

IP Allocation through DHCP Server

Table 1: Feature History

Feature Name	Release Information	Feature Description
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, on page 1
- Enabling DHCP-based IP allocation, on page 5

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 CHOOSE IPV4 (CHV4) message bit set to one. The CHV4 message bit requests the UPF for IPv4 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.

   If the DHCP configuration validation is successful, UPF accepts the PFCP Establishment Request and initiates a DHCP Discovery handshake towards 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 topic.

4. **DORA process initiation:** UPF initiates the Discovery-Offer-Request-Acknowledge (DORA) handshake process by sending a broadcast Discovery message in the subnet to all the DHCP servers. UPF acts as the DHCP client Relay and uses the received VLAN information for sending the Discovery message.

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 is sent in the VLANs source port—68 and the dst port—67.

5. **Offer and Request messages:** UPF receives the Offer message from the DHCP server with an IP address, lease time, and the server identifier.

   UPF validates the received IP with the SMF allocated IP chunks. The IP validation happens only if **skip-validation** is not confiured.

   If the IP validation is successful, UPF sends a Request message to the DHCP server. If the IP validation fails, lease validation, or any other validation fails at the Offer packet, then the Request message does not go.

   If the IP validaion fails on Reply message, UPF sends a decline message to the DHCP server. However, if any other validation fails, UPF sends a release message to the DHCP server.

   Know more about the criteria for IP validation for IPv4 in the Validation of IP addresses from DHCP server and SMF topic.

6. **Renew and rebind:**

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

If the DHCP server does not respond to renew request, the UPF will retry the renew request until the maximum retries are exhausted. If the DHCP server does not respond even after the maximum retry are exhausted, the DHCP server sends the rebind request when the allocated lease is at 88%.

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

- **Rebind request**: UPF tries to rebind with another DHCP server by broadcasting a rebind request to all the DHCP servers in the subnet 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 server replies with NAK, it implies that the lease cannot be extended. The UPF then purges the call and informs the SMF.



Note

- The values of 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.

- 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

7. **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 PFCP session Deletion request over N4 interface to UPF. Upon receiving PFCP Session Deletion Request message from SMF, the UPF initiates fire-and-forget DHCP release request towards 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 ...
CHOOSE IPV4 bit	single UE IP Address Pool Identity IE	UPF interprets as VLAN to identify the subnet for IPv4 IP address allocation.
CHOOSE IPV4 bit	more than one UE IP Address Pool Identity IEs	UPF ignores additional occurrences of the UE IP Address Pool Identity IE.

Criteria for DHCP configuration validation

Before initiating the DORA process, UPF performs these validations:

- If CHOOSE IPV4 bit is set, the UE IP Address Pool Identity IE should be present and IPv4 address should not be present.
- If the CHOOSE IPV4 bit is set and IPv4 address is not present, local APN level configuration **ip address alloc-method dhcp-proxy** should be present.
- If the CHOOSE IPv4 bit is set, then the DHCP configuration for IPv4 must be valid. It is required to start DHCP service, otherwise the call gets rejected with the cause code "**Mandatory IE Incorrect**".
- The received VLAN ID should be present for IPv4 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 DHCPv4 service is running, then UPF sends the cause code "**NO RESOURCES AVAILABLE**" to SMF.
- The Slot/Port should be present and linked to correct interfaces for IPv4 in the configuration.

Validation of IP addresses from DHCP server and SMF

The UPF compares the IP received from DHCP server with the chunks allocated by SMF during the DORA process.

These stages show the IP validation process:

1. UPF sends the DHCP Discover message to the DHCP Server.
2. UPF receives the DHCP Offer message from the DHCP 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 DHCP 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 DHCP Request message to DHCP server to receive the DHCP Acknowledgement message from the DHCP Server.
unsuccessful	UPF discards the Offer message and does not send DHCP Request message to DHCP Server. UPF then rejects the session.

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

   If the IP values received in Offer and Acknowledgement messages are same, the IP validation is considered to be successful. In this case, the UPF forwards the UE IP to the SMF.

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

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

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 DHCP service

The N4 Establishment contains CHV4 bit and UE IP Address Pool Identity IE to indiacte that SMF requires an IP address. To enable the IP allocation through 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** to define the IP address allocation as DHCP-proxy for IPv4 addresses.

Example:

```
[ingress]UPF(config-apn)# ip address alloc-method dhcp-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* to specify the DHCP service to be used for IPv4.

Example:

```
[ingress]UPF(config-apn)# dhcp service-name dhcp_service
[ingress]UPF(config-apn)# exit
```

Step 5 Use the command **bind address** *dhcp_ip_address* to bind the UPF interface under the Context Configuration mode.

Example:

```
[ingress]UPF(config-ctx)# bind address 209.165.201.1
```

Step 6 Use the command **exit** to exit the current configuration mode.

Example:

```
[ingress]UPF(config-ctx)# exit
[ingress]UPF(config)#
```

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.

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 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.

Procedure

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

Example:

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

Step 2 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.

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
```

Step 3 Use the command **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)#
```

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 Use the command **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
```

This task enables the discovery of DHCP server through a slot or port number.