقل الذي يتم اشتقاق DSCP الداخلي منه لكل حزمة، كما يلي:

- عند الاعتماد على CoS، يتم اشتقاق مستوى جودة الخدمة من رأس الطبقة 2 (L2) من بروتوكول الارتباط بين المحولات (ISL) أو الحزمة المدمجة 802.1Q.
- عند الثقة في أسبقية DSCP أو IP، يستمد النظام مستوى جودة الخدمة من حقل أسبقية DSCP أو IP للحزمة وفقا لذلك.

تكون ثقة CoS ذات معنى فقط على توصيل الواجهات، ويكون الثقة في DSCP (أو أسبقية IP) منطقية لحزم IP فقط.

عندما لا تكون الواجهة موثوق بها، يتم اشتقاق DSCP الداخلي من قوائم التحكم (CoS) الافتراضية القابلة للتكوين للواجهة المقابلة. هذه هي الحالة الافتراضية عند تمكين جودة الخدمة. إذا لم يتم تكوين أي أوامر مساعدة افتراضية، تكون القيمة الافتراضية صفر.

وبمجرد تحديد بروتوكول DSCP الداخلي، يمكن تغييره من خلال وضع العلامات وتحديد النهج أو الاحتفاظ به.

بعد أن تخضع الحزمة لمعالجة جودة الخدمة، يتم تحديث حقول مستوى جودة الخدمة الخاصة بها (داخل حقل IP/DSCP ل IP، وداخل رأس ISL/802.1Q، إن وجدت) من بروتوكول DSCP الداخلي. توجد هذه الخرائط الخاصة بجودة الخدمة (QoS) ذات الصلة بضبط الأمن:

- **DSCP إلى SCP** - يستخدم **من** أجل اشتقاق DSCP المحدد عند خفض الحزمة.
- **DSCP إلى -CoS** - يتم إستخدامها لاستخلاص مستوى CoS من بروتوكول DSCP الداخلي لتحديث رأس حزمة ISL/802.1Q الصادرة.
- **CoS إلى DSCP**—يتم إستخدامها لاستخلاص DSCP الداخلي من CoS الواردة (ISL/802.1Q) عندما تكون الواجهة في وضع CoS للثقة.

وهذه اعتبارات هامة خاصة بالتنفيذ:

- لا يمكن إرفاق سياسة خدمة الدخول بالواجهة عند تكوين الواجهة للثقة في أي من مقاييس جودة الخدمة، مثل أسبقية CoS/DSCP أو IP. للمطابقة على أسبقية DSCP/IP والشرطة على المدخل، يجب تكوين الثقة للفئة المحددة داخل السياسة، وليس على الواجهة. لوضع علامة استنادا إلى أسبقية DSCP/IP، يجب عدم تكوين أية ثقة.
- يتم إعتبار حركة مرور IPv4 فقط التي لا تتضمن خيارات IP وتضمين وكالة مشاريع البحث المتقدمة (ARPA) عبر شبكة إيثرنت من منظور الأجهزة وجودة الخدمة. تعتبر جميع حركات المرور الأخرى غير خاصة ب IP، بما في ذلك، IP مع خيارات، مثل بروتوكول الوصول إلى الشبكة الفرعية (SNAP) المغلف IP و IPv6.
- بالنسبة للحزم غير الخاصة ب IP، تكون "مجموعة الوصول المطابقة" هي الطريقة الوحيدة للتصنيف لأنك لا تستطيع مطابقة DSCP لحركة المرور غير الخاصة ب IP. يتم إستخدام قائمة الوصول (ACL) إلى التحكم في الوصول إلى الوسائط (MAC) لهذا الغرض؛ يمكن مطابقة الحزم استنادا إلى عنوان MAC المصدر، وعنوان

MAC الوجهة، و EtherType. لا يمكن مطابقة حركة مرور IP مع قائمة التحكم في الوصول (ACL) إلى MAC، نظرا لأن المحول يميز بين حركة مرور IP وغير IP.

تكوين وضع السياسات ومراقبتها

هذه الخطوات ضرورية لتكوين السياسة في Cisco IOS:

1. تحديد واضع السياسات (لواضعي السياسات المجمعة)
2. قم بتحديد معايير لتحديد حركة مرور البيانات للشرطة
3. قم بتحديد خريطة فئة لتحديد حركة المرور باستخدام معايير محددة
4. تحديد سياسة خدمة باستخدام الفئة وتطبيق واضع السياسات على الفئة المحددة
5. تطبيق سياسة الخدمة على منفذ ما

يتم دعم هذين النوعين من المنظمين:

- تجميع مسمى
- إفراديا

يقوم واضع سياسات التجميع المسمى بتخطيط حركة المرور المجمعة من جميع الفئات ضمن نفس النهج إلى حيث يتم تطبيقها. لا يتم دعم تنظيم التجميع عبر الواجهات المختلفة.

ملاحظة: لا يمكن تطبيق منظم التجميع على أكثر من نهج واحد. إذا كان كذلك، يتم عرض رسالة الخطأ هذه:

```
<QoS: Cannot allocate policer for policy map <policy name
```

تأمل في هذا المثال:

هناك مولد حركة مرور يربط إلى ميناء GigabitEthernet0/3 أن يرسل تقريبا 17 Mbps من حركة مرور UDP مع الغاية ميناء 111. هناك أيضا حركة مرور TCP من المنفذ 20. أنت تريد أن يتم تنظيم دفقات حركة المرور هذه إلى 1 ميجابت في الثانية، ويجب إسقاط حركة المرور الزائدة. يوضح هذا المثال كيفية القيام بذلك:

```
mls qos !--- Defines the QoS policer, sets the burst !--- to 16000 ---! Globally enables QoS.
mls qos aggregate-policer pol_1mbps 1000000 16000 exceed-action drop !--- Defines the QoS policer, sets the burst !--- to 16000 ---! for better TCP performance.
access-list 123 permit udp any any eq 111 !--- Defines the ACLs to select traffic. ---!
access-list 145 permit tcp any eq 20 any
class-map match-all cl_udp111 match access-group 123 !--- Defines the traffic classes to be policed. ---!
class-map match-all cl_tcp20
match access-group 145
policy-map po_test !--- Defines the QoS policy, and attaches !--- the policer to the traffic classes. ---!
class cl_udp111
police aggregate pol_1mbps
class cl_tcp20
police aggregate pol_1mbps
interface GigabitEthernet0/3 switchport switchport access vlan 2 service-policy input po_test !--- Applies the QoS policy to an interface. ---!
!
```

أستخدم المثال الأول واضع سياسات التجميع المسمى. يقوم واضع السياسات الفردي، بخلاف واضع السياسات المسمى، بتقدير حركة المرور بشكل منفصل على كل فئة يتم تطبيقها فيها. يتم تحديد واضع السياسات الفردي ضمن تكوين خريطة السياسة. في هذا المثال، يتم تنظيم فتتين من حركة المرور بواسطة إثنين من المنظمين الفرديين، ويتم تنظيم cl_udp111 إلى 1 ميجابت في الثانية لكل انفجار 8k، ويتم تنظيم cl_tcp20 إلى 512 كيلوبت في الثانية لكل

انفجار 32 كيلو:

```
Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 123 ---!
                                                        permit udp any any eq 111
                                                access-list 145 permit tcp any eq 20 any
Defines the traffic classes to be policed. class-map match-all cl_udp111 ---!
                                                          match access-group 123
                                                    class-map match-all cl_tcp20
                                                          match access-group 145
Defines QoS policy, and creates and attaches !--- the policers to the traffic classes. ---!
                                                             policy-map po_test2
                                                               class cl_udp111
                                                  police 1000000 8000 exceed-action drop
                                                                class cl_tcp20
                                                  police 512000 32000 exceed-action drop
Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport switchport ---!
                                                 access vlan 2 service-policy input po_test2
```

يتم إستخدام هذا الأمر من أجل مراقبة عملية السياسة:

```
cat3550#show mls qos interface g0/3 statistics
                                                                GigabitEthernet0/3
                                                                          Ingress
(dscp: incoming   no_change  classified policed    dropped (in pkts
Others: 267718     0          267717     0          0
                                                                           Egress
(dscp: incoming   no_change  classified policed    dropped (in pkts
Others: 590877       n/a       n/a      266303     0

                                                                 :WRED drop counts
                                                       qid  thresh1    thresh2   FreeQ
                                                        1024         0          0 : 1
                                                        1024         0          0 : 2
                                                           8         0          0 : 3
                                                        1024         0          0 : 4
```

ملاحظة: لا توجد بشكل افتراضي إحصائيات لكل DSCP. يدعم المحول Catalyst 3550 مجموعة إحصائيات لكل واجهة وكل إتجاه لما يصل إلى ثماني قيم DSCP مختلفة. يتم تكوين هذا عند إصدار الأمر **mls qos monitor**. من أجل مراقبة إحصائيات 8 DSCPs و 16 و 24 و 32، يجب عليك إصدار هذا الأمر **لكل واجهة**:

```
cat3550(config-if)#mls qos monitor dscp 8 16 24 32
```

ملاحظة: يقوم الأمر **MLS QoS monitor dscp 8 16 24 32** بتغيير إخراج الأمر **show mls qos int g0/3 statistics** إلى هذا:

```
cat3550#show mls qos interface g0/3 statistics
                                                                GigabitEthernet0/3
                                                                          Ingress
(dscp: incoming   no_change  classified policed    dropped (in pkts
0          0  675053785          0          0 : 8
per DSCP statistics ?         0          0          0          0    1811748 :16
0          0          0   15241073 1227820404 :24
0          0  539337294          0          0 :32
Others: 1658208    0          1658208    0          0
                                                                           Egress
(dscp: incoming   no_change  classified policed    dropped (in pkts
```

```
                                    n/a       n/a      0          0      675425886 : 8
n/a       n/a       0               0         ? per DSCP statistics             0 :16
                                    n/a       n/a      0          0       15239542 :24
                                    n/a       n/a      536486430  0      539289117 :32
                                    Others: 1983055       n/a       n/a       1649446    0

                                                                    :WRED drop counts
                                                          qid  thresh1    thresh2   FreeQ
                                                           1024         0          0 : 1
                                                           1024         0          0 : 2
                                                              6         0          0 : 3
                                                           1024         0          0 : 4
```

هذا وصف للحقول في المثال:

- **الوارد** — يعرض عدد الحزم التي تصل من كل إتجاه
- **NO_CHANGE**— يعرض عدد الحزم التي تم الوثوق بها (مثل مستوى جودة الخدمة الذي لم يتم تغييره)
- **المصنف** — يعرض عدد الحزم التي تم تعيينها إلى DSCP الداخلي هذا بعد التصنيف
- **بوليط**—يعرض عدد الحزم التي تم تعليمها أسفل بواسطة السياسة؛ DSCP الموضحة قبل التحديد.
- **drop** — يعرض عدد الحزم التي تم إسقاطها من قبل الشرطة

يجب أن تكون على دراية بهذه الاعتبارات الخاصة بالتنفيذ:

- إذا تم تكوين ثماني قيم DSCP عند إصدار الأمر **mls qoS monitor**، فإن العداد الآخر يظهر عند إصدار الأمر **show mls qos int statistics** يمكن أن يعرض معلومات غير كافية.
- لا يوجد أمر محدد للتحقق من معدل حركة المرور المقدمة أو الصادرة لكل منظم.
- ونظرا لأنه يتم إسترداد العدادات من الأجهزة بشكل تسلسلي، فمن الممكن ألا تتم إضافة العدادات بشكل صحيح. على سبيل المثال، يمكن أن يختلف مقدار الحزم التي تم تنظيمها أو تصنيفها أو إسقاطها إختلافا طفيفا عن عدد الحزم الواردة.

تمييز التكوين والمراقبة

هذه الخطوات ضرورية لتكوين التمييز:

1. تحديد معايير تصنيف حركة المرور
2. تحديد فئات حركة المرور التي سيتم تصنيفها باستخدام المعايير المحددة مسبقا
3. قم بإنشاء خريطة سياسة تربط إجراءات وضع العلامات وإجراءات تنظيم الفئات المعرفة
4. تكوين الواجهة (الواجهات) المطابقة لوضع الثقة
5. تطبيق خريطة السياسة على واجهة

في هذا المثال، تريد أن تستضيف حركة مرور IP الواردة 192.168.192.168 المميزة بأسبقية IP 6 والتي يتم التحكم فيها حتى 1 ميجابت في الثانية، ويجب وضع علامة على حركة المرور الزائدة حتى أسبقية IP 2:

```
Globally enables QoS. mls qos !--- Defines the ACLs to select traffic. access-list 167 ---!
                                                    permit ip any host 192.168.192.168
                                  Defines the traffic class. class-map match-all cl_2host ---!
                                                      match access-group 167
Defines QoS policy, and creates and attaches !--- the policers to the traffic classes. ---!
                                                   policy-map po_test3
                                                     class cl_2host
                                 Marks all the class traffic with the IP precedence 6. set ip precedence 6 ---!
Polices down to 1 Mbps and marks down according to the QoS map. police 1000000 8000 exceed- ---!
                                                    action policed-dscp-transmit
 Modifies the policed DSCP QoS map, so the !--- traffic is marked down from IP precedence 6 ---!
to 2. !--- In terms of DSCP, this is from 48 to 16 (DSCP=IPprec x8). mls qos map policed-dscp 48
      to 16 !--- Applies the QoS policy to an interface. interface GigabitEthernet0/3 switchport
```

```
switchport access vlan 2 service-policy input po_test3
```

يتم إصدار الأمر **show mls qos interface statistics** نفسه من أجل مراقبة العلامات. يتم توثيق نموذج المخرجات والتأثيرات في قسم هذا المستند.

كيفية تصنيف جميع حركة مرور الواجهة باستخدام واضع سياسات واحد

على المادة حفازة 3550، **ال match قارن** لا يساند أمر، وفقط واحد مطابقة أمر سمحت لكل صنف-map. علاوة على ذلك، لا يسمح المادة حفازة 3550 لحركة مرور IP أن تكون مطابقة بقوائم التحكم في الوصول (MAC). لذا يجب تصنيف حركة مرور IP وغير IP باستخدام خطتي فئة منفصلتين. وهذا يجعل من الصعب تصنيف جميع حركة المرور التي تأتي إلى واجهة والتحكم في حركة المرور بالكامل باستخدام شرطي واحد. يتيح لك نموذج التكوين هنا تحقيق ذلك. في هذا التكوين، تتم مطابقة حركة مرور IP وغير IP مع خطتي فئة مختلفتين. ومع ذلك، يستخدم كل واحد واضع سياسات مشترك لكل من حركة المرور.

```
access-list 100 permit ip any any

class-map ip
match access-group 100
This class-map classifies all IP traffic. mac access-list extended non-ip-acl ---!
permit any any

class-map non-ip
match access-group name non-ip-acl
Class-map classifies all non-IP traffic only. mls qos aggregate-policer all-traffic 8000 ---!
8000 exceed-action drop
This command configures a common policer that is applied for both IP and non-IP traffic. ---!
policy-map police-all-traffic
class non-ip
police aggregate all-traffic
class ip
police aggregate all-traffic

interface gigabitEthernet 0/7
service-policy input police-all-traffic
.This command applies the policy map to the physical interface ---!
```

معلومات ذات صلة

- تكوين جودة الخدمة على Catalyst 3550
- صفحات دعم جودة الخدمة
- صفحة دعم تحويل شبكة LAN
- صفحات دعم منتجات شبكة 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).