Mirror forward-drop packets

This chapter captures and analyzes packets dropped by a router during forwarding. It helps network administrators understand blocked traffic, identify security threats, troubleshoot issues, and optimize performance by mirroring these packets to a specified destination.

Mirror forward-drop packets

Mirroring forward-drop packets is a network monitoring feature that

- captures and analyzes packets that a router drops while forwarding them
- identifies the source of potential security threats, and
- takes proactive measures to avoid escalation of the issue.

Table 1: Feature History Table

Feature Name	Release Information	Description
Mirroring forward-drop packets	Release 25.2.1	Introduced in this release on: Centralized Systems (8400 [ASIC:K100]))(select variants only*) This feature helps identify the types of traffic that are blocked, analyze potential security threats, and optimize network performance by mirroring and analyzing the packets dropped during the forward process. *This feature is now supported on Cisco 8404-SYS-D routers.
Mirroring forward-drop packets	Release 25.1.1	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) This feature is now supported on: • 8011-4G24Y4H-I

Feature Name	Release Information	Description
Mirroring forward-drop packets	Release 24.4.1	Introduced in this release on: Fixed Systems(8200, 8700)(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*). This feature with the mirroring and analysis of packets dropped during the forwarding process helps identify the types of traffic that are blocked, analyze potential security threats, troubleshoot, and optimize network performance. *This feature is now supported on: • 8212-48FH-M • 8711-32FH-M • 8712-MOD-M • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 88-LC1-36EH
Mirroring forward-drop packets	Release 7.5.4	Mirroring forward-drop packets feature copies or mirrors the packets that are dropped during the forwarding process at the router ingress to a configured destination. These mirrored packets can be captured and analyzed using network monitoring tools. The analysis of dropped packets helps you understand the types of traffic that are blocked, analyze potential security threats, troubleshoot, and optimize network performance. This feature introduces the following changes: • **CLI: drops** • **YANG Data Model:**New XPath for Cisco-IOS-XR-um-monitor-session-cfg.yang (see GitHub, YANG Data Models Navigator)

In a network, packets are forwarded from one device to another until they reach their destination. However, in some cases, routers may drop packets during this forwarding process. These packets are known as forward-drop packets.

Packet drop can happen due to congestion on the network, errors in the packet header or payload, or blocking by firewalls or Access Control Lists (ACL). These forward-drop packets are typically discarded before they can reach their intended destination and may need to be re-transmitted by the source device.

This feature supports mirroring of these forward-drop packets at the ingress, Rx direction, to another destination. When a global forward-drop session is configured for the router, the forward-drop packets at the ingress are mirrored or copied to the configured destination. You can configure the mirror destination as a file, for SPAN to file sessions, or an IPv4 GRE tunnel ID, for ERSPAN.

Benefits of mirroring forward-drop packets

These are the benefits of mirroring forward-drop packets to a suitable destination:

- By mirroring and analyzing forward-drop packets, network administrators gain better visibility into the types of traffic that are blocked by the firewalls and access control lists (ACL).
- As the original dropped packet is forwarded without any change, it helps in identifying the source of potential security threats.
- Analyzing forward-drop packets helps troubleshoot network issues that may be causing the packet drop. This helps in taking proactive measures to avoid escalation of the issue.

Guidelines for mirroring forward-drop packets

These guidelines apply to mirroring forward-drop packets:

- Only one global forward-drop session can be configured on a router.
- When traffic-class is configured under monitor-session for forward-drop, the Type of Service (ToS) byte of the outgoing ERSPAN packet is overwritten with the configured traffic-class value.
- In-band traffic destined to router management interface cannot be captured using this functionality.
- For ERSPAN sessions that monitor forward-drop packets, a default value of 0 is used for the encapsulation traffic class, irrespective of the DSCP value assigned for the tunnel.

Restrictions for mirroring forward-drop packets

These restrictions apply to mirroring forward-drop packets:

- ERSPAN counters are not updated for forward-drop packets.
- Not all packets that are dropped by NPU are mirrored.

Configure forward-drop packets

Perform the these steps on the router to configure a global session for mirroring forward-drop packets:

Procedure

Step 1 Configure the tunnel mode.

Example:

```
Router(config)# interface tunnel-ip 2
Router(config-if)# tunnel mode gre ipv4
```

Step 2 Configure the tunnel source.

Example:

```
Router(config-if)# tunnel source 20.20.20.20
```

Step 3 Configure the tunnel destination.

Example:

```
Router(config-if)# tunnel destination 192.1.1.3
Router(config-if)# exit
```

Step 4 Configure a traffic mirroring session.

Example:

```
Router(config)# monitor-session mon2 ethernet
```

Step 5 Associate a destination interface with the traffic mirroring session.

Example:

```
Router(config)# destination interface tunnel-ip2
```

Step 6 Run **drops** command to start mirroring forward-drop packets.

Example:

```
Router(config)# drops packet-processing rx
Router(config)# commit
```

Step 7 Verify the forward-drop packets are mirrored using the **show monitor-session** command.

Example:

```
Router# show monitor-session mon2 status detail
Mon Aug 15 19:14:31.975 UTC
Monitor-session mon2
   Destination interface tunnel-ip2
   All forwarding drops:
      Direction: Rx
Source Interfaces
-----------------
```