ASR1000 Punt-Policer Logging and Monitoring

Contents

Introduction
Per Interface Punt-Policer
Configure and Verify
Logging for Default Punt-Policer
Conclusion

Introduction

This document describes 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 ASR packet drop troubleshooting document. Recently there were few changes made in punt-policer logging and operation, changes are intended to give 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 code 16.4 polaris release.

This lets the network admin configure punt-policer limits per interface basis. It is particularly helpful when you want to identify the interface which sources huge number of punt traffic and hence it lowers down 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 the time 30 seconds. After 30 seconds of time interval, the router shows a log like this to alert the admin that there has been a punt voilation 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):

<table>
<thead>
<tr>
<th>Interface</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/0</td>
<td>1000</td>
</tr>
</tbody>
</table>

You can clear this drop stats 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):

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 16.6.1 image, logging has been implemented for per cause punt policer. From now on, a log would get generated whenever there is a per cause punt violation occurs.

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

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:000000000089593031387 %PUNT_INJECT-5-DROP_PUNT_CAUSE: punt casue policer drop packet casue 60

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

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

<table>
<thead>
<tr>
<th>Punt table base addr : 0x48F46010</th>
</tr>
</thead>
<tbody>
<tr>
<td>punt cause index</td>
</tr>
<tr>
<td>punt cause name</td>
</tr>
<tr>
<td>maximum instances</td>
</tr>
<tr>
<td>punt table address</td>
</tr>
<tr>
<td>instance[0] ptr</td>
</tr>
<tr>
<td>QFP interface handle</td>
</tr>
<tr>
<td>Interface name</td>
</tr>
<tr>
<td>instance address</td>
</tr>
<tr>
<td>fast failover address</td>
</tr>
<tr>
<td>Low priority policer</td>
</tr>
<tr>
<td>High priority policer</td>
</tr>
</tbody>
</table>

Apart from this log, you can always use the old commands 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 qfp status, you should use the explained tools to further isolate the issue.