ASR1000 Punt-Policer - Protokollierung und Überwachung

Inhalt

Einführung

In diesem Dokument werden die Funktion zur Strip-Policer sowie einige neue Änderungen für Cisco Aggregation Services Router (ASR) 1000- und Integrated Service Router (ISR) G3-Geräte beschrieben. Der Punt-Policer ist standardmäßig aktiviert und regelt den gesamten auf der Steuerungsebene blockierten Datenverkehr. Weitere Informationen zu Fallrichtlinien und Fallstricken finden Sie unter Paketverluste auf Cisco Service Routern der Serie ASR 1000. Kürzlich wurden bei der Fallüberwachungsprotokollierung und dem Betrieb einige Änderungen vorgenommen, die dem gemeinsamen CLI-Benutzer einen eindeutigen Protokollierungsmechanismus zur Ermittlung der Ursachen von Paketverlusten auf dem Gerät bieten sollen.

Punt-Policer pro Schnittstelle

Diese wurde in Polaris Release 16.4 eingeführt.

Auf diese Weise kann der Netzwerkadministrator Strip-Policer-Limits pro Schnittstellenbasis konfigurieren. Es ist besonders hilfreich, wenn Sie die Schnittstelle identifizieren möchten, die eine große Anzahl von Stuntdatenverkehr verursacht und dadurch die Zeit für die Fehlerbehebung verkürzt und eine Alternative zur Paketerfassung darstellt. Bevor Sie diese Funktion nutzen konnten, mussten Sie die Quellschnittstelle des Strichverkehrs kennen, um die Paketerfassung durchzuführen, die viel Zeit und Ressourcen in Anspruch nahm.

Konfigurieren und Überprüfen

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

Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#punt-control enable
```

Diese Konfiguration ermöglicht die Überwachung von Strip-Policing pro Schnittstelle. Wenn Sie beispielsweise die Fallkontrollrate auf 1000 global sowie auf einer bestimmten Schnittstelle

konfigurieren, wird das Gerät die Fallzahl für diese Schnittstelle 30 Sekunden lang verfolgen. Nach dem 30-Sekunden-Zeitintervall zeigt der Router ein solches Protokoll an, um den Administrator darauf hinzuweisen, dass ein schwerwiegendes Verletzungsereignis aufgetreten ist.

```
*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
```

Da 30 Sekunden ein großes Intervall sind, wurde ein Befehl eingeführt, mit dem Sie die aktuelle Fallmeldung für die Schnittstelle sehen können.

```
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
```

Sie können die Drop-Statistiken löschen, um die Echtzeit-Verluste zu überwachen.

```
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#
```

Protokollierung für den Standard-Punt-Policer

Die Strip-Policer-Funktion muss entsprechend der Schnittstelle explizit konfiguriert werden. Auf ASR-Geräten weltweit ist jedoch die Richtlinie pro Ursache immer aktiv. Kürzlich wurde im Image von Release 16.6.1 die Protokollierung für Ursachenüberwachung implementiert. Von nun an wird ein Protokoll generiert, wenn es zu einem Verstoß gegen den Ursachenfall kommt.

Ab dem ersten Protokoll überwacht der Router die ungefähre Ursache für 30 Sekunden. Wenn nach 30 Sekunden eine weitere Drop-Aktivität vorhanden ist, wird ein weiteres Protokoll generiert.

Die Protokollmeldung würde so aussehen, und daher sehen Sie den Drop für punt Cause 60.

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

Mit diesem Befehl können Sie die Details zu den Ursachen überprüfen.

```
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
```

Außer diesem Protokoll können Sie immer die alten Befehle verwenden, um Fallstriche zu überwachen.

```
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
```

Schlussfolgerung

Mit der Einführung der fallbezogenen Ursachenprotokollierung und der Schnittstellenüberwachung gibt es ein besseres Tool, um genau zusammenhängende Probleme zu isolieren. Immer wenn der QFP-Status stinkt, sollten Sie die erklärten Tools verwenden, um das Problem weiter zu isolieren.