IP Source Violation

This chapter includes the following topics:

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

Feature Description

The CUPS architecture supports packet source validation on the User-Plane. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

The User-Plane checks the source IP address of the uplink data packet with the IP address of the UE for a match and decides to either drop or permit the data packet further based on configured values.

An existing configuration, which is part of the non-CUPS architecture is implemented for this feature. The **ip source-violation** command – part of the *APN Configuration* mode is used to implement packet source validation.

Configuring IP Source Violation

Use the following configuration to enable or disable packet source validation for a given APN:

```
configure
  context context_name
    apn apn_name
      ip source-violation { ignore | check [ drop-limit limit ] [
exclude-from-accounting ] }
      default ip source-violation
      end
```

NOTES:

- **default**: Enables the checking of source addresses received from subscribers for violations, with a drop limit of 10 invalid packets that can be received from a subscriber prior to their session being deleted.
- **ignore**: Disables source address checking for the APN.

  The User Plane does not increment the IP source violation counter and the dropped packet statistics will be zero. The User Plane would create a different Stream, and VPP sends these packets through fastpath using the same Stream ID.
- **check [drop-limit** *limit* **]**: Default: Enabled, limit = 10.

  Enables the checking of source addresses received from subscribers for violations. A drop-limit can be configured to set a limit on the number of invalid packets that can be received from a subscriber prior to their session being deleted.

  limit: can be configured to any integer value between 0 and 1000000. A value of 0 indicates that all invalid packets will be discarded, but the session will never be deleted by the system.
- **exclude-from-accounting**: Excludes the packets identified with IP source violation from the statistics generated for accounting records.

  When **exclude-from-accounting** is disabled:
  - Dropped packets are not accounted. However, the packets that are sent from VPP are charged.
  - Usage Report URR has dropped bytes.
  - Packet drop counter increases.

  When **exclude-from-accounting** is enabled:
  - Dropped packets are not accounted.
  - Usage Report URR will not have dropped packets.
  - Packet drop counter increases.

Monitoring and Troubleshooting

This section provides information regarding monitoring and troubleshooting the IP Source Violation feature.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

show sub user-plane-only full all

On executing the above command, the following fields are displayed for this feature:

- ip source violations