Packet Drops

This document provides information about packet drops on the Cisco 8500 Series Secure Router.

Information about packet drops

Viewing packet drops

You can run the show drops command to troubleshoot the root cause of packet drops.

With the **show drops** command, you can identify the following:

- The root cause of the drop based on the feature or the protocol.
- The history of the QFP Drops.

Viewing packet drop information

Perform the following steps to view and filter the packet drop information for your instance based on the interface, protocol, or feature:

SUMMARY STEPS

1. **enable**
2. **show drops**
3. **show drops** { **bqs** | **crypto**| **firewall**| **interface**| **ip-all**| **nat**| **punt**| **qfp**| **qos**|**history**}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**show drops** **Example:** `Router# show drops`	Displays the drop statistics.
Step 3	**show drops** { **bqs** | **crypto**| **firewall**| **interface**| **ip-all**| **nat**| **punt**| **qfp**| **qos**|**history**} **Example:** `Router# show drops qfp`	Displays the drop statistics and the summary for the interface or the protocol that you choose. **Note** From Cisco IOS XE 17.13.1a, a new keyword option history is added to the **show drops** command. The **show drops history qfp** command will allow the user to view the history of the QFP drops.

Example

Example for Viewing Packet Drop Information: Sample Output

The following is a sample output of the show drops command. This sample output displays the **packet drops** information related to the Quantum Flow Processor (QFP).

```
Router#show drops
bqs BQS related drops
crypto IPSEC related drops
firewall Firewall related drops
history History of drops
interface Interface drop statistics
ip-all IP related drops
nat NAT related drops
punt Punt path related drops
qfp QFP drop statistics
qos QoS related drops
| Output modifiers
<cr> <cr>
```

```
Router#show drops qfp
------------------ show platform hardware qfp active statistics drop detail
Last clearing of QFP drops statistics : Fri Feb 18 08:02:37 2022
(6d 23h 54m 29s ago)
-------------------------------------------------------------------------------
ID Global Drop Stats Packets
Octets
-------------------------------------------------------------------------------
319 BFDoffload 9
1350
61 Icmp 84
3780
```

```
53 IpFragErr 32136
48718168
244 IpLispHashLkupFailed 3
213
56 IpsecInput 18
4654
23 TailDrop 26713208
10952799454
216 UnconfiguredIpv6Fia 241788
26596680
------------------ show platform hardware qfp active interface all
statistics drop_summary
-----------------------------------------------------------------
Drop Stats Summary:
note: 1) these drop stats are only updated when PAL
reads the interface stats.
2) the interface stats include the subinterface
Interface Rx Pkts Tx Pkts
-------------------------------------------------------------------------------
GigabitEthernet1 60547 0
GigabitEthernet2 60782 27769658
GigabitEthernet3 60581 0
GigabitEthernet4 60502 1323990
Tunnel14095001 0 1990214
Tunnel14095002 0 3883238
Tunnel14095003 0 3879243
Tunnel14095004 0 2018866
Tunnel14095005 0 3875972
Tunnel14095006 0 3991497
Tunnel14095007 0 4107743
Tunnel14095008 0 3990601
```

Verifying packet information

This section shows examples of command output to verify packet information.

In order to display statistics of drops for all interfaces in Packet Processor Engine (PPE), use the command **show drops qfp**.

Note The wrapper command **show drops qfp** is the shorthand notation for the original **show platform hardware qfp active statistics drop** command.

```
Router#show drops qfp
-----------------------------------------------------------------
Global Drop Stats Octets
Packets
-----------------------------------------------------------------
AttnInvalidSpid 0 0
BadDistFifo 0 0
BadIpChecksum 0 0
```

In order to display the history of QFP drops for all interfaces in Packet Processor Engine (PPE), use the command **show drops history qfp**. This command can also track the number of packet drops in the last 1-min, 5-min and 30-min time period.

Note The wrapper command **show drops history qfp** is the shorthand notation for the original **show platform hardware qfp active statistics drop history** command.

```
Router#show drops history qfp
Last clearing of QFP drops statistics : Mon Jun 26 07:29:14
2023
(21s ago)
---------------------------------------------------------------
Global Drop Stats 1-Min
5-Min 30-Min All
---------------------------------------------------------------
Ipv4NoAdj 0
0 0 99818
Ipv4NoRoute 0
0 0 99853
```

Packet drops warnings

You can configure the warning thresholds for per drop cause and/or total QFP drop in packets per second. If the configured thresholds are exceeded, then a rate-limited syslog warning is generated. One warning is generated for total threshold exceeded and one warning per drop cause will be generated.

The warning is generated a maximum of once per minute for each drop cause. The drops over the previous minute are checked against the threshold (packets per second) x 60, and if the drops exceed this value, a warning is generated.

The following are the sample warnings for total and per drop cause respectively.

```
%QFP-5-DROP_OVERALL_RATE: Exceeded the overall drop threshold 10000 pps during the last
60-second measurement period, packets dropped in last 1 minute: 641220, last 5 minutes:
1243420, last 30 minutes: 124342200
```

```
%QFP-5-DROP_CAUSE_RATE: Exceeded the drop threshold 1000 pps for QosPolicing (drop code:
20) during the last 60-second measurement period, packets dropped due to QosPolicing in
last 1 minute: 61220, last 5 minutes: 43420, last 30 minutes: 4611200
```

Configuring packet drops warning thresholds

Perform the following steps to configure the warning thresholds for per drop cause and/or total QFP drop in packets per second.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **platform qfp drops threshold** {**per-cause** *drop_id threshold* | **total** *threshold*}

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**platform qfp drops threshold** {**per-cause** *drop_id threshold* | **total** *threshold*} **Example:** `Router# platform qfp drops threshold per-cause 206 10`	Specifies the per drop cause or total threshold value for the drop. **Note** Use the **show platform hardware qfp active statistics drop detail** command to view the drop cause ID.

Example

The following examples show how to configure the warning thresholds for per drop cause and total QFP drops.

Example for configuring warning threshold for per drop cause QFP drops

The following example shows how to configure the warning threshold of 15 pps for drop cause ID 24.

```
Router> enable
Router# configure terminal
Router(config)#platform qfp drops threshold ?
per-cause Set warning threshold for per cause QFP drops
total Set warning threshold for total QFP drops
Router(config)#platform qfp drops threshold per-cause ?
<0-1024> QFP drop cause ID
Router(config)#platform qfp drops threshold per-cause 24 ?
<0-2147483647> Drop threshold in packets per second (pps)
Router(config)#platform qfp drops threshold per-cause 24 15
```

Example for configuring warning threshold for total QFP drops

The following example shows how to configure the warning threshold of 100 pps for total QFP drops.

```
Router> enable
Router# configure terminal
Router(config)#platform qfp drops threshold ?
per-cause Set warning threshold for per cause QFP drops
total Set warning threshold for total QFP drops
Router(config)#platform qfp drops threshold total ?
<0-2147483647> Drop threshold in packets per second (pps)
Router(config)#platform qfp drops threshold total 100
```

Viewing packet drops warning thresholds

Perform the following steps to view the configured warning thresholds for per drop cause and total QFP drops.

SUMMARY STEPS

1. **enable**
2. **show platform hardware qfp active statistics drop threshold**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**show platform hardware qfp active statistics drop threshold** **Example:** `Router# show platform hardware qfp active statistics drop thresholds`	Displays the configured warning thresholds for per drop cause and total QFP drops. **Note** • The wrapper command **show drops thresholds** is the shorthand notation of the **show platform hardware qfp active statistics drop threshold**command.

Example

Example for Viewing Packet Drop Warning Thresholds

The following is a sample output of the **show platform hardware qfp active statistics drop threshold** command.

```
Router#show platform hardware qfp active statistics drop thresholds
-----------------------------------------------------
Drop ID         Drop Cause Name             Threshold
-----------------------------------------------------
10              BadIpChecksum                100
206             PuntPerCausePolicerDrops     10
20              QosPolicing                  200
                Total                        30
```

The following is a sample output of the **show drops thresholds** wrapper command.

```
Router#show platform hardware qfp active statistics drop thresholds
-----------------------------------------------------
Drop ID         Drop Cause Name             Threshold
-----------------------------------------------------
10              BadIpChecksum                100
206             PuntPerCausePolicerDrops     10
```

```
20              QosPolicing                 200
                Total                       30
```