ASR1000 Punt-Policer Logging and Monitoring

Contents

Introduction

This document describes the punt-policer feature and some new changes in it for Cisco Aggregation Services Router (ASR) 1000 and Integrated Service Router (ISR) G3 devices. Punt-policer is enabled by default and it polices all the control plane punted traffic. If you want to read more about punt-policer and punt related drops you can refer to Packet Drops on Cisco ASR 1000 Series Service Routers. Recently there were a few changes made in punt-policer logging and operation which are intended to give the common CLI user a clear logging mechanism to identify the reason of packet drops on the device.

Per Interface Punt-Policer

This was introduced in Polaris Release 16.4.

This lets the network administrator configure punt-policer limits per interface basis. It is particularly helpful when you want to identify the interface which sources a huge number of punt traffic and hence it lowers the troubleshooting time and gives an alternate to the packet capture. Before this feature, if you needed to know the source interface of punt traffic, then you had to perform packet capture which consumed a lot of time and resources.

Configure and Verify

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

Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#punt-control enable <packet per second>
```

This configuration enables punt-policing monitoring per interface. For example, if you configure punt-control rate as 1000 globally as well as on a particular interface, the device will keep track of the punt drop for this particular interface for 30 seconds. After the 30 second time interval, the router shows a log like this to alert the admininstrator that there has been a punt violation event.

```
*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
```

As 30 seconds is a large interval, a command with which you can see the latest punt drop for the

interface has been introduced.

```
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
```

You can clear the drop statistics in order to monitor the real time drops.

```
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#
```

Logging for Default Punt-Policer

As per interface, punt-policer needs be explicitly configured. However, on ASR devices globally, the per cause punt-policer is always active. Recently in the Release 16.6.1 image, logging has been implemented for per cause punt-policer. From now on, a log would get generated whenever a per cause punt violation occurs.

Starting from the time of the first log, the router will monitor the punt cause for 30 seconds. If after 30 seconds there is another drop activity then there would be another log generated.

The log message would look like this and therefore you see the drop for 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
```

You can check the punt cause related details with this command.

```
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
```

Apart from this log, you can always use the old commands in order to monitor punt drops.

```
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
```

Conclusion

With the introduction of punt-per cause logging and per-interface punt-monitoring, there is a better tool to isolate punt related issues. Whenever you see punt drop in the QFP status, you should use the explained tools in order to further isolate the issue.