Registrazione e monitoraggio di ASR1000 Punt-Policer

Sommario

Introduzione

Questo documento descrive la funzionalità punt-policer e alcune nuove modifiche a questa funzionalità per i dispositivi Cisco Aggregation Services Router (ASR) 1000 e Integrated Service Router (ISR) G3. Il punt-policer è abilitato per impostazione predefinita e regola tutto il traffico puntato del control plane. Per ulteriori informazioni su punt-policer e sulle perdite relative a punt, consultare il documento Packet Drops sui Cisco ASR serie 1000 Service Router. Di recente sono state apportate alcune modifiche al log e al funzionamento di punt-policer che hanno lo scopo di fornire all'utente CLI comune un chiaro meccanismo di log per identificare il motivo delle perdite di pacchetti sul dispositivo.

Per Interface Punt-Policer

Questa funzione è stata introdotta in Polaris release 16.4.

Ciò consente all'amministratore di rete di configurare i limiti del punt-policer per singola interfaccia. È particolarmente utile quando si desidera identificare l'interfaccia che genera un elevato numero di traffico punt e quindi riduce i tempi di risoluzione dei problemi e fornisce un'alternativa all'acquisizione del pacchetto. Prima di questa funzione, per conoscere l'interfaccia di origine del traffico punt, era necessario eseguire l'acquisizione dei pacchetti, che richiedeva molto tempo e molte risorse.

Configurazione e verifica

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

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

Questa configurazione consente il monitoraggio del punt-policing per interfaccia. Ad esempio, se si configura una velocità di punt-control di 1000 in tutto il mondo e su una particolare interfaccia, il dispositivo terrà traccia della velocità di punt-control per questa particolare interfaccia per 30

secondi. Trascorso l'intervallo di tempo di 30 secondi, il router visualizza un registro come questo per avvisare l'amministratore che si è verificato un evento di violazione di punt.

```
*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
```

Poiché 30 secondi sono un intervallo esteso, è stato introdotto un comando che consente di visualizzare la versione più recente del punt drop per l'interfaccia.

```
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
```

Èpossibile cancellare le statistiche di caduta per monitorare le cadute in tempo reale.

```
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#
```

Registrazione per il punt-policer predefinito

Come per interfaccia, il punt-policer deve essere configurato esplicitamente. Tuttavia, su tutti i dispositivi ASR, il punt-policer per cause è sempre attivo. Di recente nell'immagine della release 16.6.1, la registrazione è stata implementata per il punt-policer per causa. D'ora in poi, un registro verrebbe generato ogni volta che si verifica una violazione per causa punt.

A partire dall'ora del primo registro, il router monitorerà la causa del bit per 30 secondi. Se dopo 30 secondi si verifica un'altra attività di rilascio, verrà generato un altro registro.

Il messaggio del log dovrebbe essere simile a questo e quindi si vede la goccia per la 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
```

Con questo comando è possibile controllare i dettagli relativi alla causa del segno di spunta.

```
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
```

Oltre a questo registro, è sempre possibile utilizzare i vecchi comandi per monitorare le perdite di punti.

```
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
```

Conclusioni

Con l'introduzione del log delle cause punt-per e del monitoraggio delle cause punt per interfaccia, c'è uno strumento migliore per isolare i problemi relativi alle cause punt. Ogni volta che viene visualizzato lo stato di QFP, utilizzare gli strumenti illustrati per isolare ulteriormente il problema.