



IPv6 ネイバー探索

この章の内容は、次のとおりです。

- [ネイバー探索 \(1 ページ\)](#)
- [ブリッジドメインでの IPv6 ネイバー探索の設定 \(2 ページ\)](#)
- [レイヤ 3 インターフェイス上での IPv6 ネイバー探索の設定 \(6 ページ\)](#)
- [IPv6 ネイバー探索重複アドレス検出の設定 \(11 ページ\)](#)

ネイバー探索

IPv6 ネイバー探索 (ND) は、ノードのアドレスの自動設定、リンク上の他のノードの探索、他のノードのリンク層アドレスの判別、重複アドレスの検出、使用可能なルータと DNS サーバの検出、アドレスプレフィックスの探索、および他のアクティブなネイバーノードへのパスに関する到達可能性情報の維持を担当します。

ND 固有のネイバー要求/ネイバーアドバタイズメント (NS/NA) およびルータ要求/ルータアドバタイズメント (RS/RA) パケットタイプは、物理、層3 サブインターフェイス、および SVI (外部およびパーベイシブ) を含むすべての ACI ファブリックのレイヤ 3 インターフェイスでサポートされます。APIC リリース 3.1(1x) まで、RS/RA パケットはすべてのレイヤ 3 インターフェイスの自動設定のために使用されますが、拡散型 SVI の設定のみ可能です。

APIC リリース 3.1(2x) より、RS/RA パケットは自動設定のため使用され、ルーテッドインターフェイス、レイヤ 3 サブインターフェイス、SVI (外部および拡散) を含むレイヤ 3 インターフェイスで設定できます。

ACI のブリッジドメイン ND は常にフラッドモードで動作します。ユニキャストモードはサポートされません。

ACI ファブリック ND サポートに含まれるもの：

- インターフェイスポリシー (nd:IfPol) は、NS/NA メッセージに関する ND タイマーと動作を制御します。
- ND プレフィックスポリシー (nd:PfxPol) コントロール RA メッセージ。
- ND の IPv6 サブネット (fv:Subnet) の設定。

- 外部ネットワークの ND インターフェイス ポリシー。
- 外部ネットワークの設定可能 ND サブネットおよびパーベイシブ ブリッジ ドメインの任意サブネット設定はサポートされません。

設定可能なオプションは次のとおりです。

- 隣接関係
 - 設定可能な静的 Adjacencies : (<vrf、L3Iface < ipv6 address> --> mac address)
 - 動的 Adjacencies : NS/NA パケットの交換経由で学習
- インターフェイス単位
 - ND パケットの制御 (NS/NA)
 - ネイバー要求間隔
 - ネイバー要求再試行回数
 - RA パケットの制御
 - RA の抑制
 - RA MTU の抑制
 - RA 間隔、RA 最小間隔、再送信時間
- プレフィックス単位 (RA でアドバタイズ) の制御
 - ライフタイム、優先ライフタイム
 - プレフィックス コントロール (自動設定、リンク上)
- ネイバー検索重複アドレスの検出 (DAD)

ブリッジドメインでの IPv6 ネイバー探索の設定

RESTAPI を使用したブリッジドメインの IPv6 ネイバー探索対応のテナント、VRF、およびブリッジドメインの作成

手順

ネイバー探索インターフェイス ポリシーとネイバー探索プレフィックス ポリシーが適用された、テナント、VRF、ブリッジドメインを作成します。

例：

```
<fvTenant descr="" dn="uni/tn-ExampleCorp" name="ExampleCorp" ownerKey="" ownerTag="">
  <ndIfPol name="NDPol001" ctrl="managed-cfg" descr="" hopLimit="64" mtu="1500"
nsIntvl="1000" nsRetries="3" ownerKey="" ownerTag="" raIntvl="600" raLifetime="1800"
reachableTime="0" retransTimer="0"/>
  <fvCtx descr="" knwMcastAct="permit" name="pvn1" ownerKey="" ownerTag=""
pcEnfPref="enforced">
    </fvCtx>
  <fvBD arpFlood="no" descr="" mac="00:22:BD:F8:19:FF" multiDstPktAct="bd-flood"
name="bd1" ownerKey="" ownerTag="" unicastRoute="yes" unkMacUcastAct="proxy"
unkMcastAct="flood">
    <fvRsBDToNdP tnNdIfPolName="NDPol001"/>
    <fvRsCtx tnFvCtxName="pvn1"/>
    <fvSubnet ctrl="nd" descr="" ip="34::1/64" name="" preferred="no" scope="private">

      <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
    </fvSubnet>
    <fvSubnet ctrl="nd" descr="" ip="33::1/64" name="" preferred="no" scope="private">

      <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol002"/>
    </fvSubnet>
  </fvBD>
  <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001"
ownerKey="" ownerTag="" prefLifetime="1000"/>
  <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="4294967295" name="NDPfxPol002"
ownerKey="" ownerTag="" prefLifetime="4294967295"/>
</fvTenant>
```

(注) 外部ルーテッドを設定するときにパブリックサブネットがある場合は、ブリッジドメインを外部設定と関連付ける必要があります。

NX-OS スタイル CLI を使用したブリッジドメイン上の IPv6 ネイバー検索によるテナント、VRF、ブリッジドメインの設定

手順

ステップ 1 IPv6 ネイバー検索インターフェイスポリシーを設定し、ブリッジドメインに割り当てます。

a) IPv6 ネイバー検索インターフェイスポリシーを作成します。

例：

```
apicl(config)# tenant ExampleCorp
apicl(config-tenant)# template ipv6 nd policy NDPol001
apicl(config-tenant-template-ipv6-nd)# ipv6 nd mtu 1500
```

b) VRF およびブリッジドメインを作成します：

例：

```
apicl(config-tenant)# vrf context pvn1
apicl(config-tenant-vrf)# exit
```

GUI を使用して、ブリッジドメイン上に IPv6 ネイバー探索対応のテナント、VRF、およびブリッジドメインを作成する

```
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member pvnl
apic1(config-tenant-bd)# exit
```

- c) IPv6 ネイバー探索ポリシーをブリッジドメインに割り当てます。

例：

```
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ipv6 nd policy NDPol001
apic1(config-tenant-interface)#exit
```

- ステップ2** サブネット上で IPv6 ブリッジドメイン サブネットおよびネイバー検索プレフィックス ポリシーを作成します。

例：

```
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ipv6 address 34::1/64
apic1(config-tenant-interface)# ipv6 address 33::1/64
apic1(config-tenant-interface)# ipv6 nd prefix 34::1/64 1000 1000
apic1(config-tenant-interface)# ipv6 nd prefix 33::1/64 4294967295 4294967295
```

GUI を使用して、ブリッジドメイン上に IPv6 ネイバー探索対応のテナント、VRF、およびブリッジドメインを作成する

このタスクでは、テナント、VRF、およびブリッジドメイン (BD) を作成し、それらの中に 2 つの異なるタイプのネイバー探索 (ND) ポリシーを作成する方法を示します。これらは ND インターフェイス ポリシーと ND プレフィックス ポリシーです。ND インターフェイス ポリシーは BD に導入されますが、ND プレフィックス ポリシーは個々のサブネットに導入されません。各 BD に独自の ND インターフェイス ポリシーを適用することができます。ND インターフェイス ポリシーは、デフォルトですべての IPv6 インターフェイスに導入されます。Cisco APIC には、使用可能なデフォルトの ND インターフェイス ポリシーがすでに存在します。必要に応じて、代わりに使用するカスタム ND インターフェイス ポリシーを作成できます。ND プレフィックス ポリシーはサブネットレベルにあります。すべての BD が複数のサブネットを持つことができ、各サブネットが異なる ND プレフィックスを持つことができます。

手順

- ステップ1** メニューバーで、**[TENANT] > [Add Tenant]** の順にクリックします。

- ステップ2** **[Create Tenant]** ダイアログボックスで、次のタスクを実行します。

- [Name]** フィールドに、名前を入力します。
- [Security Domains +]** アイコンをクリックして **[Create Security Domain]** ダイアログボックスを開きます。
- [Name]** フィールドに、セキュリティドメインの名前を入力します。**Submit** をクリックします。

- d) [Create Tenant] ダイアログボックスで、作成したセキュリティドメインのチェックボックスをオンにし、[Submit] をクリックします。

ステップ 3 [Navigation] ペインで、[Tenant-name] > [Networking] の順に展開します。[Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次の操作を実行します。

- a) [Name] フィールドに、名前を入力します。
- b) [Submit] をクリックして VRF の設定を完了します。

ステップ 4 [Networking] 領域で、[BD] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、次の操作を実行します。

- a) [Name] フィールドに、名前を入力します。
- b) [L3 Configurations] タブをクリックし、[Subnets] を展開して [Create Subnet] ダイアログボックスを開き、[Gateway IP] フィールドにサブネットマスクを入力します。

ステップ 5 [Subnet Control] フィールドで、[ND RA Prefix] チェックボックスがオンになっていることを確認します。

ステップ 6 [ND Prefix policy] フィールドのドロップダウンリストで、[Create ND RA Prefix Policy] をクリックします。

- (注) すべての IPv6 インターフェイスに導入される使用可能なデフォルトポリシーがすでに存在しています。または、この例で示されているように、使用する ND プレフィックスポリシーを作成できます。デフォルトでは、IPv6 ゲートウェイのサブネットは ND RA メッセージの ND プレフィックスとしてアドバタイズされます。ユーザは、[ND RA prefix] チェックボックスをオフにして、ND RA メッセージでサブネットをアドバタイズしないことを選択できます。

ステップ 7 [Create ND RA Prefix Policy] ダイアログボックスで、次の操作を実行します。

- a) [Name] フィールドにプレフィックスポリシーの名前を入力します。

- (注) 特定のサブネットに対して存在できるプレフィックスポリシーは1つのみです。サブネットは共通プレフィックスポリシーを使用できますが、各サブネットに異なるプレフィックスポリシーを適用することが可能です。

- b) [Controller State] フィールドで、目的のチェックボックスをオンにします。
- c) [Valid Prefix Lifetime] フィールドで、プレフィックスを有効にする期間について目的の値を選択します。
- d) [Preferred Prefix Lifetime] フィールドで、目的の値を選択します。[OK] をクリックします。

- (注) ND プレフィックスポリシーが作成され、特定のサブネットに接続されます。

ステップ 8 [ND policy] フィールドのドロップダウンリストで、[Create ND Interface Policy] をクリックし、次のタスクを実行します。

- a) [Name] フィールドにポリシーの名前を入力します。
- b) [Submit] をクリックします。

ステップ 9 [OK] をクリックしてブリッジドメインの設定を完了します。

同様に、さまざまなプレフィックスポリシーが適用された追加のサブネットを必要に応じて作成できます。

IPv6 アドレスのサブネットが BD に作成され、ND プレフィックス ポリシーが関連付けられています。

レイヤ3 インターフェイス上での IPv6 ネイバー探索の設定

注意事項と制約事項

次のガイドラインと制限事項に適用ネイバー探索ルーター アドバタイズメント (ND RA) のプレフィックスのレイヤ3 インターフェイス。

- NDRA 設定は、IPv6 プレフィックスにのみ適用されます。IPv4 プレフィックスで ND ポリシーを設定しようとするは適用に失敗します。

GUI を使用して、レイヤ3 インターフェイス上の RA の IPv6 ネイバー探索インターフェイス ポリシーの設定



- (注) 次の手順では、レイヤ3 インターフェイスで IPv6 ネイバー探索インターフェイス ポリシーを関連付ける方法を表示します。この特定の例は、非 VPC インターフェイスを使用して設定する方法を示しています。

始める前に

- テナント、VRF、BD が作成されていること。
- 外部ルーテッドネットワークで、L3Out が作成されます。

手順

- ステップ1** ナビゲーション] ペインで、適切なテナントで、適切な外部ルーテッドネットワークに移動します。
- ステップ2** 外部ルーテッドネットワーク、展開 > 論理ノード プロファイル > 論理ノード生成 > 論理インターフェイス プロファイル。

ステップ3 適切なものをダブルクリック **論理インターフェイス プロファイル**、し、[**作業**] ペインで、をクリックして **ポリシー > ルーテッドインターフェイス** >。

(注) 作成論理インターフェイスプロファイルを持っていない場合は、ここにプロファイルを作成することができます。

ステップ4 Routed Interface ダイアログボックスで、次の操作を実行します:

- a) **ND RA プレフィックス** フィールドで、インターフェイスの ND RA プレフィックスを有効にする **チェック ボックス** をチェックします。
有効にすると、ルーテッドインターフェイスは自動設定使用できます。
また、**ND RA プレフィックス ポリシー** フィールドが表示されます。
- b) **ND RA Prefix Policy** フィールドで、ドロップダウンリストから、適切なポリシーを選択します。
- c) 必要に応じて、画面上の他の値を選択します。[Submit] をクリックします。

(注) **VPC インターフェイス** を使用してを設定する際に、**VPC** の設定内のメンバは、その両方としてに、**サイド A** と **サイド B** の両方の **ND RA プレフィックス** が有効にする必要があります。作業 () ペインで、**論理インターフェイス プロファイル** 画面で、をクリックします **SVI ()** タブ。プロパティ、有効にする **チェック ボックス** をオン、**NDRA プレフィックス サイド A** と **サイド B** の両方を選択、同一の **NDRA プレフィックス ポリシー サイド A** と **サイド B** の

REST API を使用したレイヤ3 インターフェイス上の RA による IPv6 ネイバー探索インターフェイス ポリシーの設定

手順

IPv6 ネイバー検索インターフェイス ポリシーを設定し、レイヤ3 インターフェイスに関連付けます。

次の例では、非 VPC セットアップの設定が表示されます。

例 :

```
<fvTenant dn="uni/tn-ExampleCorp" name="ExampleCorp">
  <ndIfPol name="NDPol001" ctrl="managed-cfg" hopLimit="64" mtu="1500" nsIntvl="1000"
nsRetries="3" raIntvl="600" raLifetime="1800" reachableTime="0" retransTimer="0"/>
  <fvCtx name="pvn1" pcEnfPref="enforced">
    </fvCtx>
  <l3extOut enforceRtctrl="export" name="l3extOut001">
    <l3extRsEctx tnFvCtxName="pvn1"/>
    <l3extLNodeP name="lnodeP001">
      <l3extRsNodeL3OutAtt rtrId="11.11.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2011"/>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>
```

```

<l3extLIfP name="lifP001">
  <l3extRsPathL3OutAtt addr="2001:20:21:22::2/64" ifInstT="l3-port" llAddr=":"
mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-2/paths-2011/pathep-[eth1/1]">
  <ndPfxP>
    <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
  </ndPfxP>
  </l3extRsPathL3OutAtt>
  <l3extRsNdIfPol tnNdIfPolName="NDPol001"/>
</l3extLIfP>
</l3extLNodeP>
<l3extInstP name="instp"/>
</l3extOut>
<ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001" ownerKey=""
ownerTag="" prefLifetime="1000"/>
</fvTenant>

```

- (注) VPC ポートについては、ndPfxP が l3extRsNodeL3OutAtt ではなく l3extMember の子である必要があります。次のコード スニペットは、VPC のセットアップでの設定を示します。

```

<l3extLNodeP name="lnodeP001">
<l3extRsNodeL3OutAtt rtrId="11.11.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2011"/>
<l3extRsNodeL3OutAtt rtrId="12.12.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2012"/>
  <l3extLIfP name="lifP002">
    <l3extRsPathL3OutAtt addr="0.0.0.0" encap="vlan-205" ifInstT="ext-svi"
llAddr=":" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-2/protpaths-2011-2012/pathep-[vpc7]" >
      <l3extMember addr="2001:20:25:1::1/64" descr="" llAddr=":" name=""
nameAlias="" side="A">
        <ndPfxP >
          <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </ndPfxP>
      </l3extMember>
      <l3extMember addr="2001:20:25:1::2/64" descr="" llAddr=":" name=""
nameAlias="" side="B">
        <ndPfxP >
          <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </ndPfxP>
      </l3extMember>
    </l3extRsPathL3OutAtt>
  </l3extRsNdIfPol tnNdIfPolName="NDPol001"/> </l3extLIfP>
</l3extLNodeP>

```

NX-OS スタイル CLI を使用したレイヤ3 インターフェイス上の RA による IPv6 ネイバー探索インターフェイス ポリシーの設定

この例では、IPv6 ネイバー検索インターフェイス ポリシーを設定し、レイヤ3 インターフェイスに割り当てます。次に、IPv6 レイヤ3アウトインターフェイス、ネイバー検索プレフィックス ポリシーを設定し、インターフェイスにネイバー検索ポリシーを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure 例 : apicl# configure	コンフィギュレーションモードに入ります。
ステップ 2	tenant tenant_name 例 : apicl (config)# tenant ExampleCorp apicl (config-tenant)#	テナントを作成し、テナントモードを開始します。
ステップ 3	template ipv6 nd policy policy_name 例 : apicl (config-tenant)# template ipv6 nd policy NDPol001	IPv6 ND ポリシーを作成します。
ステップ 4	ipv6 nd mtu mtu value 例 : apicl (config-tenant-template-ipv6-nd)# ipv6 nd mtu 1500 apicl (config-tenant-template-ipv6)# exit apicl (config-tenant-template)# exit apicl (config-tenant)#	IPv6 ND ポリシーに MTU 値を割り当てます。
ステップ 5	vrf context VRF_name 例 : apicl (config-tenant)# vrf context pvn1 apicl (config-tenant-vrf)# exit	VRF を作成します。
ステップ 6	l3out VRF_name 例 : apicl (config-tenant)# l3out l3extOut001	レイヤ 3 アウトを作成します。
ステップ 7	vrf member VRF_name 例 : apicl (config-tenant-l3out)# vrf member	VRF をレイヤ 3 アウトインターフェイスに関連付けます。

	コマンドまたはアクション	目的
	<pre>pvn1 apic1(config-tenant-l3out)# exit</pre>	
ステップ 8	external-l3 epg instp l3out l3extOut001 例 : <pre>apic1(config-tenant)# external-l3 epg instp l3out l3extOut001 apic1(config-tenant-l3ext-epg)# vrf member pvn1 apic1(config-tenant-l3ext-epg)# exit</pre>	レイヤ 3 アウトおよび VRF をレイヤ 3 インターフェイスに割り当てます。
ステップ 9	leaf 2011 例 : <pre>apic1(config)# leaf 2011</pre>	リーフ スイッチモードを開始します。
ステップ 10	vrf context tenant ExampleCorp vrf pvn1 l3out l3extOut001 例 : <pre>apic1(config-leaf)# vrf context tenant ExampleCorp vrf pvn1 l3out l3extOut001 apic1(config-leaf-vrf)# exit</pre>	VRF をリーフ スイッチに関連付けます。
ステップ 11	int eth 1/1 例 : <pre>apic1(config-leaf)# int eth 1/1 apic1(config-leaf-if)#</pre>	インターフェイスモードに入ります。
ステップ 12	vrf member tenant ExampleCorp vrf pvn1 l3out l3extOut001 例 : <pre>apic1(config-leaf-if)# vrf member tenant ExampleCorp vrf pvn1 l3out l3extOut001</pre>	インターフェイスで関連付けられているテナント、VRF、レイヤ 3 Out を指定します。
ステップ 13	ipv6 address 2001:20:21:22::2/64 preferred 例 :	プライマリまたは優先 Ipv6 アドレスを指定します。

	コマンドまたはアクション	目的
	<code>apicl(config-leaf-if)# ipv6 address 2001:20:21:22::2/64 preferred</code>	
ステップ 14	ipv6 nd prefix 2001:20:21:22::2/64 1000 1000 例 : <code>apicl(config-leaf-if)# ipv6 nd prefix 2001:20:21:22::2/64 1000 1000</code>	レイヤ 3 インターフェイス下で IPv6 ND プレフィックス ポリシーを設定します。
ステップ 15	inherit ipv6 nd NDPol001 例 : <code>apicl(config-leaf-if)# inherit ipv6 nd NDPol001</code> <code>apicl(config-leaf-if)# exit</code> <code>apicl(config-leaf)# exit</code>	レイヤ 3 インターフェイス下で ND ポリシーを設定します。

設定が完了します。

IPv6 ネイバー探索重複アドレス検出の設定

ネイバー探索重複アドレス検出について

重複アドレス検出 (DAD) は、ネットワーク内で重複アドレスを検出するためにネイバー探索が使用するプロセスです。デフォルトでは、ACI ファブリック リーフ レイヤ 3 インターフェイスで使用されているリンクローカルアドレスとグローバルサブネット IPv6 アドレスの DAD が有効になっています。オプションとして、REST API (`ipv6Dad="disabled"` 設定を使用) または GUI を通してノブを構成することにより、IPv6 グローバルサブネットの DAD プロセスを無効にすることができます。外部接続されたデバイスに境界リーフ冗長性を提供するため、異なる境界リーフ スイッチ上の L3Outs にわたって同じ共有セカンダリ アドレスが必要な場合には、このノブを構成します。このような場合、DAD プロセスを無効にすれば、DAD が複数の境界リーフ スイッチ上の同じ共有セカンダリ アドレスを重複と見なすことを避けられます。このような場合には DAD プロセスを無効にしないと、共有セカンダリ アドレスが DUPLICATE DAD 状態に入り、使用できなくなることがあります。

REST API を使用したネイバー探索重複アドレス検出の設定

手順

ステップ 1 サブネットの ipv6Dad エントリの値を **disabled** に変更することによって、サブネットのネイバー探索重複アドレス検出プロセスを無効にします。

次の例は、2001:DB8:A::11/64 サブネットのネイバー探索重複アドレス検出エントリを **disabled** に設定する方法を示しています:

(注) 次の REST API の例では、読みやすくなるように、長い行を \ 文字で分割しています。

例:

```
<l3extRsPathL3OutAtt addr="2001:DB8:A::2/64" autostate="enabled" \
  childAction="" descr="" encap="vlan-1035" encapScope="local" \
  ifInstT="ext-svi" ipv6Dad="enabled" llAddr=": : " \
  mac="00:22:BD:F8:19:DD" mtu="inherit" \
  rn="rspathL3OutAtt-[topology/pod-1/paths-105/pathep-[eth1/1]]" \
  status="" tDn="topology/pod-1/paths-105/pathep-[eth1/1]" >
  <l3extIp addr="2001:DB8:A::11/64" childAction="" descr="" \
    ipv6Dad="disabled" name="" nameAlias="" \
    rn="addr-[2001:DB8:A::11/64]" status=""/>
</l3extRsPathL3OutAtt>
</l3extLIIfP>
</l3extLNodeP>
```

ステップ 2 リーフスイッチで **show ipv6 int** コマンドを入力して、設定がリーフスイッチに正しくプッシュされたか確認してください。次に例を示します。

```
swtb23-leaf5# show ipv6 int vrf icmpv6:v1
IPv6 Interface Status for VRF "icmpv6:v1"(9)

vlan2, Interface status: protocol-up/link-up/admin-up, iod: 73
if_mode: ext
  IPv6 address:
    2001:DB8:A::2/64 [VALID] [PREFERRED]
    2001:DB8:A::11/64 [VALID] [dad-disabled]
  IPv6 subnet: 2001:DB8:A::/64
  IPv6 link-local address: fe80::863d:c6ff:fe9f:eb8b/10 (Default) [VALID]
```

GUI を使用したネイバー探索重複アドレス検出の設定

サブネットのネイバー探索重複アドレス検出プロセスを無効にするには、このセクションの手順に従ってください。

手順

ステップ 1 適切なページに移動して、そのインターフェイスの DAD フィールドにアクセスします。次に例を示します。

- a) **Tenants > Tenant > Networking > External Routed Networks > L3Out > Logical Node Profiles > node > Logical Interface Profiles** に移動し、設定するインターフェイスを選択します。
- b) *Routed Sub-interfaces* または *SVI* をクリックし、作成 (+) ボタンをクリックしてインターフェイスを設定します。

ステップ 2 このインターフェイスで、DAD エントリを次のように設定します:

- プライマリ アドレスでは、DAD エントリの値を **enabled** に設定します。
- 共有セカンダリ アドレスでは、DAD エントリの値を **disabled** に設定します。セカンダリ アドレスが境界リーフ スイッチ間で共有されていない場合には、そのアドレスの DAD を無効にする必要がないことに注意してください。

例 :

たとえば、SVI インターフェイスのこの設定を構成する場合には、次のようになります:

- サイド A の IPv6 DAD を **enabled** に設定します。
- サイド B の IPv6 DAD を **disabled** に設定します。

例 :

別の例として、ルーテッドサブインターフェイスの設定を構成する場合には、次のようになります:

- メインの [Select Routed Sub-Interface] ページで、ルーテッドサブインターフェイスの IPv6 DAD を **enabled** に設定します。
- [IPv4 Secondary/IPv6 Additional Addresses] エリアで作成 (+) ボタンをクリックして [Create Secondary IP Address] ページにアクセスし、IPv6 DAD の値を **disabled** に設定します。[OK] ボタンをクリックして、この画面での変更点を適用します。

ステップ 3 [Submit] ボタンをクリックして、変更を適用します。

ステップ 4 リーフスイッチで **show ipv6 int** コマンドを入力して、設定がリーフスイッチに正しくプッシュされたか確認してください。次に例を示します。

```
swtb23-leaf5# show ipv6 int vrf icmpv6:v1
IPv6 Interface Status for VRF "icmpv6:v1" (9)

vlan2, Interface status: protocol-up/link-up/admin-up, iod: 73
if_mode: ext
IPv6 address:
  2001:DB8:A::2/64 [VALID] [PREFERRED]
  2001:DB8:A::11/64 [VALID] [dad-disabled]
IPv6 subnet: 2001:DB8:A::/64
IPv6 link-local address: fe80::863d:c6ff:fe9f:eb8b/10 (Default) [VALID]
```

