

User Plane Selection

- APN and APN Profile-Based User Plane Selection, on page 1
- Dynamic User Plane Selection, on page 6
- Multiple UP Group Support, on page 21
- Priority between UP Groups, on page 25
- User Plane Selection based on TAC Range, on page 36
- UP Selection During Session Creation Failures, on page 40

APN and APN Profile-Based User Plane Selection

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

In the CUPS architecture, SAEGW-C selects a user plane by using an algorithm that selects the least connected user plane. It also selects the user plane from a flat list of user planes.

This feature enables the operator to select a user plane from a specific UP group associated with an APN or APN Profile.

In S-GW, UP groups are associated with an Access Point Name (APN) profile. An APN profile groups a set of APN-specific parameters that are applicable to one or more APNs. A single APN profile can be associated with multiple operator policies.

How It Works

Cisco CUPS solution supports static UP selection. This is based on static selection of active and available SAEGW-U. The static UP selection uses the UP Group concept. UP group is a group of UP SAEGW-Us. Each APN is then associated with one UP group. APN is served by the UP groups associated with it. UPs are selected using an algorithm that selects the least connected UP available in that particular group.

UP Group

A UP can be part of only one UP group. In a UP Group, all UPs must be of the same capacity and capability. Different type of UPs must be part of different UP groups.

CUPS supports the following types of UP groups:

- Specific UP Group—It is a set of explicitly configured UPs. The specific group gives the flexibility to group certain specific types of UPs together. This helps in reserving specific set of UPs for a specific purpose. There can be multiple specific groups that can be configured.
- Default UP Group—This is a default group that groups all UPs that are registered and are not explicitly configured as part of any specific UP group. The default group has advantage of registering UPs in a zero touch manner without configuring a UP on the CP explicitly. This type of group is suited for collocated CUPS cases where all UPs with the same capacity and capability are in the same data center. The default group optimizes the UP configuration on CP.

An APN can be associated with UP group. If no group is associated with an APN, then default UP group is used to serve that APN. Similarly, for selecting UP for Pure-S calls, UP group can be associated to an APN profile. If there is no APN Profile/Operator-Policy defined or no group is associated with APN Profile, then SAEGW-C uses the "default" UP group for selection.

An operator can reserve certain UPs for certain applications. For example, IMS, Internet, and IOT can have different UP groups.

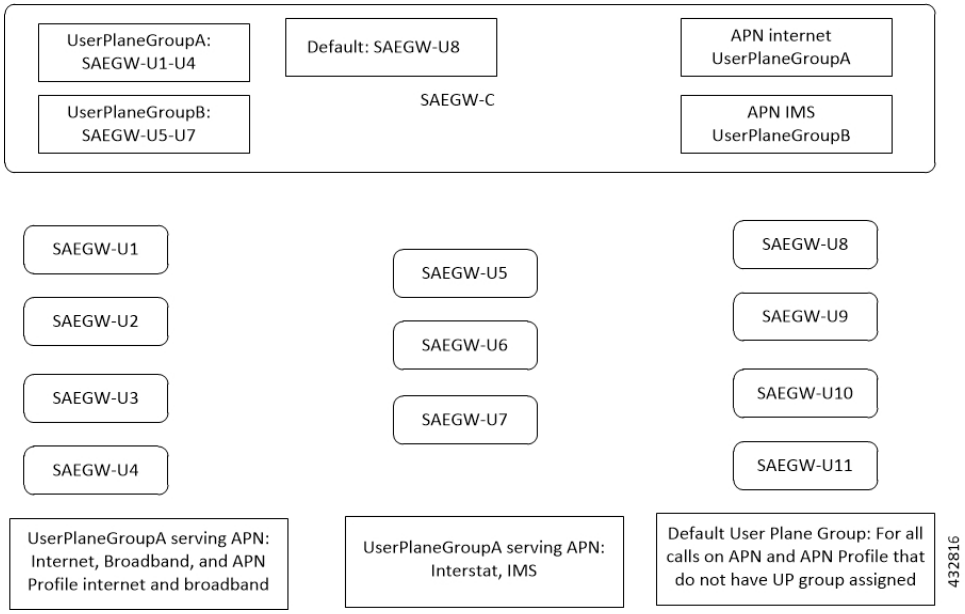
With this feature:

- SAEGW-C always has one user plane group with the name "default".
- SAEGW-C supports a maximum number of 100 user planes.
- The user planes can be organized in different groups.
- Currently, 100 user-plane-groups can be configured, and a single group can have a maximum number of 100 user planes.
- One user plane can be part of only one user plane group.
- Multiple user planes can be configured in specific user-plane-groups and default group.
- The user planes associated with SAEGW-C but not defined in any user plane group are added in the default group.
- An operator can associate a User Plane Group to APN and APN Profile.
- If there is no User Plane group associated to an APN for Pure-P and Collapsed calls, SAEGW-C uses the default group to select user plane for that session.
- If there is no user plane group associated to APN Profile or no APN Profile is defined, then SAEGW-C uses the "default" user plane group for Pure-S calls.

- For multi-PDN call with same APN, the same user plane is selected. For multi-PDN call with different APN, a different user plane from a different user plane group is selected.
- User Plane group associated with APN is also used while sending IP Pool chunks to User Plane. IP Pool associated with APN is broken down to chunks and are available for distribution to all UPs from group associated with APN.
- For user-plane-groups that are not associated with any APN, SAEGW-C does not send any IP pool chunks to UPs belonging to these groups. This is also applicable to the default group.
- Sessions with static IP address (IPv4 or IPv6) are supported. The user plane selection of static session is fixed as per chunk allocation to user plane from user plane group associated to an APN.
- If the same static IP address range is used across multiple APNs, it is recommended to use the same user plane group in those APNs.

Architecture

The following figure depicts a high-level architecture of this feature.



Session Recovery and ICSR

Sx-Demux Recovery, ICSR and Sessmgr and VPNmgr recovery is supported

Limitations

In CUPS architecture, this feature has the following known limitations:

- SAEGW-C does not support IPv4v6 PDN type call with static address received from UE, even if one of the IP address (either IPv4 or IPv6, or both) is static address.
- SAEGW-C does not support “allow-static” type pool configuration.
- Multi-PDN call with static IP address allocation is not supported.

Licensing

This feature is license-controlled. Contact your Cisco Account representative for license related details.

Configuring APN-Based UP Grouping

This section provides information about configurations available in support of this feature.

Prerequisites:

- Same IP context should be present at Control-Plane as well as in User-Plane.
- IP context name which is specified in APN configuration should be same at Control-Plane and User-Plane.

Configuring User Plane Group in Control Plane

New user-plane-group is defined at the global configuration mode which lists User Plane endpoints

1. User Plane Group name “default” is created by default. Operator can add and remove peer-node-id in default group. Operator cannot delete user-plane-group “default
2. If Sx Association Setup Request is received for any User plane node-id which is not part of any defined User Plane Group, it will be part of Default User Plane Group.

Configuring User Plane Group

Use the following CLI commands to configure User Plane endpoint group in Control Plane.

```
configure
   [ no ] user-plane-group group_name
   end
```

Notes:

- Removal of user-plane-group will trigger Sx-Association release from Control Plane of individual peer id from that group.

Configuring Peer Node ID and User Plane Node IP Address

Use the following configuration commands to configure time-based PCC rule.

```
configure
   user-plane-group group_name
      [ no ] peer-node-id { ipv4-address | ipv6-address }
      end
```

Notes:

- Removal of peer-node-id will trigger Sx-Association Release from Control Plane for that peer id.

Verifying the User Plane Group

Use the following CLI command for verification.

```
show user-plane-group { all | name group_name }
```

Associating User Plane Group with APN

It is desired that calls to a particular APN be connected to a certain group of user-planes based on some predefined selection criteria. Operator can associate User Plane Group to APN Configuration.

User Plane group configured to APN is also used while sending IP Pool chunks to User Plane. If there is IP Pool associated with APN, only then the chunks from that pool will be sent to all User Planes in this group.

User Plane Group configuration in APN is used to select User Plane for P-GW Pure-P and Collapsed Call.

If there is no specific group is configured in APN then “default” group will be used.

Configuring User Plane Group in APN

Use the following CLI commands to configure User Plane group in APN.

```
configure
  context context_name
    apn apn_name
      [ no ] user-plane-group group_name
      end
```

NOTE: In this EFT release, removal or change of user-plane-group from APN is not supported.

Verifying the User Plane Group in APN

Use the following CLI command for verification.

```
show apn name apn_name }
```

Associating User Plane Group with APN Profile

To select User Plane for S-GW Pure-S calls, SAEGW-C uses user-plane-group associated with APN Profile under Operator Policy. When APN profile do not have any user-plane-group associated or no APN profile was used, then SAEGW-C will select User Plane from default user-plane-group.

Configuring User Plane Group in APN Profile

Use the following CLI commands to configure User Plane group in APN.

```
configure
  apn-profile profile_name
    [ no ] user-plane-group group_name
    end
```

Method of Procedure (MOP) to Remove or Change User Plane Group from APN

When explicit user-plane-group is configured, or implicit default group is used, the SAEGW-C sends IP Pool chunks from the pool that is configured (or global pool when there is no explicit pool configuration in APN) to the user planes in the group.

If you want to change or remove user-plane-group associated to a APN, then it is recommended to follow this MOP because, currently, there is no support of run time config change of user-plane-group in APN after User Plane is associated with SAEGW-C.

Before changing user-plane-group in APN it is recommended to use the following CLI command to first gracefully clear all existing calls belonging to user-plane-group associated with APN.

clear subscribers saegw-only user-plane-group *group_name* **no-select-up**

Executing this CLI command releases all sessions from User Plane belonging to the mentioned user-plane-group gracefully, and marks that User Plane as "Not Available for Session Selection". This User Plane continues to be in Associated state, but it will not be available for Session selection.

Note When the **clear subscribers** command is executed on UP, CP will not be informed and CP will consider the sessions as running.

After clearing the session, execute either of the following CLI command on User Plane to remove its association from Control Plane, and make required changes after UP association is released.

no user-plane-service *service_name*

Or:

no peer-node-id { ipv4-address *ipv4_address* **| ipv6-address** *ipv6_address***}**

Monitoring and Troubleshooting APN-Based UP Grouping

This feature supports the following CLI commands:

- **show sx peers**
  - Group Name Column in the output of this command displays the name of the user-plane-group under which the peer is configured at Control Plane.
  - Peer, which is not part of any group, will be added under "default" user-plane-group
  - For a user-plane-group that is not associated with any "apn", SAEGW-C will not send any IP pools to user planes from this group. Hence, in the output of this command, for the Group Name that is not associated with "apn", the IP Pool status will be "N – Not Applicable". Also, for user planes in this group, when **show sx peers** is executed on UP, it displays Peer ID as "0".
- **show ip user-plane**
- **show ip pool-chunks up-id** *up_id* **user-plane-group name** *up_group_name*

Dynamic User Plane Selection

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

In a Multi-access Edge Computing (MEC) architecture, selecting an edge User Plane (UP) provides low latency and maximum bandwidth efficiency. The location information of the user equipment (UE) is used to select an UP.

For selecting an edge UP, the following levels of granularity are considered:

- E-UTRAN Cell Global Identifier (ECGI) or Cell Global Identification (CGI) offers the lowest level of granularity.
- Tracking Area Identifier (TAI) or Routing Area Identity (RAI) or Service Area Identifier (SAI) offers the next level of granularity.
- TAI-SAI-RAI-ECGI offers fixed priority of TAI, SAI, RAI and ECGI in which the ULI type is matched when more than one ULI type is received.

Architecture

To select a UP based on the location parameter of the upcoming session, a DNS Name Authority Pointer (NAPTR) query including TAI/RAI /SAI or ECGI/CGI is sent to the DNS server. The DNS (NAPTR) response contains a list of UP IPs. To select an UP from this list, a Load Control Information (LCI) and session count is applied to shortlist.

This feature enables virtual APN selection along with dynamic UP selection. As a result, APN is selected based on the specified criteria. The selection criteria for the virtual APN is also based on location, for example, the Radio Admission Control (RAC) range.

Dynamic UP selection is based on the **`configure fqdn postfix`** CLI command and the type of selected APN. If the type is ECGI or CGI, then a DNS Straightforward NAPTR (S-NAPTR) query is sent based on the cell ID. If the type is configured as tracking or routing area, then TAI or RAI or SAI is used for DNS (S-NAPTR) query.

To get the list of associated Sx peers, UP group from the selected APN is used. The UP IPs in DNS (S-NAPTR) response is matched with the list of Sx peers in the group. The peer that is either least loaded or have the least sessions is selected from this list.

If ULI contains unsupported location data, dynamic UP selection is based on the RAI IE that comes outside ULI.

How it Works

This section describes the sequence of operation.

1. For P-GW, GGSN, or SAEGW, Fully Qualified Domain Names (FQDN) in UP, which contains **`fqdn-postfix`** and FQDN type (EGCI/CGI or TAI/RAI/SAI) are configured at APN level.
2. During an S6b interface protocol-based authorization, the **`fqdn-postfix`** value in the authorization response is used (applicable for P-GW, GGSN, or SAEGW service only).
3. The DNS (S-NAPTR) query is sent to the DNS server.

Note DNS (S-NAPTR) is generated based on the type (E-CGI | RAI-TAI-SAI | TAI-SAI-RAI-ECGI) configured in user plane FQDN at APN level for GGSN.

4. The response that is received from the DNS server is matched for service **x-3gpp-upf:x-sxb** for P-GW/GGSN/SAEGW (Collapsed) and **x-3gpp-upf:x-sxa** for S-GW.
5. The matching DNS (S-NAPTR) response is processed recursively for UP IPs.
   - If enabled, the processed IPs are shortlisted for LCI-based UP selection.
   - If not enabled, the processed IPs are shortlisted for session count based UP selection (with or without LCI).
6. If none of the UP IPs present in the response match with the associated Sx peers, then it leads to a session creation failure.
7. For S-GW dynamic UP selection, the DNS client context must be the same as **`sgw-service`** context.
8. If there is a successful DNS response for S-GW dynamic UP selection, UPs are selected from the DNS dynamic list of UP addresses. If there is DNS failure (DNS response is empty without any UP address or DNS time-out), the UP selection falls back to the statically configured APN profile based user-plane-groups functionality.

Note
- Pure S-GW multi-PDNs work with independent DNS-based UP selection.
- S-GW relocation use cases work with independent DNS-based UP selection during a handover. If user-plane-group is configured under APN-profile, dynamic UP selection takes preference.
- After the DNS (NAPTR) query is sent, there is a delat of few seconds (equivalent to tx + rx) to receive the response.
- If the DNS server is not reachable, session establishment might be delayed upto a maximum of 30 seconds before it uses the legacy method to select an UP.

The following sections describe various scenarios that are associated with the Dynamic UP Selection feature.

P-GW Dynamic UP Selection Having Virtual APN with Associated IP Pool

This section describes the sequence of operation for P-GW to dynamically select an UP having a virtual APN with an associated IP pool.

1. As part of create session handling, PGW-C selects a virtual APN based on the TAC range.
2. The DNS (S-NAPTR) query is sent to the DNS server based on the configuration of the selected APN.
3. The response that is received from the DNS server is matched for service. The records with matching service fields are considered for selection.
4. The UP IPs that are part of a configured IP pool and present in the response are matched with the associated Sx peers that are based on the UP group of the selected APN.

5. From the matching list, P-GW selects the UP that is least loaded.

P-GW Dynamic UP Selection Having Virtual APN without Associated IP Pool

This section describes the sequence of operation for P-GW to dynamically select an UP having a virtual APN without an associated IP pool.

1. As part of create session handling, PGW-C selects a virtual APN based on the TAC range.
2. The DNS (S-NAPTR) query is sent to the DNS server based on the configuration of the selected APN.
3. The response that is received from the DNS server is matched for service. The records with matching service fields are considered for selection.
4. The UP IPs that are part of any public IP pool and present in the response are matched with the associated Sx peers that are based on the UP group of the selected APN.
5. From the matching list, P-GW selects the UP that is least loaded.

S-GW Dynamic UP Selection for Successful DNS Response

This section describes the sequence of operation for S-GW to dynamically select an UP after receiving a successful response from the DNS server.

1. After an UE in a tracking area (or Cell ID) sends an attach request to S-GW with Dynamic ECGI, RAI-TAI-SAI | TAI-SAI-RAI-ECGI based UP selection feature enabled and the DNS (S-NAPTR) query is sent to the DNS server.
2. S-GW receives the query response from the DNS server, which contains the list of UP IPs.
3. From the list of UP IPs, S-GW selects the UP that is least loaded.

S-GW Dynamic UP Selection for DNS Response Time-out

This section describe the sequence of operation for S-GW to dynamically select an UP after the DNS server time-out or the server sends a negative response.

1. The S-GW sends the DNS (S-NAPTR) query to the DNS server.
2. If there is a DNS server timeout or the server sends a negative response after the DNS (S-NAPTR) query is sent to the DNS server, then S-GW selects an UP from the APN-profile UP group that are configured with static IPs.
3. From the list of UP IPs, S-GW selects the UP that is least loaded.

Call flows

This section includes the following call flows.

DNS Query Generation and Response Handling Call Flow

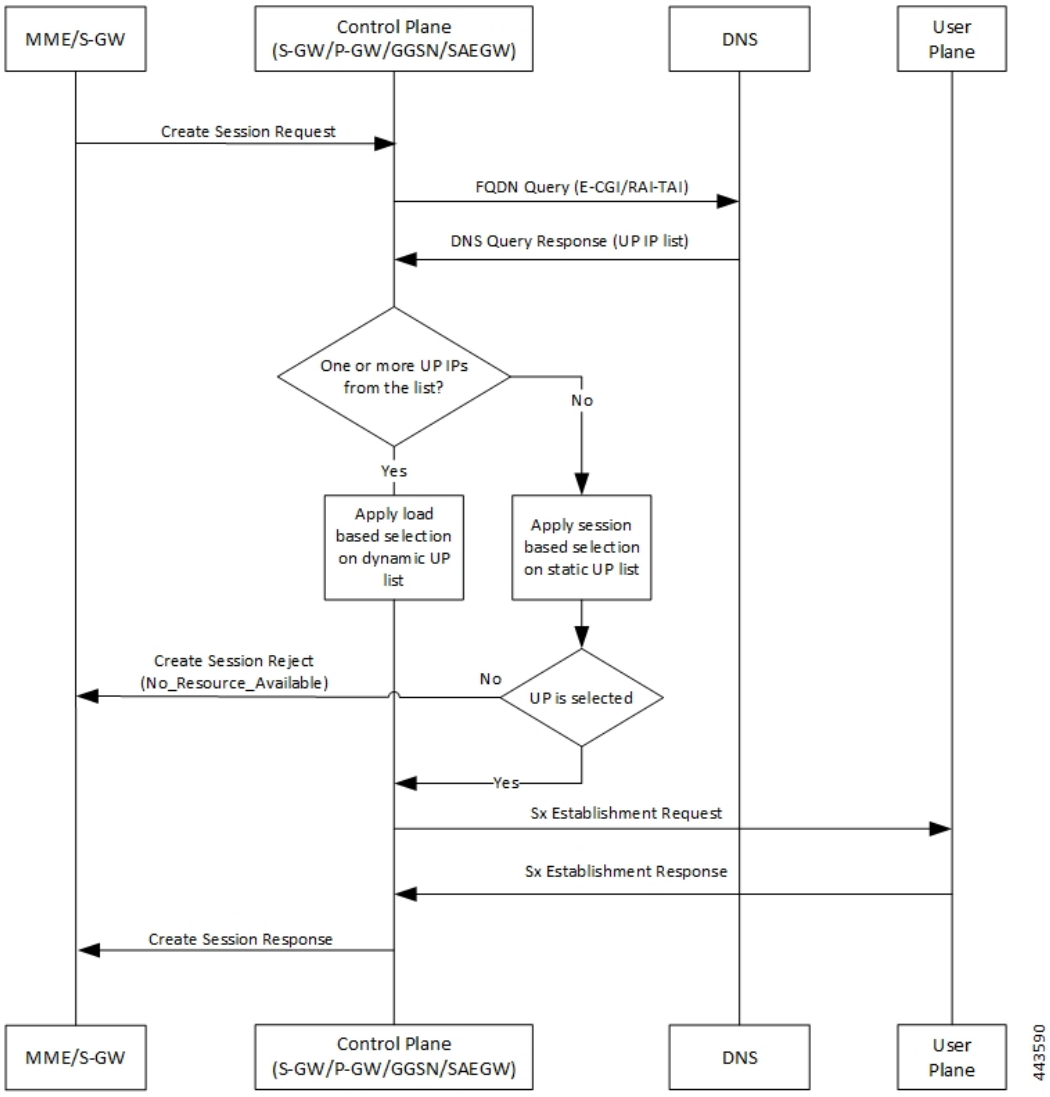


Table 1: DNS Query Generation and Response Handling Call Flow Description

Step	Description
1	MME or S-GW sends a Create Session Request message to the Control Plane (S-GW, P-G GGSN, or SAEGW).
2	Control Plane (CP) sends an FQDN query (E-CGI or TAI-RAI -SAI or TAI-SAI-RAI-EC to the DNS server.
3	CP receives the response to the FQDN query with a list of UP IPs.
4	• If there are one or more UP IPs in the received list, CP applies LCI to the dynamic IP to select an UP IP. • Or else, CP applies session count to the static IP list to select an UP IP.

Step	Description
5	• If an UP is selected, CP sends an Sx Establishment Request message is sent to U to step 6). • Or else, a Create Session Reject message is sent to MME or S-GW.
6	UP responds and sends an Sx Establishment Response message to CP.
7	CP sends a Create Session Response message to MME or S-GW.

DNS Query Timeout for Primary DNS Call Flow

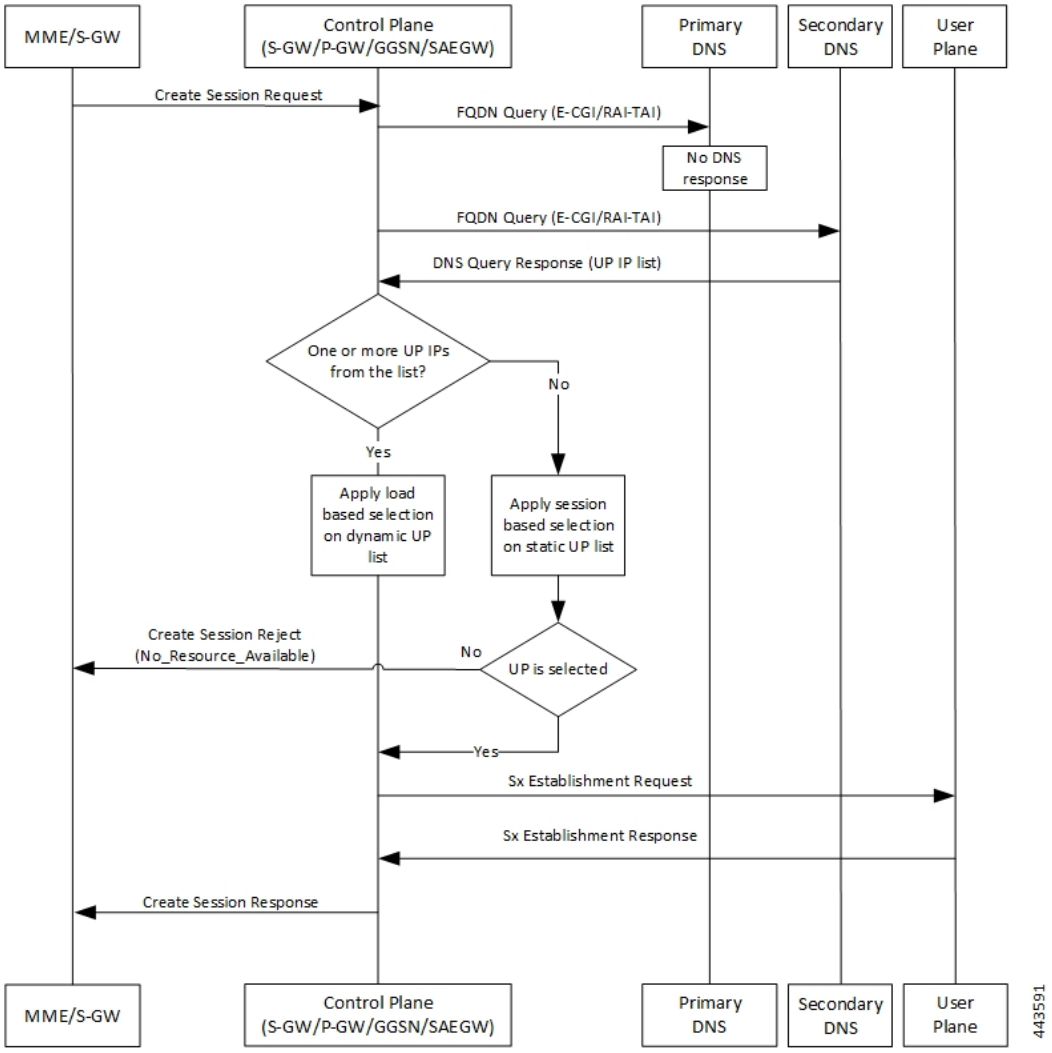


Table 2: DNS Query Timeout for Primary DNS Call Flow Description

Step	Description
1	MME or S-GW sends a Create Session Request message to the Control Plane (S-GW, P-GW, or SAEGW).
2	Control Plane (CP) sends an FQDN query (E-CGI or TAI-RAI-SAI or TAI-SAI-RAI-ECGI) t primary DNS server.
3	When there is no response to the query from the primary DNS server due to a time-out, CP re send the FQDN query to the secondary DNS server.
4	CP receives the response to the FQDN query from the secondary DNS server with a list of UP
5	• If there are one or more UP IPs in the received list, CP applies LCI to the dynamic IP list an UP IP. • Or else, CP applies session count to the static IP list to select an UP IP.
6	• If an UP is selected, CP sends an Sx Establishment Request message is sent to UP (skip t 7). • Or else, a Create Session Reject message is sent to MME or S-GW.
7	UP responds and sends an Sx Establishment Response message to CP.
8	CP sends a Create Session Response message to MME or S-GW.

DNS Query Timeout for Primary and Secondary DNS Call Flow

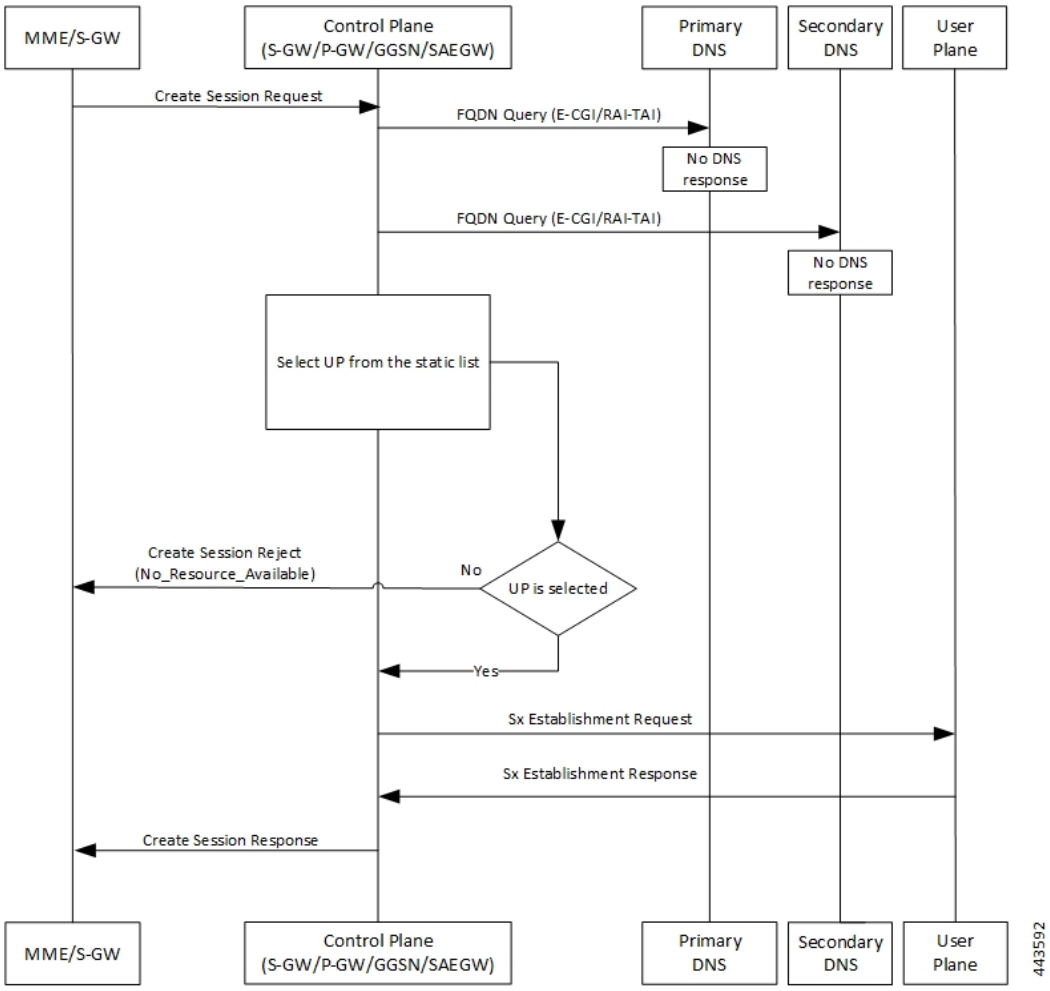


Table 3: DNS Query Timeout for Primary and Secondary DNS Call Flow Description

Step	Description
1	MME or S-GW sends a Create Session Request message to the Control Plane (S-GW GGSN, or SAEGW).
2	Control Plane (CP) sends an FQDN query (E-CGI or TAI-RAI-SAI or TAI-SAI-RAI- the primary DNS server.
3	When there is no response to the query from the primary DNS server due to a time-out, to send the FQDN query to the secondary DNS server.
4	When there is no response to the query from the secondary DNS server also, CP selec IP from the list of static IPs.
5	• If an UP is selected, CP sends an Sx Establishment Request message is sent to U step 6). • Or else, a Create Session Reject message is sent to MME or S-GW.

Step	Description
6	UP responds and sends an Sx Establishment Response message to CP.
7	CP sends a Create Session Response message to MME or S-GW.

Limitations

The Dynamic UP Selection feature has the following limitations:

- It is applicable to P-GW, S-GW, and SAEGW only.
- For SR and ICSR, no specific parameters are stored. If **smgr** is reset, the configured values are pushed again from **sessctrl**.
- Any changes to the DNS Server is not considered.
- The number of IPs handled for UP are limited to six. These IPs are a combination of IPv4 and IPv6 addresses.

Configuring the Dynamic User Plane Selection Feature

This section describes how to configure the Dynamic User Plane Selection feature.

Configuring FQDN for P-GW or GGSN

To configure FQDN for P-GW or GGSN (Pure-P and Collapsed calls), use the following configuration:

```
configure
   context context_name
      apn apn_name
         user-plane-fqdn
         user-plane-fqdn fqdn_postfix_string type [ E-CGI | RAI-TAI -SAI |
TAI-SAI-RAI-ECGI ]
         end
```

NOTES:

- **user-plane-fqdn**—Enable locally configured FQDN-postfix for dynamic UP selection (DNS-based).
- **E-CGI**—Configure FQDN query type as E-CGI for UP selection.
- **RAI-TAI-SAI**—Configure FQDN query type as RAI-TAI-SAI for UP selection.
- **TAI-SAI-RAI-ECGI**—Configure FQDN query type as TAI-SAI-RAI-ECGI for UP selection.

Configuring FQDN for S-GW

To configure FQDN for S-GW (Pure-S calls), use the following configuration:

```
configure
   context context_name
      sgw-service sgw-service_name
         user-plane-fqdn
         user-plane-fqdn fqdn_postfix_string type [ E-CGI | RAI-TAI -SAI |
```

```
TAI-SAI-RAI-ECGI ]
       end
```

NOTES:

- **user-plane-fqdn**—Enable locally configured FQDN-postfix for dynamic UP selection (DNS based).
- **E-CGI**—Configure FQDN query type as E-CGI for UP selection.
- **RAI-TAI-SAI**—Configure FQDN query type as RAI-TAI-SAI for UP selection.
- **TAI-SAI-RAI-ECGI**—Configure FQDN query type as TAI-SAI-RAI-ECGI for UP selection.

Boxer Configurations

This section describes the following boxer configurations and restrictions:

1. DNS client must be configured and associated with P-GW and GGSN service.
2. UP FQDN must be configured in APN.
3. IP addresses of the primary and secondary DNS servers must be configured in the ISP context.
4. UP FQDN must be configured in S-GW service for S-GW dynamic UP selection.

DNS Server Configurations

This section describes the following guidelines and restrictions to configure an external DNS server:

1. DNS must be configured for NAPTR to record for ECFI/CGI/TAI/RAI/SAI, as applicable.
2. NAPTR record must have service field as **"x-3gpp-upf:x-sxb"** for P-GW/SAEGW (Collapsed) and GGSN service, and **"x-3gpp-upf:x-sxa"** for S-GW.
3. NAPTR record must have flags as **a** to indicate that the replacement string is FQDN for A or AAAA records.

The following CLI commands represent a sample DNS server configuration:

```
$ORIGIN 3gppnetwork.org.

$TTL 60              ; Put the Default
        TTL in seconds here (Its 1 day currently)

3gppnetwork.org.     IN SOA  nsbng.3gppnetwork.org. root.3gppnetwork.org.

273 ; serial

7200 ; refresh (2 hours)

3600 ; retry (1 hour)

86400 ; expire (1 day)

43200 ; minimum (12 hours)

)

 NS    nsbng.3gppnetwork.org.

ns AAAA 3001::41
```

```
;CUPS NAPTR Records Start From Here

;TAI NAPTR Records

tac-lb89.tac-hb67.tac.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxb" ""
        uplane-address1-v4.3gppnetwork.org.

tac-lb89.tac-hb67.tac.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxb" ""
        uplane-address1-v6.3gppnetwork.org.

tac-lb89.tac-hb67.tac.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxa" ""
        uplane-address1-v4.3gppnetwork.org.

tac-lb89.tac-hb67.tac.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxa" ""
        uplane-address1-v6.3gppnetwork.org.

;RAI NAPTR Records

rac34.lac-lb34.lac-hb12.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"   "x-3gpp-upf:x-sxb"
 ""
          uplane-address1-v4.3gppnetwork.org

.

rac34.lac-lb34.lac-hb12.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  2  "a"   "x-3gpp-upf:x-sxb"
 ""
        uplane-address1-v6.3gppnetwork.org.

;SAI NAPTR Records

sac1234.lac-lb34.lac-hb12.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  'a'
'x-3gpp-upf:x-sxb' ''
           uplane-address1-v4.3gppnetwork.org.

sac1234.lac-lb34.lac-hb12.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  2  'a'
'x-3gpp-upf:x-sxb' ''
         uplane-address1-v6.3gppnetwork.org.

;ECGI NAPTR Records

eci-b167.eci-b245.eci-b323.eci-b401.eci.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1
"a"   "x-3gpp-upf:x-sxb" ""
        uplane-address1-v4.3gppnetwork.org.

eci-b167.eci-b245.eci-b323.eci-b401.eci.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1
"a"   "x-3gpp-upf:x-sxb" ""
        uplane-address1-v6.3gppnetwork.org.

;CGI NAPTR Records

ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org. IN NAPTR
          1  1
          "a"   "x-3gpp-upf:x-sxb" ""
        uplane-address1-v4.3gppnetwork.org.

ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org. IN NAPTR
          1  1
          "a"   "x-3gpp-upf:x-sxb" ""s
        uplane-address1-v6.3gppnetwork.org.

;A Records

uplane-address1-v4   100     IN
          A    209.165.200.225
```

```
;uplane-address1-v4   100     IN      A
      209.165.200.225

uplane-address1-v4   100     IN
          A    209.165.200.225

;uplane-address2-v4   100     IN
          A    209.165.200.225

;AAAA Records

uplane-address1-v6   100     IN
          AAAA    1::1:111

uplane-address1-v6   100     IN
          AAAA    1111::1:111

;uplane-address2-v6   100     IN
          AAAA    1111::1:111
```

S6b Configuration (Optional)

This section describes guidelines to configure an external S6b to support custom attribute **aaa-uplane-fqdn** and **fqdn_post_fix_string**.

```
AA-Answer
   apn-config
     uplane-fqdn
```

Interface

The following sections describe the format of the DNS query and response.

DNS (S-NAPTR) Query Format

This section describes the format of the DNS (S-NAPTR) query message.

Important SAI-based FQDN is proprietary formatted and not as specified in 3GPP TS 23.003 19.4.2 Fully Qualified Domain Names.

Network Node	Query format
SGW-C	**ECGI-based** eci b1<ECI byte-1>.eci b2<ECI-byte-2>. Eci b3<ECI byte-3> .eci b4<ECI-byte-4>.eci.epc.mnc <MNC.mcc<MCC>.3gppnetwork.org **TAI-based** tac lb<TAC low byte>.tac hb<TAC-high-byte> .tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Network Node	Query format
PGW-C	**ECGI-based** eci-b1<TAC-byte-1>.eci-b2 <ECI-byte-2.Eci-b3<TAC-byte-3> .eci-b4<ECI-byte-4>.eci.epc.mnc<MNC> .mcc<MCC>.3gppnetwork.org **TAI-based** tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte> .tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
GGSN-C	**CGI-based** ci-lb<CI-low-byte>.ci-hb<CI-high-byte> .eci.lac-lb<LAC-low-byte>.lac-hb<LAC-high-byte> .lac.ggsn.mnc<MNC>.mcc<MCC>. 3gppnetwork.org **RAI-based** rac<RAC>.lac-lb<LAC-low-byte> .lac-hb<LAC-high-byte>.lac.ggsn.mnc<MNC> .mcc<MCC>.3gppnetwork.org **SAI-based** sac<SAC>.lac-lb<LAC-low-byte>. lac-hb<LAC-high-byte>.lac.ggsn mnc<MNC>.mcc<MCC>.3gppnetwork.org
SAEGW-C (Collapsed)	**ECGI-based** eci-b1<TAC-byte-1>.eci-b2<ECI-byte-2> . Eci-b3<TAC-byte-3>.eci-b4<ECI-byte-4> .eci.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org **TAI-based** tac-lb<TAC-low-byte> .tac-hb<TAC-high-byte>.tac.epc.mnc <MNC>.mcc<MCC>.3gppnetwork.org **SAI-based** sac<SAC>.lac lb<LAC low byte> .lac hb<LAC-high-byte>.lac.epc. mnc<MNC>.mcc<MCC>.3gppnetwork.org

DNS (S-NAPTR) Response Format

This section describes a sample format of the DNS (S-NAPTR) response message.

```
Query ID              : 22290

Type                  : Response

Question              : NAPTR ?
          ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org.

Answer                :

  Name                :
          ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org.

  TTL                 : 60

  Type                : NAPTR

  Order               : 1

Preference : 1

  Flags               : a

  Service             : x-3gpp-upf:x-sxb

  Regexp              :

Replacement : uplane-address2.3gppnetwork.org.

  Name                :
        ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org.

  TTL                 : 60

  Type                : NAPTR

  Order               : 1

  Preference          : 1

  Flags               : a

  Service             : x-3gpp-upf:x-sxb

  Regexp              :

Replacement : uplane-address1.3gppnetwork.org.

Query ID              : 44640

Type : Query

Question              : A?
         uplane-address2.3gppnetwork.org.

Query ID : 55480

Type                  : Query

Question              : A?
         uplane-address1.3gppnetwork.org.

Query ID : 55480

Type                  : Response

Question              : A?
          uplane-address1.3gppnetwork.org.

Answer                :

Name : uplane-address1.3gppnetwork.org.

  TTL                 : 100
```

```
  Type                : A
Address : 20.20.20.108
Query ID              : 44640
Type                  : Response
Question              : A?
          uplane-address2.3gppnetwork.org.
Answer                :
  Name                : uplane-address2.3gppnetwork.org.
  TTL                 : 100
  Type                : A
Address : 209.165.200.225
```

Show Commands

This section describes the supported commands for the Dynamic UP Selection feature.

show apn name *apn_name*

This command displays DNS related information for Pure-P and collapsed calls.

The output of this command can be used to check the following values:

- FQDN of APN
- Type of FQDN

show sgw-service name *sgw_service_name*

This command displays DNS related information for Pure-S calls.

The output of this command can be used to check the following values:

- FQDN of APN
- Type of FQDN

show saegw-service statistics

Use the **show saegw-service statistics** CLI command to collect the statistics information.

The following is a sample partial output of the **show saegw-service statistics all** and **show saegw-service statistics name** *SAEGW21* CLI commands:

```
Dynamic Uplane Selection Statistics:
   Attempted              :             x
   Successful             :             x
   Failure                :             x
   Peer not Found         :             x
   Negative DNS response  :             x
   DNS timed out          :             x
   Unsolicited UP Selection Response:   x
   DNS Query Response post DNS timeout: x
```

The following is a sample partial output of the **show saegw-service statistics all function sgw** CLI command:

```
Dynamic Uplane Selection Statistics:
  Attempted:                            7
  Successful                            4
  Failure:                              3
    Mismatch DNS response:              1
    Negative DNS response:              1
    DNS timed out:                      1
    Unsolicited UP Selection Response:  1
    DNS Query Response post DNS timeout: 1
```

Bulk Statistics

SAEGW Schema

Use this schema to collect the following bulk statistics pertaining to the Dynamic User Plane Selection feature:

- saegw-dyn-up-attempt
- saegw-dyn-up-attempt
- saegw-dyn-up-success
- saegw-dyn-up-success
- saegw-dyn-up-failure
- saegw-dyn-up-failure
- saegw-dyn-up-peer-not-found
- saegw-dyn-up-peer-not-found
- saegw-dyn-up-dns-timeout
- saegw-dyn-up-dns-timeout
- saegw-dyn-up-neg-resp
- saegw-dyn-up-neg-resp

Multiple UP Group Support

Revision History

Table 4: Revision History

Revision Details	Release
First introduced.	21.25

Feature Description

Remote CUPS allows a progressive configuration rollout on an operator network. You can deploy and activate a pilot or canary version N+1 on a given CP or UPs pool, while the version N configuration is still active on the other CP or UP pool until the operator decides to roll out this N+1 configuration to all the CP or UP pools after the monitoring period.

Use cases for this feature are as follows:

- ECS or ADC configuration update rollout: The ability to test the configuration using one CP or UP pilot, while the other CP or UP uses the old configuration.
- New APN configuration update: Ability to test new APN configuration using a set of CP or UP pilot, while another component uses the old configuration.
- Add or remove the IP pool configuration update.

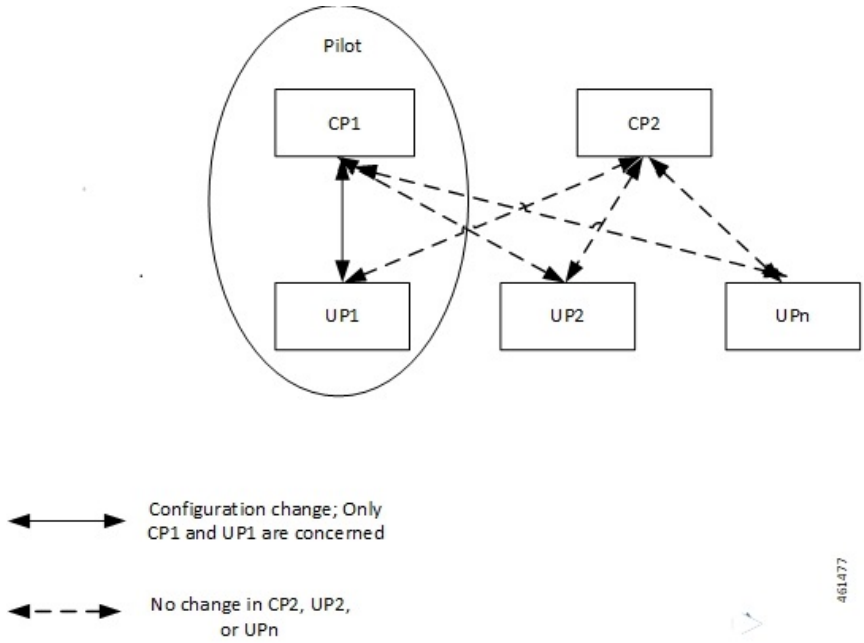
Relationships

TAC RAC profile support feature is related to the Multiple UP Group Support feature, which is used to select a test virtual APN.

Architecture

The following diagram depicts the progressive configuration rollout architecture.

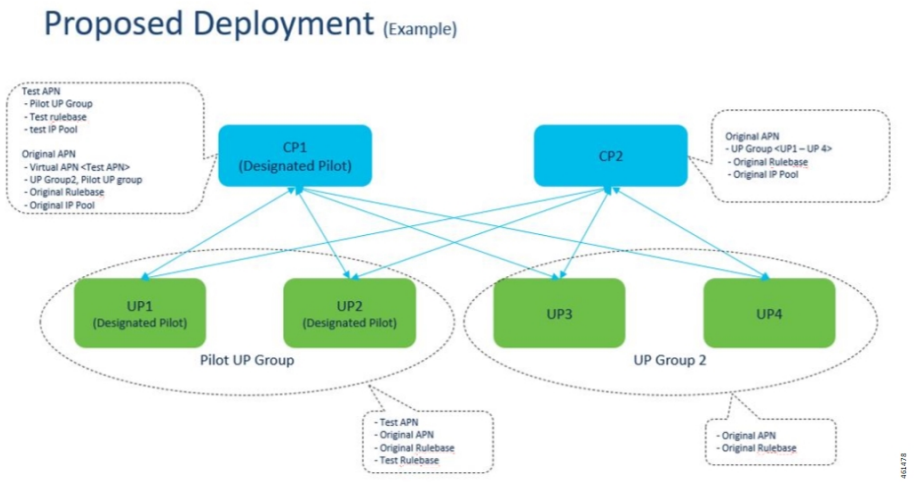
Figure 1: Progressive Configuration Rollout



Components

The following diagram depicts the proposed deployment components.

Figure 2: Proposed Deployment



How It Works

Pilot CP routes the incoming test pilot calls to the pilot UP group.

Pilot CP also routes usual business calls to any UP as per its original deployment. Therefore, this feature supports multiple UP groups under an APN. The first UP group includes the pilot UPs, and the second UP group includes all the other nonpilot UPs. A single UP cannot exist in two UP groups simultaneously. There is a strict 1:1 mapping between UP and the UP group.

Limitations and Restrictions

The Multiple UP Group Support feature has the following limitations and restrictions:

- You can apply the pilot configuration only at the UP-group level.
- Configure CP and UP independently.
- ECS configuration changes that occur at lower levels like ruledef, Charging Action, and so on, cannot be isolated from the pilot UP. Rule base level differentiation is required.
- Pilot CP and UPs must be designated at deployment. Post deployment designation requires the existing sessions to be cleared.
- If any user group is not attached to any of the APNs, then the corresponding UP nodes must be de-registered and removed from the CP configuration.
- Static-IP-Pools are not supported.
- **Deployment Restriction**: When deploying multiple User Plane (UP) groups on a single Control Plane (CP), the PFD push configuration must be applied consistently across all groups. You must either enable or disable PFD push for all UP groups; mixed configurations are not supported, have not been validated in Cisco Labs, and are not recommended.

Configure the Multiple UP Group Support Feature

This section describes how to configure the Multiple User Plane (UP) Group support feature.

Configuring the Multiple UP Group support feature involves the following steps:

Serial Number	Configuration	For Pilot Configuration
1	ECS or ADC configuration (For example, ruledef, rulebase, charging action)	On Pilot CP: Configuration differentiation must be performed at the rulebase level. Changes in configuration entities like ruledef, charging action, and so on, needs duplication. On Pilot UP: Corresponding configuration changes must be performed on one or more pilot UPs directly.
2	APN configuration	• Create a new APN with desired configuration changes. • Configure the test APN as a virtual APN in the existing APN with required redirecting rules. Alternatively, use MME to redirect calls to the test APN.
3	UP group configuration	• Select pilot CP and UPs at the time of deployment. • Enable multiple UP-groups that must be configured for an APN.
4	IP pool configuration	New IP pool: • Create a new IP Pool and associate it with the test APN. Update existing IP pool: • Perform the configuration changes to the IP pool directly. **Note:** Change cannot be localized to one or more pilot UPs only.

Configuring UP Management Policy

To configure the UP management policy, use the following configuration:

```
configure
  up-mgmt-policy policy_name
    user-plane-group group_name
    end
```

NOTES:

- **up-mgmt-policy** *policy_name*—Specify the UP management policy as a string of size 1 to 31 characters.
- **user-plane-group** *group_name*—Specify the name of the user plane group.
- **secondary**— UP groups configured as secondary act as backup for UP selection.

  By default, UP groups defined in UP management policy are primary groups. If no UPs are available in the primary UP group(s), the UP selection is done from the secondary UP group(s).

  To support site backup, the secondary user groups must have sufficient IPs to serve subscribers redirecting if the primary user-groups are down.

  The maximum number of UP groups per UP management policy will be a combination of primary and secondary groups.

Selecting UP for Pure-S Calls

To configure UP selection on a Pure-S call type, use the following configuration:

```
configure
   context context_name
      apn-profile profile_name
         up-mgmt-policy policy_name
         end
```

NOTES:

- **up-mgmt-policy** *policy_name* must be a string of size 1 to 31 characters.
- You can configure either the APN profile level UP-group or UP management policy.
- For an APN profile, you can configure only a single UP management policy.
- Assign a pool name for the IP address allocation.

Priority between UP Groups

Revision History

Revision Details	Release
Enhanced the number of UP groups allowed in the IP pool management policy. For more information, refer to the *Limitations* section.	2025.01.0
First introduced.	21.27.2

Feature Description

In CUPS, support is enabled for overlapping IP pools between different UPs which are associated with the same CP. All UP groups that are associated with the same CP get the same IP Pool range. Disjointed IP pools are configured on different CPs that enables assignment of the same IP to UEs at different location. The Virtual Routing and Forwarding (VRF) used on the pools is used to differentiate the traffic for the two UEs.

How It Works

User Planes are clustered in a UP group based on common characteristics, that is, geographical location. The CP associates these UP groups with specific IP pool such that UPs from same geographical location can never have the same IP Pool range, and UPs from different geographical location can get the same IP Pool range. This behavior is achieved by introducing a new policy that is called as IP Pool Management Policy. IP Pool Management Policy is applied on APN.

For UP selection, the DNS-based UP selection algorithm is used on UP groups of IP Pool Management Policy. DNS query response list out the eligible UP IP addresses based on TAC/RAC value that is sent in DNS query request. Least load algorithm is then used on eligible UP IP addresses to finally select the UP.

For supporting the overlapping of mobile IP pools, the following requirements are met:

- Support of UP group-specific IP pool
- IP pool chunk allocation to UP if pools are configured specific to any UP group
- DNS-based UP selection algorithm on multiple UP groups

The following is a list of considerations for DNS-based UP selection feature:

- If the UP groups are not configured with specific IP pool/group name, it takes chunks from the public pools when APN is configured with IP Pool Management Policy.
- UP selection occurs among those returned UP IP addresses based on the Least Session UP selection algorithm and UP availability status, even if other UPs in that group are less loaded.
- In DNS query response, the list of UPs received for up to a maximum number of six UP IP addresses can belong to different UP groups when configured in the IP pool management policy and among these, the UP with the least session is selected.
- After the UP selection is complete, if the Sx Establishment is rejected from UP, there are no more reattempts for the same.
- If the IP pool or group name is shared among multiple UP groups, then the IP chunk allocation occurs on a first come first serve basis during UP registration. There is a possibility of unequal distribution of IP pool chunks.
- Configuration of UP Group and IP Pool Management Policy at the same time in APN is not allowed.
- After the UP is selected and if that UP does not have sufficient IP addresses, the call gets rejected as not enough resources being available.
- There is no change that is required at RCM during configuration.
- Configuring disjoint IP Pools across CP instances is required.

Dynamic APN IP Pool Update

Dynamic APN IP Pool Update takes place when you need to assign or release IP Pool chunks on the UP without breaking the UP association. You should run the below CLI command after any IP Pool related configuration change. This CLI was earlier supported for UP group and IP Pools on APN level. This is now extended for UP group and IP Pools on IP Pool Management Policy level.

```
update ip-pool apn all
```

For more details, see the *Dynamic APN and IP Pool Support* chapter.

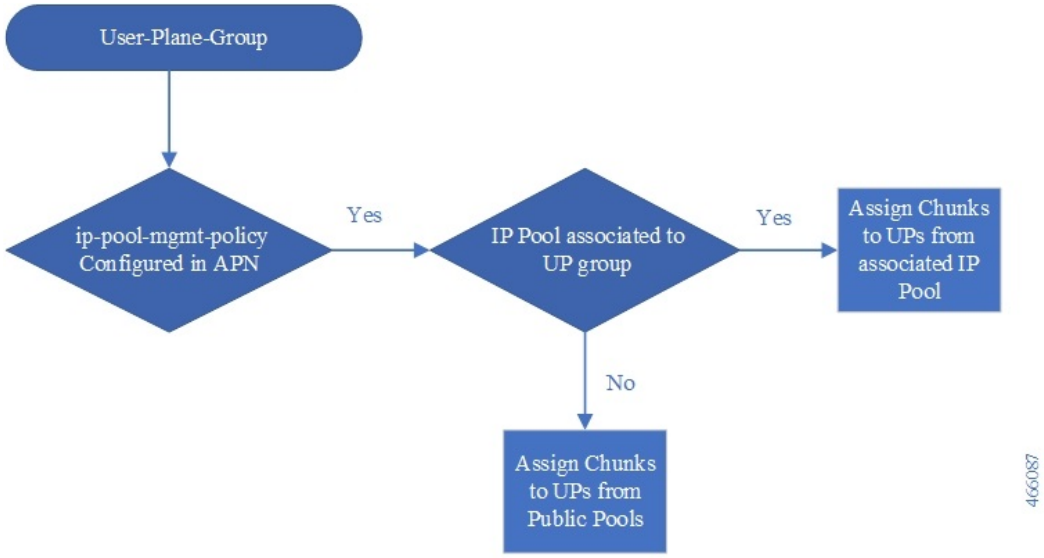
Support of UP Group Specific IP Pool

Configuration of multiple UP groups and UP group-specific IP pools for an APN is possible through IP Pool Management Policy. For any modification on APN with respect to IP Pool, given that UP is already associated, you must run the Dynamic IP Pool procedure that is explained in the *Dynamic APN and IP Pool Support* chapter of this guide. It will reassign the IP Pool chunks to UP groups.

IP Pool Chunk Allocation to UP

When the UP associates, UP registration request is sent toward the VPN and the request message has the list of IP pools from which chunk is allocated to UP. That list of IP Pool is constructed now as per the behavior that is depicted in the following diagram.

Figure 3: Chunk Allocation for UP Groups Associated in APN Through IP Pool Management Policy

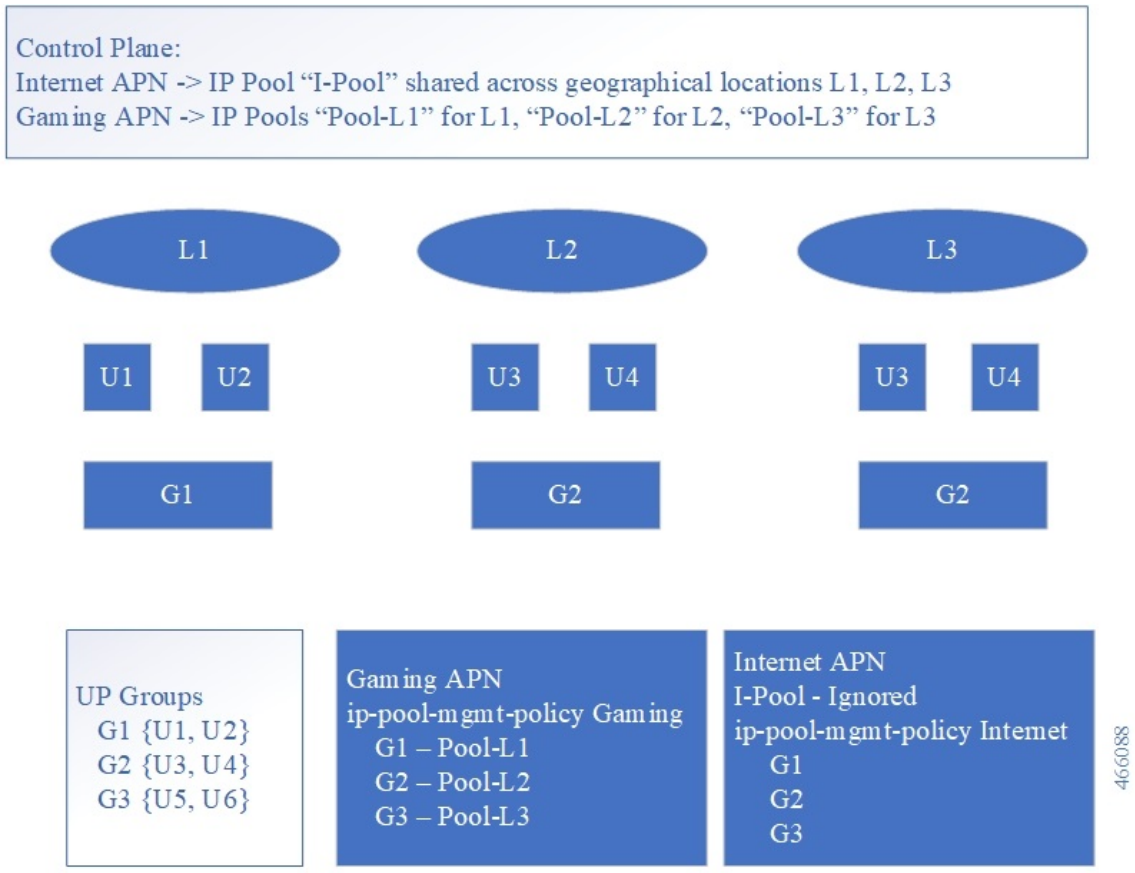


The following table is an example of expected behavior considering G4/G6 as Global/Public IPv4/IPv6 pools, and U4/U6 is the UP group-level IPv4/IPv6 pools.

UP Group level IPv4 Pools (U-4)	UP Group level IPv6 Pools (U-6)	Expected Behavior
F	F	G4+G6
F	T	U6+G4
T	F	U4+G6
T	T	U4+U6

The following diagram indicates APN-level IP pool configuration with UP Group-level IP pool.

Figure 4: APN-Level IP Pool Configuration with UP Group-Level IP Pool



The associated IP pools are updated in the **user-plane-group** configured in **ip-pool-mgmt-policy** without reassociating the UPs. This is possible due to enabling the support of dynamic IP pool update feature for IP pool management policy. UP gets the IP pool chunks based on status of the APN configuration.

Also, during the call establishment, the current ip-pool name that is configured in APN is used with the corresponding ip-pool name for the selected UP group name.

You can update the associated IP pools on "user-plane-group" configured in the "ip-pool-mgmt-policy" without reassociating the UPs. This is possible by extending the support of Dynamic IP Pool Update feature (see *Dynamic APN and IP Pool Support* chapter) for IP Pool Management Policy. UP gets the IP pool chunks based on current snapshot of the APN configuration.

Also, during the call establishment, the ip-pool name that is configured in APN is used with corresponding ip-pool name for the selected UP-group-name.

DNS-Based UP Selection Algorithm on Multiple UP Groups

DNS is queried with location (TAC/RAC) information. Based on the list of UPs (UP IP addresses) received from DNS, UP selection algorithm filters the UPs from the configured UP group, and then runs the UP-selection algorithm (LCI/OCI or session count) on the resulting set of UPs. This functionality is extended for "ip-pool-mgmt-policy". Filtering is now applied to all UP groups that are part of "ip-pool-mgmt-policy".

The following diagram provides the general flow of events and data for DNS-based UP selection.

Figure 5: Flow of Events and Data for DNS-Based UP Selection

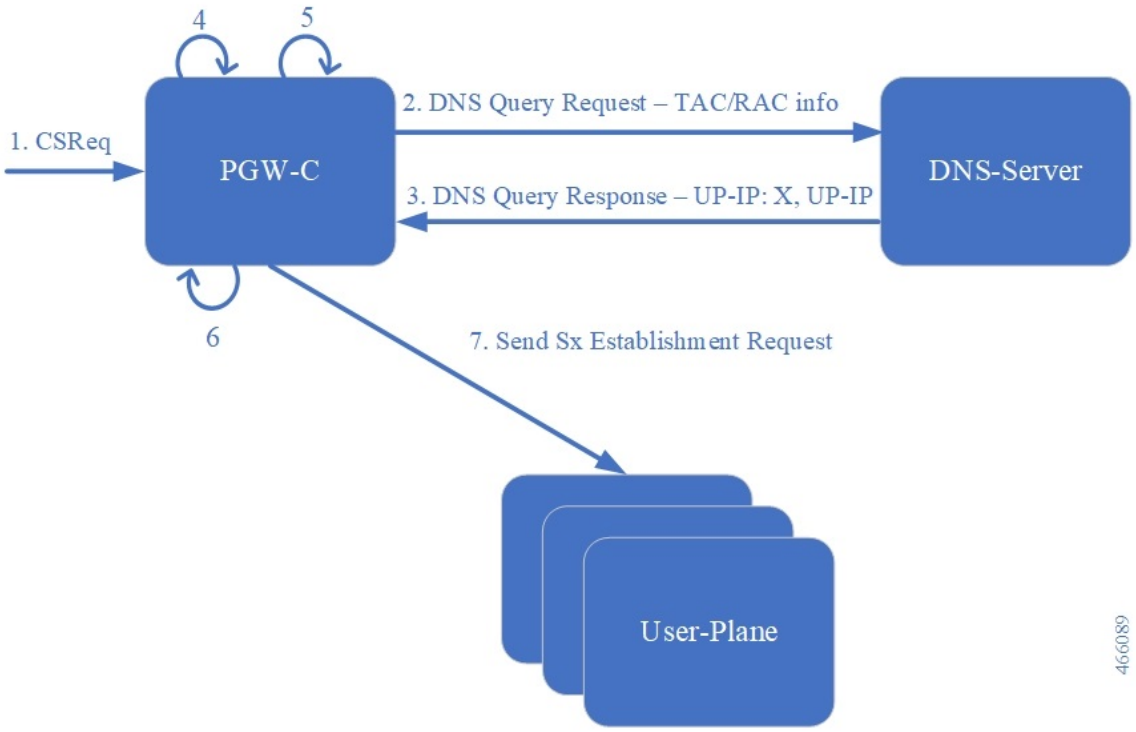


Table 5: General Flow of Events and Data for DNS-Based UP Selection

Steps	Description
1.	CS Request message is sent to PGW-C.
2.	DNS Query Request with TAC/RAC information is sent by PGW-C to DNS server.
3.	DNS Query Response is sent by the DNS server back to the PGW-C.
4.	The PGW-C finds intersection set of UPs from DNS response and UP group or "ip-pool-mgmt-policy".
5.	The PGW-C selects UP and UP group from the resulting set.
6.	The PGW-C selects IP address based on UP group and pool name.
7.	The PGW-C sends Sx Establishment Request to the User Plane.

Limitations

The following are the known limitations of this feature:

- The UP override feature is not supported in the IP Pool Management Policy.

- The maximum number of UPs allowed per TAC/RAC location that is processed by the DNS-based UP selection process is six.
- DNS-based UP selection can lead to non-uniform distribution of calls among UP and IP pool exhaustion. This occurs due to TTL as the DNS server is unaware of any session counts in the UP.
- There is no default IP pool management policy like the default UP group.
- Static calls are not supported with the IP pool management policy.
- An IP pool management policy can either have disjoint UP groups or if two IP pool management policies share a common UP group, then the other UP Groups of the two policies must be the same. Otherwise, it can lead to uneven load balancing and IP pool exhaustion.
- A maximum number of 100 UP groups are allowed inside each IP pool management policy.

  Earlier, 20 UP groups were allowed inside each IP pool management policy. When a downgrade is performed from a release supporting 100 UP groups to a release that supports only 20 UP groups, existing calls continue to work. For new calls, the remaining UP groups specified in the IP pool management policy are used.

  For a stable system, it is recommended to keep the UP groups under 20 when downgrading to an older release that supports only 20 UP groups under the IP pool management policy.
- The maximum number of UP groups that are allowed in the CP system wide is 100.
- The maximum number of UPs allowed in a UP group is 100.
- The maximum number of UPs allowed in a CP is 100.

Configuring IP Pool Management Policy and UP Group with Specific IP Pool

To configure the IP Pool Management Policy, use the following configuration:

```
configure
  context context_name
    apn apn_name
      ip-pool-mgmt-policy policy_name
      end
```

NOTE:

- **ip-pool-mgmt-policy** *policy_name*: Specify the IP Pool Management Policy name and must be a string of size 1 to 32 characters.

To configure the UP group with specific IP pool, use the following configuration:

```
configure
  ip-pool-mgmt-policy policy_name
    user-plane-group group_name { ip-address-pool-name ipv4_pool_name |
ipv6-address-pool-name ipv6_pool_name } [ secondary ]
    end
```

NOTES:

- **ip-pool-mgmt-policy** *policy_name*—Specify the IP Pool Management Policy name as a string of size 1 to 31 characters.

- **user-plane-group** *group_name*—Specify the UP Group name as a string of size 1 to 31 characters.
- **ip-address-pool-name** *ipv4_pool_name*—Specify the IPv4 address pool name as a string of size 1 to 31 characters.
- **ipv6-address-pool-name** *ipv6_pool_name*—Specify the IPv6 address pool name as a string of size 1 to 31 characters.
- **secondary**— UP groups configured as secondary act as backup for UP selection.

  By default, UP groups defined in IP Pool Management Policy are primary groups. If no UPs are available in the primary UP group(s), the UP selection is done from the secondary UP group(s).

  To support site backup, the secondary user groups must have sufficient IPs to serve subscribers redirecting if the primary user-groups are down.

  The maximum number of UP groups per IP Pool Management Policy will be a combination of primary and secondary groups.

MOP for Adding and Deleting UP and UP Group

MOP for Removing UP

1. On the CP, execute the command to block new sessions being placed on that UP and, optionally, clear subscribers with up-ip-address. For details, see the *User Plane Node Bring Down Procedure* chapter.



Note When the **clear subscribers** command is executed on UP, CP will not be informed and will consider the sessions as running.

2. Verify that all subscribers are gracefully released or are forced torn down on UP. Also verify that all the sessions have been torn down.
3. On the UP, execute the command to disassociate from CP. It will disassociate the UP from CP and CP will not choose this UP for further sessions.
4. On the CP, execute the command to remove the UP from the UP Group (this will also deregister the BFD monitoring of the UP).
5. Disable the BFD configurations for monitoring at UP and at CP using **no monitor-group** commands.

MOP for Removing UP Group

1. Use the "MOP for Removing UP" to remove UP from UP group.
2. Delete UP Group from the configurations. Check if UP Group is associated on APN scope or IP Pool Management Policy.
   - APN level
     - Disassociate the UP Group from APN
   - IP Pool Management Policy
     - Disassociate the UP Group from IP Pool Management Policies

MOP for Adding UP Group

1. Add UP IP address and new UP Group to the configuration.
2. UP Group can either be added on APN scope or the IP Pool Management Policy.
   - APN level
     - Associate UP Group and IP pools on APN
   - IP Pool Management Policy
     - Associate UP Group and IP pools in IP Pool Management Policy

MOP for Removal and Modification of IP Pool Management Policy on APN

Modification is done by performing Delete followed by Add.

1. Use the "MOP for Removing UP" to remove UP from UP group
2. Delete the UP Group from the configurations.
   - Disassociate the UP Group from IP Pool Management Policies
3. Can change or remove the IP Pool Management Policy on APN

Add Operations on UP Group

Following are the ways of associating IP Pools to a UP Group.

Adding Both IPv4 and IPv6 Pools to a UP Group

Use the following configuration to add both the IPv4 and IPv6 pool to a UP Group.

```
configure
  ip-pool-mgmt-policy policy_name
    user-plane-group group_name ip-address-pool-name ipv4_pool_name
ipv6-address-pool-name ipv6_pool_name
    end
```

Adding Only IPv4 Pool to a UP Group

Use the following configuration to add only the IPv4 pool to a UP Group.

```
configure
  ip-pool-mgmt-policy policy_name
    user-plane-group group_name ip-address-pool-name ipv4_pool_name
    end
```

Note If APN is IPv4v6 type, then it implies IPv6 prefix and the public pool is used in this situation.

Adding Only IPv6 Pool to a UP Group

Use the following configuration to add only the IPv6 pool to a UP Group.

```
configure
  ip-pool-mgmt-policy policy_name
    user-plane-group group_name  ipv6-address-pool-name ipv6_pool_name
    end
```

Note If APN is IPv4v6 type, then it implies IPv4 address and the public pool is used in this situation.

Delete Operations on a UP Group

Following are the ways of disassociating IP Pools from a UP Group.

Removing UP Group

Use the following configuration to remove the UP Group itself.

```
configure
  ip-pool-mgmt-policy policy_name
    no user-plane-group group_name
    end
```

Removing Both IPv4 and IPv6 Pools from UP Group

For deleting both IPv4 and IPv6 pools from the UP Group, reconfigure UP group without any IP Pool.

Example Configuration:

```
configure
  ip-pool-mgmt-policy xyz
    user-plane-group G1 ip-address-pool-name v4-pool
ipv6-address-pool-name v6-pool
    end
```

Reconfigure the UP Group by using the following CLI commands:

```
configure
  ip-pool-mgmt-policy xyz
    user-plane-group G1
    end
```

Note If APN is IPv4v6 type, then the public pool will be used for IPv4 and IPv6 address.

Removing Only IPv4 or IPv6 Pools from UP Group

For deleting either IPv4 or IPv6 pools, reconfigure the UP Group accordingly.

Example Configuration:

```
configure
   ip-pool-mgmt-policy xyz
     user-plane-group G1 ip-address-pool-name v4-pool
ipv6-address-pool-name v6-pool
     end
```

Reconfigure the UP Group by using the following CLI commands:

```
configure
   ip-pool-mgmt-policy xyz
     user-plane-group G1 ipv6-address-pool-name v6-pool
     end
```



Note If APN is IPv4v6 type, and only IPv6 pool is associated to UP Group, then public pools are used for IPv4 address. And if IPv4 pool is associated to UP Group, then public pools are used for IPv6 address.

Sample Configuration

Control Plane - 1

```
config
   context egress
      ip pool PRIVATE-1 192.168.0.0/16 private chunk-size 1024 vrf-name vf-name-1
      ip pool PRIVATE-2 192.168.0.0/16 private chunk-size 1024 vrf-name vf-name-2
      ip pool PRIVATE-3 192.168.0.0/16 private chunk-size 1024 vrf-name vf-name-3
   exit
#exit
user-plane-group UP-Grp-1
   peer-node-id ipv4-address 192.168.0.1
exit
user-plane-group UP-Grp-2
   peer-node-id ipv4-address 192.168.0.2
exit
user-plane-group UP-Grp-3
   peer-node-id ipv4-address 192.168.0.3
exit
ip-pool-mgmt-policy xyz
   user-plane-group UP-Grp-1 ip-pool name PRIVATE-1
   user-plane-group UP-Grp-2 ip-pool name PRIVATE-2
   user-plane-group UP-Grp-3 ip-pool name PRIVATE-3
end

config
   context ingress
      apn intershat
         ip context-name egress
         ip-pool-mgmt-policy xyz
      exit
  #exit
end

UP-Grp-1 ===> Region 1 (192.168.0.0/16)
UP-Grp-2 ===> Region 2 (192.168.0.0/16)
UP-Grp-3 ===> Region 3 (192.168.0.0/16)
```

Control Plane - 2

```
config
   context egress
      ip pool PRIVATE-1 172.16.0.0/12 private chunk-size 1024 vrf-name vf-name-1
      ip pool PRIVATE-2 172.16.0.0/12 private chunk-size 1024 vrf-name vf-name-2
      ip pool PRIVATE-3 172.16.0.0/12 private chunk-size 1024 vrf-name vf-name-3
   exit
#exit
user-plane-group UP-Grp-1
   peer-node-id ipv4-address 192.168.0.1
exit
user-plane-group UP-Grp-2
   peer-node-id ipv4-address 192.168.0.2
exit
user-plane-group UP-Grp-3
   peer-node-id ipv4-address 192.168.0.3
exit
ip-pool-mgmt-policy xyz
   user-plane-group UP-Grp-1 ip-pool name PRIVATE-1
   user-plane-group UP-Grp-2 ip-pool name PRIVATE-2
   user-plane-group UP-Grp-3 ip-pool name PRIVATE-3
end

config
   context ingress
      apn intershat
         ip context-name egress
         ip-pool-mgmt-policy xyz
      exit
  #exit
end

UP-Grp-1 ===> Region 1 (172.16.0.0/12)
UP-Grp-2 ===> Region 2 (172.16.0.0/12)
UP-Grp-3 ===> Region 3 (172.16.0.0/12)
```

Verifying IP Pool Management Policy Configuration

Use the following CLI command to check IP Pool Management Policy:

show ip-pool-mgmt-policy all

Use the following CLI command to check IP Pool Management Policies for any specific UP Group:

show ip-pool-mgmt-policy user-plane-group-name *group_name*

Use the following CLI command to check for used and free IP chunks for a pool name:

show ip pool-chunks pool-name

User Plane Selection based on TAC Range

Revision History



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

Revision Details	Release
With this release, support is added for TAC/RAC profile configuration.	21.25
First introduced	Pre 21.24

Feature Description

With this feature, User Plane group can be selected based on Access Point Name (APN). The ability to configure Tracking Area Code (TAC) range, in rule combinations in virtual APN selection, helps in giving more flexible network design for location-based User Plane selection for edge computing and other services.

With 21.25 and later releases, support is added to configure TAC and Routing Area Code (RAC) profile in the Control Plane node. Using this feature, it is now possible to select APN based on discrete values of TAC/RAC profile instead of range.

How It Works

In non-CUPS architecture, Virtual APN selection is based on the following parameters:

- Subscriber IP
- Access-gw-address
- Bearer-access
- cc-behavior
- cc-profile
- domain
- mcc
- msisdn-range
- pdp-type
- rat-type
- roaming-mode
- serv-gw-plmnid

In CUPS architecture, Virtual APN selection is based on Tracking Area Code range with other options, such as cc-profile or mcc/mnc.

To support this feature:

- A new CLI keyword is introduced to accommodate new parameter.
- During call processing, incoming tracking area code is compared with the configured tracking area code range to determine the Virtual APN.

The Tracking Area Code based Virtual APN selection:

- Supports at least 30 tracking-area-code-range configured for Virtual APN.
- Supports overlapping ranges (subset or superset). Duplicate of tracking-area-code-range is not allowed for different priority.
- Selects a Virtual APN based on CLI configuration and User Plane is selected based on Virtual APN for a new call based on the tracking-area-code for that UE.
- Supports a combination of tracking-area-code-range and cc-profile in same priority.

Virtual APN functionality includes storing all the Virtual APN selection rules per real/Gn APN. Every rule has multiple criteria. Rule is identified by preference number. The list of APNs are stored and within APN a rule is identified using preference number.

New parameter has been introduced to pass Tracking Area Code, received in CSReq (TAI).

Limitations

Following are the known limitations and restriction of this feature.

- New configuration with multiple selection criteria in Virtual APN selection does not work with older builds/releases. User should have separate copies of the configuration for older builds/releases.
- Modify operation on the Virtual APN rule is not supported. User should delete the existing rule and add new rule to achieve modify operation.
- If same option is provided multiple times in the same rule, then the value of later option is considered for selection.
- Total number of Virtual APN rules added across all APNs is limited to 2048. This limitation exists in non-CUPS architecture.
- Upto 1000 TAC/RAC profiles can be configured. Memory usage is based on the number of profiles configured.
- The maximum number of TAC/RAC discrete values supported in a profile are 100. Memory usage is fixed per profile.
- TAC/RAC range or discrete values can overlap between profiles to support maintenance activities like split existing profile or others.
- This is Day-0 and Day-1 configuration.
- Multiple profiles can be associated with an APN.
- There are no changes in existing IP pool functionality.

- There is no specific impact on ICSR or Multi-Sx configurations.
- There is no Service Area Code (SAC) support.
- Pure-S calls aren't supported.
- UP selection requirements are handled in multi-UP group support features.

Configuring User Plane Selection based on TAC Range

This section provides information about CLI commands available in support of this feature.

Configuring Tracking Area Code Range

Use the following CLI commands to configure APN for Tracking Area Code range in Control Plane node.

```
configure
  context context_name
    apn apn_name
     virtual-apn preference preference apn apn_name tracking-area-code-range
 tac_range
      end
```

NOTES:

- **tracking-area-code-range** *tac_range*: Configures APN for Tracking Area Code range. The *tac_range* is an integer value ranging from 0 to 65535.

Verifying the Tracking Area Code Range Configuration

Use the following CLI commands to verify if the feature is enabled and the range that is configured for Tracking Area Code.

- **show configuration apn** *apn_name*
- **show apn name** *apn_name*

Configuring Tracking Area Code Profile

From 21.25 and later releases, Tracking Area Code profile can be configured in the Control Plane node. Using this feature, it is now possible to select APN based on discrete values of TAC instead of only range.

The following CLI commands are used to configure Tracking Area Code profile with discrete values and range.

```
configure
  context context_name
    tac-profile tac_profile_name
      tac range X to Y
      tac value
```

NOTES:

- **tac-profile** *tac_profile*: Configures APN for Tracking Area Code profile. The *tac_profile* is any range or discrete integer value ranging from 0 to 65535.
- The number of discrete TAC values supported per CLI command is 16.

Associating TAC Profile with APN

Use the following configuration to associate TAC profile with APN:

```
configure
  context context_name
    apn apn_name
      virtual-apn preference preference apn apn_name tac-profile tac_profile
      end
```

Verifying the Tracking Area Code Profile Configuration

Use the following CLI commands to verify if the feature is enabled and the range that is configured for Tracking Area Code profile.

- **show configuration apn** *apn_name*
- **show apn name** *apn_name*
- **show rule definition** *tac_profile*

Configuring Routing Area Code Profile

From 21.25 and later releases, Routing Area Code profile can be configured in the Control Plane node. Using this feature, it is now possible to select APN based on discrete values of RAC profile instead of range.

The following CLI commands are used to configure Routing Area Code profile with discrete values.

```
configure
  context context_name
    rac-profile rac_profile_name
      rac range X to Y
      rac value
```

NOTES:

- **routing-area-code-profile** *rac_profile*: Configures APN for Routing Area Code profile. The *rac_profile* is any range or discrete integer value ranging from 0 to 255.
- The number of RAC profile values supported is upto 16.

Associating RAC Profile with APN

Use the following configuration to associate TAC profile with APN:

```
configure
  context context_name
    apn apn_name
      virtual-apn preference preference apn apn_name
```

```
routing-area-code-profile rac_profile
        end
```

Verifying the Routing Area Code Profile Configuration

Use the following CLI commands to verify if the feature is enabled and the range that is configured for Routing Area Code profile.

- **show configuration apn** *apn_name*
- **show apn name** *apn_name*
- **show rule definition** *rac_profile*

UP Selection During Session Creation Failures

Table 6: Feature History

Feature Name	Release Information	Description
Selection of UP During Session Creation Failures	2025.01.0	While selecting a UP, the CP can rule out if a UP is down or in the overload state. When a UP is in normal load state, it connects with the CP, or it rejects the call if the UP is in overload state. However, due to some issues (such as configuration, software, or interface down issues) at the UP, it rejects the calls even if it is in the normal load state. This feature enhances the UP selection mechanism by marking the UP as "Busy-Out" in case of high volumes of call failures. This keeps the specific UP out of repeated selections and therefore improves the overall user experience. **Commands Introduced:** A new CLI is introduced to configure the parameters to exclude a UP: **[no] exclude-user-plane minimum-call-failures** *min_callfail* **failure-threshold-percentage** *fail_threshold_percentage* **failure-rejection-interval** *fail_reject_int* **Default Settings:** Disabled—Configuration Required to Enable

Session Creation Failures at UP

The CP selects a UP to serve a subscriber UE based on various criteria, such as the UE's location, capability and proximity of UP with respect to the RAN site, dynamic load of the UP, and so on.

The UP shares the load and overload information with the peer CP, based on which the CP selects a UP according to the UP selection mechanism.

To know more about the UP selection mechanism during load and overload scenarios, see the User Plane Selection topic.

However, a peer UP with normal load state may keep rejecting the Sx Establishment requests from CP, due to some errors on UP, such as wrong configuration, software issues, internal issues like interface down, and so on. The CP might be unaware of these issues and keep selecting the same UP repeatedly.

Due to a high volume of call rejections, the situations like partial outages and drop in KPIs arise causing service disruption that affects the overall customer experience.

Rejection Rate as a UP Selection Criteria

In order to prevent CP from selecting a UP with high call rejections, the CP needs to consider **Rejection Rate** as a criteria for UP selection. When the Rejection Rate for session creations (Sx Session Establishment) crosses a specified configured threshold, then CP takes that UP out from selection.

How Rejection Rate Monitoring Helps Avoid Session Creation Failures

When a CP continuously receives session creation failures from a UP, it starts recording the information until the Rejection Rate Threshold against the total number of calls attempted, is reached.

CP uses following configuration paramemeters to compute Rejections and mark UP BusyOut:

- **Minimum Number of Call Rejections**: It is a counter that records the number of rejected session creations. This feature takes into account the Sx Session Establishment rejections due to any of the following cause codes:
  - **64**- Request Rejected – Reason not specified
  - **75**- No Resources Available
  - **76**- Service Not Supported
  - **77**- System Failure
- **Failure Threshold Percentage**: This is the percentage of failures calculated based on attempted and rejected calls within the Failure Threshold Interval.
- **Failure Rejection Interval**: This is the configurable interval in which the data are computed for the usage.

When there are call rejections from the peer UP, the rejections are cumulated based on the rejection cause. When the minimum number of call rejections is reached and it crosses the **Failure Threshold Percentage** within the **Failure Rejection Interval**, the UP is taken out from the selection criteria.

Note The limitations and considerations applied in the feature User Plane Node Bring Down Procedure, also applies in this feature. To know more about the limitations of UP Selection During Session Creation Failures, Refer to the section Limitations and Considerations.

Configuration for Handling UP Selection During Session Creation Failures

Handling the UP selection during the session creation failures requires the operator to configure the parameters that are required for computing the Rejection Rate.

For more information on how to configure the parameters to exclude a UP, see Configure the Parameters to Exclude a UP.

Once the UP is taken out from the selection criteria, the UP needs to be manually restored using this configuration. For more information on how to manually restore the busy-out User Plane, see the Configuring UP Node Bring Down Procedure topic.

Note When a UP is busied-out, the UP's busy-out status is displayed in the **show sx peers** output. However, the busy-out CLI is not added to the configuration file, unlike the manual busy-out.

Configure the Parameters to Exclude a UP

This configuration allows you to define the Rejection Rate that allows to exclude the peer UP node from the selection criteria that crosses this threshold.

These are the steps to exclude the UP that repeatedly reject session creation calls from CP:

Procedure

Step 1 Enter the Context mode from the Global Configuration mode using the command **context** *context_name*.

Example:

```
[local]qvpc-si# config
[local]qvpc-si(config)# context ingress
[ingress]qvpc-si(config-ctx)#
```

Step 2 Define the Sx-Service name using the command **sx-service** *sx-service-name*.

Example:

```
[ingress]qvpc-si(config-ctx)# sx-service sx-1
[ingress]qvpc-si(config-sx-service)#
```

Step 3 Configure the rejection parameters to exclude a specific UP post crossing a threshold, using the command **[no] exclude-user-plane minimum-call-failures** *min_callfail* **failure-threshold-percentage** *fail_threshold_percentage* **failure-rejection-interval** *fail_reject_int*.

Example:

```
[ingress]qvpc-si(config-sx-service)# exclude-user-plane minimum-call-failures 200
failure-threshold-percentage 90 failure-rejection-interval 120
[ingress]qvpc-si(config-sx-service)# no exclude-user-plane
```

- **minimum-call-failures** *min_callfail* configures the minimum number of call failures within failure-rejection-interval to exclude a specific UP. The suggested value for **minimum-call-failures** is 200.
- **failure-threshold-percentage** *fail_threshold_percentage* configures the failure threshold percentage to exclude a specific UP. The suggested value for **failure-threshold-percentage** is >=90%.
- **failure-rejection-interval** *fail_reject_int* configures the failure rejection interval to exclude a specific UP. The suggested value for **failure-rejection-interval** is 120 seconds.
- **[no]**: This is an optional command. It disables the exclusion of the UP.

Note
When the configured values are lower than the suggested values, this warning is displayed:

"Lower values config options are allowed for experimental purpose and if configured can lead to false-positive scenarios."

Step 4 Exit the configuration mode using the command **end**.

```
[ingress]qvpc-si(config-sx-service)# end
[local]qvpc-si#
```

Monitoring and Troubleshooting

This section describes the information used for monitoring and troubleshooting this feature.

Show Commands and Outputs

This section discusses the show commands used in this feature.

show sx-service name

The show command **show sx-service name** *sx-service name* displays the configured parameters to exclude a UP under an Sx service. .

```
[ingress]qvpc-si# show sx-service name upservice
Service name                          : sxc0
  Service-Id                            : 20
  Context                               : ingress
  Status                                : STARTED
  Instance Type                         : controlplane
  UPF-id                                : Not configured
  SX Bind IPv4 Address                  : 192.60.181.1
  SX Bind IPv6 Address                  : 4122::192:60:181:1
  SX Association Reattempt Timeout      : 30 (sec)
  SX Association Release Timeout        : 90 (sec)
  SX Recovery Time Stamp                : Fri Dec 20 13:16:07 2024 UTC
  SXA:
    SX Retransmission Timeout             : 20000 (milliseconds)
    SX Maximum Request Retransmissions    : 15
  SXB:
    SX Retransmission Timeout             : 20000 (milliseconds)
    SX Maximum Request Retransmissions    : 15
  SXAB:
    SX Retransmission Timeout             : 20000 (milliseconds)
    SX Maximum Request Retransmissions    : 15
  N4:
    N4 Retransmission Timeout             : 5000 (milliseconds)
    N4 Maximum Request Retransmissions    : 4
  SX Heartbeat                          : Disabled
  SX path failure detection policy:
    Heartbeat Timeout                               : Enabled
    Heartbeat Req/Rsp Recovery timestamp change     : Enabled
    Control Msg Recovery timestamp change           : Enabled
  SX PDI Optimisation                     : Enabled

  Supported Features :
       LOAD CONTROL                     : Disabled
       OVERLOAD CONTROL                 : Disabled
```

```
Exclude User Plane: Enabled
  Minimum Call Failure               : 200
  Failure Threshold Percentage       : 90%
  Failure Rejection Interval         : 120 (seconds)
```

SNMP Trap

These SNMP traps are triggered when a UP is busied-out:

- **UPBusyOut–1455**: This SNMP trap is triggered to indicate that the UP is busied-out.
- **UPBusyOutClear–1456**: This SNMP trap clears the UPBusyOut trap.

```
Internal trap notification 1455 (UPlaneBusyOut) Marking User Plane  Busyout:192.60.182.1
via sxdemux as exclude-user-plane config is enabled.

Internal trap notification 1456 (UPlaneBusyOutClear) Clearing User Plane Busyout:192.60.182.1

Internal trap notification 1455 (UPlaneBusyOut) Marking User Plane  Busyout:192.60.182.1
via CLI.
```