IP Source Violation

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- Configuring IP Source Violation, on page 2
- Monitoring and Troubleshooting, on page 3

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *P-GW Administration Guide* • *Command Line Interface Reference*

Revision History

Revision Details	Release
First introduced.	21.28

Feature Description

The P-GW supports packet source validation on the control-Plane. Configuration from Control Plane gets pushed to User Plane and based on that information, User Plane acts on the source violated packet.

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network. Source validation requires the source address of received packets to match the IP address that is assigned to the subscriber either statically or dynamically during the session.

In the StarOS 21.28.0 and later releases the **ip source-violation** command, which is part of the APN configuration mode is used to track the behavior of IP source violation for IPv4 and IPv6 addresses.

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 ][ drop-count-timeout time-interval ] }[
traffic-type { ipv4 | ipv6 } ]
         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.
- **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 10000. 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.
- **check [drop-count-timeout time-interval]**: The **drop-count-timeout** is used to configure the time interval for violation drop count update timer. This specifies in which time interval drop counter value should be updated. Time interval should be specified in minutes. Default value is 120 seconds (2 minutes).
- **check [traffic-type { ipv4 | ipv6 }]**: Specifies the packet traffic type as IPv4 or ipv6. By default configurations will be common for both IPv4 and IPv6. If CLI is configured with a "traffic-type" then "ip source violation" cli for that traffic-type takes priority than the CLI configured w/o "traffic-type".

Note The violation count increments even if the drop limit and timer values are zero. The session is not deleted, but the violated packets gets dropped.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show subscribers full all

Display all statistics that are related to the IPv4 and IPv6 counter violations separately.

Table 1: show subscribers full all Command Output Descriptions

Field	Description
ipv6 source violations	The number of IPv6 source validation violations.
ipv6 source violations no acct	The IPv6 source validation violations that were detected but not included in the statistics.
ipv6 source violations ignored	The IPv6 source validation violations that were detected but then ignored.
ipv6 source violations active	The total number of active IPv6 source validation violations.

show apn name *apn_name*

Display all statistics that are related to the IPv4 and IPv6 counter violations separately.

Table 2: show apn name apn_name Command Output Descriptions

Field	Description
ipv4 source violations	The number of IPv4 source validation violations.
drop limit	The number of drop limits for IPv4 source validation violations.
ipv4 source violations no acct	The IPv4 source validation violations that were detected but not included in the statistics.
ipv6 source violations	The number of IPv6 source validation violations.
drop limi	The number of drop limits for IPv6 source validation violations.

Field	Description
ipv6 source violations no acct	The IPv6 source validation violations that were detected but not included in the statistics.

show apn statistics name *apn_name*

Display all statistics that are related to the IPv4 and IPv6 counter violations separately.

Table 3: show apn statistics name apn_name Command Output Descriptions

Field	Description
IPv4 src violations	The number of IPv4 source validation violations.
IPv4 src violations no acct	The IPv4 source validation violations that were detected but not included in the statistics.
IPv4 src violations ignored	The IPv4 source validation violations that were detected but then ignored.
ipv6 src violations	The number of IPv6 source validation violations.
ipv6 src violations no acct	The IPv6 source validation violations that were detected but not included in the statistics.
IPv6 src violations ignored	The IPv6 source validation violations that were detected but then ignored.