

Priority between UP Groups

- Revision History, on page 1
- Feature Description, on page 1
- How It Works, on page 1
- Configuring IP Pool Management Policy and UP Group with Specific IP Pool, on page 6
- Verifying IP Pool Management Policy Configuration, on page 11

Revision History

Revision Details	Release
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.

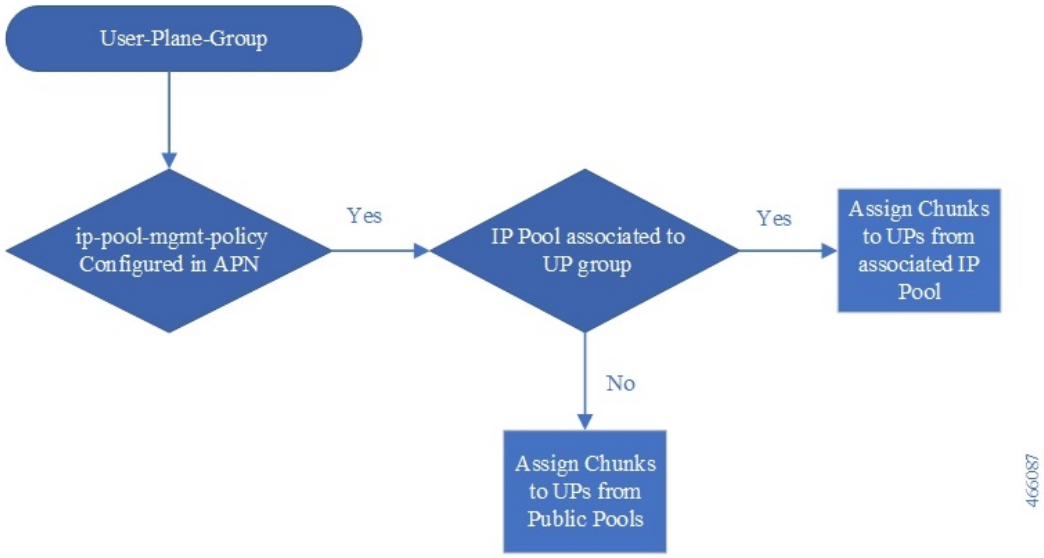
Support of UP Group Specific IP Pool

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

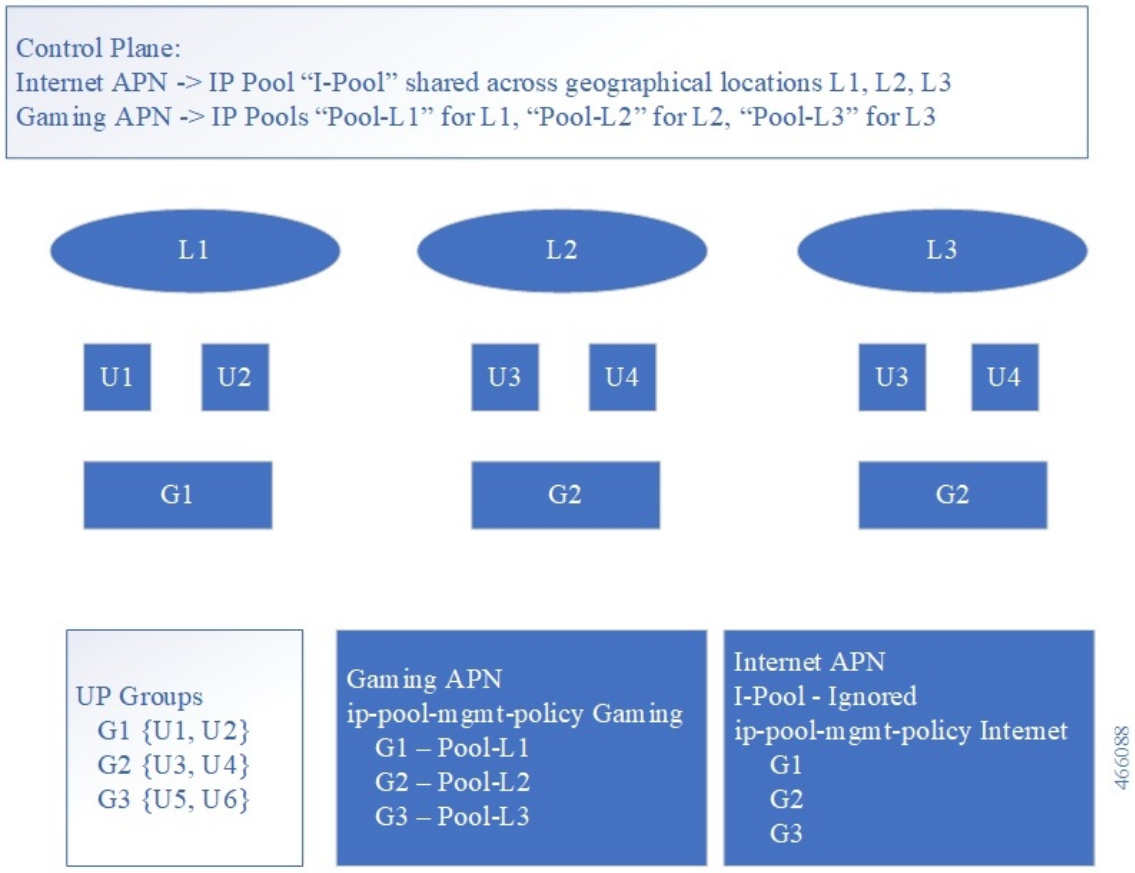


The following table is an example of expected behavior considering G4/G6 as Global/Public IPv4/IPv6 pools, and U4/U6 is the UP group-level IPv4/IPv6 pools.

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 2: 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 3: Flow of Events and Data for DNS-Based UP Selection

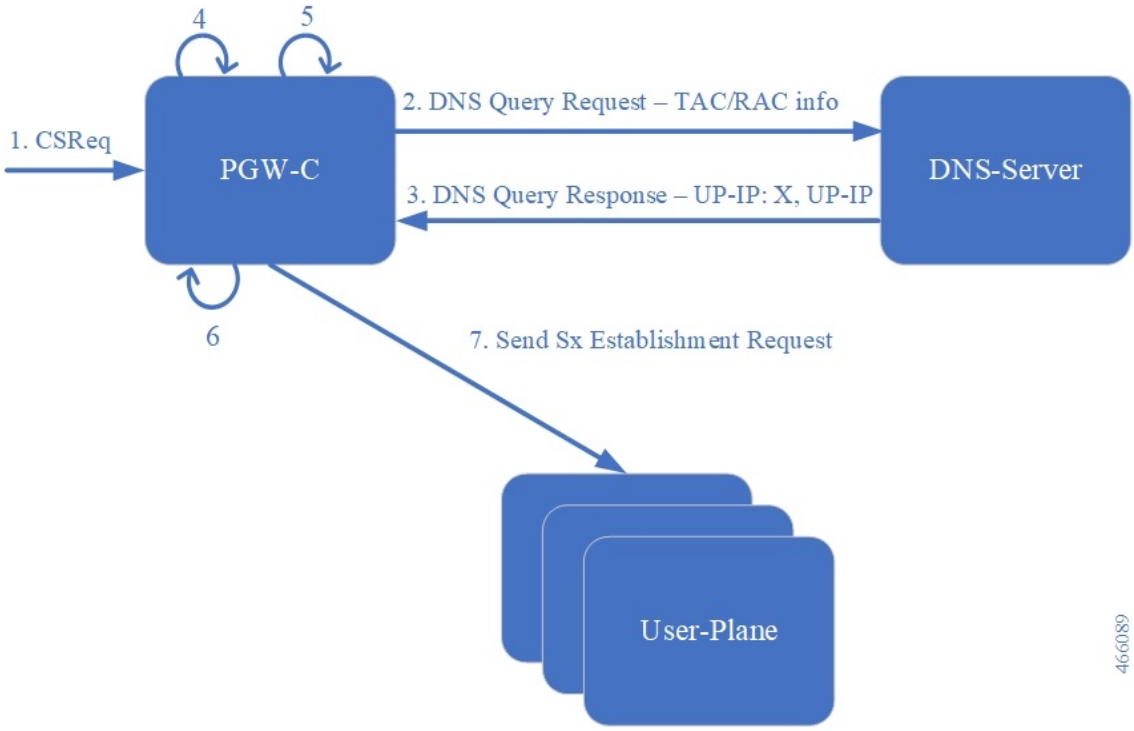


Table 1: General Flow of Events and Data for DNS-Based UP Selection

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 20 UP groups are allowed inside each 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