

تاهجوم اليف ةمدخل الةدوج ةيولوا نيوكت RSP2 و ASR 920 الةدنتسم ال

تايوتحمل

[ةمدقمل](#)

[ةيساس الابلطتم ال](#)

[تابلطتم ال](#)

[ةمدختسم ال تانوكمل](#)

[لكاشم](#)

[دوهج اللف مزح ةزيم يف اهطاقسا متي يتل ةيولوال تاذ مزح ال](#)

[لحل](#)

[تائف ال دح يف اهم يدقتل ي ددرت ال قاطن ال ضرع ةبسن باسح ةيفي ك](#)

[RSP2 ةمدخ ةدوج ةيولوا رابتخا](#)

[نيوكت ال](#)

[رورم ال ةكرح](#)

[راطال ال لعل لاثم](#)

[رورم ةكرح دلوم عم رابتخا](#)

[بلاس رابتخا](#)

[تانوس ول كنوك](#)

ةمدقمل

ةيفي ك و ةمدخل الةدوج تايولوال ASR920/RSP2 تاهجوم ةجلعم ةيفي ك دنتسم ال اذه حضوي
اهنيوكت.

ةيساس الابلطتم ال

تابلطتم ال

ةيلات ال عيضاوم لابل ةفرعم لكي دل نوكت نأب Cisco ي صوت:

- ASR 920 ةلسلس ال نم تاهجوم ال
- ةمدخل الةدوج تاسايس

ةمدختسم ال تانوكمل

رادص ال لغشي يذل RSP2 هجوم عم ASR 9xx ال دنتسم ال اذه يف ةدراول تامولعمل دنتست
جم انرب ال نم 17.x يتح 16.x.

ةيولوال مزح عم لماعتت يتل فئاظول رابتخال رورم ةكرح دلوم مادختسا متي.

ةصاخ ةيلمعم ةئيب يف ةدوجوم ال ةزهجال نم دنتسم ال اذه يف ةدراول تامولعمل عاشنإ مت
تناك اذ (يضا رتفا) حوسمم نيوكتب دنتسم ال اذه يف ةمدختسم ال ةزهجال عيمج تادب
رمأ ال لم تحمل ال ريثأتلل كمهف نم دكأ تف، ليغشت ال دي قكتك بش.

لكاشم

RSP2 و ASR 920 لى ةدننسملا تاهجوملاب ةصاخلال لكاشملا هذه دننسملا اذه لوانتي

- RSP2 لى ASIC دييقت ببسب دوهجال لضفأ مزح ةزيم دنن ةيولوالا مزح تطقس
- تائفلا دحأ يف اهميدقتل يدرتلا قاطنلا ضرع ةبسن باسح ةييفيك

لضفأ مزح ةزيم يف اهطاقسا متي يتلا ةيولوالا تاذ مزجال دوهجال

اذهو. دهج لصفأ ةمزح ةزيم يف ةيولوالا ةمزح طاقسا نكمي هنأ ديحت مت، رابتخال اناثأ ببستت وجرخملا ةهجاو نم لىل ةعرس تاذ ةهجاو لالخنم ةدراولا رورملا ةكرح لصت امدنن رهظي تانايبلا رورم ةكرح يقلت دنن، لاثملا لىبس لىل. جارخال اجاتا يف كارتشالا ةدايزي يف يف تباچي 1 ةعرسب ةهجاو ربع هيحوتلا ةداعا لىل ةجالحاو ةيناثلا يف تباچي 5 ةعرسب ةيناثلا.

تنالك لاجي يف. رغاش مادختساب اهنيوكت مت يتلا جورخال تاهجاو ل ردقلا سفنب حيحص اذهو ةمزجال طاقسا كلذ عم نكمي، جرخملا ةيولوا يف هنيوكت مت يذال CIR نم لىل ةعرسب لصفألا دهجال ةمزح ةزيمب.

ةيولوا يذ ريغ دلاول ةيولوا عبات انيدل نوكي نأ نكمي ال ASIC دح كانه: **ةظحالم**

اهب ةصاخلا ةيولوالا ةيولوالا ةانقلا نكت ملو عرسا اهنأ لىل راطتنا ةمئاق نيوكت مت اذا، يوتسم لىل مكيحتلا لاقتنا ةنمزا ببسب ةيولوالا تاذ راطتنا ال ةمئاق يف رتوت كانهف ةيولوالا ةانقلا.

لجال

1. EFP نيوكت
2. ةيولوالا ةمئاق لىل لكش قيبطت
3. EFP لىل ةبولطملا ةمدخل ةدوج قيبطت
4. BDI ةهجاو يف IP لاصتا قيبطت

لاثم:

configuration with issue

```
interface GigabitEthernet0/0/0
description this is my egress interface
service-policy output PM-1G-Out
```

configuration without issue

```
interface GigabitEthernet0/0/0
description this is egress interface
service-policy output POL-PRIO-MAIN-1G ==> shaper, useful to allow internal priority like BDF
service instance 200 ethernet
encapsulation dot1q 200
rewrite ingress tag pop 1 symmetric
service-policy output PM-1G-Out ==> the original QoS previously applied in the physical
interface
bridge-domain 200
```

!
interface BDI200 ==> BDI must match the bridge-domain defined under the service-instance
description this is L3 egress
ip address 10.20.2.45 255.255.255.0
ip mtu 9000
=> no QoS applied under the BDI, all QoS are in the service-instance with a backpressure of the shaper in the physical

يأ طاقسإ متي ملوحيحص لكشب ةيولوالأ مزح عي مج تايولوأ بيترت مت ، نيوكتلا اذه عم
صصخملا يددرتلا قاطنلا باسح ىلإ ةجأب تنأف ، كلذ عمو ، دوهجال لضفأ ةمزح ةزيم دنع انه م
جحيحص لكشب

دحأ يف اهم يدقتل يددرتلا قاطنلا ضرع ةبسن باسح ةيفي تائفلا

نم ريثكلا يفو . نيعم كولس اضيأ RSP2 ةصنم يف يددرتلا قاطنلا ضرع صيصخت ىدل
ىرخأ تاصنمك ةمدخللا ةدوج ةئيهت ءانثأ طوقسلا تالاح ةظحالم متي نايحألا

يف تباچيم 2 ةعرسب فنصم مادختساب ةمدخللا ةدوج نيوكتب تمق اذا ، لاثملا لبيس ىلع
يه الو ، ةيناثلا يف تباچيم 2 ىلإ لوصولا لبق طقسلا ال انه إف ، ASR1K هجوم يف ةيناثلا
RSP2 عم كلذ ثدحي ، كلذ عمو . ةئفلا يف مزحلا راطنلا مئاقو

ىرت ام دنع هب حومس مالا صقلا دحلا ىتح ةضورعملا ةعرسلا غلبت ال ، ةريثك تالاح يفو
اقبس م تاطقسلا

رورملا ةكرح سفنل ميقلال سفن امنيب ، RSP2 ىلع هتيرورم نكمي ام ىلع يجزومن لاثم اذه
طاقسإ ي رهظت نل رخأ يساسا ماظن ىلع ةقبطملا

```
ASR903#show ethernet service instance policy-map | s EXP-5
```

```
Class-map: EXP-5 (match-all)
```

```
58803127 packets, 5488269944 bytes
```

```
5 minute offered rate 279000 bps, drop rate 35000 bps
```

```
Match: mpls experimental topmost 5
```

```
Priority: 3% (297 kbps), burst bytes 37000, b/w exceed drops: 60373
```

```
Priority Level: 1
```

لكشبو . زاهجال يف رورملا ةكرح عم لماعتلا اهب متي يتلا ةقيرطلا ىلإ ةلكشملا عجرت
امم ، لمالكلا راطنلا لبق طقف 3 ةقبطلا رابتعالا يف RSP2 ةزهجأ ذيفنت ذخأي ال ، يساسا
رابتعالا يف اهذخأ متي سوورلا عي مج نأ ينع

RSP2 ةمدخ ةدوج ةيولوأ رابتخا

ةيولوالأ كولس رابتخالا CEM رورم ةكرح مادختسا متي ، ةلحال هذه يف

دوهجال ىصقأ لذب ةزيم ب طاقسإلا تالاح ب نجتلا ةيولوالأ نيوكت ةيفي كحضوي لاثم اذه
يددرتلا قاطنلا ضرع صيصخت طبضو

نيوكتلا

```
policy-map POL-PRIO-MAIN-1G
```

```
class class-default
```

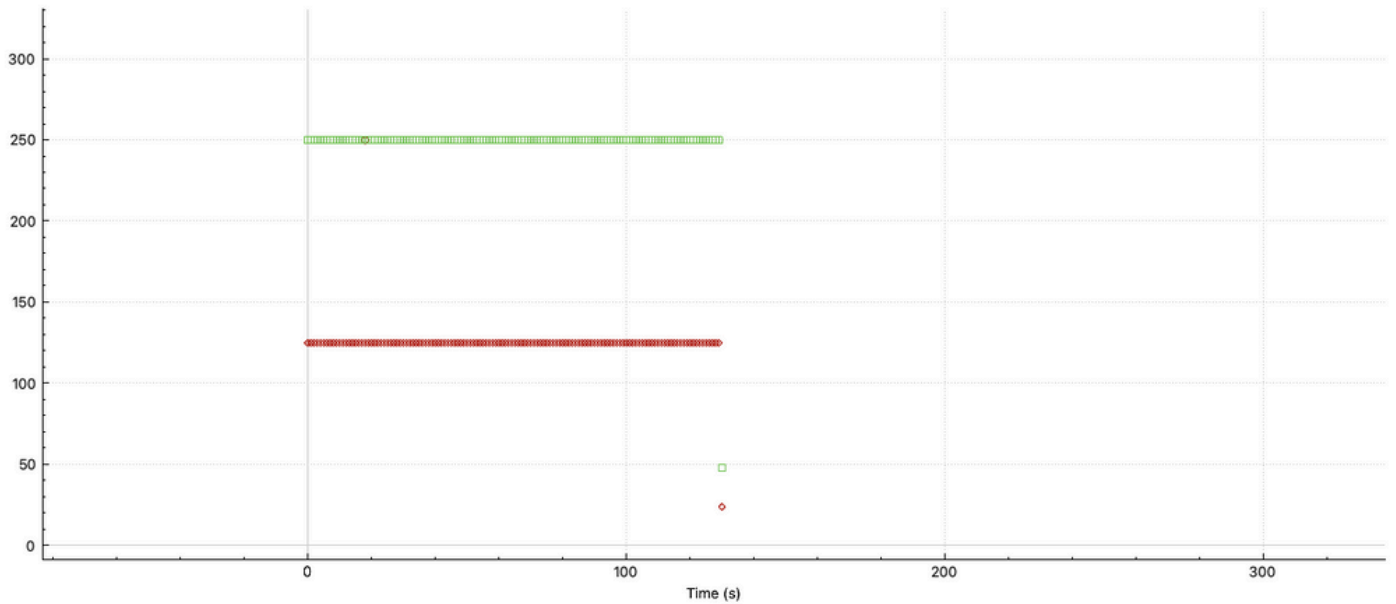
```

shape average 8650000
!
policy-map PM-MPLS-1G-Out
class EXP-5
priority level 1 percent 4
class EXP-4
priority level 2 percent 24
class EXP-6
bandwidth percent 2
queue-limit 25000 us
class EXP-3
bandwidth percent 2
queue-limit 10000 us
class EXP-2
bandwidth percent 2
queue-limit 50000 us
class EXP-1
bandwidth percent 2
queue-limit 20000 us
class class-default
bandwidth percent 1
queue-limit 40000 us
!
interface GigabitEthernet0/0/0
no ip address
negotiation auto
service-policy output POL-PRIO-MAIN-1G
service instance 200 ethernet
encapsulation dot1q 200
rewrite ingress tag pop 1 symmetric
service-policy output PM-MPLS-1G-Out
bridge-domain 200
!
interface CEM0/1/8
no ip address
cem 0
service-policy input PM-CEM-in
payload-size 128
dejitter-buffer 20
!
interface CEM0/1/9
no ip address
cem 0
service-policy input PM-CEM-in
payload-size 64
dejitter-buffer 16
!
interface BDI200
description path for qos stress
ip address 10.20.2.45 255.255.255.0
ip mtu 9000
ip router isis
carrier-delay msec 0
cdp enable
mpls traffic-eng tunnels
bfd template BFD-lhop-5ms
isis circuit-type level-2-only
isis network point-to-point
isis metric 15 level-1
isis metric 15 level-2
ip rsvp bandwidth percent 90
ip rsvp signalling hello graceful-restart

```

رورملا ةكح

رضخألاب CEM0/1/9 و رورملا ةكرح نم رايث قـلخي 2



طبر نم لسري ام فعض CEM0/1/9 لسري ،فلتخم ةمزح مـجـح عم كولسلا ىرن نأ اننكمي تـيـاب 128 ل تلـكـش نوـكي يـأ ،CEM0/1/8.

يـف RSP2 ذـخـأي امنـيـب ،طقف CEM ةلومـح رابـتـعـالـا يـف RP يـلـع ةـمـدـخـلـا ةـدـوـج ةـئـيـهـت عـضـت ،ةـدـاع كـلـذ نم الـدب لم الـلاب راطـالـا رابـتـعـالـا.

راطالال يـلـع لائـم

يـلـع كـلـذ حـرـش نـكـمـي و CEM. نمـض ةـنـوـكـمـلا ةـيـلـصـالـا ةـلومـحـلـل ةـيـفـاضـا تـيـاب 30 ةـيـؤـر كـنـكـمـي يـلـاتـالـا و حـنـلـل:

```
Ethernet header = 14 Bytes
Dot1q header    = 4 Bytes
Mpls header     = 4 Bytes
PW Header       = 4 Bytes
CEM trailer     = 4 Bytes
Total           = 30 Bytes
```

رابط إلة اعارم بجي ه نأب ركذت، زاهجلا يف بولطملا يدرتلا قاطنلا باسح:

```
CEM 0/1/8 125 Packet/sec, size 128bytes ==> 125*128*8 = 128000 bps
CEM 0/1/9 250 Packet/sec, size 64bytes ==> 250*64*8 = 128000 bps
on each frame we need an extra 30bytes ==> 375*30*8 = 90000 bps
Total = 346000 bps
```

يف تب 8650000 ىلع اهنيوكت مت يتلا ةهجاو لا ىلع هتقدو ربدملا كولس نم ققححتلل ةيولوالا ةئفل طبضلاب 4% ىلع لوصح لل كلذب مايقلا متي، ةيناثلا

باسحلا: $346000.000/8650000.000 = 0.04 = 4\%$.

ناق يقو د باسحلا ونيوكتلا نأ جئاتنلا دكؤتو. هالعأ نيوكتلا يف رهظي ام اذهو.

جهنلا جارخا:

```
ASR903#show ethernet service instance policy-map | s EXP-5
Class-map: EXP-5 (match-all)
3063745 packets, 285949512 bytes
5 minute offered rate 279000 bps, drop rate 0000 bps
Match: mpls experimental topmost 5
Priority: 4% (346 kbps), burst bytes 8650, b/w exceed drops: 0
```

Priority Level: 1

نم ريثكب رثكأ يه يساسألا ماظنلا نع لقتسم يف ةقبطملا ةيناثلا يف تبوليك 346 L2 رورم ةكرح لثمت امامت اهنكل L3.

رورم ةكرح دلوم عم رابتخا

قبطت متي شيح 1G جتنني —> ASR9xx RSP2 —> TenGig ةهجاو —> تانايبلا رورم ةكرح دلوم ةساسلا.

```
ASR903#show clock
22:54:40.976 CET Wed Nov 30 2022
ASR903#show ethernet service instance policy-map | inc Class-map:|drop rate
Class-map: EXP-5 (match-all)
5 minute offered rate 279000 bps, drop rate 0000 bps
Class-map: EXP-4 (match-all)
5 minute offered rate 0000 bps, drop rate 0000 bps
Class-map: EXP-6 (match-any)
5 minute offered rate 0000 bps, drop rate 0000 bps
Class-map: EXP-3 (match-any)
5 minute offered rate 0000 bps, drop rate 0000 bps
Class-map: EXP-2 (match-all)
5 minute offered rate 0000 bps, drop rate 0000 bps
Class-map: EXP-1 (match-any)
5 minute offered rate 0000 bps, drop rate 0000 bps
Class-map: class-default (match-any)
5 minute offered rate 762348000 bps, drop rate 756024000 bps
```

ASR903#show clock

17:41:16.110 CET Thu Dec 1 2022

ASR903#show ethernet service instance policy-map | inc Class-map:|drop rate

Class-map: EXP-5 (match-all)

5 minute offered rate 279000 bps, drop rate 0000 bps

Class-map: EXP-4 (match-all)

5 minute offered rate 0000 bps, drop rate 0000 bps

Class-map: EXP-6 (match-any)

5 minute offered rate 0000 bps, drop rate 0000 bps

Class-map: EXP-3 (match-any)

5 minute offered rate 0000 bps, drop rate 0000 bps

Class-map: EXP-2 (match-all)

5 minute offered rate 0000 bps, drop rate 0000 bps

Class-map: EXP-1 (match-any)

5 minute offered rate 0000 bps, drop rate 0000 bps

Class-map: class-default (match-any)

5 minute offered rate 762400000 bps, drop rate 756077000 bps

ريثكلا كانه نأ نم مغرلا ىلع، ةيولوالا يف دحاو ضافخنا كانه نكي مل ةعاس 18 يلاوح دعب كلذو، ةئفلا ريصقت نم طوبهلا لدعم يف حضوم وه امك، ةهجاولا ىلع طوقسلا تالاح نم رغاشلل هب حومسمل دجالاب صاخلا CIR ببسب.

معدل يددرتلا قاطنلا طبض لجأ نم: همادختسا مت راطت نالا ةمئاقلا يضارتفالا دجال نأ طحال راطت نالا مئاقو طبض ىل جاتحت ال، لمكلا ل2 راطا مجح.

بلاس رابتخا

تثدح اذا ام ةفرعمو CEM ةروطقم نم تياب 4 فذح وه ةديجلا ةقدلا نم ققحتلل رخا رابتخا ةريغص طاقس تاي لمع:

ASR903#show ethernet service instance policy-map | s EXP-5

Class-map: EXP-5 (match-all)

352466 packets, 32896848 bytes

5 minute offered rate 279000 bps, drop rate 5000 bps

Match: mpls experimental topmost 5

Priority: 4% (334 kbps), burst bytes 8350, b/w exceed drops: 271

Priority Level: 1

تارطق ببسي هنإ راطلا كلذ نم عزج فذحب تمق اذا، ىرت امك.

تانوسولكنوك

قاطنلا باسحل رابتعالا يف لمكلا ل2 راطا نأ بجي هنأ CEM رورم ةكرح عم رابتخالا اذه دكؤي يددرتلا.

ححصلا باسحل نأ حضاولا نم نكلو، راطت نالا ةمئاق دح ةدايز يف جئاتنلا ىدل لثمتت يساسالا ماطنلا لبق نم ةمدختسمل ةركاذلا دراوم ىلع طغضلا نم للقي ل2 راطلا.

لثم، بسانملا تقولا يف ةطقن لك يف رورملا ةكرح عيمجب وبنتلان كميا ال هنأ حضاولا نم سوؤر ةاعارم كمزلي، قيقد نيوكت ىلع لوصحلل ريغتملا ةمزحلا مجح مادختساب لقنلا مزلحلا لدعم كلذكو ةمزحلا مجح طسوتم ىل MPLS (تامالع) ةمالع، dot1q(s)، تنرتي.

لكب ةيارد ىلع نوكت نأ كمزلي، RSP2 لوكوتوربل ASIC ربعت رورم ةكرح ياب قلعتي امي (CRC) نيضت مدع عم) يساسالا ماطنلا جراخ هلاسرا متي راطا يف دوجوم يدرف تياب.

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إامئاد ةوچرلاب يصوت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزىلچنل دن تسمل