

Traffic Monitoring

For a router to function smoothly and effortlessly, monitoring traffic is an essential task. Traffic Monitoring helps you get count of packets going inwards and outwards.

This chapter describes the process to monitor packet drops as part of troubleshooting process.

In routing, the information is passed around in the form of packets. Packets contains unit size data. Sometimes,due to network congestion, or outdated software/hardware the packets fail to reach at their destined location.You can identify packet loss in the form of incomplete information or missing information.

- Traffic Statistics with Packet Drop Location, on page 1
- Monitor interface, on page 5

Traffic Statistics with Packet Drop Location

Table 1: Feature History Table

Feature Name	Release	Description
Traffic Statistics with Packet Drop Location	Release 24.2.11	This feature now extends support on the Cisco NCS 540 Series routers running on Cisco IOS XR7.

Feature Name	Release	Description
Traffic Statistics with Packet Drop Location	Release 24.2.1	Introduced in this release on the following Cisco NCS 540 router variants running on Cisco IOS XR: • N540-ACC-SYS • N540X-ACC-SYS • N540-24Z8Q2C-SYS We help you save debugging time to locate packet drops by automatically detecting nonzero traffic drops from the commands running in the background and giving you the exact location of the packet drop. In earlier releases, you used multiple show commands with their respective locations to detect packet drops. This feature introduces the **show drops all** command.

Earlier, finding the exact location of packet drop was a long and tedious process as there are multiple node locations. You were executing show commands with their different locations to detect the packet drop location.

Starting Cisco IOS XR Software Release 24.2.1, finding a packet drop location has become easy and quick. You can use the **show drops all** command to know the exact packet drop location. This command shows all nonzero traffic-drops in the node at one place. This command automatically runs the required IOS XR debug commands in the background and removes insignificant information from the command output.

The following commands outputs are integrated in the **show drops all** command:

- **show arp traffic location**
- **show cef drops location**
- **show lpts pifib hardware entry brief location**
- **show netio drops location**
- **show controllers npu stats counters-all instance all location**
- **show controllers npu stats counters-all detail instance all location**
- **show controllers npu stats traps-all instance all location**
- **show controllers npu stats voq base 0 instance all location**
- **show controllers npu stats voq base 24 instance all location**
- **show controllers npu stats voq base 32 instance all location**
- **show controllers npu stats voq ingress interface all instance all location**

- **show spp node-counters location**
- **show spp client detail location**
- **show fwd statistics location**
- **show controller fia statistics detail instance all location**
- **show controller fia diagshell all "diag counter nZ" location**
- **show interfaces location**

Restrictions for Detecting Packet Drop Location

- If MACsec is enabled on routers, then this command doesn't show packet drops. To check if MACsec is enabled, you can use the **show macsec mka summary** command.

Monitor Packet Drops

Use **show drops all location all** to see the drops from all location or node that have happened in the system. Also, you can use **show drops all ongoing** to see ongoing drops on the system. This command output shows ongoing drops since the last time command was executed.

The command output given here is the truncated version.

```
Router#show drops all ongoing location all
====================================
Checking for ongoing drops on 0/4/CPU0
====================================
filtering...


====================================
Checking for ongoing drops on 0/4/CPU0
====================================


====================================
Checking for ongoing drops on 0/3/CPU0
====================================


show controllers npu stats counters-all instance all location:
.
.
.
[np:Slot: 3, instance: 3] ENQ_DISCARDED_PACKET_COUNTER   : +1950


show controllers npu stats counters-all detail instance all location:
[np:Slot: 3, instance: 0] IQM1 TotDscrdByteCnt                 : +133008


show controller fia statistics detail instance all location:

[fia:FIA Statistics Rack: 0, Slot: 3, instance: 0] IQM0 QueueEnqDscrdPktCnt: +1304

show controller fia diagshell all "diag counter nZ" location:
.
.
```

```
.
[fia:R/S/I: 0/3/1] IQM0 IqmQueueEnqDiscardedPacketCounter: +45

====================================
Checking for ongoing drops on 0/RP0/CPU0
====================================


show interfaces:
[Interface:Bundle-Ether10000] input errors: +65
[Interface:Bundle-Ether10001] input errors: +65
[Interface:Bundle-Ether10002] input errors: +65
[Interface:Bundle-Ether10003] input errors: +64
[Interface:Bundle-Ether10004] input errors: +65
[Interface:Bundle-Ether10005] input errors: +65
[Interface:Bundle-Ether10006] input errors: +65
[Interface:Bundle-Ether10007] input errors: +64
[Interface:Bundle-Ether10008] input errors: +64
[Interface:Bundle-Ether10009] input errors: +65
[Interface:Bundle-Ether20001] input errors: +65

====================================
Checking for ongoing drops on 0/2/CPU0
====================================

show controller fia statistics detail instance all location:
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM0 IqmCntCmdErrorsFilterA: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM0 IqmCntCmdErrorsFilterB: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM0 IrppCntCmdErrorsFilterA: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM0 IrppCntCmdErrorsFilterB: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM1 IqmCntCmdErrorsFilterA: +4590
[fia:FIA Statistics Rack: 0, Slot: 2, instance: 0] IQM1 IqmCntCmdErrorsFilterB: +4590


show controller fia diagshell all "diag counter nZ" location:
[fia:R/S/I: 0/2/0] IPS0 IpsFsmrqDelayCounter: +9
[fia:R/S/I: 0/2/0] IPS1 IpsFsmrqDelayCounter: +7
[fia:R/S/I: 0/2/1] IPS0 IpsFsmrqDelayCounter: +10
[fia:R/S/I: 0/2/1] IPS1 IpsFsmrqDelayCounter: +7


show interfaces:
[Interface:HundredGigE0/2/0/28] input errors: +113
```

Monitor interface

Table 2: Feature History Table

Feature Name	Release	Description
Monitor interface	Release 24.4.1	The **filter physical** keyword was introduced, along with new columns `InDrops` and `OutDrops` in the output, to provide enhanced monitoring capabilities for physical interfaces. **CLI:** • The **filter physical** keyword is added to the **monitor interface** command.
Monitor interface	Release 7.5.4	The keyword **full-name** is added, allowing users to display the full names of interfaces, which is particularly useful for interfaces with long or descriptive names. **CLI:** • The **full-name** keyword is added to the **monitor interface** command.
Monitor interface	Release 7.0.12	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) Monitor interface is introduced to enable real-time monitoring of interface counters on Cisco routers. This feature introduces the **monitor interface** command.

The **monitor interface** command is used to monitor network interface counters in real-time.

This command provides valuable insights into the performance and status of both physical and virtual interfaces on a router.

By leveraging various arguments, you can customize the output to display

- detailed statistics,
- full interface names, and

- filter for physical interfaces.

The **monitor interface** command is essential for network administrators to diagnose and troubleshoot interface-related issues effectively.