

# ASR1000 vastlegging en bewaking van subpolicers

## Inhoud

[Inleiding](#)

[Per interface-point-policer](#)

[Configureren en controleren](#)

[Aanmelden voor standaard puntenbalk](#)

[Conclusie](#)

## Inleiding

Dit document beschrijft de optie-politiereigenschappen en een aantal nieuwe veranderingen in de functie voor Cisco Aggregation Services Router (ASR) 1000 en Geïntegreerde Service Router (ISR) G3-apparaten. Punt-politier is standaard ingeschakeld en hij controleert al het besturing vlak dat het verkeer bepaalt. Als u meer wilt lezen over punten-politier en punt-gerelateerde druppels, kunt u [Packet Drops](#) raadplegen [op Cisco ASR 1000 Series servicrouters](#). Onlangs werden een aantal wijzigingen aangebracht in de vastlegging en de bediening van punten-politiers die bedoeld zijn om de gemeenschappelijke CLI-gebruiker een duidelijk houtkapmechanisme te geven om de reden van pakketdruppels op het apparaat te identificeren.

## Per interface-point-policer

Dit werd ingevoerd in Polaris release 16.4.

Dit laat de netwerkbeheerder de punten-politielimiten per interfacebasis configureren. Het is vooral behulpzaam wanneer u de interface wilt identificeren die een groot aantal puntverkeer veroorzaakt en daardoor de tijd voor het opsporen en verhelpen van problemen vermindert en een alternatief voor de pakketvastlegging geeft. Voor deze optie moest je, als je de broninterface van het puntenverkeer moest kennen, pakketvastlegging uitvoeren die veel tijd en middelen verteerde.

## Configureren en controleren

```
Router(config)#platform punt-intf rate < packet per second>
```

```
Router(config)#interface gigabitEthernet 0/0/0
```

```
Router(config-if)#punt-control enable
```

Deze configuratie maakt monitoring per interface mogelijk. Bijvoorbeeld, als u het punt-control tarief op 1000 globaal zowel als op een bepaalde interface aanpast, zal het apparaat het spoor van de puntvaling voor deze specifieke interface 30 seconden bijhouden. Na het 30 tweede interval toont de router een logboek zoals dit om de beheerder te waarschuwen dat er een punt

schending gebeurtenis was.

```
*Jun 21 23:01:01.476: %IOSXE-5-PLATFORM: F1: cpp_cp: QFP:0.1 Thread:076 TS:00000044123616602847
%PUNT_INJECT-5-DROP_PUNT_INTF: punt interface policer drop packet from GigabitEthernet0/0/0
```

Aangezien 30 seconden een groot interval is, is een opdracht waarmee u de laatste puntdaling voor de interface kunt zien geïntroduceerd.

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-intf-drop latest
```

```
Punt Intf Drop Statistics (lastest 1000 dropped packets):
```

Interface	Packets
GigabitEthernet0/0/0	1000

U kunt de valstatistieken wissen om de real-time-druppels te controleren.

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-intf-drop latest clear
```

```
Punt Intf Drop Statistics (lastest 1000 dropped packets):
```

Interface	Packets
-----------	---------

```
Router#
```

## Aanmelden voor standaard puntenbalk

Zoals per interface moet de stip-politier expliciet worden geconfigureerd. Maar op ASR-apparaten wereldwijd is de per-oorzaakregelaar altijd actief. Recentelijk is in de afbeelding release 16.6.1 de houtkap geïmplementeerd voor stippolitie per oorzaak. Vanaf nu wordt er een logbestand gegenereerd wanneer er een schending van het punt per oorzaak optreedt.

Vanaf het tijdstip van het eerste logbestand zal de router de oorzaak van het punt 30 seconden controleren. Als er na 30 seconden nog een druppelactiviteit is, wordt er een nieuw logbestand gegenereerd.

Het logbericht zou er zo uitzien en daarom zie je de druppel voor punt 60.

```
F1: cpp_cp: QFP:0.1 Thread:035 TS:00000000089593031387 %PUNT_INJECT-5-DROP_PUNT_CAUSE: punt
cause policer drop packet cause 60
```

U kunt de gegevens over de oorzaak van het punt met deze opdracht controleren.

```
BGL14.Q.20-ASR1006-1#show platform hardware qfp active infrastructure punt config cause 60
QFP Punt Table Configuration
```

```
Punt table base addr : 0x48F46010
punt cause index     60
punt cause name      IP subnet or broadcast packet
maximum instances    1
punt table address   : 0x48F46100
instance[0] ptr      : 0x48F46910
  QFP interface handle : 3
  Interface name       : internal1/0/rp:1
  instance address     : 0x48F46910
```

```
fast failover address   : 0x48F2B884
Low priority policer    : 70
High priority policer   : 71
```

Naast dit logbestand kunt u altijd de oude opdrachten gebruiken om puntdruppels te bewaken.

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-drop
Router#show platform hardware qfp active infrastructure punt statistics type per-cause
Router#show platform hardware qfp active infrastructure punt statistics type global-drop
```

## Conclusie

Met de introductie van de opgraving van een punt per oorzaak en de monitoring per interface is er een beter middel om puntgerelateerde kwesties te isoleren. Wanneer u puntdaling in de QFP status ziet, dient u de toegelichte gereedschappen te gebruiken om het probleem verder te isoleren.