DNN Support

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

Revision Details	Release
Added override keyword in the CLI to support virtual DNN from RADIUS server.	2023.02.0
Added support for IP pool allocation per slice and DNN.	2022.04.0
Added support for: • Charging Characteristics lookup parameter in the subscriber policy configuration. • Extension in Charging Characteristics ID range values.	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: • Precedence • Operator policy • DNN policy • DNN profile	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 (vDNN) 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.

For 5G subscribers, SMF allows a higher number of vDNNs 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. 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.

Note As the DNN profile is under the operator policy, the reselection of the vDNN profile implies the reselection of the 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 the operator policy.

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 7
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
         instance-start-range start_range_value
         instance-stop-range 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 999999999999999.
- **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 999999999999999.
- **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 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.
- **serving-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.

- **instance-start-range** *start_range_value*: Specify the SMF instance start range value. *start_range_value* must be an integer in the range from 1 to 8.
- **instance-stop-range** *stop_range_value*: Specify the SMF instance stop range value. *stop_range_value* must be an integer in the range from 1 to 8.

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
  serving-plmn mcc 210
  serving-plmn mnc 90
  supi-start-range 100000000000001
  supi-stop-range  100000000000010
  gpsi-start-range 1000000000
  gpsi-stop-range  9999999999
  cc-start-range 0001
  cc-stop-range 0005
  operator-policy  opPol1
!
!
```

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.

  The maximum limit for DNN policy is 2048.

- **dnn** *dnn_name*: Specify the virtual DNN profile to map with the specified network DNN profile. *dnn_name* must be an alphanumeric string.

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

- **profile** *dnn_profile_name*: Specify the network DNN profile. *dnn_profile_name* must be an alphanumeric string.

  The maximum 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 | cgf ]
   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, UPF, and CGF.**

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 | cgf ]
       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.
- 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.

Network Function Selection based on SMF Instances

Table 3: Feature History

Feature Name	Release Information	Description
UPF Selection based on SMF Instances	2024.01.2	This feature allows you to customize SMF instances in the Subscriber Policy Configuration and to bind SMF instances to the colocated UPFs in the inter-site GR deployment model. When the user selects operator policies, the SMF instances act as a filter and allow the SMF to select a specific DNN profile. The DNN selection helps in finding the closest and active Network functions (for example, UPFs) and ensures routing the user traffic only to the colocated UPFs. This implementation reduces the latency and improves user experience. To implement this feature, the following keywords are added under the policy subscriber command: • **instance-start-range** • **instance-stop-range** **Default Setting**: Disabled – Configuration required to enable

Instance-based Network Function Selection

Feature Description

During the subscriber session creation, SMF selects operator policy based on the SMF instance IDs configured in the Subscriber Policy Configuration mode. For each subscriber, SMF associates the selected operator policies with different DNN profiles, virtual DNNs, IP pools, and UPF profiles.

SMF provides the flexibility to choose appropriate DNN profiles corresponding to the SMF instances.

For example, in an active-standby Geo Redundancy (GR) deployment scenario, assume that there are two racks (Rack 1 and Rack 2) with each rack comprising two regions (Region 1 and Region 2), two active and standby SMF instances (SMF instance 1 and SMF instance 2), IP pools (Pool 1 and Pool 2), virtual DNNs (vdnn 1 and vdnn 2), and two UPF sets (UPF Set 1 (UPF 1 and UPF 3) and UPF Set 2 (UPF 2 and UPF 4)).

SMF is configured in such a way that vdnn 1 is associated to SMF Instance 1, Pool 1, and UPF Set 1, and vdnn 2 is associated to SMF Instance 2, Pool 2, and UPF Set 2. When the subscriber attempts to establish PDU connection, SMF instance is selected based on the Virtual IP (VIP) of the session it lands. If SMF instance 1 in one region is active and selected, SMF chooses vdnn1, Pool 1, and UPF Set 1 even though the SMF instances have the same DNN in both the regions.

SMF subsequently distributes the IP pools from Pool 1 only to the UPFs in UPF Set 1. If the SMF instance IDs are not configured, SMF allocates the available IP addresses to the UPFs associated to both the SMF instances.

Configuring SMF Instances

To configure the SMF instances, use the following sample configuration:

Note It is recommended to add this configuration at runtime. A new operator policy selection post configuration change uses new configuration.

```
config
   policy subscriber subscriber_policy_name
      precedence precedence_value
         instance-start-range start_range_value
         instance-stop-range stop_range_value
         operator-policy operator_policy_name
         end
```

NOTES:

- **precedence** *precedence_value*: Specify the precedence value associated with the subscriber policy.

  The maximum limit for precedence is 2048.

- **instance-start-range** *start_range_value*: Specify the SMF instance start range value. *start_range_value* must be an integer in the range from 1 to 8.

- **instance-stop-range** *stop_range_value*: Specify the SMF instance stop range value. *stop_range_value* must be an integer in the range from 1 to 8.

Configuration Example

The following is an example of a configuration **show running-config policy subscriber** command that describes SMF instances for DNN profile selection.

```
 [smf] smf# show running-config policy subscriber
Wed Mar  6  05:09:45.143 UTC+00:00
policy subscriber polSub
 precedence 1
  sst                 02
  sdt                 Abf123
  serving-plmn mcc 123
  serving-plmn mnc 456
  supi-start-range     100000000000001
  supi-stop-range      999999999999999
  gpsi-start-range     100000000000001
  gpsi-stop-range      999999999999999
  instance-start-range 1
  instance-stop-range  1
  operator-policy      opPolHomer
 exit
```

Switching DNN Profile to Offline Mode During Dynamic Config Update

Feature Description

This feature enables SMF to switch the DNN to offline mode to support dynamic configuration update. SMF allows dynamic configuration update of some DNN profile parameters only when the DNN profile is changed to offline mode.

When the DNN is in offline mode, new sessions or subsequent messages of existing sessions, will use the updated configuration values.

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 this 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 4: 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

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
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
- SMF instance range

A 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.

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_UNAVILABLE, 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 Offline DNN Profile

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

Switching the DNN Profile to Offline Mode

To change 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 udm1
        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
```

OAM Support for DNN Profile Offline Mode Setting

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.

DNN Inheritance

Feature Description

Table 5: Feature History

Feature Name	Release Information	Description
DNN Inheritance for 4G Sessions on Legacy Interfaces	2024.02.0	SMF with legacy interfaces support the DNN inheritance feature.

SMF provides a way to configure common attributes in a parent DNN profile template and reuse it in other DNN profiles, for example, child DNN profiles as and when required. This feature optimizes the DNN profile configurations and improves the operational efficiency.

Note The DNN Inheritance feature is currently qualified only for SMF (including legacy interfaces) and not for cnSGW-C.

How it Works

This section provides details about how the network operators can perform the DNN profile configuration to inherit or reuse a parent DNN profile.

Table 6: Preparation to Configure the Parent DNN Profile

Step	Description
1	Configure parent DNN profile having common attributes.
2	Inherit the configured parent DNN profile in a child DNN profile. The following conditions apply: • If a child profile is trying to inherit a DNN profile that doesn't exists, then the SMF CLI displays an error while committing the changes. • If the parent DNN profile is deleted but found in a child profile, then SMF CLI displays an error while committing the changes. **Note** Delink the parent profile from the child DNN profile to delete the parent DNN profile. • If the attributes configured in a child DNN profile do not belong to any parent DNN profile, then the operator can modify those attributes in an individual child DNN profile.

Step	Description
3	

Step	Description
	SMF receives request for the child DNN profile. If the child DNN profile has an *inherit* attribute, then SMF resolves the inherited/parent profile based on the following conditions:

- If the parent profile is found and the child profile doesn't override parent attributes, then SMF updates the child profile with inherited attributes.
- If a parent profile is found and a child profile overrides some or all the parent attributes, then SMF prioritizes overridden attributes over a parent profile and updates the child profile by taking overridden attributes from a child profile and the rest of the attributes from a parent profile.
- If a parent profile has attributes in the form of arrays or slices, and the child profile also has the same attributes configured, then the resultant DNN profile overrides that attribute completely from the child profile, which means the combined profile contains the value of the child attribute.

  Example for DNN profiles:

  ```
  profile dnn intershat_Parent // parent dnn profile
            ims mark qci [ 83 128 ]
            network-element-profiles chf chf1
            network-element-profiles amf amf1
            network-element-profiles pcf pcf1
            network-element-profiles udm udm1
            charging-profile chgprfFBC
            override         [ charging-profile charging-characteristics-id ]
            virtual-mac      b6:6d:47:47:47:47
            session type IPV4 allowed [ IPV6 IPV4V6 ]
            dcnr             true
          exit

   profile dnn intershatRoamer // child dnn profile
      inherit  intershat_Parent
      override [ charging-characteristics-id charging-qbc-profile ]
   exit
  ```

  Example for resultant profiles:

  ```
   profile dnn intershatRoamer // Resultant dnn profile
             ims mark qci [ 83 128 ]
             network-element-profiles chf chf1
             network-element-profiles amf amf1
             network-element-profiles pcf pcf1
             network-element-profiles udm udm1
             charging-profile chgprfFBC
             override        [charging-characteristics-id charging-qbc-profile ]
             virtual-mac      b6:6d:47:47:47:47
             session type IPV4 allowed [ IPV6 IPV4V6 ]
             dcnr             true
           exit
  ```

- If a parent profile has attributes in the form of structures and the child profile also has the same attributes configured, then the resultant DNN profile overrides that attribute completely from child, which means the combined profile contains the value of a child attribute.

  Example for DNN profiles:

  ```
  profile dnn intershat_Parent // parent dnn profile
          charging-profile chgprfFBC
          virtual-mac      b6:6d:47:47:47:47
  ```

Step	Description

	`dcnr             true`
	`network-element-profiles chf chf1`
	`network-element-profiles amf amf1`
	`network-element-profiles udm udm1`
	`exit`
	
	`profile dnn intershatRoamer // child dnn profile`
	`inherit intershat_Parent`
	`network-element-profiles pcf pcf1`
	`exit`
	
	Example for resultant profiles:
	
	`profile dnn intershatRoamer // Resultant dnn profile`
	`charging-profile chgprfFBC`
	`virtual-mac      b6:6d:47:47:47:47`
	`dcnr             true`
	`network-element-profiles pcf pcf1`
	`exit`
	
	Note When the SMF receives a request for the child DNN profile and the child DNN profile doesn’t have an inherit attribute, then the SMF returns all attributes from the child DNN profile.

4	Update the parent and child DNN profile at runtime. After the changes are committed, SMF picks the latest attributes from the child and parent profiles.

Configuring DNN Inheritance

You can define all the common attributes in a separate DNN profile and then use this parent profile in other DNN profiles by using the CLI configuration.

To inherit the parent DNN profile with common attributes, use the following sample configuration:

```
config
   profile dnn dnn_profile_name
      inherit dnn_template_name
       dnn rmgr   ims_pool_ipv6
      end
```

NOTES:

- **inherit** *dnn_template_name*: Specify the name of parent DNN profile to inherit to child profile(s).

Configuration Example

The following is an example configuration to inherit the attributes from a parent DNN profile and use them in a child profile.

```
// Parent DNN profile
profile dnn dnnprof-ims.epdg.prod
  dns primary ipv4 10.177.0.34
  dns primary ipv6 fd00:976a::9
  dns secondary ipv4 10.177.0.210
  dns secondary ipv6 fd00:976a::10
  network-element-profiles chf nfprf-chf1
  network-element-profiles amf nfprf-amf1
  network-element-profiles pcf nfprf-pcf1
  network-element-profiles udm nfprf-udm1
  dnn ims.epdg.prod network-function-list [ chf pcf udm upf ]
  timeout up-idle 3600 cp-idle 7320
  charging-profile           chgprof-1
  pcscf-profile              pcscf1
  ppd-profile                ppd-prof1
  ssc-mode 1 allowed [ 2 ]
  session type IPV6
  session skip-ind false
  upf apn ims.epdg.prod
  qos-profile                5qi-to-dscp-mapping-table-IMS
  always-on                  true
  dcnr                       true
  userplane-inactivity-timer 3600
  only-nr-capable-ue         false
exit

// Child DNN profile
profile dnn dnnprof-ims.prod
  inherit dnnprof-ims.epdg.prod
  dnn rmgr ims-pool-ipv6
exit
```

IP Pool Allocation per DNN

Feature Description

The IP Pool Allocation 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.

SMF supports the following functionalities:

- Supports 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 configuration for IP pool DNN over the virtual DNN with Redundancy Manager, if available.
- Sends the UE-requested DNN when both the configuration for IP pool and the virtual DNN are unavailable.

How it Works

This section provides a brief of how the IP Pool Allocation 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 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

- 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 feature.

Configuring the IP Pool Allocation 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 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*: Specifiy 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      ppd1
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 equipent (UE) can access multiple slices over one access network, such as over the same radio interface.

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.

Configuring this feature involves 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 statistice. 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

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

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