

DHCP サーバー経由の IP 割り当て

表 *1*：機能の履歴

機能名	リリース情報	機能説明
プレフィックス制限のない DHCP ベースの IPv6 アドレス割り当て	2025.03.0	この機能により、UPF は、プレフィックスの制限なしに、外部 DHCP サーバーを介したサブスクライバ UE への IPv6 アドレス割り当てをサポートできます。 **導入されたコマンド**： **disable ipv6-validation**：この CLI は、IPv6 検証を無効にするように DHCP クライアントプロファイル構成モードで設定されます。 **コマンドの拡張**： **disable dhcpv6-client-unicast slot/port** *slot-port_number*：この CLI は、DHCP クライアントプロファイル構成モードで、ユニキャストオプションを無効にしてマルチキャストを有効にするように設定されます。 **デフォルト設定**無効：有効にするには構成が必要です。

機能名	リリース情報	機能説明
DHCP ベースの IP アドレス割り当て	2025.02.0	この機能により、ネットワークオペレータは、外部 DHCP サーバーを使用してサブスクライバ UE の IP アドレスを受信できます。 DHCP サーバーを使用して IP アドレスを割り当てることにより、複雑な 5Gネットワークを持つエンタープライズは、IP アドレスの割り当てを一元的に管理および制御できます。 **導入されたコマンド**： **dhcp server enable-discover slot/port** *slot_port_number* **dhcp-node-id** *node_id*：この CLI は、DHCP サービス構成モードで構成され、UPF が DHCP サーバーを検出できるようにします。 **強化されたコマンド**： **dhcp ip skip-validation**：この CLI は、IPv4 アドレス検証をスキップするようにDHCP サービス構成モードで構成されます。 **デフォルト設定**無効：有効にするには構成が必要です。

5G ネットワークでは、SMF はローカル IPAM プールからのダイナミックな IP アドレスの割り当てを処理します。ただし、複雑な5Gエンタープライズ ネットワークでは、IPアドレスの割り当てと管理の一元化が必要です。

これを容易にするため、UPF では DHCP サーバーを使用してサブスクライバ UE に IP アドレスを割り当てることがサポートされています。これにより、ネットワーク オペレータは、複雑で大規模なエンタープライズ環境のニーズに合わせて、一元化された IP 管理を行うことができます。

• UPF が DHCP サーバー経由で UE IP を割り当てる方法 （2 ページ）
• DHCP ベースの IP 割り当てを有効にする （8 ページ）
• 制限事項 （13 ページ）

UPF が DHCP サーバー経由で UE IP を割り当てる方法

これらの段階では、外部 DHCP サーバー経由で UPF が UE IP アドレスを割り当てるプロセスを示しています。

1. **Session Establishment Request**： SMF が、UPF から UE IP アドレスを取得するように構成されている場合、SMF は、PFCP Session Establishment 要求メッセージの PDI IE の UE IP Address IE を UPD に送信します。

   このメッセージには、UE IP Address Pool Identity IE の Create PDR IE の VLAN ID が含まれており、次のメッセージビットの一方または両方が 1 に設定されています。

- **CHOOSE IPV4（CHV4）**： SMF は、割り当てに向けて IPv4 アドレスの UPF をリクエストします。
- **CHOOSE IPV6（CHV6）**：SMF は、割り当てに向けて IPv6 アドレスの UPF をリクエストします。

2. **DHCPサブネット選択**： UPF は、受信した VLAN ID を使用して、いくつかの条件に基づいて UE IP のサブネットを選択します。

   条件の詳細については、「DHCP サブネット選択の基準」に関するトピックを参照してください。

3. **DHCP 構成の検証**：UPF は、構成検証基準をチェックすることにより、DHCP サービスが構成され、実行されているかどうかを検証します。

   DHCP 構成の詳細については、「DHCP ベースの IP 割り当てを有効にする」項を参照してください。

   DHCP 構成検証に成功すると、UPF は、PFCP Establishment 要求を受け入れ、受信した VLAN ID を使用して指定のサブネットで DHCP サーバーに対して DHCP Discovery ハンドシェイクを開始します。基準に基づいた構成検証に失敗すると、UPF は、Establishment 要求を拒否します。

   構成検証の詳細については、「DHCP 構成検証の基準」項を参照してください。

4. **DORA または SARR ハンドシェイクプロセスの開始**：UPF は、IPv4 アドレスと IPv6 アドレスのそれぞれに対して、Discovery-Offer-Request-Acknowledge（DORA）または Solicit-Advertise-Request-Reply （SARR）ハンドシェイクを開始します。

   UPF は、DHCPv4 の場合は、**Discovery** メッセージをブロードキャストし、DHCPv6 の場合は、**Solicit** メッセージをサブネットにマルチキャストします。UPF はDHCPクライアントリレーとして機能し、受信した VLAN とともに 検出メッセージまたは要請メッセージを送信します。

（注）
- UPF は、宛て先ポート 67 で DHCP サーバーからユニキャストレスポンスを受信します。
- UPF は、VLAN のソースポート（68）および宛先ポート（67）で broadcast DHCPDISCOVER メッセージを送信すると、クライアントとして機能します。
- IPv6 プレフィックス割り当ての場合、UPF から DHCPv6 サーバーへのすべてのメッセージに、要求された 64 のプレフィックス長 の IA_PD オプションが含まれます。

5. **Offer または Advertise メッセージ**： IPv4 の場合、UPF は、DHCPv4 サーバーから、IPv4 アドレス、リース時間、およびサーバー識別子を含む **Offer** メッセージを受信します。

   IPv6 の場合、UPF は、DHCPv6 サーバーから、クライアント IPv6 アドレス、リース時間、およびサーバー識別子を含む、unicast **Advertise** メッセージを受信します。

6. **IPv4 および IPv6 検証**：UPF は、DHCP サーバーから受信した IP アドレスを検証します。検証プロセスは、要求された IP アドレスのタイプ（IPv4 または IPv6）によって異なります。

   - **IPv4 検証**： CLI **[no] skip-validation** が構成されている場合、UPF は、SMF に割り当てられた IPチャンクで受信した IPv4 アドレスを検証します。

     IPv4 検証が成功すると、UPF は要求メッセージを DHCP サーバーに送信します。IPv4 検証が失敗した場合、UPF は DHCPv4 サーバーに要求メッセージを送信せず、IPv4 アドレス割り当てプロセスは失敗します。

     IPv4v6 セッションの場合、IPv4 検証が失敗すると、UPF は、UE に割り当てられた IPv6 アドレスを使用して、コード **Partial Success** を含む Sx Session Establishment 応答を送信します。

   - **IPv6 検証**：CLI **enable ipv6-validation** が構成されている場合、UPF は、**要求**メッセージを DHCPv6 サーバーに送信します。DHCPv6 サーバーは、**Reply** メッセージを UPF に送信します。

     IPv6 の場合、プレフィックス検証は SARR ハンドシェイクで Reply メッセージを受信した後に行われます。

     IPv6 の検証に失敗した場合、UPF は DHCP v6 サーバーに DHCP DECLINE メッセージを送信して、UPF が DHCPv6 サーバーによって指定された IPv6 アドレスを使用しないことを示します。

     IPv4v6 セッションの場合、IPv6 検証が失敗すると、UPF は、UE に割り当てられた IPv4 アドレスを使用して、コード **Partial Success** を含む Sx Session Establishment 応答を送信します。

   IPv4 および IPv6 検証アドレスの基準とプロセスの詳細については、「DHCP サーバーと SMF からのIP アドレスの検証」項を参照してください。

7. **Renew と Rebind**：

   - **Renew 要求**：UPF は、割り当てられたリース時間が期限切れになると、リースの更新を試行します。この場合、UPF は割り当てられたリース時間の 50%（T1 しきい値）で DHCP サーバーに Renew 要求をユニキャストします。

     DHCP サーバーが Renew 要求に応答しない場合、UPF は最大再試行回数に達するまで Renew 要求を再試行します。

     サーバーが NAK（否定確認応答）で応答した場合は、リースを延長できないことを示しています。その後、UPF はコールを消去し、SMF に通知します。

     IPv6 アドレスの場合、Renew 要求は Reply パケットの T1 タイマー値になります。

   - **Rebind 要求**：最大再試行回数を超えても DHCP サーバーが Renew 要求に応答しない場合、割り当てられたリースが割り当てられたリース時間の 88%（T2 しきい値）に達すると、DHCP サーバーは Rebind 要求をブロードキャストします。

     DHCP サーバーが Rebind 要求に応答しない場合、UPF は再試行回数が上限に達するまで Rebind 要求を再試行します。最大再試行回数を超えても DHCP サーバーが応答せ

ず、割り当てられたリースの期限が切れた場合、コールは消去されます。UPF は、コールの削除について SMF に通知します。

サーバーが NAK に応答した場合は、リースを延長できないことを示しています。その後、UPF はコールを消去し、SMF に通知します。

IPv6 アドレスの場合、再バインドパケットは Reply パケットの T2 タイマー値になります。

T1 および T2 しきい値の値は設定可能です。

T1 および T2 しきい値の設定の詳細については、『*CLI*（コマンド ライン インターフェイス）リファレンス、モード *C - D*、*StarOS*』ガイドの「*DHCP Service Configuration Mode* コマンド」章を参照してください。

（注） Renew や Rebind のエラーを処理するには、EPFAR 構成が必須です。構成されていない場合、UPF は、ローカルパージを実行しますが、SMF と UPF 間で不一致が発生します。

8. **セッションの削除**：UPF はローカルにセッションを消去し、リース時間が期限切れになると、UPF が Session Report 要求でコールを削除したという通知を SMF に送信します。

   SMF は、N4 インターフェイス経由で PCRF Session Deletion 要求を UPF に送信します。UPF は、SMF から PFCP Session Deletion 要求メッセージを受信すると、DHCP サーバーに対して fire-and-forget DHCP release 要求を開始します。

DHCP サブネット選択基準

UPF は、次の条件に従って IPv4 サブネットを選択するために、UE IP Address Pool Identity IE を VLAN ID として解釈します。

N4 Session Establishment に以下が含まれている場合…	また **Create PDR IE** に以下が含まれている場合…	結果…
CHOOSE IPV4 ビットのみ	単一の UE IP Address Pool Identity IE	UPF は、IPv4 IP アドレス割り当てのサブネットを識別する VLAN として解釈されます。
CHOOSE IPV4 ビットのみ	1 つ以上の UE IP Address Pool Identity IE	UPF は、UE IP Address Pool Identity IE の追加の発生を無視します。
CHOOSE IPV6 ビットのみ	単一の UE IP Address Pool Identity IE	UPF は、IPv6 IP アドレス割り当てのサブネットを識別する VLAN として解釈されます。
CHOOSE IPV6 ビットのみ	1 つ以上の UE IP Address Pool Identity IE	UPF は、UE IP Address Pool Identity IE の追加の発生を無視します。

N4 Session Establishment に以下が含まれている場合...	また Create PDR IE に以下が含まれている場合...	結果...
CHOSE IPV4 ビットと CHOSE IPV6 ビットの両方。	単一の UE IP Address Pool Identity IE	UPF が、「原因コード：必須 IE が正しくない」の Session Establishment 要求を拒否します。
CHOSE IPV4 ビットと CHOSE IPV6 ビットの両方。	2 つの UE IP Address Pool Identity IE	UPF は、最初と 2 番目の UE IP Address Pool Identity IE を VLAN として解釈し、IPv4 と IPv6 IP アドレス割り当てのサブネットをそれぞれ識別します。
CHOSE IPV4 ビットと CHOSE IPV6 ビットの両方。	2 つ以上の UE IP Address Pool Identity IE	UPF は、UE IP Address Pool Identity IE の追加の発生を無視します。

DHCP 構成の検証基準

DORA または SARR プロセスを開始する前に、UPF は次の検証を実行します。

- CHOSE IPV4 ビットと CHOSE IPV6 ビットのいずれかまたは両方が設定されている場合、IPv4 と IPv6 の両方の DHCP 設定は存在しません。それ以外の場合、UPF は、原因コード**「必須 IE が間違っています」**を SMF に送信します。
- CHOOSE IPV4 および CHOOSE IPV6 ビットのいずれかまたは両方が設定されているか、IPv4 アドレスまたは IPv6 アドレスが存在しない場合は、ローカル APN レベル構成である **ip address alloc-method dhcp-proxy** および **ipv6 address alloc-method dhcpv6-proxy** が、DHCPv4 と DHCPv6 それぞれに存在するはずです。それ以外の場合、UPF は原因コード**「IP 割り当てエラー」**を UPF に送信します。
- 受信した VLAN ID は、UPF の構成で IPv4 と IPv6 のいずれかまたは両方に存在するはずです。

  受信した VLAN ID が UPF 構成に存在しない場合、UPF は原因コード**「RESourCES がありません」**を SMF に送信します。
- DHCP サーバーの検出が無効で、DHCP サーバーの IP アドレスが構成されていないが、DHCPv4 サービスが実行されている場合、UPF は、原因コード**「RESources がありません」**を SMF に送信します。
- ユニキャストが有効で、DHCP サーバーの IP アドレスも構成されていないが、DHCPv6 サービスが実行されている場合、UPF は原因コード**「リソースがありません」**を SMF に送信します。
- スロット/ポートが存在し、設定内の IPv4 または IPv6 の正しいインターフェイスにリンクされている必要があります。それ以外の場合、UPF は原因コード**「IP 割り当てエラー」**を SMF に送信します。

- CHOSE IPV4 ビットと CHOSE IPV6 ビットのいずれかまたは両方が設定されている場合、v4 と v6 の DHCP 設定が有効である必要があります。DHCPv4 および DHCPv6 サービスを開始する必要があります。それ以外の場合、コールは拒否され、UPF は原因コード**「IP 割り当てエラー」**を UPF に送信します。

IPv4 および IPv6 アドレスの検証

UPF は、DORA または SARR プロセス中に SMF によって割り当てられたチャンクと、DHCP サーバーから受信した IPv4 または IPv6 アドレスを比較します。

DORA プロセス中の IPv4 検証

次の段階は、DORA ハンドシェイクプロセス中の IPv4 検証プロセスを示しています。

1. UE/CPE は DHCP Discover メッセージを UPF に送信します。
2. UPF は、クライアント IPv6 アドレス、リース時間、およびサーバー識別子と一緒に DHCPv4 サーバーから DHCP Offer メッセージを受信します。

   UPF は、受信した最初の Offer メッセージを受け入れ、別の DHCPv4 サーバーからの後続のすべての Offer メッセージを無視します。
3. UPF は、SMF から送信された IP プールチャンクで受信した IP アドレスを検証します。

IP 検証が...	結果
成功した場合	UPF は、DHCP 要求メッセージを DHCPv4 サーバーに送信し、DHCPv4 サーバーから DHCP 確認応答メッセージを受信します。
失敗した場合	UPF は、Offer メッセージを破棄し、DHCP 要求メッセージを DHCPv4 サーバーに送信しません。その後、UPF はセッションを拒否します。

4. UPF は DHCP サーバーから確認応答メッセージを受信します。UPF は、Offer と確認応答メッセージで受信した IP が同一であるかどうかを検証します。UPF は、リース検証、chadr 検証、サーバー識別子検証などの他の検証も実行します。

   Offer メッセージと確認応答メッセージで受信した IP 値が同じ場合、UPF は IP 検証が成功したと見なします。この場合、UPF は UE IP を SMF に転送します。

   Offer メッセージと確認応答メッセージで受信した IP アドレスが一致しない場合、UPF は IP 検証プロセスが失敗したと見なします。この場合、UPF は DHCP decline メッセージを DHCPv4 サーバーに送信し、セッションを削除します。

   IP アドレス検証を除き、オファーパケットと確認応答パケットの値に不一致がある場合、UPF は DHCP release メッセージを DHCPv4 サーバーに送信します。

SARR プロセス中の IPv6 検証

IPv6 セッションの場合、**enable ipv6-validation** が構成されていると、UPF は、SARR プロセス後に IPv6 検証を実行します。これらの段階は、IPv6 検証プロセスを示しています。

1. UPF は、Solicit メッセージを DHCPv6 サーバーに送信します。
2. UPF は、DHCPv6 サーバーから Advertise メッセージを受信します。
3. UPF は、要求メッセージを DHCPv6 サーバーに送信します。
4. UPF は、DHCPv6 サーバーから Reply メッセージを受信します。
5. UPF は、SMF から送信された IPv6 プールチャンクで受信した IPv6 アドレスを検証します。

IP 検証が...	結果
成功した場合	UPF は、受信した IPv6 アドレスを使用して正常な Establishment 応答を送信します。
失敗した場合	UPF は、DHCPv6 サーバーによって指定された IPv6 を UPF が使用しないことを示す DHCP DECLINE メッセージを DHCPv6 サーバーに送信します。 Establishment 要求は、IPv6 専用 PDN セッションを拒否します。Establishment 要求は、IPv4v6 PDN セッションに対する部分成功の原因コードで受け入れられます。

DHCP ベースの IP 割り当てを有効にする

UPF で DHCP ベースのIP 割り当てを有効にするために必要な手順は次のとおりです。

重要 DHCP機能を有効にする際には、最初にスタンバイ UPF でDHCP サービスを有効にしてから、アクティブな UPF で DHCP サービスを有効にすることを常にお勧めします。機能の CLI を変更した後、変更した設定を起動設定に保存して機能を有効にします。

既存のDNNに対してこの機能を有効にすると、進行中の通話でサービスの中断が発生します。新しい DNN に対してこの機能を有効にすると、新しい通話には常に DHCP サーバーからの IP 割り当てが設定されるため、サービスの中断は発生しません。

手順

ステップ 1 DHCP サービスを開始します。

ステップ 2 DHCP サーバーの検出を有効にするようにスロット/ポートを設定します。

DHCPv4 または DHCPv6 サービスを開始する

N4 Establishment には、CHV4 ビットまたは CHV6 メッセージビットと、SMF が IP アドレスを必要とすることを示す UE IP Address Pool Identity IE が含まれます。DHCP サーバーを介した IP 割り当てを有効にするには、UPF は DHCP サービスが有効になっていることを確認する必要があります。

したがって、UPF は、ローカルの APN レベルの設定を使用して、DHCP サーバーを使用した IP アドレス割り当てを実行します。

このタスクにより、DHCP プロキシベースの IP 割り当てを有効にするように APN を構成できます。

手順

ステップ 1 コマンド **context** *context_name* を使用して、コンテキストのインスタンスを作成します。

例：

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

ステップ 2 コマンド **apn** *apn_name* を使用して、APN 構成モードでインスタンスを作成します。

例：

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

（注） DHCPv4 では、DHCP コンテキスト名が、APN で構成されていない場合、構成された IP コンテキスト名が、DHCP コンテキストとして使用されます。

ステップ 3 コマンド **ip address alloc-method dhcp-proxy** または **ipv6 address alloc-method dhcpv6-proxy** を使用して、IPv4 および IPv6 用にそれぞれ、DHCP プロキシとして IP アドレス割り当てを定義します。

例：

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

（注） DHCPv4 では、DHCP サービス名が、APN で構成されていない場合、構成された IP コンテキスト名からの DHCP サービスまたは DHCP コンテキストが使用されます。

ステップ 4 コマンド **dhcp service-name** *dhcp_service_name* **| { dhcpv6 service-name** *dhcpv6_service_name* **server-profile** *dhcpv6_server_prof* **client-profile dhcpv6-client-prof }** を使用して、IPv4 または IPv6 に使用する DHCP サーバーを指定します。

例：

```
[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
```

ステップ 5 コマンド **bind address** *dhcp/dhcpv6_ip_address* を使用してコンテキスト構成モードで、UPF インターフェイスをバインドします。現在の構成モードを保存して、終了します。

例：

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

この構成は、DHCP サービスを開始し、アドレス割り当てメソッドを DHCP プロキシとして定義します。

次のタスク

スロット/ポートを構成して、DHCP サーバーにブロードキャストメッセージを送信します。詳細については、「スロット/ポートを構成して DHCP セールスフォースの検出を有効にする」項を参照してください。

スロット/ポートを構成して DHCP サーバーの検出を有効にする

このタスクは、DHCP サーバーにブロードキャストメッセージを送信するように UPF のスロットまたはポートを構成するのに役立ちます。

（注） スロット/ポートが構成されている場合、UPF はブロードキャストメッセージを送信します。ただし、スロット/ポートが構成されていない場合は、DHCP サーバーの IP アドレスを設定する必要があります。この場合、UPF はユニキャストパケットを送信します。

始める前に

DHCP サーバーの検出を有効にするようにスロットを構成する前に、IPv4 の DHCP サービスを有効にする必要があります。詳細については、項を参照してください。

手順

ステップ 1 コマンド **context** *context_name* を使用して、コンテキスト構成モードに入り、インスタンスを作成します。

例：

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

ステップ 2 UPF が DHCP または DHCPv6 サーバーに接続する際に経由するスロット/ポートを構成します。

a) **DHCPv4の場合**：コマンド **dhcp-service** *dhcp_service_name* **dhcp server enable-discover slot/port** *slot_port_number* **dhcp-node-id** *node_id* を使用して、コンテキスト構成モードでスロット/ポートを構成します。

例：

```
[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)#
```

（注）
- SMF が IPv4 と IPv6 の両方のコールに同じ VLAN ID を送信する場合、IPv4 と IPv6 のスロットとポートの構成は両方のコールで同じである必要があります。
- VLAN 構成は、すべての UPF ノードで同じである必要があります。

b) **DHCPv6 の場合**：コンテキスト構成モードで、CLI **dhcp-server-profile** *dhcpv6_server_prof* **{ enable | disable } dhcpv6-server-unicast** を使用して、DHCPv6 サーバーの [サーバーユニキャスト（server unicast）] オプションを有効または無効にします。また、CLI **dhcp-client-profile** *dhcpv6-client-prof* **{ enable | disable } dhcpv6-client-unicast slot/port***slot_port_number* を使用して、特定のスリットやポートの DHCPv6 の [クライアントユニキャスト（client unicast）] オプションを有効または無効にします。

例：

```
[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)#
```



重要 CLI **disable dhcpv6-client-unicast** を使用するには、「Unicast Address Support for DHCPv6 Messages」ライセンスが必要です。

CLI **slot/port** *slot_port_number* を使用するには、UPF ライセンスが必要です。

ライセンスの詳細については、シスコのアカウント担当者にお問い合わせください。

ステップ 3 受信した IPv4 アドレスと IPv6 アドレスのいずれかまたは両方の IP 検証を無効または有効にします。

a) **IPv4 の場合**：コマンド **[no] dhcp ip skip-validation** を使用して、DHCP サーバーから受信した IPv4 アドレスの検証をスキップします。これは任意のコマンドです。

例：

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

b) **IPv6 の場合**：コマンド **disable ipv6-validation** を使用して、DHCP サーバーから受信した IPv6 アドレスの IP 検証プロセスを無効にします。

例：

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

ステップ 4 コマンド **dhcp lease-expiration-policy { auto-renew | disconnect }** を使用して、IP アドレスのリースが期限切れになった場合の必要なアクションを構成します。

例：

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

ステップ 5 IPv4 または IPv6 の DHCP サービスの状態を確認します。

a) **IPv4 の場合**：CLI **show dhcp-service all** を使用して、すべての IPv4 DHCP サービスの状態を確認します。

例：

```
[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) コマンド **show dhcpv6-client-profile { all | name }** *client-profile-name* を使用して、IPv6 サービスの状態を検証します。

例：

```
[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
```

このタスクにより、スロットまたはポート番号を使用して DHCPv4 および DHCPv6 サーバーの検出が可能になります。

制限事項

APN が DHCP サービスにリンクされ、DHCP サービスが APN にリンクされたコンテキストとは異なるコンテキストで定義されている場合、DORA プロセスは発生しません。

異なるコンテキスト間で複数の APN があるデプロイメントでは、各コンテキスト内で個別の DHCP サービスを設定する必要があります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。