

APN Profile Support

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- Feature Configuration, on page 2
- Validation of Uplink Packets for IP Source Violation, on page 4
- Troubleshooting Information, on page 8

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Configuration Required
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Introduced support for IPv6.	2022.04.0
First introduced.	2021.01.0

Feature Description

This feature supports Access Point Name (APN) or Data Network Name (DNN) profile for the SGW (cnSGW-C) service. DNN is equivalent to APN in Evolved Packet System (EPS).

Using the Operator Policy and the Subscriber map, you can determine the DNN Profile for the cnSGW-C service.

Feature Configuration

Configuring this feature involves the following steps:

- Configure DNN Profile. For more information, refer to Configuring DNN Profile, on page 2.
- Configure Network Element Profile. For more information, refer to Configuring Network Element Profile, on page 2.

Configuring DNN Profile

To configure this feature, use the following configuration:

```
config
  profile dnn dnn_name
    upf-selection-policy upf_select_name
      dnn dnn_name network-function-list network_function_list
      end
```

NOTES:

- **dnn** *dnn_name*—Specify the DNN profile name. Must be a string.
- **upf-selection-policy** *upf_select_name*—Specify the UPF selection policy name. Must be a string.
- **network-function-list** *network_function_list*—Specify the list of network functions to which the selected DNN profile is sent. Must be a string.

Configuring Network Element Profile

Network element profile represents peer IP (UPF) profile and has the following configurations:

- Peer address and Port configuration
- Peer-supported DNNs or APNs. This configuration helps in UPF selection.

UPF selection considers priority and capacity parameters.

upf-group-profile indicates the UPF group to which it belongs.

To configure this feature, use the following configuration:

```
config
  profile network-element upf upf_name
    node-id  node_id_value
```

```
n4-peer-address ipv6 ipv6_address
n4-peer-address ipv4 ipv4_address
n4-peer-port port_number
dual-stack-transport { true | false }
dnn-list dnn_list
capacity capacity_value
priority priority_value
upf-group-profile upf_group_name
end
```

NOTES:

- **network-element**—Specify the peer network element.
- **upf** *upf_name*—Specify the UPF peer name.
- **node-id** *node_id_value*—Specify the Node ID of the UPF node.
- **n4-peer-address ipv4** *ipv4_address*—Specify the IPv4 address.
- **n4-peer-address ipv6** *ipv6_address*—Specify the IPv6 address.
- **n4-peer-port** *port_number*—Specify the N4 peer port number. Must be an integer in the range of 0-65535.
- **dual-stack-transport { true | false }**—Enable the dual stack feature that allows you to specify IPv6 or IPv4 address. Specify true to enable this feature.
- **dnn-list** *dnn_list*—Specify the DNN list supported by UPF node.
- **capacity** *capacity_value*—Specify the capacity relative to other UPFs. This is used for load balancing. Must be an integer in the range of 0-65535. Default value is 10.
- **priority** *priority_value*—Specify the static priority relative to other UPFs. This is used for load balancing. Must be an integer in the range of 0-65535. Default value is 1.
- **upf-group-profile** *upf_group_name*—Specify the UPF group profile name. Must be a string.

Configuration Modification Impact

The following table indicates the impact or the configuration change behavior on an existing call, a new PDN, or a new subscriber.

Modification	cnSGW-C Existing Call	cnSGW-C New PDN or New subscriber
Delete the apn-profile	No impact	Applied new configuration based on the changes for the following: • subscriber policy • operator policy • dnn policy • dnn profile

Modification	cnSGW-C Existing Call	cnSGW-C New PDN or New subscriber
Modify the apn profile name in the operator policy	No impact	Applied new configuration based on the changes for the following: • subscriber policy • operator policy • dnn policy • dnn profile

Validation of Uplink Packets for IP Source Violation

Table 3: Feature History

Feature Name	Release Information	Description
Validation of Uplink Packets for IP Source Violation	2024.03.0	When the IP source violation detection feature is enabled, cnSGW validates the invalid packets by checking the source IP address of incoming packets against the valid User Equipment (UE) IP address. The cnSGW derives the UE IP address from the Create Session Request or Response, and includes the IP Source Violation Information Element (IE) to be sent to UPF in the Sx Session Establishment Request Message. This IE indicates the configured action, which is either IGNORE or DISCARD, for the UPF to act on the packets with invalid source IP addresses. This feature enhances the network security and subscriber privacy by preventing the leakage of their data to unauthorized parties. This feature further reduces the risk of legal and regulatory issues for the service provider by complying with the lawful interception requirements. **CLI Introduced**: **ip source-violation [ignore | discard]** in the DNN profile. **Default Setting**: Disabled – Configuration Required to Enable

By default, the IP Source violation detection for uplink packets is disabled. You must enable this feature with either the IGNORE or DISCARD action for the invalid packets. Once enabled, the cnSGW derives the UE

IP address from the Session Create Request or Response and sends it to the UPF. The action that UPF has to take on the packets with invalid source IP addresses is indicated using the IP Source Violation IE in the Sx Session Establishment Request Message.

You can choose between the following options for the IP source violation detection feature depending on the specific requirements and policies of the network operator.

- IGNORE—Choose this option if the network does not have stringent security requirements and ignore the invalid source IP addresses to maintain operational flexibility. Ignoring invalid packets while incrementing statistics allows you to monitor and analyze the occurrence of invalid source IP addresses without immediately discarding the traffic. By forwarding the packets despite invalid source IP addresses, the network can maintain a consistent user experience, in scenarios where the impact of invalid traffic is minimal.
- DISCARD—Choose this option if the network has stringent security requirements and discard packets with invalid source IP addresses to prevent potential security threats, such as IP spoofing. Discarding packets with invalid source IP addresses ensures that only valid traffic is processed and forwarded, maintaining the integrity of the network. By discarding invalid packets, the network avoids potential misrouting that arise from handling packets with incorrect source IP addresses.



Note If this feature is disabled, P Source Violation IE is not included in the Sx Session Establishment Request Message.

Corresponding statistics are incremented for packets with invalid source IP addresses, regardless of whether the packets are ignored or discarded.

You can configure this feature through the **ip source-violation [ignore | discard]** CLI command.

For details on the enabling IP source violation for uplink packets on UPF, see Enablement of IP Source Violation for Uplink Packets in the *UPF Configuration and Admininstration Guide*.

How Validation of Uplink Packets for IP Source Violation Works

The IP Source Violation Information Element (IE) data structure indicates the actions to be taken on packets with invalid source IP addresses from cnSGW to UPF. This IE is part of the Sx Session Establishment Request message and is included when the IP source violation detection feature is enabled.

Table 4: Handling of Uplink Packets with Invalid Source IP Addresses

If Disabled then	If Enabled then

The IP Source Violation IE is not included in the Sx Session Establishment Request message.	Configure one of the following options:
	• IGNORE
	  • Packets with an invalid source IP addresses are validated and then forwarded through the network according to the applicable policy.
	  • Corresponding statistics, which are maintained at cnSGW, are incremented for the detection of the invalid source IP address.
	  • Ignored packets continue to reside in the network traffic flow and are processed as valid packets.
	• DISCARD
	  • Packets with an invalid source IP addresses are identified and then dropped.
	  • Corresponding statistics, which are maintained at cnSGW, are incremented for the action of discarding the packet.
	  • Discarded packets are not processed further by the network device and are not stored, logged, or forwarded.

Enable and Disable Validation of Uplink Packets for IP Source Violation

You can enable or disable IP source violation detection feature in the DNN profile. With the CLI command, you can configure how packets with invalid source IP addresses are handled within the network.

Procedure

Step 1 Log in to the profile DNN mode and enter the DNN profile name.

Example:

```
[sgw] smf(config)# profile dnn <profile name>
```

Step 2 Enter the **ip source-violation** command to configure the IP source violation detection.

Example:

```
[sgw] smf(config)# profile dnn <profile name> ip source-violation
```

Step 3 Choose either the *ignore* or *discard* option for the **ip source-violation** command.

Example:

```
[sgw] smf(config-dnn-intershat)# ip source-violation [ ignore | discard ]
```

To disable IP source violation in the DNN profile, use the **no ip source-violation** CLI command.

If you enter the *ignore* option, the UPF does not check the packets for IP source violation. If you enter the *discard* option, the UPF discards the errant packets.

What to do next

To verify if this feature is configured, use one of the following options:

- Verify Uplink Packet Source Validation on DNN Profile, on page 7
- Verify Uplink Packet Source Validation for NF Service, on page 7

Verify Uplink Packet Source Validation on DNN Profile

Use the procedure in the DNN profile to verify if IP source violation is disabled or enabled with the configured action.

Procedure

Enter the **show running-config profile dnn** *dnn_name* in the DNN profile.

Example:

```
show running-config profile dnn intershat
```

The following is an example output of the **show running-config profile dnn** *dnn_name* CLI command where the *discard* option is configured.

```
show running-config profile dnn intershat
 profile dnn intershat
 dns primary ipv4 209.165.200.229
 dns primary ipv6 66:66:1::aa
 session type IPV4 allowed [ IPV6 IPV4V6 ]
 upf apn intershat
 ip source-violation discard
exit
```

Verify Uplink Packet Source Validation for NF Service

Use this procedure to verify the details about the subscriber, such as the IMSI, MEI, MSISDN, and the configuration of the IP source violation feature for a specific subscriber.

Procedure

Enter the **show subscriber nf-service sgw imsi** *imsi_value*.

Example:

```
show subscriber nf-service sgw imsi ABX
```

The following is an example output of the **show subscriber nf-service sgw imsi** *imsi_value* CLI command where the *ignore* option is configured.

```
show subscriber nf-service sgw imsi ABX
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "imsi": "imsi-204163553638360",
        "mei": "imeisv-3590730650683317",
        "msisdn": "msisdn-31638577770",
        "accessType": "EUTRAN",
        "plmnId": {
          "mcc": "310",
          "mnc": "260"
        },
        "sgwProfileName": "cn-sgw",
        "unAuthenticatedImsi": "No"
      },
      "s11cInterfaceInfo": {
        "sgwTeid": "[0x1265a5a7] 308651431",
        "sgwIPv4Address": "10.210.81.0",
        "mmeTeid": "[0xa61f5cc] 174192076",
        "mmeIPv4Address": "172.57.38.19"
      },
      "pdnInfoList": {
        "totalPdn": 1,
        "pdnInfo": [
          {
            "pdnId": "PDN-1",
            "apn": "smartsites.t-mobile",
            "attachType": "Initial Attach",
…
…
            "plmnType": "ROAMER",
            "s5ePeerType": "ROAMER",
            "collocatedSub": "NonCollocated"
            "ipSrcViolation": "ignore"
          }
        ]
      }
    }
  ]
}
```

Troubleshooting Information

This section describes troubleshooting information for this feature.

Configuration Errors

This section describes the errors that cnSGW-C might report during the APN profile configuration.

```
show config-error | tab
ERROR COMPONENT   ERROR DESCRIPTION
-------------------------------------------------------------------------------------------------------
SGWProfile        Subscriber policy name : sub_policy in profile sgw1 is not configured
SubscriberPolicy  Operator policy : op_policy1 under subscriber policy sub_policy2 is not
configured
OperatorPolicy    Dnn policy name : dnn_policy1 in operator policy op_policy2 is not
configured
DnnPolicy        Dnn profile name : dnn_profile1 in dnn policy dnn_policy2 is not configured
DnnProfile        UPF selection policy name : upf_sel_policy1 in dnn profile dnn_profile2
is not configured
```