



# Multiple and Virtual DNN Support

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 2](#)
- [How It Works, on page 3](#)
- [Configuring Virtual DNN, on page 3](#)
- [DNN Profile Offline Mode Support, on page 8](#)
- [IP Pool Allocation per DNN, on page 12](#)
- [IP Pool Allocation per Slice and DNN, on page 14](#)

## Feature Summary and Revision History

### Summary Data

**Table 1: Summary Data**

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

**Table 2: Revision History**

Revision Details	Release
Added dynamic configuration change support for DNN profile.	2023.03.0
Added override keyword in the CLI to support virtual DNN from RADIUS server.	2023.02.0

Revision Details	Release
Added support for IP pool allocation per slice and DNN.	2022.04.0
Added support for: <ul style="list-style-type: none"> <li>• Charging Characteristics lookup parameter in the subscriber policy configuration.</li> <li>• Extension in Charging Characteristics ID range values.</li> </ul>	2021.02.3.t3
Added support for IPv6 interface ID generation based on SBI VIP address and CommonId of the subscriber.	2021.01.1
SMF supports the maximum limit of 2048 for the following configurations: <ul style="list-style-type: none"> <li>• Precedence</li> <li>• Operator policy</li> <li>• DNN policy</li> <li>• DNN profile</li> </ul>	2021.01.0
SMF supports case insensitive DNN configuration.	2020.02.5.t1
First introduced.	Pre-2020.02.0

## Feature Description



**Important** The PGW-C term used in this chapter denote the EPS interworking functionality supported by SMF and must not be assumed as a standalone P-GW that is used in the LTE network.

The multi-DNN support enables the SMF to have multiple PDN connections for end users to provide different services including Internet and VoNR services.

The SMF fetches the locally configured profile-based Data Network Name (DNN) in PDU Session Establishment Request from the AMF. Then, the SMF maintains the PDN connections based on using SUPI and PDU Session ID. The SMF includes the received DNN in all SBI interfaces to authorize the end user to fetch subscription information, policy, and charging related information. The SMF provisions the forward path information to the UPF. The SMF integrates the multi-DNN support with the IP Address Management (IPAM) module to allocate address to the end user based on received DNN. The SMF maps the DNN profile that is derived from subscriber policies. The SMF also fetches DNN and IPv4 and IPv6 path information based on IPAM pool configuration and updates the UPF as part of node association interactions.



**Note** Multiple DNN is supported only for 5GS procedures and is not qualified for EPS Session using SBI interfaces.

The SMF supports virtual DNN mapping based on a subscriber profile. It supports mapping of a UE-requested DNN to a configured DNN and sends the selected DNN profile towards the configured network interfaces.

### DNN Case Insensitive Support

The DNN configuration in SMF is case insensitive. The configuration accepts a string from 1 through 62 alphanumeric characters, that is case insensitive. It can also contain dots (.) and/or dashes (-).

This feature is extended to support all DNN configurations and validations.

## How It Works

The DNN profile lookup is based on subscriber policy or DNN policy. You can associate these policies in the SMF profile configuration. The subscriber policy has a higher precedence over the DNN policy when both the configurations are available.

The subscriber policy consists of a list of precedence values. The selection of precedence is based on various values. For example, the subscriber SUPI, GPSI, Serving PLMN, NSSAI, Charging Characteristics, and IMSI. Each precedence has an associated operator policy and the DNN policy is chosen from the selected operator policy.

The DNN policy can have a DNN profile configuration for each UE-requested DNN. The DNN profile has a Virtual or Mapped DNN with its list of interfaces.

The order of selection for a Virtual DNN is as follows:

- Based on subscriber policy, the order of selection is as follows: smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile (based on UE-requested DNN) > Virtual DNN mapping.
- Based on the DNN policy, the order of selection is as follows: smf-profile > dnn-policy > dnn-profile (based on UE-requested DNN) > Virtual DNN mapping.

PCF, CHF, UDM, UPF, and Resource Manager (RMGR) are the supported interfaces for Virtual DNN mapping.

If the Virtual DNN mapping is not configured, the UE-requested DNN is used across all the interfaces.

## Limitations

This feature has the following limitation:

- The SMF includes first-configured DNN profile in "dnnSmfInfoList" of NFProfile during registration with NRF.

## Configuring Virtual DNN

This section describes how to configure the Virtual DNN feature.

Configuring the Virtual DNN feature involves the following steps:

1. [Configuring Subscriber Policy, on page 4](#)

2. [Configuring Operator Policy and Associating a DNN Policy, on page 6](#)
3. [Configuring a DNN Policy, on page 6](#)
4. [Configuring a Virtual DNN under a DNN Profile, on page 7](#)
5. [Associating Subscriber Policy under the SMF Service, on page 8](#)

## Configuring Subscriber Policy

To configure the subscriber policy, use the following sample configuration:

```

config
  policy subscriber subscriber_policy_name
    precedence precedence_value
    cc-start-range cc_start_range_value
    cc-stop-range cc_stop_range_value
    gpsi-start-range gpsi_start_range_value
    gpsi-stop-range gpsi_stop_range_value
    imsi { mcc mcc_value | mnc mnc_value | msin msin_value }
    imsi-start-range imsi_start_value
    imsi-stop-range imsi_stop_value
    operator-policy operator_policy_name
    pei-start-range pei_start_range_value
    pei-stop-range pei_stop_range_value
    sdt sdt_value
    serving-plmn { mcc mcc_value | mnc mnc_value | mnc-list mnc_list_value
  }

  serving-plmn serving_plmn_value
  sst sst_value
  supi-start-range supi_start_range_value
  supi-stop-range supi_stop_range_value
end

```

### NOTES:

- **precedence** *precedence\_value*: Specify the precedence value associated with the subscriber policy. The maximum limit for precedence is 2048.
- **cc-start-range** *cc\_start\_range\_value*: Specify the charging characteristics start range value associated with the subscriber policy. *cc\_start\_range\_value* must be a 1 to 4 digit hexadecimal string in the range of 0x1 to 0xffff. For example, 0001.
- **cc-stop-range** *cc\_stop\_range\_value*: Specify the charging characteristics end range value associated with the subscriber policy. *cc\_stop\_range\_value* must be a 1 to 4 digit hexadecimal string in the range of 0x1 to 0xffff. For example, 12AB.
- **gpsi-start-range** *gpsi\_start\_range\_value*: Specify the GPSI start range value to be associated with the subscriber policy. *gpsi\_start\_range\_value* must be an integer in the range from 1000000000 through 9999999999999999.
- **gpsi-stop-range** *gpsi\_stop\_range\_value*: Specify the GPSI stop range value to be associated with the subscriber policy. *gpsi\_stop\_range\_value* must be an integer in the range from 1000000000 through 9999999999999999.

- **imsi** { **mcc** *mcc\_value* | **mnc** *mnc\_value* | **msin** *msin\_value*}: Specify the IMSI value by providing the MCC, MNC, or MSIN value that is to be associated with the subscriber policy.
- **imsi-start-range** *imsi\_start\_value*: Specify the IMSI start range value. *imsi\_start\_value* must be an integer in the range from 1000000000 through 999999999999999.
- **imsi-stop-range** *imsi\_stop\_value*: Specify the IMSI stop range value. *imsi\_stop\_value* must be an integer in the range from 1000000000 through 999999999999999.
- **operator-policy** *operator\_policy\_name*: Specify the operator policy to be associated with the subscriber policy.

The maximum limit for operator policy is 2048.

- **pei-start-range** *pei\_start\_range\_value*: Specify the PEI start range value. *pei\_start\_range\_value* must be an integer in the range from 1000000000 through 999999999999999.
- **pei-stop-range** *pei\_stop\_range\_value*: Specify the PEI stop range value. *pei\_stop\_range\_value* must be an integer in the range from 1000000000 through 999999999999999.
- **sdt** *sdt\_value*: Specify the SDT value to be associated with the subscriber policy. *sdt\_value* must be a 6-digit octet string in the [0-9a-fA-F]{6} - 000000 - ffffff format. For example, 1A2B3c.
- **servicing-plmn** { **mcc** *mcc\_value* **mnc** *mnc\_value* **mnc-list** *mnc\_list\_values* } : Specify the 3-digit Mobile Country Code (MCC), 2- or 3-digit Mobile Network Code (MNC), or the list of MNC values of the serving PLMN. *mcc\_value* and *mnc\_value* must be a string. *mnc\_list\_values* must be a string, such as [580 660].
- **sst** *sst\_value*: Specify the Slice/Service Type (SST) value. *sst\_value* must be a 2-digit octet string in the [0-9a-fA-F]{2} - 00 to FF format. For example, A8.
- **supi-start-range** *supi\_start\_range\_value*: Specify the SUPI start range value. *supi\_start\_range\_value* must be an integer in the range from 1000000000 through 999999999999999.
- **supi-stop-range** *supi\_stop\_range\_value*: Specify the SUPI stop range value. *supi\_stop\_range\_value* must be an integer in the range from 1000000000 through 999999999999999.

## Configuration Verification

To verify the policy-related configuration details, use one of the following commands:

**show subscriber policy** *policy\_name* or **show full** in the policy configuration mode.

The following is an example output of the show command:

If the subscriber policy configuration includes the charging characteristics parameter, then the value appears as part of **cc-start-range** and **cc-stop-range** in the following output.

```
smf(config-subscriber-polSub)# show full
policy smf polSmf
precedence 1
sst                22
sdt                232322
servicing-plmn mcc 210
servicing-plmn mnc 90
supi-start-range  1000000000000001
supi-stop-range   1000000000000010
gpsi-start-range  10000000000
gpsi-stop-range   99999999999
```

```

cc-start-range 0001
cc-stop-range 0005
operator-policy opPoll
!
!

```

## Configuring Operator Policy and Associating a DNN Policy

To configure the operator policy, use the following sample configuration:

```

config
  policy operator operator_policy_name
    policy dnn dnn_policy_name [ [ secondary secondary_dnn_policy_name ] [
network-capability network_capability ] ]
  end

```

### NOTES:

- **policy dnn** *dnn\_policy\_name* [ [ **secondary** *secondary\_dnn\_policy\_name* ] [ **network-capability** *network\_capability* ] ]: Specify the parameters of primary DNN policy to be associated with the operator policy. *dnn\_policy\_name* must be a string.
  - **secondary** *secondary\_dnn\_policy\_name*: If the parameters of DNN policy to be associated with the operator policy don't match with the primary policy, specify the secondary DNN policy for fallback. *secondary\_dnn\_policy\_name* must be a string.
  - **network-capability** *network\_capability*: Specify the network capability configuration details for the respective operator policy that you have selected. The *network\_capability* value must be a string.

## Configuring a DNN Policy

To configure the DNN policy, use the following configuration:

```

config
  policy dnn dnn_policy_name
    dnn dnn_name profile dnn_profile_name dnn-list dnn_list
  exit
exit

```

### NOTES:

- **policy dnn** *dnn\_policy\_name*: Specify the DNN policy. *dnn\_policy\_name* must be an alphanumeric string.
  - In releases prior to 2021.01.0: The maximum limit for DNN policy is 512.
  - In 2021.01.0 and later releases, the limit for DNN policy is increased from 512 to 2048.
- **dnn** *dnn\_name*: Specify the virtual DNN profile to map with the specified network DNN profile. *dnn\_name* must be an alphanumeric string.
- **profile** *dnn\_profile\_name*: Specify the network DNN profile. *dnn\_profile\_name* must be an alphanumeric string.
  - In releases prior to 2021.01.0: The maximum limit for DNN profile is 512.

In 2021.01.0 and later releases, the limit for DNN profile is increased from 512 to 2048.

- **dnn-list** *dnn\_list*: Specify the list of DNNs supported by the UPF node.

## Configuring a Virtual DNN under a DNN Profile

The SMF provides flexibility to send Virtual-DNN value on all northbound interfaces. Virtual DNN to be send on each interface can be configured as follows. The Resource Manager (RMGR) virtual DNN is used to map IP pool to DNN.

To configure a virtual DNN under a DNN profile, use the following sample configuration:

```
config
  profile dnn profile_name
    dnn dnn_name network-function-list [ chf | ocs | pcf | pcrf | radius
| upf ]
  profile profile_name
  end
```

### NOTES:

- **dnn** *dnn\_name*: Specify the DNN name. *dnn\_name* must be an alphanumeric string.
- **network-function-list**: Specify the network functions. The DNN profile goes to these network functions. Supported values are **CHF, OCS, PCF, PCRF, RADIUS and UPF**.

### Configuring Override Command

In addition to the preceding CLI, SMF has the capability to override the access DNN with the vDNN received from the RADIUS server.

RADIUS-ep is upgraded to decode Starent VSA attribute “SN-Virtual-APN-Name (Type: 94)“ and application is enhanced to support this attribute.

RADIUS Server sends vDNN to SMF in access accept and SMF includes this DNN in N4 messages to UPF. A new configuration is added on the SMF to decide whether to override the DNN sent on specific interfaces with the value received from RADIUS server.

Override keyword is added to support virtual DNN from the Radius Server.

```
config
  profile dnn profile_name
    dnn override network-function-list [ chf | ocs | pcf | pcrf | radius
| upf ]
    dnn override rmgr
  end
```

Details of attribute used for receiving virtual DNN on RADIUS interface is as follows:

- **SN**: Virtual-APN-Name
- **Syntax**: Opaque Value
- **Length**: 1-64
- **Type**: 26

- **Vendor ID:** 8164
- **VSA Type:** 94
- Override keyword takes priority over the locally configured value.
- Override keyword is present but RADIUS isn't providing any vDNN then SMF uses the locally configured value (if present) or gnDNN.
- If for an interface, there's no configuration (either override or local-dnn-name), it takes the gnDNN. Override vDNN isn't applicable for UDM network-function.
- The framed-ip received from the RADIUS server must be a part of the IP pool associated to the vDNN received from the RADIUS server. If there's mismatch, session creation fails.
- with this feature, different RMGR vDNN can be assigned to the same UE for same DNN for dynamic and static ip allocation case and hence IP can be assigned from dynamic or static pool.

## Associating Subscriber Policy under the SMF Service

To associate a subscriber policy under SMF service, use the following sample configuration:

```
config
  profile smf smf_profile_name
    service name service_name
      subscriber-policy subscriber_policy_name
    end
```

### NOTES:

- **subscriber-policy *subscriber\_policy\_name*:** Specify the subscriber policy name. *subscriber\_policy\_name* must be an alphanumeric string.

## DNN Profile Offline Mode Support

### Feature Description

The Data Network Name (DNN) Profile Offline Mode Support feature allows new sessions, or subsequent messages of existing sessions, to use the updated configuration values when the DNN is in offline mode. This feature enables SMF to switch the DNN to offline mode.



#### Important

You must clear the subscriber sessions before switching DNN to offline mode while changing the configuration for which dynamic change is not allowed. New session requests are rejected until the DNN is changed back to online mode.



## How it Works

This section describes how the DNN Profile Offline Mode Support feature works for the supported SMF configurations.

### DNN Policy

DNN Policy configuration defines the DNN Profile mapping with the DNN. After the DNN to profile mapping is changed, new subscriber for the same DNN uses the updated DNN Profile. So, there is no impact on existing subscribers.

### DNN Profile

DNN profile defines various parameters for a particular DNN.

The following table describes if the dynamic configuration change is allowed or if the DNN must be set to an offline mode.

**Table 3: DNN Profile Configuration and its Impact During Dynamic Update**

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
DnsServers	Allowed	No impact
DnnInfo	Allowed	New values are used after database reload of the session
NetworkElementProfile	Not recommended (See NOTES)	
Timeout	Allowed	No impact
ChargingProfile	Not recommended (See NOTES)	
RemoteVmac	Allowed	No impact
PcscfProfile	Allowed	No impact
PpdProfile	Allowed	Immediate (new values are used)
DefaultSscMode	Allowed	No impact
DefaultPduSession	Allowed	No impact
AllowedPduSession	Allowed	No impact
QosProfile	Allowed	Immediate (new values are used)
UpfApn	Allowed	No impact
SecondaryAuthen	Allowed	No impact
LocalAuthorization	Allowed	No impact
NetworkCapability	Allowed	No impact
PolicyProfile	Allowed	No impact

**NOTES:**

- It's recommended not to modify or delete the NetworkElementProfile and ChargingProfile configuration parameters. If the parameters are changed, then the behavior for:
  - NetworkElementProfile: Messages for the existing sessions may be sent on new servers.
  - ChargingProfile: There may be some inconsistencies related to Usage Reporting Rules (URRs) between SMF and UPF.
- For modifying the DNN profile mapping, the DNN profile must be in the offline mode.
- It's recommended to review the messages shown in the help string before executing the CLI commands.
- Switch the DNN profile to an offline mode when configuring the parameters dynamically. This step avoids the network impact, which is caused by the configuration changes.

## Subscriber Policy

SMF uses subscriber policy to select the operator policy based on the following options:

- SUPI range
- SST (Slice/Service Type)
- IMSI range
- GPSI
- PEI
- SDT (Slice Differentiator Type)
- S-NSSAI
- PLMN ID
- CC (Charging Characteristics) range

Change in Subscriber Policy configuration can be applied dynamically as it has no impact on the existing sessions. SMF selects the operator policy for the new sessions based on the updated configurations.

For 5G subscribers, SMF allows higher number of virtual DNNs (vDNN) with slice-based vDNN selection. However, when 5G subscribers connect from 4G access network, the slice information is unavailable until SMF fetches the UE subscription data from UDM. In such scenarios, SMF performs initial vDNN selection based on the CC lookup parameter as well. After the subscription data is fetched, the SMF reselects the vDNN based on the slice-id information and uses the new vDNN profile. This approach remains the same for the Wi-Fi calls as well.

SMF provides the flexibility of vDNN selection based on using either Charging Characteristics or slice through the CLI configuration. For more information on the configuration part, see the [Configuring Subscriber Policy, on page 4](#) section.

For details, see the "Configuration-based Control of UDM Messages" and "Configuration-based Control of PCF Messages" sections in the [Interfaces Support](#) chapter.



**Note** As DNN profile is under the operator policy, the reselection of vDNN profile implies the reselection of operator policy as well. SMF supports the configuration so that the reselection doesn't impact the existing features that are associated to other parameters in operator policy.

## Limitations

The following limitations apply when the DNN is in the offline mode:

- The subsequent 5G calls for the offline DNN are rejected with the HTTP Cause - HTTP\_STATUS\_CODE\_503\_SERVICE\_UNAVAILABLE, and 5GSMCause as “Service option temporarily out of order”.
- The subsequent 4G calls for the offline DNN are rejected with the GTP cause “No resources available”.

## Configuring the DNN Profile Offline Mode Support Feature

This section describes how to enable the offline mode for a DNN profile.

### Configuring the DNN Profile to Offline Mode

To configure the DNN profile to offline mode, use the following sample configuration:

```
config
  profile dnn dnn_profile_name
  mode dnn_mode
end
```

#### NOTES:

- **profile dnn dnn\_profile\_name**: Specify the DNN profile.
- **mode dnn\_mode**: Specify the DNN mode of operation. When the DNN mode is set to **offline**, the new sessions are rejected. The default value is **online**.

### Verifying the DNN Profile Offline Mode Configuration

This section describes how to verify if the DNN profile is set to the offline mode.

The following is an example output of the **show running-config profile dnn profile\_name** command.

```
show running-config profile dnn intershat
profile dnn intershat
  mode offline
  network-element-profiles chf chf1
  network-element-profiles amf amf1
  network-element-profiles pcf pcf1
  network-element-profiles udm udml
  charging-profile chgprf1
  virtual-mac b6:6d:47:47:47:47
  ssc-mode 2 allowed [ 3 ]
  session type IPV4 allowed [ IPV6 IPV4V6 ]
  upf apn intershat
```

```

    dcnr true
exit

```

## DNN Profile Offline Mode OAM Support

This section describes operations, administration, and maintenance information for this feature.

### Bulk Statistics Support

The following label is introduced as part of this feature:

- `LABEL_DISC_PDUSETUP_DNN_OFFLINE`: This label is defined to indicate that the call is rejected because the DNN is in the offline mode.

## IP Pool Allocation per DNN

### Feature Description

The IP Pool Allocation per DNN feature supports mapping of a UE-requested DNN to a configured DNN for IP Pool selection. This feature is supported for the SMF and PGW-C in 5G and 4G.

The IP Pool Allocation per DNN feature supports the following functionalities:

- Enables SMF to support a new configuration under the DNN profile to enable mapping of the UE-requested DNN to a DNN that is associated with an IP pool.
- Sends the mapped DNN over Remote Procedure Call (gRPC) to the Resource Manager functionality under Node Manager service for IP allocation.
- Supports the new configuration for IP Pool DNN over the virtual DNN with Redundancy Manager, if available.
- Sends the UE-requested DNN when both the new configuration for IP pool and the virtual DNN are unavailable.

### How it Works

This section provides a brief of how the IP Pool Allocation per DNN feature works.

- The DNN profile lookup is based on the subscriber policy or DNN policy. The DNN profiles are associated in the SMF profile configuration. The subscriber policy takes precedence over the DNN policy when both the configurations are present.
- The subscriber policy contains a list of precedence values. The selection of the precedence is based on the SUPI, GPSI, serving PLMN, and NSSAI value of the subscriber.
- Each precedence has an associated operator policy. The DNN policy is picked from the selected operator policy.
- The DNN policy can have a DNN profile configuration for each of the UE-requested DNNs.

- The DNN profile contains the virtual or mapped DNN with its list of interfaces. This is an existing configuration and Redundancy Manager is also in the list of interfaces. For more information, see the [Configuring a Virtual DNN under a DNN Profile, on page 7](#) section.
- The new configuration under the DNN profile contains the mapping of the UE-requested DNN to IP Pool DNN.
- The DNN profile selection occurs in the following order:
  - Based on subscriber policy, the order of selection is as follows: smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile (based on UE-requested DNN) > Virtual DNN mapping.
  - Based on the DNN policy, the order of selection is as follows: smf-profile > dnn-policy > dnn-profile (based on UE requested Dnn) > Virtual DNN mapping.

**Note**

- New IP pool DNN mapping takes precedence over the existing virtual DNN configuration if the Redundancy Manager configuration exists.
- If both the configurations for the Redundancy Manager are not present, the UE-requested DNN is used to select the IP pool.
- If the mapped DNN does not have the IP pool configured, then IP allocation fails, and the call is deleted.
- Both the EPS and 5G calls follow the same principles for IP allocation for a DNN.

## Configuring IP Pool Allocation

This section describes how to configure the IP Pool Allocation per DNN feature.

Configuring the IP Pool Allocation per DNN involves either one of the following steps:

1. Configuring virtual DNN under DNN profile. For more information, see the [Configuring a Virtual DNN under a DNN Profile, on page 7](#) section.

**Note**

This is a generic configuration along with other interfaces as an option.

2. Allocating the IP pool per DNN

**Note**

This configuration is specifically only for IP allocation.

## Allocating the IP Pool per DNN

To allocate the IP pool per DNN, use the following sample configuration:

```

config
  profile dnn dnn_profile_name
    dnn rmgr rmgr_name
  end

```

**NOTES:**

- **profile dnn** *dnn\_profile\_name*: Map the Virtual DNN profile with the specified network DNN profile. *dnn\_profile\_name* must be an alphanumeric string.
- **dnn rmgr** *rmgr\_name*: Specify the Redundancy Manager to which the DNN profile will be sent. *rmgr\_name* must be an alphanumeric string.

## Verifying IP Pool Allocation Configuration

This section describes how to verify the IP pool allocation configuration.

Use the **show full** CLI command in the DNN Profile Configuration mode to verify the configuration associated with IP pool allocation per DNN.

The following is an example output of this show command.

```

[unknown] smf(config-dnn-cisco123)# show full
profile dnn intershat
dns primary ipv4 209.165.200.231
dns primary ipv6 2001:DB8:1::1
dns secondary ipv4 209.165.200.232
dns secondary ipv6 2001:DB8:1::2
network-element-profile-list chf [ chgser1 ]
dnn starent.com network-function-list [ upf chf rmgr ]
dnn rmgr cisco.com
charging-profile chgprf1
virtual-mac      01-00-5E-90-10-00
pcscf-profile    pcscf1
ppd-profile      ppdl
ssc-mode 1
session type IPV4
.
.
.

```

# IP Pool Allocation per Slice and DNN

## Feature Description

SMF supports IP pool allocation per slice with the same DNN. A slice is a logical end-to-end network that is created dynamically. A user equipment (UE) can access multiple slices over one access network, such as over the same radio interface.

For this feature, SMF performs the following tasks:

- Register, discover, subscribe, and send traffic to all the external NFs based on the slice ID.
- Provide slice-based procedure and session statistics.
- Provide slice information on an EDR.

- Provide slice information on logs.
- Limit the maximum number of supported slices on SMF to 512.

## How it Works

SMF selects NFs, such as PCF, CHF, UDM, and AMF through the static configuration or NRF-based dynamic selection. In both these options, the messaging includes the slice information that is used in those interfaces.

SMF performs the following tasks:

- Register slice with NRF.
- Receive slice information on the N11 and N10 interfaces.
- Use slice for peer NF discovery and UPF selection.
- Send slice information on the N7 and N40 interfaces.

## Limitations

The IP Pool Allocation per Slice and DNN feature has the following limitations:

- Only the procedure and session statistics have the slice information. Other statistics are on NF level.
- Enabling or disabling logging based on slice information is not supported.

## Feature Configuration

This section describes how to configure the IP Pool Allocation per slice and DNN feature.

This feature includes the following steps:

1. Configure tags. For details, see [Configuring SMF Tags](#).
2. Perform the dynamic node selection with slice using the following tasks:
  - Register NRF. For details, see [Registering NRF](#).
  - Configure allowed NSSAI values. For details, see [Configuring Allowed NSSAI Values](#).
  - Discover NRF. For details, see [Discovering NRF](#).
3. Configure NSSAI labels of `smf_service_stats` metrics for slice information on procedure and session statistic. For details, see [Configuring Metrics Collection](#).

## Configuring Allowed NSSAI Values

To configure the allowed NSSAI values for slicing, use the following sample configuration:

```
config
  profile smf smf_profile_name
    instances instance_id
```

```

allowed-nssai allowed_nssai_values
end

```

**NOTES:**

- **allowed-nssai** *allowed\_nssai\_values* : Specify one or multiple values for the allowed NSSAI for slicing.

## Configuring Slice-based IP Pool Allocation

To configure the slice-based pool allocation, use the following sample configuration.

```

config
nssai name nssai_name
  sst sst_value
  sdt sdt_value
  dnn dnn_name_value
  pool-selection pool_selection_value
end

```

**NOTES:**

- **pool-selection** *pool\_selection\_value* : Configure the IP pool selection methods as DNN or NSSAI. The default pool selection method is DNN. If the pool selection method is slice or slice DNN only, then based on the slice and the DNN, the IP pools are selected.

**Note**

- When you configure the pool selection method as NSSAI for a slice, then in IPAM configuration for all the DNN for that UPF, you must configure "slice1" and "dnn" as values.
- In IPAM, tag "nssai" is a string and must match with the SMF slice configuration name.

### Configuration Example of the slice-based pool allocation

The following is an example configuration of the slice-based pool allocation.

```

nssai name slice1
sst 02
sdt Abf123
pool-selection [ dnn nssai ]
exit

```