IP Allocation through DHCP Server

Table 1: Feature History

Feature Name	Release Information	Feature Description
DHCP-based IPv6 address allocation without prefix limitations	2025.03.0	This feature allows the UPF to support IPv6 address allocation to the subscriber UEs through external DHCP server, without prefix limitations. **Commands introduced:** **disable ipv6-validation**: This CLI is configured under DHCP Client Profile configuration mode to disable IPv6 validation. **Commands enhanced:** **disable dhcpv6-client-unicast slot/port** *slot_port_number*: This CLI is configured under DHCP Client Profile configuration mode to disable unicast option and thus enable multicast. **Default Settings:** Disabled—Configuration Required to Enable
DHCP-based IP Address Allocation	2025.02.0	This feature allows the network operator to use an external DHCP server to receive IP addresses for subscriber UEs. Allocating IP addresses using a DHCP server enables the enterprises with complex 5G networks to manage and control the IP address allocation centrally. **Commands Introduced:** **dhcp server enable-discover slot/port** *slot_port_number* **dhcp-node-id** *node_id*: This CLI is configured under DHCP service configuration mode to allow UPF to discover the DHCP server. **Commands Enhanced:** **dhcp ip skip-validation**: This CLI is configured under the DHCP service configuration mode to skip the IPv4 address validation. **Default Settings:** Disabled—Configuration Required to Enable

In a 5G network, SMF handles the dynamic IP address allocation from the local IPAM pool. However, the complex 5G enterprise networks require centralization of IP address allocation and management.

To facilitate this, UPF supports using a DHCP server to allocate the IP addresses to the subscriber UEs. It allows the network operator to have a centralized IP management that aligns with the needs of complex and large-scale enterprise environments.

How UPF allocates the UE IP through DHCP server

These stages show the process in which the UPF allocates the UE IP address through external DHCP server:

1. **Session establishment request:** The SMF sends the UE IP Address IE in PDI IE within the PFCP Session Establishment Request message to the UPF, if the SMF is configured to obtain UE IP addresses from the UPF.

   This message contains the VLAN ID(s) in the Create PDR IE in UE IP Address Pool Identity IE and either or both of these message bits are set to one:

   - **CHOOSE IPV4 (CHV4):** SMF requests the UPF for IPv4 address allocation.
   - **CHOOSE IPV6 (CHV6):** SMF requests the UPF for IPv6 address allocation.

2. **DHCP subnet selection:** UPF uses the received VLAN ID(s) for selecting the subnet for UE IP based on some conditions.

   Learn more about the conditions in the DHCP subnet selection criteria topic.

3. **DHCP configuration validation:** UPF validates if the DHCP service is configured and running by checking the configuration validation criteria.

   To know more about the DHCP configuration, see the Enabling DHCP-based IP allocation section.

   If the DHCP configuration validation is successful, UPF accepts the PFCP Establishment Request and initiates a DHCP Discovery handshake toward DHCP server in the given subnet using the received VLAN ID. If the configuration validation fails based on the criteria, the UPF rejects the Establishment Request.

   To know more about the configuration validation, see the Criteria for DHCP configuration validation section.

4. **DORA or SARR handshake process initiation:** UPF initiates the Discovery-Offer-Request-Acknowledge (DORA) or Solicit-Advertise-Request-Reply (SARR) handshake process for IPv4 or IPv6 address allocation respectively.

   UPF broadcasts a **Discovery** message in case of DHCPv4 and multicasts a **Solicit** message in case of DHCPv6 in the subnet. UPF acts as the DHCP client Relay and uses the received VLAN information for sending the Discovery or Solicit messages.

Note

- The UPF receives the unicast response from the DHCP server on the destination port 67.
- UPF acts as client when it sends the broadcast DHCPDISCOVER message in the VLANs source port—68 and the dst port—67.
- For IPv6 prefix allocation, all the messages from UPF to the DHCPv6 server include the IA_PD option, with a requested prefix length of 64.

5. **Offer or Advertise messages:** In case of IPv4, UPF receives the **Offer** message from the DHCPv4 server with an IPv4 address, lease time, and the server identifier.

   In case of IPv6, the UPF receives a unicast **Advertise** message from the DHCPv6 server along with client IPv6 address, lease time, and server identifer.

6. **IPv4 and IPv6 validation:** UPF validates the IP addresses received from the DHCP server. The validation process differs based on the requested type of IP address, that is, IPv4 or IPv6.

   - **IPv4 validation:** If the CLI **[no] skip-validation** is configured, UPF validates the received IPv4 address with the SMF allocated IP chunks.

     If the IPv4 validation is successful, UPF sends a Request message to the DHCP server. If the IPv4 validation fails, UPF does not send the Request message to the DHCPv4 server and the IPv4 address allocation process fails.

     For an IPv4v6 Session, if IPv4 validation fails, UPF sends Sx Session Establishment Response with cause code **Partial Success** with IPv6 address allocated to the UE.

   - **IPv6 validation:** If the CLI **enable ipv6-validation** is configured, UPF sends a **Request** message to the DHCPv6 server. The DHCPv6 server sends a **Reply** message to the UPF.

     For IPv6, prefix validation is done after receiving the Reply message in the SARR handshake.

     If the IPv6 validation is unsuccessful, UPF will send a DHCP DECLINE message to DHCPv6 server to indicate that the UPF will not use the IPv6 address given by DHCPv6 server.

     For an IPv4v6 Session, if IPv6 validation fails, UPF sends Sx Session Establishment Response with cause code **Partial Success** with IPv4 address allocated to the UE.

   Know more about the criteria and process of IPv4 and IPv6 validation addresses in the Validation of IP addresses from DHCP server and SMF section.

7. **Renew and rebind:**

   - **Renew request:** UPF tries to renew the lease when the allocated lease time is about to expire. In this case, UPF unicasts a renew request to the DHCP server at 50% (T1 threshold) of the allocated lease time.

     If the DHCP server does not respond to the renew request, the UPF retries the renew request until the maximum retries exhaust.

     If the server replies with NAK (Negative Acknowledgement), it implies that the lease cannot be extended. The UPF then purges the call and informes the SMF.

     For the IPv6 address, the renew request goes at the T1 timer value in the Reply packet.

- **Rebind request**: If the DHCP server does not respond to the renew request even after the maximum retries exhaust, the DHCP server broadcasts the rebind request when the allocated lease is at 88% (T2 threshold) of the allocated lease time.

  If the DHCP server does not respond to the rebind request, the UPF retries the rebind request until the maximum retries are exhausted. If the DHCP server does not respond even after maximum retries are exhausted, and the allocated lease gets expired, the call gets purged. The UPF notifies about the call deletion to the SMF.

  If the server replies with NAK, it implies that the lease cannot be extended. The UPF then purges the call and informs the SMF.

  For IPv6 address, the rebind packet goes at the T2 timer values in the Reply packet.

The values of the T1 and T2 thresholds are configurable.

To know more about configuring T1 and T2 thresholds, see the *DHCP Service Configuration Mode Commands* chapter in the *Command Line Interface Reference, Modes C - D, StarOS Release 21.28* guide.

Note EPFAR configuration is mandatory to handle renew/rebind failure, and if not configured UPF will do a local purge leading to mismatch between SMF and UPF.

8. **Session deletion:** UPF locally purges the session and sends an indicationtion to SMF that UPF has deleted the call in session report request, once the lease time is expired.

   SMF sends a PFCP session Deletion request over the N4 interface to UPF. Upon receiving the PFCP Session Deletion Request message from SMF, the UPF initiates a fire-and-forget DHCP release request toward the DHCP server.

DHCP subnet selection criteria

The UPF interprets the UE IP Address Pool Identity IE as the VLAN ID for selecting IPv4 subnet according to these conditions:

When N4 session establishment contains...	And Create PDR IE contains ...	Then ...
only CHOOSE IPV4 bit	single UE IP Address Pool Identity IE	UPF interprets as VLAN to identify the subnet for IPv4 IP address allocation.
only CHOOSE IPV4 bit	more than one UE IP Address Pool Identity IEs	UPF ignores additional occurrences of the UE IP Address Pool Identity IE.
only CHOOSE IPV6 bit	single UE IP Address Pool Identity IE	UPF interprets as VLAN to identify the subnet for IPv6 IP address allocation.
only CHOOSE IPV6 bit	more than one UE IP Address Pool Identity IEs	UPF ignores additional occurrences of the UE IP Address Pool Identity IE.
both CHOOSE IPV4 and CHOOSE IPV6 bits	single UE IP Address Pool Identity IE	UPF rejects the Session Establishment Request with a cause code- Mandatory IE incorrect.

When N4 session establishment contains...	And Create PDR IE contains ...	Then ...
both CHOOSE IPV4 and CHOOSE IPV6 bits	two UE IP Address Pool Identity IE	UPF interprets the first and second UE IP Address Pool Identity IEs as the VLANs to identify the subnets for IPv4 and IPv6 IP address allocations respectively.
both CHOOSE IPV4 and CHOOSE IPV6 bits	more than two UE IP Address Pool Identity IE	UPF ignores the additional occurrences of the UE IP Address Pool Identity IE.

Criteria for DHCP configuration validation

Before initiating the DORA or SARR process, UPF performs these validations:

- If either or both CHOOSE IPV4 and CHOOSE IPV6 bits are set, then the DHCP configuration for both IPv4 and IPv6 should not be present. Otherwise, UPF sends the cause code "**Mandatory IE Incorrect**" to SMF.
- If either or both CHOOSE IPV4 and CHOOSE IPV6 bits are set and IPv4 or IPv6 addresses are not present, local APN level configurations **ip address alloc-method dhcp-proxy** and **ipv6 address alloc-method dhcpv6-proxy** should be present for DHCPv4 and DHCPv6, respectively. Otherwise, UPF sends the cause code "**IP Allocation Failure**" to UPF.
- The received VLAN ID should be present for either or both IPv4 and IPv6 in the configuration on UPF.

  If the received VLAN ID is not present in the UPF configuration, then the UPF sends the cause code "**NO RESOURCES AVAILABLE**" to SMF.
- If the DHCP server discovery is disabled and the DHCP server IP address is not configured, but the DHCPv4 service is running, then UPF sends the cause code "**NO RESOURCES AVAILABLE**" to SMF.
- When unicast is enabled and the DHCP server IP addresses are also not configured, but the DHCPv6 service is running, then the UPF sends the cause code "**NO RESOURCES AVAILABLE**" to SMF.
- The Slot/Port should be present and linked to the correct interfaces for IPv4 or IPv6 in the configuration. Otherwise, UPF sends the cause code "**IP Allocation Failure**" to SMF.
- If either or both CHOOSE IPV4 and CHOOSE IPV6 bits are set, then the DHCP configuration for both v4 and v6 must be valid. It is required to start DHCPv4 and DHCPv6 services. Otherwise, the call gets rejected and UPF sends the cause code "**IP Allocation Failure**" to UPF.

Validation of IPv4 and IPv6 addresses

The UPF compares the IPv4 or IPv6 address received from the DHCP server with the chunks allocated by SMF during the DORA or SARR process.

IPv4 validation during DORA process

These stages show the IPv4 validation process during the DORA handshake process:

1. UPF sends the DHCP Discover message to the DHCPv4 server.

2. UPF receives the DHCP Offer message from the DHCPv4 server along with a client IP address, lease time, and server identifier.

   UPF accepts the first Offer message it receives and ignores all the subsequent Offer messages from other DHCPv4 servers.

3. UPF validates the received IP address with the IP pool chunks sent by SMF.

If the IP validation is ...	then...
successful	UPF sends a DHCP Request message to the DHCPv4 server and receives the DHCP Acknowledgement message from the DHCPv4 server.
unsuccessful	UPF discards the Offer message and does not send a DHCP Request message to the DHCPv4 server. The UPF then rejects the session.

4. The UPF receives an Acknowledgment message from the DHCP server. The UPF validates if the IP received in the Offer and the Acknowledge messages are the same. UPF also performs other validations like lease validation, chaddr validation, server identifier validation, etc.

   If the IP values received in the Offer and Acknowledgment messages are the same, UPF considers the IP validation as successful. In this case, the UPF forwards the UE IP to the SMF.

   If there is a mismatch between the IP addresses received in the Offer and Acknowledgment messages, UPF considers the IP validation process as unsuccessful. In this case, the UPF sends a DHCP decline message to the DHCPv4 server and the deletes the session.

   If there is a mismatch in the values of Offer packet and Acknowledgment packet except the IP address validation, then the UPF sends a DHCP release message to the DHCPv4 server.

IPv6 validation during SARR process

For IPv6 sessions, UPF performs IPv6 validation after the SARR process when the **enable ipv6-validation** is configured. These stages show the IPv6 validation process:

1. UPF sends the Solicit message to the DHCPv6 server.
2. UPF receives the Advertise message from the DHCPv6 server.
3. UPF sends the Request message to the DHCPv6 server.
4. UPF receives the Reply message from the DHCPv6 server.
5. UPF validates the received IPv6 address with the IPv6 pool chunks sent by SMF.

If the IP validation is ...	then...
successful	UPF sends the successful establishment response with the received IPv6 address.
unsuccessful	UPF sends DHCP DECLINE message to DHCPv6 server to indicate that the UPF will not use the IPv6 given by DHCPv6 server. Establishment Request is rejected for IPv6 only PDN session. Establishment Request is accepted with cause code partial success for IPv4v6 PDN session.

Enabling DHCP-based IP allocation

These are the necessary steps to enable DHCP-based IP allocation in UPF:

Important While enabling the DHCP feature, it is always recommended to enable the DHCP service on the standby UPF first and then on the active UPF. After making the feature CLI changes, save the changed config at boot config to enable the feature.

If you enable this feature for an existing DNN, the ongoing calls will experience service interruptions. If you enable this feature for a new DNN, there will be no service disruptions, as the new call will always have IP allocation from the DHCP server.

Procedure

Step 1 Start the DHCP service .

Step 2 Configure slot/port to enable discovery of DHCP server.

Start the DHCPv4 or DHCPv6 service

The N4 Establishment contains CHV4 bit or CHV6 message bits and UE IP Address Pool Identity IE to indicate that SMF requires an IP address. To enable the IP allocation through the DHCP server, UPF needs to ensure that the DHCP service is enabled.

Therefore, the UPF uses local APN-level configuration to perform the IP address allocation using the DHCP server.

This task allows you to configure the APN to enable DHCP-proxy based IP allocation.

Procedure

Step 1 Use the command **context** *context_name* to create an instance of the context.

Example:

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

Step 2 Use the command **apn** *apn_name* to create an instance under the APN configuration mode.

Example:

```
[local]UPF(config)# context ingress
[ingress]UPF(config-ctx)# apn intershat
[ingress]UPF(config-apn)#
```

Note

For the DHCPv4, if the DHCP context name is not configured in the APN, the configured IP context name is used as the DHCP context.

Step 3 Use the commands **ip address alloc-method dhcp-proxy** or **ipv6 address alloc-method dhcpv6-proxy** to define the IP address allocation as DHCP-proxy for IPv4 and IPv6 addresses respectively.

Example:

```
[ingress]UPF(config-apn)# ip address alloc-method dhcp-proxy
[ingress]UPF(config-apn)# ipv6 address alloc-method dhcpv6-proxy
[ingress]UPF(config-apn)#
```

Note
For the DHCPv4, if the DHCP service name is not configured in the APN, the DHCP service from the configured IP context name or the DHCP context is used.

Step 4 Use the command **dhcp service-name** *dhcp_service_name* **| { dhcpv6 service-name** *dhcpv6_service_name* **server-profile** *dhcpv6_server_prof* **client-profile dhcpv6-client-prof }** to specify the DHCP service to be used for IPv4 or IPv6.

Example:

```
[ingress]UPF(config-apn)# dhcp service-name dhcp_service
[ingress]UPF(config-apn)# dhcpv6 service-name dhcpv6-service server-profile
dhcpv6-server-prof client-profile dhcpv6-clientprof
[ingress]UPF(config-apn)# exit
```

Step 5 Use the command **bind address** *dhcp/dhcpv6_ip_address* to bind the UPF interface under the Context Configuration mode. Save and exit the current configuration mode.

Example:

```
[ingress]UPF(config-ctx)# bind address 209.165.201.1
[ingress]UPF(config-ctx)# bind address 2001:DB8::1
[ingress]UPF(config-ctx)# exit
```

This configuration starts the DHCP service and defines the address allocation method as DHCP-proxy.

What to do next

Configure the slot/port to send broadcast messages to the DHCP server. For more details, see the Configure slot/port to enable discovery of DHCP server section.

Configure slot/port to enable discovery of DHCP server

This task helps you configure the slot or port for UPF to send broadcast messages to the DHCP server.

Note If the slot/port is configured, then the UPF sends a broadcast message. However, if the slot/port is not configured, then the DHCP server IP addresses have to be configured. In this case, the UPF sends unicast packets.

Before you begin

Before configuring the slot to enable the discovery of DHCP server, you should enable the DHCP service for IPv4. For more details, see the section.

Procedure

Step 1 Enter the Context configuration mode using the command **context** *context_name* to create an instance.

Example:

```
[local]UPF(config)# context ISP
[egress]UPF(config-ctx)#
```

Step 2 Configure the slot/port through which the UPF connects with the DHCP or DHCPv6 server.

a) **For DHCPv4:** Use the command **dhcp-service** *dhcp_service_name* **dhcp server enable-discover slot/port** *slot_port_number* **dhcp-node-id** *node_id* to configure the Slot/port under the Context configuration mode.

Example:

```
[egress]UPF(config-ctx)# dhcp-service dhcp_service
[egress]UPF(config-dhcp-service)# dhcp server enable-discover slot/port 1/10
dhcp-node-id 5
[egress]UPF(config-dhcp-service)# dhcp client-identifier { msisdn | imsi }
[egress]UPF(config-ctx)#
```

Note

- If SMF sends the same VLAN ID for both IPv4 and IPv6 calls, then the slot and port configuration for IPv4 and IPv6 should be the same for both the calls.
- The VLAN configuration shall be the same on all UPF nodes.

b) **For DHCPv6:** Use the CLI **dhcp-server-profile** *dhcpv6_server_prof* **{ enable | disable } dhcpv6-server-unicast** under the Context configuration mode to enable or disable the server unicast option for DHCPv6 server. Also, use the CLI **dhcp-client-profile** *dhcpv6-client-prof* **{ enable | disable } dhcpv6-client-unicast slot/port***slot_port_number* to enable or disable the client unicast option for DHCPv6 on a specific slot or port.

Example:

```
[egress]UPF(config-ctx)# dhcp-server-profile dhcpv6-server-prof
[egress]UPF(config-dhcp-server-profile)# enable dhcpv6-server-unicast
[egress]UPF(config-dhcp-server-profile)# exit
[egress]UPF(config-ctx)# dhcp-client-profile dhcpv6-client-prof
[egress]UPF(config-dhcp-client-profile)# disable dhcpv6-client-unicast slot/port 1/11
[egress]UPF(config-dhcp-client-profile)# exit
[egress]UPF(config-ctx)#
```

Important

In order to use the CLI **disable dhcpv6-client-unicast**, you must have the "Unicast Address Support for DHCPv6 Messages" license.

Also, to use the CLI **slot/port** *slot_port_number*, you must have UPF license.

For more information on the license, contact your Cisco account representative.

Step 3 Disable or enable IP validation for either or both the received IPv4 and IPv6 addresses.

a) **For IPv4:** Use the command **[no] dhcp ip skip-validation** to skip the validation of IPv4 address received from DHCP server. This is an optional command.

Example:

```
[egress]UPF(config-dhcp-service)# dhcp ip skip-validation
[egress]UPF(config-dhcp-service)#
```

b) **For IPv6:** Use the command **disable ipv6-validation** to disable the IP validation process for IPv6 address received from the DHCP server.

Example:

```
[egress]UPF(config-dhcp-client-profile)# disable ipv6-validation
[egress]UPF(config-dhcp-client-profile)# exit
[egress]UPF(config-ctx)#
```

Step 4 Use the command **dhcp lease-expiration-policy { auto-renew | disconnect }** to configure the action required when the IP address lease expires.

Example:

```
[egress]UPF(config-dhcp-service)# dhcp lease-expiration-policy auto-renew
```

Step 5 Verify the status of DHCP service for IPv4 or IPv6.

a) **For IPv4:** Use the CLI **show dhcp-service all** to verify all the IPv4 DHCP service status.

Example:

```
[local]UPF# show dhcp-service all

Service name:                 dhcp_service
  Context:                      ISP
  Bind:                         Done
  Local IP Address:                100.100.103.20
  Next Hop Address:                None
  DHCP Subnet mask used:           host mask
      MPLS-label:                  None

  Service Status:                  Started
  Retransmission Timeout:          3000 (milli-secs)
  Max Retransmissions:             5
  Lease Time:                      600 (secs)
  Minimum Lease Duration:          600 (secs)
  Maximum Lease Duration:          86400 (secs)
  DHCP Dead Time:                  120 (secs)
  DHCP Dead consecutive Failure:   5
  DHCP T1 Threshold Timer:         50
  DHCP T2 Threshold Timer:         88
  DHCP Client Identifier:          Use MSISDN
  DHCP Server Discovery:        Enabled
      Slot/Port:  1/10
      Node Id:    5
  DHCP Algorithm:                  First Server
  DHCP Servers configured:         None
  DHCP server port: 67
  DHCP server rapid-commit:        disabled
  DHCP client rapid-commit:        disabled
  DHCP server check msg size:      disabled
  DHCP relay agent option:         disabled
  DHCP chaddr validation:          enabled
  DHCP IP address validation:   enabled
```

b) Use the command **show dhcpv6-client-profile { all | name }** *client-profile-name* to verify the status of IPv6 services.

Example:

```
[local]UPF# show dhcpv6-client-profile name dhcpv6-client-prof
Client Profile name: dhcpv6-client-prof
Context: ISP
Rapid-commit-dhcpv4: disabled
Rapid-commit-dhcpv6: disabled
Dhcp_msg_spray: disabled
Dns_address: enabled
Netbios_address: disabled
Sip_server_address: enabled
Client_Unicast_to_Server: disabled
IPV6 Validation: disabled
Slot/Port: 1/11
Client identifier: MSISDN
User Class Option: NONE
```

This task enables the discovery of DHCPv4 and DHCPv6 servers through a slot or port number.

Limitations

If an APN is linked to a DHCP service, where the DHCP service is defined in a context different than the context linked to APN, then DORA process does not take place.

For deployments with multiple APNs across different contexts, a separate DHCP service must be configured within each context.