



IPv6 機能

この章では、Cisco SD-WAN テンプレートとポリシーの IPv6 機能を有効にするオプションについて説明します。展開で IPv6 を使用する場合は、この章の情報を使用してください。

インターフェイスまたはサブインターフェイス テンプレートの IPv6 機能の設定

インターフェイスまたはサブインターフェイス テンプレートの IPv6 機能を設定するには、次の手順を実行します。

Cisco SD-WAN でのデュアルスタックのサポート：同じ展開で IPv4 と IPv6 を設定できます。インターフェイスごとに最大 3 つのグローバル IPv6 アドレスを設定できます。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. テンプレートのリストから [Cisco VPN Interface Ethernet] を選択します。
4. [Basic Configuration] で、[IPv6] をクリックし、次の表に記載されているパラメータを設定します。

パラメータ名	説明
スタティック	IPv6 アドレスは固定であるため、このラジオボタンはデフォルトで選択されています。
IPv6 Address	インターフェイスまたはサブインターフェイスの IPv6 アドレスを入力します。

CLI の同等の設定：

```
interface GigabitEthernet1
  no shutdown
  ipv6 address 2001:DB8:1::1/64
  ipv6 enable
```

OMP テンプレートの IPv6 機能の設定

オーバーレイ管理プロトコル（OMP）テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. テンプレートのリストから [Cisco OMP] を選択します。
4. [Advertise] をクリックし、[IPv6] を選択して、次の表に示すパラメータを設定します。

パラメータ名	説明
接続済み	OMP への接続ルートのアドバタイズを無効にするには、[Off] をクリックします。 デフォルトでは、接続ルートは OMP にアドバタイズされます。
スタティック	OMP へのスタティックルートのアドバタイズを無効にするには、[Off] をクリックします。 デフォルトでは、スタティックルートは OMP にアドバタイズされます。
BGP	BGP ルートを OMP にアドバタイズするには、[On] をクリックします。デフォルトでは、BGP ルートは OMP にアドバタイズされません。

CLI の同等の設定：

まず、IPv6 のサービス VRF を有効にします。

```
config-transaction
vrf definition 1
  rd 1:1
  address-family ipv6
```

次に OMP を有効にします。

OMP ではグローバル IPv6 設定がサポートされます。また、VRF レベルごとの設定が可能です。VRF レベルごとの設定により、グローバル設定はオーバーライドされます。

```

config-transaction
sdwan
  omp
  !
  address-family ipv6
    advertise bgp
    advertise connected

  address-family ipv6 vrf 1
    advertise static

```

グローバル設定がデフォルトの設定であるため、IPv6 は OMP に対してデフォルトで有効になっています。特定の VRF の IPv6 OMP ルート再配布を無効にするには、次のように再配布プロトコルを **no** に設定します。

```

config-transaction
sdwan
  omp
  !
  address-family ipv6
    advertise bgp
    advertise connected

  address-family ipv6 vrf 1
    no advertise connected
    no advertise static
    no advertise bgp

```

BGP テンプレートの IPv6 機能の設定

ボーダー ゲートウェイ プロトコル (BGP) テンプレートの IPv6 機能を設定するには、次の手順を実行します。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. テンプレートのリストから [Cisco BGP] を選択します。
4. [Unicast Address Family] をクリックし、[IPv6] を選択して、次の表に示すパラメータを設定します。

タブ	パラメータ名	説明
	Maximum Paths	IBGP マルチパス ロードシェアリングを有効にするために、ルートテーブルにインストールできるパラレル IBGP パスの最大数を指定します。範囲：0 ~ 32
	Address Family	BGP IPv6 ユニキャストアドレスファミリーを入力します。

タブ	パラメータ名	説明
RE-DISTRIBUTE		[Redistribute] タブをクリックし、[Add New Redistribute] をクリックします。
	プロトコル	すべての BGP セッションでルートを BGP に再配布するプロトコルを選択します。オプションは、[Connected]、[NAT]、[OMP]、[OSPF]、および [Static] です。少なくとも、次のように選択します。 <ul style="list-style-type: none"> サービス側 BGP ルーティングの場合は、[OMP] を選択します。デフォルトでは、OMP ルートは BGP に再配布されません。 トランスポート側 BGP ルーティングの場合は、[Connected] を選択し、[Route Policy] で、BGP がループバック インターフェイスアドレスをネイバーにアドバタイズするルートポリシーを指定します。
	ルート ポリシー (ルート ポリシー)	再配布されるルートに適用するルートポリシーの名前を入力します。
		[Add] をクリックして再配布情報を保存します。
NETWORK		[Network] タブをクリックし、[Add New Network] をクリックします。
	[Network Prefix]	BGP によってアドバタイズされるネットワークプレフィックスを <i>prefix/length</i> の形式で入力します。
		[Add] をクリックして、ネットワークプレフィックスを保存します。
AGGREGATE ADDRESS		[Aggregate Address] タブをクリックして、[Add New Aggregate Address] をクリックします。
	[Aggregate Prefix]	すべての BGP セッションに対して集約するアドレスのプレフィックスをプレフィックス/長さの形式で入力します。
	[AS Set Path]	集約されたプレフィックスの設定パス情報を生成するには、[On] をクリックします。
	[Summary Only]	BGP 更新から詳細ルートを除外するには、[On] をクリックします。
		[Add] をクリックして、集約アドレスを保存します。

1. [Neighbor] 領域で、[IPv6] をクリックし、新しいネイバーを作成するか、既存のネイバーを編集して、次の表に記載されているパラメータを設定します。

アスタリスクの付いたパラメータは必須です。

パラメータ名	説明
IPv6 Address*	BGP ネイバーの IPv6 アドレスを指定します。
説明	BGP ネイバーの説明を入力します。
Remote AS*	リモート BGP ピアの AS 番号を入力します。
Address Family	ドロップダウンリストから [Global] を選択し、[On] をクリックしてアドレスファミリーを選択します。アドレスファミリー情報を入力します。
シャットダウン	テンプレートをプッシュするときに BGP ネイバーをシャットダウンする場合は、ドロップダウンリストから [Global] を選択し、[Yes] をクリックします。 デフォルト：[Off]

CLI の同等の設定：

```
config-transaction
router bgp 1
  bgp log-neighbor-changes
  address-family ipv6 unicast vrf 1
  neighbor 2001:DB8:19::1 remote-as 2
  neighbor 2001:DB8:19::1 activate
  neighbor 2001:DB8:19::1 advertisement-interval 1
  neighbor 2001:DB8:19::1 password cisco
  redistribute omp
  redistribute static
  exit-address-family
```

VRRP テンプレートの IPv6 機能の設定

Virtual Router Redundancy Protocol (VRRP) テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. テンプレートのリストから [Cisco VPN Interface Ethernet] を選択します。
4. [VRRP] をクリックし、[IPv6] を選択します。
5. [New VRRP] をクリックします。

6. 次の表に示すパラメータを設定します。

パラメータ名	説明
グループ ID (Group ID)	ルータのグループを表す仮想ルータ ID を入力します。 範囲： 1 ~ 255
プライオリティ	VRRP グループ内のルータの優先度を入力します。 <ul style="list-style-type: none"> • 範囲：1 ~ 254 • デフォルト：100
Timer	未使用です。
Track OMP	プライマリ VRRP 仮想ルータを決定するとき、WAN 接続で実行されているオーバーレイ管理プロトコル (OMP) セッションをトラッキングする場合は、[On] を選択します。デフォルト：[Off]
Track Prefix List	IPv6 リモートプレフィックスのリストをトラッキングするための値を入力します。この値は、ポリシーで設定されている英数字の文字列です。
Link Local IPv6 Address	グループのリンクローカルアドレスを表す仮想リンクローカル IPv6 アドレスを入力します。アドレスは、標準のリンクローカルアドレス形式になっている必要があります。たとえば、FE80::AB8 です。
Global IPv6 Address	グループのグローバルアドレスを表す仮想グローバルユニキャスト IPv6 アドレスを入力します。このアドレスは、VRRP グループが設定されているインターフェイス転送アドレスと同じマスクを持つ IPv6 グローバルプレフィックス アドレスである必要があります。たとえば、2001::2/124 です。 最大 3 つのグローバル IPv6 アドレスを設定できます。

CLI の同等の設定：

```

config-transaction
interface GigabitEthernet1

  vrrp 10 address-family ipv6
    priority 20
    track omp shutdown
    address FE80::10:100:1 primary
    address 2001:10:100::1/64

Prefix-list tracking
track 1 ipv6 route 1:1::1/128
  reachability
  ipv6 vrf 1

```

```

track 2 ipv6 route 2:2::2/128
reachability
ipv6 vrf 2

track 20 list boolean or
  object 1
  object 2

vrrp 10 address-family ipv6
  track 20 shutdown

```

SNMP テンプレートの IPv6 機能の設定

SNMP テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. テンプレートのリストから [Cisco SNMP] をクリックします。
4. [SNMP Version] > [TRAP TARGET SERVER] を選択し、SNMP トラップターゲットを作成または編集します。
5. 次の表に示すパラメータを設定します。

パラメータ名	説明
VPN ID	トラップサーバーに到達するために使用する VPN の番号を入力します。範囲：0 ~ 65530。
IP アドレス	SNMP サーバーの IP アドレスを入力します。
UDP Port	SNMP サーバーに接続するための UDP ポート番号を入力します。範囲：1 ~ 65535。
Trap Group Name	[Group] タブで設定したトラップグループの名前を選択します。
User Name	[Community] タブで設定されたコミュニティの名前を選択します。
Source Interface	トラップ情報を受信している SNMP サーバーにトラップを送信するために使用するインターフェイスを入力します。



- (注) SNMP コミュニティとトラップターゲットグループがすでに設定されていることを確認してください。

CLI の同等の設定 :

次に、コミュニティストリング **public** を使用して、SNMP が読み取り専用アクセス権ですべてのオブジェクトにアクセスすることを許可する例を示します。また、デバイスは **SNMP v1** を使用して、ボーダーゲートウェイプロトコル (BGP) トラップ IPv6 ホスト **3ffe:b00:c18:1::3/127** を送信します。 **public** という名前のコミュニティ文字列が、トラップとともに送信されます。

```
デバイス# config-transaction
デバイス(config)# snmp-server community public
デバイス(config)# snmp-server enable traps bgp
デバイス(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

次に、SNMP コンテキスト **A** を **SNMPv2c** グループ **GROUP1** のビューと **IPv6** の名前付きアクセスリスト **public2** に関連付ける例を示します。

```
デバイス# config-transaction
デバイス(config)# snmp-server context A
デバイス(config)# snmp mib community-map commA context A target-list comm AVpn
デバイス(config)# snmp mib target list commAVpn vrf CustomerA
デバイス(config)# snmp-server view viewA ciscoPingMIB included
デバイス(config)# snmp-server view viewA ipForward included
デバイス(config)# snmp-server group GROUP1 v2c contextA read viewA write viewA notify
access ipv6 public2
```

次に、IPv6 ホストを通知サーバとして設定する例を示します。

```
デバイス> enable
デバイス# config-transaction
デバイス(config)# snmp-server community mgr view restricted rw ipv6 mgr2
デバイス(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
デバイス(config)# snmp-server group publicv2c access ipv6 public2
デバイス(config)# snmp-server hosthost1.com2c vrf trap-vrf mgr
デバイス(config)# snmp-server user user1 bldg1 remote3ffe:b00:c18:1::3/127 v2c access ipv6
public2
デバイス(config)# snmp-server enable traps bgp
デバイス(config)# exit
```

DHCP リレー エージェント テンプレートの IPv6 機能の設定

DHCP リレー エージェント テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. テンプレートのリストから [Cisco VPN Interface Ethernet] を選択します。
4. [Basic Configuration] で、[IPv6] をクリックします。
5. [DHCP Helper] の横にある [Add] をクリックします。
6. 次の表に示すパラメータを設定します。

表 1:

パラメータ名	説明
DHCPv6 Helper #	DHCP ヘルパーの IP アドレス
DHCPv6 Helper VPN	DHCP ヘルパーの VPN 送信元インターフェイスの VPN ID。

CLI の同等の設定 :

```
device-configuration
interface GigabitEthernet8
vrf forwarding 2
no ip address
ipv6 address 2001:A14:99::F/64
ipv6 dhcp relay destination vrf 1 2001:A14:19::12 GigabitEthernet2
```

ACL テンプレートまたは QoS テンプレートの IPv6 機能の設定

ACL および QoS テンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックし、[Add Template] をクリックして適切なデバイスモデルを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. テンプレートのリストから [Cisco VPN Interface Ethernet] を選択します。
4. [ACL/QoS] で、次の表に示すパラメータを設定します。

パラメータ名	説明
入力 ACL - IPv6	[On] をクリックして、IPv6 入力アクセスリストを有効にします。

パラメータ名	説明
IPv6 Ingress Access List	IPv6 入力アクセスリストの名前を入力します。
出力 ACL – IPv6	[On] をクリックして、IPv6 出力アクセスリストを有効にします。
IPv6 Egress Access List	IPv6 出力アクセスリストの名前を入力します。

ACL テンプレートの IPv6 機能の設定に相当する CLI :

```

デバイス(config)# policy
デバイス(config-policy)# ipv6
デバイス(config-ipv6)# access-list ipv6_acl
デバイス(config-access-list-ipv6_acl)# sequence 11
デバイス(config-sequence-11)# match
デバイス(config-match)# source-ip 2001:380:1::64/128
デバイス(config-match)# destination-ip 2001:3c0:1::64/128
デバイス(config-match)# source-port 4000
デバイス(config-match)# destination-port 3000
デバイス(config-match)# traffic-class 6
デバイス(config-match)# next-header 6
デバイス(config-match)# packet-length 1000
デバイス(config-match)# action accept
デバイス(config-action)#

デバイス(config)# sdwan interface GigabitEthernet6 ipv6 access-list ipv6_acl in
デバイス(config-interface-GigabitEthernet6)#
デバイス(config-interface-GigabitEthernet6)#

デバイス(config)# policy lists data-ipv6-prefix-list source_ipv6_list
デバイス(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64

デバイス(config)# policy
デバイス(config-policy)# ipv6
デバイス(config-ipv6)# access-list ipv_ipv6_prefix
デバイス(config-access-list-ipv_ipv6_prefix)# sequence 11
デバイス(config-sequence-11)# match
デバイス(config-match)# source-data-prefix-list data-ipv6-prefix-list
デバイス(config-match)# destination-data-prefix-list source_ipv6_list
デバイス(config-match)# destination-ip 2001:3c0:1::64/128
デバイス(config-match)# source-port 4000
デバイス(config-match)# destination-port 3000
デバイス(config-match)# traffic-class 6
デバイス(config-match)# next-header 6
デバイス(config-match)# packet-length 1000
デバイス(config-match)# !
デバイス(config-match)# action accept

```

QoS テンプレートの IPv6 機能の設定に相当する CLI :

```

デバイス(config)# class-map match-any class0
デバイス(config-cmap)# match qos-group 0
デバイス(config-cmap)# class-map match-any class1

```

```

デバイス(config-cmap)# match qos-group 1
デバイス(config-cmap)# !
デバイス(config-cmap)# policy-map qos_map_for_data_policy
デバイス(config-pmap)# class class0
デバイス(config-pmap-c)# bandwidth percent 10
デバイス(config-pmap-c)# random-detect
デバイス(config-pmap-c)# class class1
デバイス(config-pmap-c)# bandwidth percent 10
デバイス(config-pmap-c)# random-detect
デバイス(config-pmap-c)#
デバイス(config-pmap-c)# policy
デバイス(config-policy)# no app-visibility
デバイス(config-policy)# class-map
デバイス(config-class-map)# class class0 queue 0
デバイス(config-class-map)# class class1 queue 1
デバイス(config-class-map)# !
デバイス(config-class-map)# ipv6
デバイス(config-ipv6)# access-list fwd_class_data_policy
デバイス(config-access-list-fwd_class_data_policy)# sequence 5
デバイス(config-sequence-5)# match
デバイス(config-match)# traffic-class 0
デバイス(config-match)# !
デバイス(config-match)# action accept
デバイス(config-action)# count fwd_class_data_policycnt_5
デバイス(config-action)# class class0
デバイス(config-action)# !
デバイス(config-action)# !
デバイス(config-action)# sequence 6
デバイス(config-sequence-6)# match
デバイス(config-match)# traffic-class 1
デバイス(config-match)# !
デバイス(config-match)# action accept
デバイス(config-action)# count fwd_class_data_policycnt_6
デバイス(config-action)# class class1
デバイス(config-action)# !
デバイス(config-action)# !
デバイス(config-action)# !
デバイス(config-action)# default-action drop

class-map match-any class0
match qos-group 0
class-map match-any class1
match qos-group 1
!
policy-map qos_map_for_data_policy
class class0
bandwidth percent 10
random-detect
class class1
bandwidth percent 10
random-detect

policy
no app-visibility
class-map
class class0 queue 0

```

```

class class1 queue 1
!
ipv6
access-list fwd_class_data_policy
sequence 5
match
traffic-class 0
!
action accept
count fwd_class_data_policycnt_5
class class0
!
sequence 6
match
traffic-class 1
!
action accept
count fwd_class_data_policycnt_6
class class1
!
default-action drop

```

ロギングテンプレートの IPv6 機能の設定

ロギングテンプレートの IPv6 機能を設定するには、次の手順に従います。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Feature Templates]** をクリックし、**[Add Template]** をクリックして適切なデバイスモデルを選択します。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** のタイトルは **[Feature]** です。

3. テンプレートのリストから **[Cisco Logging]** を選択します。
4. **[Server]** で、**[IPv6]** をクリックします。
5. 次の表に示すパラメータを設定します。

パラメータ名	説明
IPv6 Hostname/IPv6 Address	ロギング情報を送信するサーバーのホスト名または IP アドレス。
VPN ID	VPN 送信元インターフェイスの VPN ID。
Source Interface	送信元インターフェイスの名前。
プライオリティ	ログに記録されるメッセージの最大重大度を選択します。

CLI の同等の設定 :

```
config-transaction
デバイス(config)# logging host ipv6
AAAA:BBBB:CCCC:DDDD::FFFF
```



- (注) 同じトランザクションでロギングホスト設定を作成および削除すると、予期しない動作が発生します。たとえば、同じトランザクションで **logging host ipv6-address** を削除し、**logging host ipv6-address vrf vrf-name** 設定を作成すると、両方の設定がデバイスから消えます。2つのリクエストを別々のトランザクションで送信することをお勧めします。

新しいプレフィックスリストの IPv6 機能の設定

新しいプレフィックスリストの IPv6 アドレスを設定するには、次の手順に従います。

1. Cisco vManage メニューから、**[Configuration]** > **[Policies]** を選択します。
2. **[Custom Options]** ドロップダウンリストから、**[Lists]** を選択します。**[Centralized Policy]** または **[Localized Policy]** に対してこの選択を行うことができます
3. 左側のリストから **[Prefix]** を選択し、**[New Prefix List]** を選択します。
4. **[IPv6]** をクリックし、**[Add Prefix]** に IPv6 アドレスを入力します。

CLI の同等の設定 :

```
config-transaction
デバイス(config)# policy
デバイス(config-policy)# ipv6
デバイス(config-ipv6)# access-list ipv6_acl
デバイス(config-access-list-ipv6_acl)# sequence 11
デバイス(config-sequence-11)# match
デバイス(config-match)# source-ip 2001:380:1::64/128
デバイス(config-match)# destination-ip 2001:3c0:1::64/128
```

データプレフィックスの IPv6 機能の設定

新しいプレフィックスリストの IPv6 アドレスを設定するには、次の手順に従います。

1. Cisco vManage のメニューから **[Configuration]** > **[Policies]** を選択します。
2. **[Custom Options]** ドロップダウンリストから、**[Lists]** を選択します。**[Centralized Policy]** または **[Localized Policy]** に対してこの選択を行うことができます
3. 左側のリストから **[Data Prefix]** を選択し、**[New Data Prefix List]** を選択します。
4. **[Internet Protocol]** で **[IPv6]** をクリックし、**[Add Prefix]** に IPv6 アドレスを入力します。

CLI の同等の設定 :

```
デバイス(config)# policy lists data-ipv6-prefix-list source_ipv6_list
デバイス(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64
```

一元化されたポリシーの IPv6 機能の設定

IPv6 アドレスファミリーに適用する一元化されたポリシーを設定するには、次の手順に従います。

1. Cisco vManage のメニューから [Configuration] > [Policies] を選択します。
2. [Custom Options] ドロップダウンメニューの [Centralized Policy] で [Traffic Policy] を選択します。
3. [Traffic Data] を選択します。
4. [Add Policy] をクリックし、[Create New] をクリックします。
5. [Sequence Type] をクリックし、[Traffic Engineering] を選択します。
6. [Sequence Rule] をクリックします。
7. [Protocol] ドロップダウンリストから、[IPv6] を選択してポリシーを IPv6 アドレスファミリーのみに適用するか、[Both] を選択してポリシーを IPv4 および IPv6 アドレスファミリーを適用します。
8. [Sequence Type] をクリックし、[QoS] を選択します。
9. [Sequence Rule] をクリックします。
10. [Protocol] ドロップダウンリストから、[IPv6] をクリックしてポリシーを IPv6 アドレスファミリーのみに適用するか、[Both] を選択してポリシーを IPv4 および IPv6 アドレスファミリーを適用します。

CLI の同等の設定 :

```
config-transaction
(config)# policy
(config-policy)# lists ipv6-prefix-list foo ipv6-prefix 1::1/64
                ipv6-prefix-list ipv6-1
                ipv6-prefix 1::1/128
```

ローカライズされたポリシーの IPv6 機能の設定

IPv6 アドレスファミリーに適用するローカライズされたポリシーを設定するには、次の手順に従います。

1. Cisco vManage のメニューから [Configuration] > [Policies] を選択します。
2. [Custom Options] ドロップダウンリストの [Localized Policy] で [Access Control Lists] を選択します。
3. [Add Access Control List Policy] をクリックし、[Add IPv6 ACL Policy] を選択します。作成したポリシーは、IPv6 アドレスファミリーにのみ適用されます。

CLI の同等の設定 :

次の例では、marketing という名前のプレフィックスリストで指定されたアドレスを持つ IPv6 ルートが一致します。

```

config-transaction
デバイス(config)# route-map name
デバイス(config-route-map)# match ipv6 address prefix-list marketing

```

- [DHCP for IPv6 \(15 ページ\)](#)

DHCP for IPv6

表 2:機能の履歴

機能名	リリース情報	説明
DHCP for IPv6	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	<p>この機能を使用すると、Cisco IOS XE SD-WAN デバイスで DHCP for IPv6 (DHCPv6) を構成して、IPv6 アドレスを IPv6 対応ネットワーク上のホストに割り当てることができます。</p> <p>IPv6 アドレスの割り当ては、SLAAC、DHCPv6、DHCPv6 プレフィックス委任、または DHCPv6 リレーを使用して行われます。</p> <p>Cisco IOS XE SD-WAN デバイスは、DHCPv6 用に DHCP サーバー、DHCP クライアント、または DHCP リレーエージェントとして設定できます。</p>

DHCPv6 の前提条件

- Cisco IOS XE SD-WAN デバイスに接続されたホストに IPv6 アドレスを割り当てるための基本的な IPv6 接続。

DHCPv6 の制約事項

- この機能は、CLI 設定を使用する場合のみサポートされます。
- VRF ごとに一意の DHCPv6 プール名を指定する必要があります。

DHCPv6 に関する情報

IPv6 の Dynamic Host Configuration Protocol (DHCP) を設定して、IPv6 対応ネットワークにアドレスを割り当てることができます。または、Stateless Address Autoconfiguration (SLAAC) を設定して、IPv6 対応ネットワークにアドレスを割り当てすることもできます。

SLAAC

IPv6 クライアントアドレス割り当て用の最も一般的な方法は、SLAAC です。SLAAC はホストが IPv6 プレフィックスに基づいてアドレスを自己割り当てするシンプルなプラグアンドプレイ接続を提供します。

SLAAC は次のように設定されます。

- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータアドバタイズメント (RA) メッセージを待機します。
- ホストは、RA メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス (イーサネットの場合、MAC アドレスから作成されます) と組み合わせて、グローバルユニキャストメッセージを作成します。ホストは、デフォルトゲートウェイとして、RA メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出 (DAD) は、選択されるランダムアドレスが他のクライアントと重複しないように、IPv6 クライアントによって実行されます。
- アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

次の 2 種類のアプローチに基づいて IPv6 アドレスの最後の 64 ビットが学習可能です。

- インターフェイスの MAC アドレスに基づく EUI-64、または
- ランダムに生成されるプライベートアドレス。

SLAAC および DHCPv6

DHCPv6

IPv6 デバイスはマルチキャストを使用して IP アドレスを取得し、DHCPv6 サーバを見つけます。DHCPv6 クライアント/サーバの基本概念は、IPv4 の DHCP に似ています。クライアントが設定パラメータを受信する必要がある場合は、接続しているローカルネットワークで要求を送信し、利用可能な DHCPv6 サーバを検出します。サーバは要求された情報を応答メッセージで返します。

DHCPv6 クライアントは、リンクローカル ネットワーク上のルータからの指示に基づいて DHCPv6 を使用するかどうかを認識します。デフォルトゲートウェイの RA には、この目的で使用できる 2 つの設定可能なビットがあります。

- **O ビット**：このビットを設定すると、クライアントは自身の IP アドレスではなく、その他の設定パラメータ（たとえば、TFTP サーバーアドレスまたは DNS サーバーアドレス）を取得するために DHCPv6 を使用できます。
- **M ビット**：このビットを設定すると、クライアントは DHCPv6 サーバから管理対象 IPv6 アドレスとその他の設定パラメータを取得するために DHCPv6 を使用できます。

ステートレス DHCP

ステートレス DHCPv6 は、SLAAC と DHCPv6 の組み合わせです。このオプションでは、IP アドレスを取得するために SLAAC を使用し、TFTP サーバーアドレスまたは DNS サーバーアドレスなどの追加情報を取得するために DHCP を使用します。この場合、デバイスは O ビットが設定された RA を送信しますが、M ビットは設定しません。DHCPv6 サーバーがクライアントアドレスバインディングを追跡する必要がないため、これはステートレス DHCPv6 と呼ばれます。

ステートフル DHCP

ステートフル DHCPv6 は、ホストが IPv6 アドレスと追加パラメータの両方を DHCP サーバーから受信する DHCP IPv4 とまったく同じように機能します。M ビットが設定された RA をデバイスが送信する場合、クライアントは DHCP を使用して自身の IP アドレスを取得する必要があります。M ビットが設定されている場合、DHCP サーバはアドレスとともに他の設定情報も返すので、O ビットの設定は意味がありません。DHCPv6 サーバーがクライアントアドレスバインディングを追跡するため、これはステートフル DHCPv6 と呼ばれます。

DHCPv6 プレフィックス委任

DHCPv6 プレフィックス委任機能は、委任側エッジデバイス（DHCP サーバー）から要求側エッジデバイス（DHCP クライアント）にプレフィックスを単純に委任するためのステートフルな動作モードです。

DHCPv6 プレフィックス委任機能は、次のような状況に最適です。

- 要求側のエッジデバイスが接続されているネットワークのトポロジに関する情報を持たない委任側のエッジデバイス。
- 委任するプレフィックスを選択するために要求側のエッジデバイスの ID 以外の情報を必要としない委任側のエッジデバイス。このメカニズムは、ISP がプレフィックスをサブスクライバに委任するために使用するのに適しています。ISP がプレフィックスをサブスクライバに委任した後、サブスクライバはプレフィックスをさらにサブネット化してサブスクライバのネットワーク内のリンクに割り当てることができます。

DHCPv6 リレー

DHCPv6 リレーエージェントは、クライアントのネットワーク上にあるエッジデバイスであり、DHCPv6 サーバーが DHCPv6 クライアントと同じネットワークにない場合に、クライアントとサーバーの間でメッセージをリレーするために使用されます。

DHCPv6 の利点

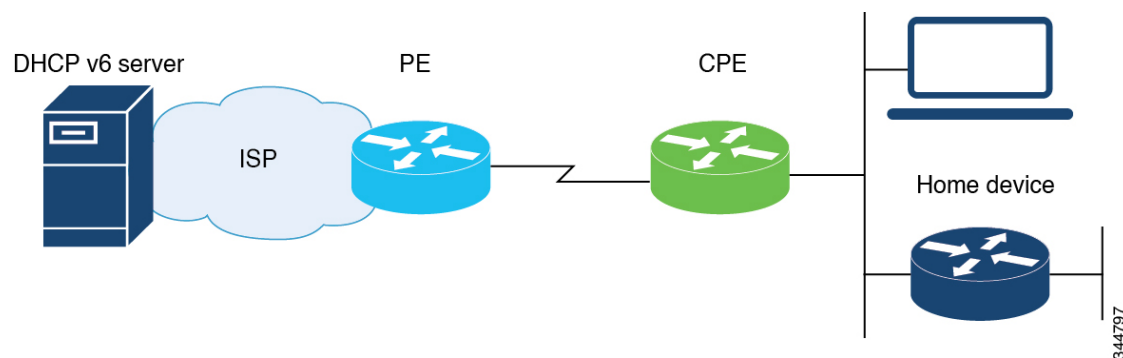
IPv6 用に DHCP を設定すると、IPv4 と比較してより多くの IP アドレスを持つことができます。IPv6 では、IP アドレスが枯渇することはありません。

DHCPv6 の使用例

Cisco IOS XE SD-WAN デバイスは、サーバー、クライアント、またはリレーエージェントとして DHCPv6 用に設定できます。サーバーとして、Cisco IOS XE SD-WAN デバイスは SLAAC、ステートレス DHCP、またはプレフィックス委任に設定できます。

DHCP を使用した SLAAC

次の図に、一般的なブロードバンド展開を示します。



顧客宅内（CPE）に展開され、ISP エッジ（PE）デバイスに接続されている Cisco IOS XE SD-WAN デバイスは、ステートレスまたはステートフルな DHCPv6 クライアントにすることができます。どちらの場合も、ISP 側の DHCPv6 サーバは、ドメインネームシステム（DNS）サーバアドレス、ドメイン名、Simple Network Time Protocol（SNTP）サーバなどの設定パラメータを CPE 上の DHCP クライアントに提供できます。このような情報は ISP に固有です。

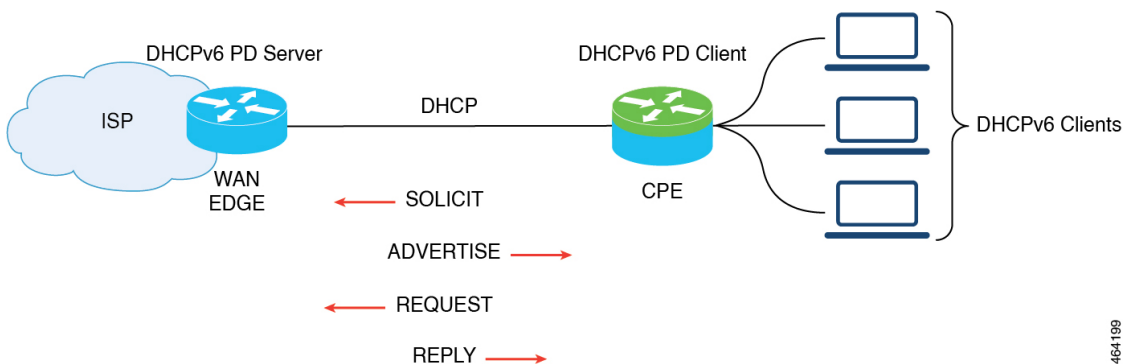
CPE は、DHCPv6 クライアント（ISP に対するクライアント）であるだけでなく、ホームネットワークに対する DHCPv6 サーバとして機能する場合があります。たとえば、ネイバー探索に続いて、ステートレスまたはステートフルの DHCPv6 クライアントが CPE とホームデバイスの間のリンクに現れることがあります。また、ホームネットワークに提供される情報は、ISP 側の DHCPv6 サーバから取得されたものと同じでなくなります。そのため、CPE 上の DHCPv6 コンポーネントでは、設定パラメータを DHCPv6 クライアントから DHCPv6 サーバプールに自動的にインポートできます。

DHCPv6 プレフィックス委任

プレフィックス委任の運用モデルは次のとおりです。このサンプルトポロジでは、エッジデバイスは、DHCP クライアントに委任されるプレフィックスでプロビジョニングされた DHCP サーバとして構成されています。Cisco IOS XE SD-WAN デバイスは DHCP クライアントとして構成され、サーバからのプレフィックスを要求します。サーバは、委任のプレフィッ

クスを選択し、DHCP クライアントにプレフィックスを付けて応答します。DHCP クライアントは、委任されたプレフィックスを担当します。

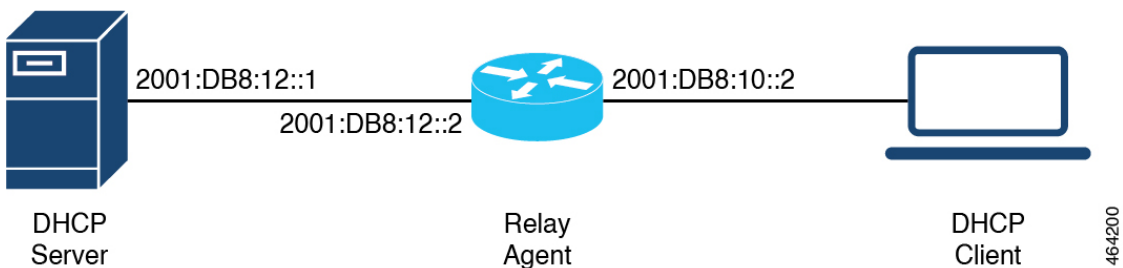
たとえば、クライアントは、委任されたプレフィックスからそのインターフェイスのいずれかにサブネットを割り当て、そのリンクのプレフィックスのルータアドバタイズメントの送信を開始できます。各プレフィックスには優先ライフタイムと有効なライフタイムが関連付けられており、クライアントがプレフィックスを使用できる時間の長さに関する合意が構成されます。クライアントは、委任されたプレフィックスのライフタイムの延長を要求でき、プレフィックスの有効なライフタイムが期限切れになった場合に委任されたプレフィックスの使用を終了する必要があります。



464199

DHCPv6 リレー

このサンプルトポロジでは、DHCP サーバーは DHCP クライアントと同じネットワークにありません。クライアントのネット上に常駐する Cisco IOS XE SD-WAN デバイスは、リレーエージェントとして動作し、クライアントとサーバー間のメッセージの中継に使用されます。



464200

DHCPv6 の設定

1. [Cisco vManage] メニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンから、[CLI Template] を選択します。



(注) CLI アドオンテンプレートを使用して、クライアントとサーバーの IPv6 の DHCP を構成することもできます。詳細については、「[Create a CLI Add-On Feature Template](#)」を参照してください。

4. [Device Model] から、テンプレートを作成するデバイスモデルを選択します。
5. [Template Name] フィールドに、デバイステンプレートの名前を入力します。このフィールドは必須で、使用できるのは、英大文字と小文字、0～9 の数字、ハイフン (-)、下線 (_) のみです。スペースやその他の文字を含めることはできません。
6. [Description] フィールドにデバイステンプレートの説明を入力します。このフィールドは必須であり、任意の文字とスペースを含めることができます。
7. [CLI Configuration] フィールドで、クライアントとサーバーの IPv6 の DHCP 構成を手入力するか、カットアンドペーストするか、ファイルをアップロードして入力します。
8. [Save] をクリックします。

SLAAC の設定

この例は、クライアント側で SLAAC を設定する方法を示しています。

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address autoconfig
device(config-if)# ipv6 enable
device(config-if)# end
```

この例は、サーバー側で SLAAC を設定する方法を示しています。

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# end
```

オプションの SLAAC および DHCPv6 プールの設定

次に、クライアント側で SLAAC および DHCPv6 プールを設定する例を示します。

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address autoconfig
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

次に、サーバー側で SLAAC および DHCPv6 プールを設定する例を示します。

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd other-config-flag
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
```

DHCPv6 (ステートフル) アドレス割り当ての設定

この例は、クライアント側で DHCPv6 アドレス割り当てを設定する方法を示しています。

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address dhcp
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

この例は、サーバー側で DHCPv6 アドレス割り当てを設定する方法を示しています。

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd managed-config-flag
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# address prefix 2010:AB8:0:1::1/64 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
```

プレフィックス委任を使用した DHCPv6 の設定 (ステートフル)

次に、クライアント側でプレフィックス委任を使用して DHCPv6 を設定する例を示します。

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client pd prefix_from_provider
```

```
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

次に、サーバー側でプレフィックス委任を使用して DHCPv6 を設定する例を示します。

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd managed-config-flag
device(config-if)# ipv6 nd ra interval 20
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# prefix-delegation pool dhcpv6-pool1 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
device(config)# ipv6 local pool dhcpv6-pool1 2001:DB8:1200::/40 48
```

リレーを使用した DHCPv6 の設定

次に、クライアント側でリレーを使用して DHCPv6 を設定する例を示します。

```
device(config)# interface GigabitEthernet3
device(config-if)# ipv6 address dhcp
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp client pd pr-from-pd
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# no mop enabled
device(config-if)# no mop sysid
device(config-if)# end
```

次に、リレーエージェントとして機能するクライアント側 WAN エッジデバイスの設定を示します。

```
device(config)# interface TenGigabitEthernet0/0/5
device(config-if)# vrf forwarding 10
device(config-if)# load-interval 30
device(config-if)# ipv6 address 2001:BB:1000::10/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp relay destination 2001:BB8:1200::2
device(config-if)# ipv6 dhcp relay option vpn
device(config-if)# end
```

次に、サーバー側 WAN エッジデバイスの設定を示します。

```
device(config)# interface GigabitEthernet0/0/3
device(config-if)# vrf forwarding 10
device(config-if)# no ip address
device(config-if)# negotiation auto
device(config-if)# ipv6 address 2001:BB8:1200::1/64
device(config-if)# ipv6 enable
device(config-if)# end
```

次に、サーバー側でリレーを使用して DHCPv6 を設定する例を示します。

```
device(config)# interface GigabitEthernet2
device(config-if)# ipv6 address 2001:BB8:1200::2/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# prefix-delegation pool dhcpv6-pool10 lifetime infinite infinite
device(config-dhcpv6)# address prefix 2001:BB:1000::/64 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:BB:1200::42
device(config-dhcpv6)# domain-name relay.com
device(config)# ipv6 local pool dhcpv6-pool10 8001:ABCD::/40 48
```

DHCPv6 クライアントおよびサーバー設定の確認

DHCPv6 インターフェイス情報の確認

次に、DHCPv6 アドレス割り当てに関する詳細を提供する **show ipv6 dhcp interface** コマンドの出力例を示します。

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 00:01:09
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:BD1
    DUID: 00030001001EBD43F800
    Preference: 0
  Configuration parameters:
    IA NA: IA ID 0x00080001, T1 100, T2 160
    Address: 2010:AB8:0:1:95D1:CFC:F227:23FB/128
             preferred lifetime 200, valid lifetime 200
             expires at Oct 26 2021 07:28 AM (170 seconds)
    DNS server: 2001:DB8:3000:3000::42
    Domain name: example.com
    Information refresh time: 0
  Vendor-specific Information options:
    Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

次に、DHCPv6 プレフィックス委任に関する詳細を提供する **show ipv6 dhcp interface** コマンドの出力例を示します。

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:01:34
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:BD1
    DUID: 00030001001EBD43F800
    Preference: 0
  Configuration parameters:
    IA PD: IA ID 0x00080001, T1 100, T2 160
    Prefix: 2001:DB8:1202::/48
             preferred lifetime 200, valid lifetime 200
```

```

        expires at Oct 26 2021 07:30 AM (194 seconds)
    DNS server: 2001:DB8:3000:3000::42
    Domain name: example.com
    Information refresh time: 0
Prefix name: prefix_from_server
Prefix Rapid-Commit: disabled
Address Rapid-Commit: disabled

```

次に、DHCP を使用した SLAAC に関する詳細を提供する **show ipv6 dhcp interface** コマンドの出力例を示します。

```

Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
Prefix State is IDLE (0)
Information refresh timer expires in 23:59:49
Address State is IDLE
List of known servers:
  Reachable via address: FE80::250:56FF:FEBD:BD1
  DUID: 00030001001EBD43F800
  Preference: 0
Configuration parameters:
  DNS server: 2001:DB8:3000:3000::42
  Domain name: example.com
  Information refresh time: 0
Vendor-specific Information options:
  Enterprise-ID: 100
Prefix Rapid-Commit: disabled
Address Rapid-Commit: disabled

```

DHCPv6 プール情報の表示

次に、DHCPv6 アドレス割り当てに関する詳細を提供する **show ipv6 dhcp pool** コマンドの出力例を示します。

```

Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
VRF 10
Prefix pool: dhcpv6-pool2
Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (1 in
use, 0 conflicts)
  preferred lifetime 200, valid lifetime 200
DNS server: 2001:BB8:3000:3000::42
Domain name: relay.com
Information refresh: 60
Vendor-specific Information options:
Enterprise-ID: 10
  suboption 1 address 2001:DB8:1234:42::10
  suboption 2 ascii 'ip phone'
Active clients: 1
Pool is configured to include all configuration options in REPLY

```

次に、DHCPv6 プレフィックス委任に関する詳細を提供する **show ipv6 dhcp pool** コマンドの出力例を示します。

```

Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
VRF 10
Prefix pool: dhcpv6-pool2
Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (0 in
use, 0 conflicts)
  preferred lifetime 200, valid lifetime 200
DNS server: 2001:BB8:3000:3000::42
Domain name: relay.com

```



```
Information refresh: 60
Vendor-specific Information options:
Enterprise-ID: 10
  suboption 1 address 2001:DB8:1234:42::10
  suboption 2 ascii 'ip phone'
Active clients: 1
Pool is configured to include all configuration options in REPLY
```

DHCPv6 バインディングの表示

次に、DHCPv6 アドレス割り当てに関する詳細を提供する **show ipv6 dhcp binding** コマンドの出力例を示します。

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
DUID: 00030001001EE6DBF500
Username : unassigned
VRF : 10
IA NA: IA ID 0x00080001, T1 10000, T2 16000
Address: 5001:DB8:1234:42:500C:B3FA:54A7:F63D
preferred lifetime 20000, valid lifetime 20000
expires at Oct 26 2021 01:17 PM (19925 seconds)
```

次に、DHCPv6 プレフィックス委任に関する詳細を提供する **show ipv6 dhcp binding** コマンドの出力例を示します。

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
DUID: 00030001001EE6DBF500
Username : unassigned
VRF : 10
Interface : GigabitEthernet0/0/3
IA PD: IA ID 0x00080001, T1 100, T2 160
Prefix: 2001:BB8:1602::/48
preferred lifetime 200, valid lifetime 200
expires at Oct 26 2021 08:01 AM (173 seconds)
```

DHCPv6 データベースの表示

次に、**show ipv6 dhcp database** コマンドの出力例を示します。

```
Device# show ipv6 dhcp database
Database agent bootflash:
write delay: 300 seconds, transfer timeout: 300 seconds
last written at Oct 26 2021 08:01 AM, write timer expires in 250 seconds
last read at never
successful read times 0
failed read times 0
successful write times 2
failed write times 0
```

DHCPv6 リレーバインディングの表示

次に、DHCPv6 リレーに関する詳細を提供する **show ipv6 dhcp relay bindings** コマンドの出力例を示します。

```
Device# show ipv6 dhcp relay binding

Relay Bindings associated with default vrf:
```

```
Relay Bindings associated with vrf 10:  
Prefix: 2001:AA8:1100::/48 (GigabitEthernet3)  
  DUID: 00030001001E49674C00  
  IAID: 851969  
  lifetime: INFINITE  
  expiration: INFINITE  
Summary:  
  Total number of Relay bindings = 1  
  Total number of IAPD bindings = 1  
  Total number of IANA bindings = 0  
  Total number of Relay bindings added by Bulk lease = 0
```

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。