فهم تجاهل الحزمة الانتقائي (SPD)

المحتويات

المقدمة
قبل البدء
الاصطلاحات
المتطلبات الأساسية
المكونات المستخدمة
نظرة عامة
عملية شرطة مدينة سياتل
فحص حالة SPD
فحص قائمة انتظار الإدخال
منوعات
معلومات ذات صلة

المقدمة

يشرح هذا المستند آلية تجاهل الحزمة الانتقائي (SPD) وكيف يمكن مراقبتها وملاحقتها.

ملاحظة: لا يشرح هذا المستند كيفية أستكشاف أخطاء عدد متزايد من عمليات إسقاط الإدخال وإصلاحها في إخراج **show interfaces** على موجه إنترنت من السلسلة 12000 من Cisco. لمزيد من المعلومات حول هذه المشكلة، ارجع إلى أستكشاف أخطاء الإدخال وإصلاحها على موجه الإنترنت من السلسلة Cisco 12000 Series.

قبل البدء

الاصطلاحات

أحلت cisco في طرف إتفاق لمعلومة على وثيقة إتفاق.

المتطلبات الأساسية

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- سلسلة موجهات طراز 7200 من Cisco
- سلسلة موجهات طراز 7500 من Cisco
- سلسلة موجهات الإنترنت طراز 12000 من Cisco
- جميع إصدارات برنامج Cisco IOS®

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

نظرة عامة

تجاهل الحزمة الانتقائي (SPD) هو آلية لإدارة قوائم انتظار إدخال مستوى العملية على معالج التوجيه (RP). الهدف من بروتوكول SPD هو توفير الأولوية لحزم بروتوكول التوجيه وحزم keepalive الأخرى المهمة للتحكم في حركة المرور من الطبقة 2 أثناء فترات إزدحام قائمة انتظار مستوى العملية.

تاريخيا، على الأنظمة الأساسية مثل أنظمة Cisco 7x00 وغير 7500 Cisco Express Forwarding (CEF)، تمت إعادة توجيه أعداد كبيرة من حزم النقل بواسطة معالج التوجيه من أجل ملء ذاكرة التخزين المؤقت للتحويل السريع. ونتيجة لذلك، كان يتعين على شرطة مدينة سياتل في هذه الحالة ترتيب أولويات حزم بروتوكول التوجيه عبر حزم النقل التي تشترك في نفس قائمة الانتظار.

حاليا، على موجه الإنترنت من السلسلة Cisco 12000 وعلى حركة مرور 7500 التي تشغل CEF، يتم إرسال حركة المرور الموجهة إلى الموجه نفسه إلى مستوى العملية. في هذه الحالة، يتم إستخدام بروتوكول SPD لتحديد أولويات حزم بروتوكول التوجيه عند وجود حركة مرور بيانات خاصة بالإدارة مثل بروتوكول إدارة الشبكة البسيط (SNMP) أو عند حدوث هجوم لرفض الخدمة (DoS) يؤدي إلى إرسال حركة مرور البيانات إلى RP.

عملية شرطة مدينة سياتل

على السلسلة Cisco 12000، عندما تحدد بطاقة خط أن حزمة واردة تحتاج إلى الضرب على بروتوكول RP لمعالجتها، تنتقل الحزمة عبر بنية المحول كخلايا Cisco ويتم استقبالها في نهاية المطاف بواسطة مصفوفة البوابات القابلة للبرمجة في حقل (Cisco Cell Segmentation and Reassembly (CSAR.

والغرض منه هو معالجة حركة مرور البيانات بين بنية المحول ووحدة المعالجة المركزية ل RP، وهذا هو المكان الذي يتم فيه إجراء فحوصات SPD. ينطبق هذا على حزم IP وحزم خدمة الشبكة (CLNS) غير المتصلة وحزم رسائل keepalive من الطبقة 2 والحزم المماثلة التي يتم تثبيتها على RP. تقوم شرطة مدينة سياتل بالتحقق من الأمر وتستطيع إسقاط الحزمة في إحدى هاتين الحالتين:

- فحص حالة SPD
- فحص قائمة انتظار الإدخال

فحص حالة SPD

تنقسم قائمة انتظار عملية IP الموجودة على RP إلى جزئين: قائمة انتظار حزم عامة وقائمة انتظار أولوية. تخضع الحزم التي يتم وضعها في قائمة انتظار الحزمة العامة إلى فحص حالة SPD، ولا تخضع الحزم التي يتم وضعها في قائمة انتظار الأولوية. الحزم التي تكون مؤهلة لقائمة انتظار حزم الأولوية هي حزم ذات أولوية عالية مثل حزم IP ذات أسبقية 6 أو 7 ويجب عدم إسقاطها أبدا. ومع ذلك، يمكن إسقاط الفئات غير المؤهلة هنا وفقا لطول قائمة انتظار الحزمة العامة وفقا لحالة SPD. يمكن أن تكون قائمة انتظار الحزم العامة في ثلاث حالات، وعلى هذا النحو، يمكن خدمة الحزم ذات الأولوية المنخفضة بشكل مختلف:

- عادي: حجم قائمة الانتظار <= الحد الأدنى
- إسقاط عشوائي: الحد الأدنى <= حجم قائمة الانتظار <= الحد الأقصى
- إسقاط كامل: الحد الأقصى <= حجم قائمة الانتظار

في الحالة العادية، لا نقوم أبدا بإسقاط حزم مكونة بشكل جيد ومشوهة.

في حالة الإسقاط العشوائي، نقوم بشكل عشوائي بإسقاط الحزم ذات التكوين الجيد. إذا تم تكوين الوضع القوي، فإننا تسقط جميع الحزم التي تم تكوينها بشكل غير صحيح؛ وإلا، فإننا نعالجها كحزم مكونة بشكل جيد.

ملاحظة: تسمى هذه النقاط العشوائية تنوعات SPD. بشكل أساسي، عندما يتم تحميل الواجهة بشكل زائد، تحدث التوهجات. تتسبب أخطاء المخزن المؤقت في زيادة عداد التسييل.

في حالة الإسقاط الكامل، نقوم بإسقاط جميع الحزم التي تم تكوينها بشكل جيد والتي تم تكوينها بشكل غير صحيح. يتم اشتقاق القيم الدنيا (الافتراضية 73) والقيمة القصوى (الافتراضية 74) من أصغر قائمة انتظار على الهيكل، ولكن يمكن تخطيها باستخدام الأوامر العامة **ip spd queue min-threshold** و**ip spd queue max-threshold**.

وضع عدواني

يمكن تكوين SPD لوضعين مختلفين: normal (default) and aggressive. يكمن الفرق الوحيد بين الاثنين في كيفية حساب الموجه لحزم IP غير الصالحة (المجموع الاختباري غير الصحيح، الإصدار غير الصحيح، طول الرأس غير الصحيح، طول الحزمة غير الصحيح). يتم إسقاط حزم IP التي تم تكوينها بشكل غير صحيح بواسطة بروتوكول SPD عندما نكون في وضع التثاقل وفي حالة الإسقاط العشوائي. يمكن تكوين الوضع المتميز باستخدام الأمر **ip spd mode aggressive**.

ملاحظة: لا يتم تنفيذ الوضع العدواني على موجه الإنترنت من السلسلة Cisco 12000 Series لأن حزم IP التي تم تكوينها بشكل غير صحيح يتم إسقاطها مباشرة من خلال بطاقة خط الدخول، ولا يتم إخضاع هذه الحزم إلى معالج توجيه جيجابت (GRP). ونتيجة لذلك، لا توجد حاجة إلى وضع المرونة على هذا النظام الأساسي المعين.

فحص قائمة انتظار الإدخال

يتم الاحتفاظ بقائمة انتظار الإدخال لكل واجهة جهاز، ويتم مشاركتها بين جميع الواجهات الفرعية. بدون SPD، يتم إسقاط جميع الحزم إذا كانت قائمة انتظار الإدخال ممتلئة عند إستلام الحزمة. الحجم الافتراضي لقائمة انتظار الإدخال هو 75 وهو قابل للتكوين لكل واجهة باستخدام *أمر تكوين الواجهة size* [**hold-queue** **في**]. يمكن ملاحظة عدد الحزم في قائمة انتظار الإدخال في حقل "قائمة انتظار الإدخال" في الأمر **show interfaces**.

```
router#show interfaces pos 3/0
POS3/0 is up, line protocol is up
    Hardware is Packet over SONET
    Internet address is 137.40.55.2/24
MTU 4470 bytes, BW 2488000 Kbit, DLY 100 usec, rely 255/255, load 1/255
    Encapsulation PPP, crc 32, loopback not set
    Keepalive not set
    Scramble disabled
    LCP Open
    Open: IPCP, CDPCP, OSICP, TAGCP
Last input 00:00:01, output 00:00:00, output hang never
    Last clearing of "show interface" counters 2w3d
    Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
      second input rate 9000 bits/sec, 0 packets/sec 30
      second output rate 0 bits/sec, 0 packets/sec 30
    packets input, 917329913 bytes, 0 no buffer 456292
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
                parity 0
input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 0
    packets output, 32078928095 bytes, 0 underruns 112046977
    output errors, 0 applique, 3 interface resets 0
  output buffer failures, 0 output buffers swapped out 0
    carrier transitions 1
```

ملاحظة: يمكن أن يؤدي تقليل حجم قائمة انتظار الإدخال على واجهة واحدة إلى حدوث عدد كبير من حالات إسقاط الإدخال على جميع الواجهات الأخرى. تأكد من أن الحد الأدنى لحجم قائمة الانتظار قيد التعليق للإدخال هو 75 على الأقل.

مساحة SPD

حتى مع SPD، لا يتم تغيير سلوك حزم IP العادية، ومع ذلك، يتم إعطاء حزم بروتوكول التوجيه أولوية أعلى لأن SPD يتعرف على حزم بروتوكول التوجيه بواسطة حقل أسبقية IP. لذلك، إذا تم تعيين أسبقية IP على 6، فعندئذ يتم إعطاء الأولوية للحزمة.

تقوم حماية مستوى التحكم (SPD) بترتيب هذه الحزم حسب الأولوية من خلال السماح للبرنامج بإدراجها في قائمة انتظار إدخالات مستوى العملية التي تتجاوز الحد العادي لقائمة انتظار الإدخال. يسمى عدد الحزم المسموح بها بما يزيد عن الحد العادي "غرفة عمل SPD"، حيث يكون الافتراضي هو 100، مما يعني أنه لا يتم إسقاط حزمة ذات أسبقية عالية إذا كان حجم قائمة انتظار الإدخال أقل من 175 (الحجم الافتراضي لقائمة انتظار الإدخال + حجم غرفة عمل SPD).

وكما هو الحال مع برنامج Cisco IOS الإصدار 12.0S(22)، يكون إعداد غرفة عمل SPD الافتراضي هو 1000 لموجه الإنترنت من السلسلة Cisco 12000 Series لاستيعاب شبكات SP الأكبر. وهذا يرجع إلى حقيقة إستخدام تجفيف بروتوكولات العبارة الحدودية (BGP) مع عدد متزايد باستمرار من الجيران للإعلان عن عدد متزايد دوما من المسارات عبر واجهات متزايدة السرعة. وقد يؤدي مسح واحد لبروتوكول BGP غالبا إلى آلاف من حالات سقوط قائمة انتظار الإدخال على واجهة واحدة، وهو ما يمكن أن يعيق أوقات التقارب بشدة.

غرفة الاستقبال والبث الخاصة ب SPD قابلة للتكوين باستخدام أمر **غرفة الاستقبال والبث الخاصة ب SPD**. يمكن ملاحظة مستواه الحالي في إخراج الأمر **show spd** أو **show ip spd**.

```
Router#show spd
Headroom: 1000, Extended Headroom: 10

Router#show ip spd
Current mode: normal
Queue min/max thresholds: 73/74, Headroom: 1000, Extended Headroom: 10
.IP normal queue: 0, priority queue: 0
SPD special drop mode: none
```

ملاحظة: يمكن أيضا مراقبة حجم قائمة انتظار IP العادية بواسطة الأمر **show ip spd**.

مساحة SPD الممتدة

كانت الحزم غير الخاصة ب IP، مثل حزم Network Service الوسيطة للنظام إلى النظام الوسيط (CLNS ISIS)، وحزم بروتوكول الاتصال من نقطة إلى نقطة (PPP)، وحزم رسائل التحكم في إرتباط البيانات عالية المستوى (HDLC)، حتى وقت قريب، يتم التعامل معها كأولوية عادية نتيجة لكونها الطبقة 2 بدلا من الطبقة 3. وبالإضافة إلى ذلك، تم منح بروتوكولات العبارة الداخلية (IGPs) التي تعمل في الطبقة 3 أو أعلى الأولوية على حزم IP العادية، ولكن تم منحها نفس أولوية حزم BGP. لذلك، أثناء تقارب BGP أو أثناء أوقات نشاط BGP المرتفع جدا، غالبا ما يتم إسقاط فئتي IGP و keepalives، مما يؤدي إلى انخفاض عمليات تجاور IGP.

ونظرا لأن إستقرار بروتوكول العبارة الداخلية والارتباط أكثر هشاشة وأهمية من إستقرار BGP، فهذه الحزم يتم منحها الآن الأولوية العليا ويتم منحها مساحة عمل موسعة لبروتوكول SPD مع إعداد افتراضي يبلغ 10 حزم. وهذا يعني أنه لا يتم إسقاط هذه الحزم إذا كان حجم قائمة الانتظار قيد الانتظار للإدخال أقل من 185 (الحجم الافتراضي لقائمة انتظار الإدخال + حجم غرفة الاستقبال الخاصة ب SPD + مساحة الاستقبال الموسعة ل SPD).

تعد غرفة عمل SPD الموسعة قابلة للتكوين باستخدام الأمر **SPD Extended** [*size*]، ويمكن ملاحظة مستواها الحالي من إخراج الأمر **show spd** أو **show ip spd**.

```
Router#show ip spd
Current mode: normal
Queue min/max thresholds: 73/74, Headroom: 100, Extended Headroom: 10
.IP normal queue: 0, priority queue: 0
```

```
SPD special drop mode: none
```

ملاحظة: على موجه الإنترنت من السلسلة Cisco 12000، تتم معالجة حزم HDLC و PPP keepalives، بالإضافة إلى CLNS حزم بروتوكول التوجيه ISIS على أنها أولوية عالية وقد يتم وضعها في قائمة الانتظار في مساحة عمل SPD الموسعة منذ برنامج Cisco IOS الإصدار S1(12)12.0. ومنذ الإصدار S(18)12.0 من برنامج Cisco IOS Software، يمكن إدراج جميع حزم IGP في مساحة SPD الإضافية أيضا.

رسم تخطيطي لقائمة انتظار الإدخال

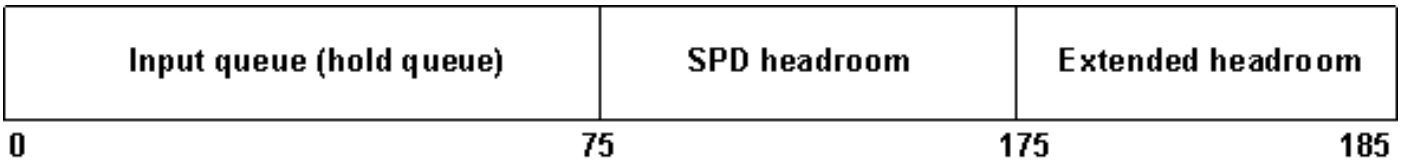
القيم الافتراضية، قبل برنامج CISCO IOS الإصدار S(22)12.0، هي:

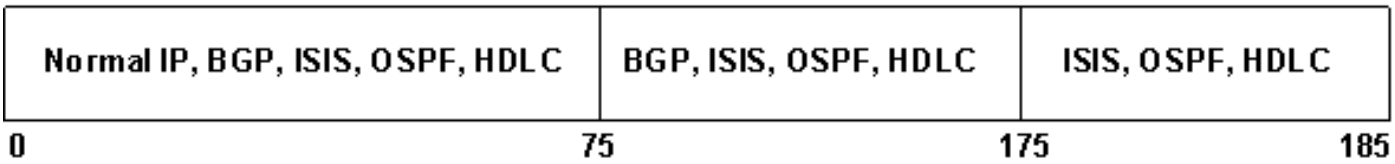
- حجم قائمة انتظار الإدخال = 75
- حجم غرفة الاستقبال والبث ل SPD = 100
- حجم غرفة الاستقبال الممتدة = 10

القيم الافتراضية، بعد برنامج Cisco IOS الإصدار S(22)12.0، هي:

- حجم قائمة انتظار الإدخال = 75
- حجم غرفة الاستقبال والبث ل SPD = 1000
- حجم غرفة الاستقبال الممتدة = 10

في الحالة الأولى، يعطي هذا:





- يسمح لحزم IP ذات الأولوية العادية بالوصول إلى حد قائمة الانتظار الافتراضي (75)
- يسمح لحزم IP ذات الأولوية العالية بالتسجيل حتى حد قائمة الانتظار الافتراضي + spd_headroom (175 أو 1075 استنادا إلى إصدار برنامج Cisco IOS)
- يسمح لحزم CLNS و IGP و LC keepalive بالوصول إلى حد قائمة الانتظار الافتراضي + + spd_headroom spd_ext_headroom (185 أو 1085 استنادا إلى إصدار برنامج Cisco IOS).

منوعات

فيما يلي بعض التلميحات/المعلومات الإضافية حول SPD:

- بشكل افتراضي، تكون SPD "قيد التشغيل". يمكن تمكينها/تعطيلها باستخدام الأمر global **SPD enable**.
- في البداية، كانت شرطة مدينة سياتل متوفرة فقط على واجهات الحزمة عبر بروتوكول PoS (SONET).
- قبل برنامج Cisco IOS الإصدار S(21)12.0، لم تعمل بطاقة SPD على بطاقات خط إيثرنت جيجابت (Engine 1 و Engine 2) وبطاقات خط الإيثرنت السريع التي يتم تثبيتها في موجه الإنترنت من السلسلة Cisco 12000. يجب زيادة قائمة انتظار تعليق الإدخال لتخزين الحزم الزائدة.
- على موجه السلسلة 7500/7200 من Cisco، يمكن ملاحظة عداد (عمليات إسقاط) تدفق SPD في إخراج الأمر **show interfaces** منذ إصدارات البرنامج Cisco IOS Software، الإصدار 12.1(1) و 12.1(1)T و 12.0(9)ST لقوائم انتظار غير FIFO (أول خروج أول) ومنذ الإصدار 12.2(7) و 12.2(7)T و 12.1(7)E لقوائم انتظار FIFO.

في الإصدارات الأخرى وعلى موجه الإنترنت من السلسلة Cisco 12000 Series، يتم ملاحظة هذا العداد فقط من خلال كتابة الأمر **show interface switching**. على سبيل المثال، يمكن إستخدام الأمر **show interface pos 0/1 switching** لعرض نتوءات SPD وحالات الإسقاط العدوانية والأولوية.فيما يلي مثال:

```
Router#show interfaces_7500

FastEthernet0/0/0 is up, line protocol is up

(Hardware is cyBus FastEthernet Interface, address is 0090.9282.7000 (bia 0090

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255

Encapsulation ARPA, loopback not set

(Keepalive set (10 sec

Full-duplex, 100Mb/s, 100BaseTX/FX

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:00:01, output 00:00:01, output hang never

Last clearing of "show interface" counters never

Queueing strategy: fifo

Output queue 0/40, 0 drops; input queue 0/75, 0 drops, 0 flushes

second input rate 4000 bits/sec, 9 packets/sec 30

second output rate 0 bits/sec, 0 packets/sec 30

packets input, 546327119 bytes, 0 no buffer 2628397

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0

watchdog, 0 multicast 0

input packets with dribble condition detected 0

packets output, 225434458 bytes, 0 underruns 264792

output errors, 0 collisions, 20 interface resets 0

babbles, 0 late collision, 0 deferred 0

lost carrier, 0 no carrier 22

output buffer failures, 0 output buffers swapped out 0
```

معلومات ذات صلة

- أستكشاف أخطاء الإدخال وإصلاحها على موجه الإنترنت Cisco 12000 Series
- أستكشاف أخطاء وحدة المعالجة المركزية (CPU) العالية وإصلاحها والتي تتسبب فيها عملية ماسح BGP الضوئي أو موجه BGP
- 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).