ASR1000 Punt-Policer日志记录和监控

目录

简介

本文档介绍Cisco聚合服务路由器(ASR)1000和集成服务路由器(ISR)G3设备的punt-policer功能及其中的一些新更改。Punt-policer默认启用，它会监控所有控制平面传送的流量。如果想了解有关punt-policer和punt相关丢包的更多信息，可以参[阅Cisco ASR 1000系列服务路由器上的数据包丢弃](#)。最近，在punt-policer日志记录和操作中进行了一些更改，这些更改旨在为普通CLI用户提供明确的日志记录机制，以确定设备上丢包的原因。

每接口Punt-Policer

这在Polaris版本16.4中引入。

这样，网络管理员就可以按接口配置punt-policer限制。当您想要确定来源大量传送流量的接口时，它特别有用，因此它会缩短故障排除时间，并提供数据包捕获的替代方法。在此功能之前，如果您需要了解传送流量的源接口，则必须执行耗费大量时间和资源的数据包捕获。

配置和验证

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

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

此配置启用每个接口的punt-policing监控。例如，如果全局以及在特定接口上将punt-control rate配置为1000，设备将跟踪此特定接口的punt丢弃30秒。在30秒的时间间隔后，路由器会显示类似此的日志，以提醒管理员已发生传送违规事件。

```
*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
```

由于30秒是较大的间隔，因此引入了一个命令，您可以通过该命令查看接口的最新丢弃。

```
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
```

您可以清除丢弃统计信息以监控实时丢包。

```
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#
```

默认Punt-Policer的日志记录

根据接口，需要显式配置punt-policer。但是，在全局ASR设备上，每个原因的punt-policer始终处于活动状态。最近在版本16.6.1映像中，已针对每个原因实施日志记录。从现在开始，每当发生每个原因的punt违规时，都会生成日志。

从第一个日志开始，路由器将监控传送原因30秒。如果30秒后有另一个丢弃活动，则会生成另一个日志。

日志消息将如下所示，因此您会看到丢弃原因60。

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

您可以使用此命令检查发送原因相关详细信息。

```
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
```

除此日志外，您始终可以使用旧命令来监控丢包。

```
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
```

结论

随着引入punt-per-cause日志记录和每接口punt-monitoring，有了更好的工具来隔离punt相关问题。每当您在QFP状态中看到丢弃时，应使用说明的工具以进一步隔离问题。