NAT64 の設定

NAT64 設定では、IPv6 および IPv4 ネットワークを接続するために、IPv6 アドレスを IPv4 アドレスに変換できます。

トラフィックの発信は常に、オーバーレイネットワークのトランスポート側（WAN）からサービス側（LAN）に行われます。

NAT64 ダイレクト インターネット アクセス

表 *1*：機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイス の NAT64 DIA	Cisco IOS XE SD-WAN リリース 16.12.1b Cisco vManage リリース 19.2.1	NAT64 ダイレクト インターネット アクセス（DIA）機能は、インターネットトラフィックを中央サイトまたはインターネットアクセス用のデータセンターにトンネリングする代わりに、ブランチサイトからインターネットに直接トラフィックのルーティングをサポートします。 NAT64 DIA を使用すると、ブランチサイトの IPv6 クライアントは、データセンターまたはブランチのローカルにある IPv4 エンタープライズアプリケーション サーバーにアクセスできます。IPv6 クライアントは、インターネットを使用してブランチから IPv4 サーバーに直接アクセスすることもできます。

NAT64 DIA に関する情報

NAT64 DIA を使用すると、IPv4 サーバーはリモートブランチまたはデータセンターから IPv6 サーバーにアクセスできます。

NAT64 DIA のトラフィックフローは、LAN から DIA です。

NAT64 DIA の仕組み

1. [Cisco VPN Interface Ethernet] テンプレートを使用して、IPv4 および IPv6 を有効にします。
2. サービス側 VPN である [Cisco VPN] テンプレートに IPv6 ルートを設定します。

   送信元と宛先の IPv6 アドレスが変換されます。
3. NAT IPv4 DIA が設定されているため、インターフェイスが過負荷になり、送信元 IPv4 アドレスが変換されます。宛先 IPv4 アドレスは同じままです。

NAT64 DIA の利点

- 優れたアプリケーション パフォーマンスを実現
- 帯域幅の消費と遅延の削減に貢献
- 帯域幅コストの削減に貢献
- リモートサイトに DIA を提供することで、ブランチオフィスのユーザーエクスペリエンスを向上させます。

NAT64 DIA の制限事項

- NAT64 DIA は、インターフェイス オーバーロードのみを使用します。
- NAT DIA プールまたはループバックは、NAT64 ではサポートされていません。

NAT64 DIA ルートの制限事項

- ルーティングテーブルにルートをインストールするには、次の NAT64 DIA ルートを使用できます。

  /128 プレフィックスの NAT64 DIA ルートの例：

  ```
  nat64 route vrf 4 64:FF9B::1E00:102/128 global
  ```

  /96 プレフィックスの NAT64 DIA ルートの例：

  ```
  nat64 route vrf 4 64:FF9B::/96 global
  ```
- ルーティングテーブルにルートをインストールするために、次の NAT64 DIA ルート設定を使用することはできません。

```
nat64 route vrf 4 64:ff9b::/64 global
nat64 route vrf 4 ::0/0 global
```

NAT64 DIA と DIA ルートの設定

NAT64 DIA を有効にするためのワークフロー

1. IPv4 と IPv6 の両方で、[Cisco VPN Interface Ethernet] テンプレートを使用して NAT64 を有効にします。

（注） NAT64 IPv4 DIA は、デフォルトでインターフェイスの過負荷を使用します。

IPv6 DIA の NAT64 を構成する場合、インターフェイスの過負荷は既に設定されています。

[Cisco VPN Interface Ethernet] テンプレートは、トランスポート インターフェイスです。

2. サービス VPN である [Cisco VPN] テンプレートを使用して、NAT64 DIA IPv6 ルートを設定します。

NAT64 DIA の設定

インターフェイスの過負荷での NAT64 DIA の設定

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. [Cisco VPN Interface Ethernet] テンプレートを編集するには、**...** をクリックし、[Edit] をクリックします。
4. [Interface Name] フィールドで、インターフェイスを選択します。
5. [NAT] をクリックし、[IPv4] を選択します。
   1. スコープを [Default] から [Global] に変更します。
   2. [オン] をクリックして、IPv4 の NAT を有効にします。
   1. [NAT Type] フィールドで、インターフェイス過負荷の [Interface] をクリックします。

      [Interface] オプションが IPv4 に対して [On] に設定されていることを確認します。

表 *2 : NAT IPv4* パラメータ

パラメータ名	説明
NAT	NAT 変換を使用するかどうかを指定します。 デフォルトは [オフ（Off）] です。
NAT Type	IPv4 の NAT 変換タイプを指定します。 使用可能なオプションには、[Interface]、[Pool]、および [Loopback] が含まれます。 デフォルトは [Interface] オプションです。[Interface] オプションは、NAT64 でサポートされています。
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 536870 秒 デフォルト：300 秒（5 分） （注） Cisco IOS XE リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降、NAT64 のデフォルトの [UDP Timeout] 値は 300 秒（5 分）に変更されました。
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 タイムアウト値を入力します デフォルト：3600 秒（1 時間） （注） Cisco IOS XE リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降、NAT64 のデフォルトの [TCP Timeout] 値は 3600 秒（1 時間）に変更されました。

6. ステップ 5 を繰り返しますが、[IPv6] を選択して IPv6 の NAT を有効にします。

（注） NAT64 DIA に IPv4 と IPv6 の両方を設定します。

7. [NAT Selection] フィールドで、[NAT64] をクリックして NAT64 を有効にします。

（注） IPv6 の場合、インターフェイスの過負荷はすでに設定されています。

表 *3 : NAT IPv6* パラメータ

パラメータ名	説明
NAT	NAT変換を使用するかどうかを指定します。 デフォルトは [オフ（Off）] です。
[NAT Selection]	NAT64 を指定します。 デフォルトは [NAT66] オプションです。

8. [更新（Update）] をクリックします。

NAT64 DIA ルートの設定

Cisco VPN テンプレートを使用した NAT64 DIA ルートの設定

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. [Cisco VPN] 機能テンプレートを編集するには、**...** をクリックし、[Edit] をクリックします。

（注） サービス側 VPN である [Cisco VPN] 機能テンプレートで IPv6 DIA ルートを設定します。

4. [IPv6 Route] をクリックします。
5. [New IPv6 Route] をクリックします。
6. [Prefix] フィールドに、よく知られたプレフィックス [64:FF9B::/96] を入力します。
7. [Gateway] フィールドで、[VPN] をクリックします。
8. [Enable VPN] フィールドで、スコープを [Default] から [Global] に変更し、[On] をクリックして VPN を有効にします。
9. [NAT] フィールドで、[NAT64] をクリックします。

10. [更新（Update）] をクリックします。

CLI を使用した NAT64 DIA ルートの設定

例：NAT64 DIA ルートの設定

```
Device(config)# nat64 route vrf 4 64:FF9B::1E00:102/128 global
```

NAT64 DIA ルート設定の確認

例 1

以下は、サービス VPN 用の **show ipv6 route vrf** コマンドからの出力例です。

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP
m   64:FF9B::/96 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
```

この例では、64:FF9B::/96 は、IPv6 を IPv4 アドレスに変換するための NAT64 の既知のプレフィックスです。

例 2

NAT64 DIA がトランスポート VPN で設定されているため、トランスポート VPN のルーティングテーブルは次のように表示されます。

```
Device# show ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP, Nd - Nat-Route DIA
S   64:FF9B::/96 [1/0]
```

NAT64 DIA の設定例

この例は、NAT64 DIA の設定を示しています。

```
interface GigabitEthernet1
          no shutdown
          arp timeout 1200
          ip address 10.1.15.15 10.255.255.255
```

```
 no ip redirects
 ip mtu    1500
 ip nat outside
 load-interval 30
 mtu           1500
 negotiation auto
 nat64 enable
 !
 nat64 v6v4 list nat64-global-list interface GigabitEthernet1 overload
 !
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1
overload
```

（注） GigabitEthernet1 は、トランスポート VPN インターフェイスです。

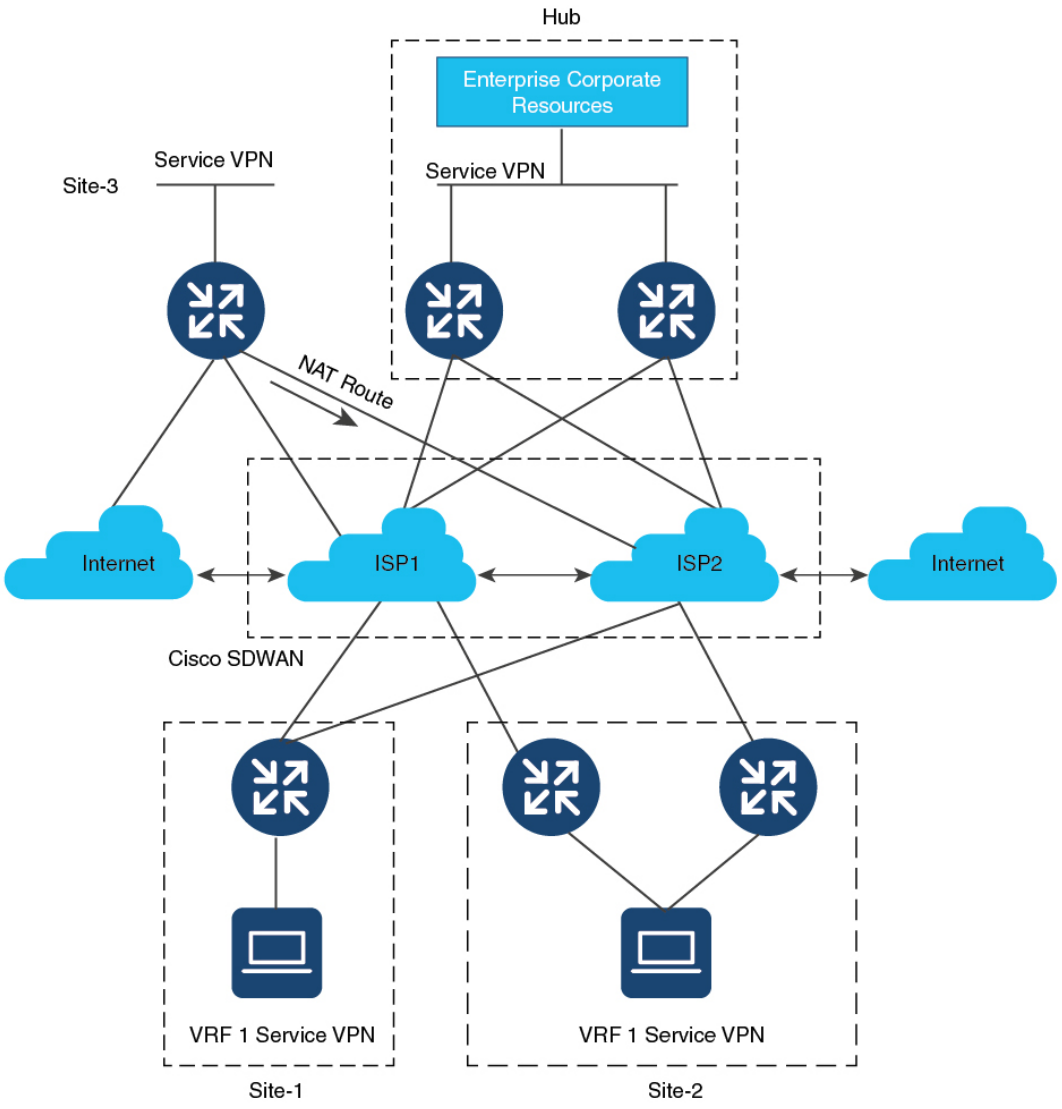
OMP を介した NAT64 ルートのアドバタイズ

NAT64 DIA アドバタイズメントがネットワーク上の指定された Cisco IOS XE SD-WAN デバイス のいずれかに設定されている場合、OMP は NAT デフォルトルートをブランチにアドバタイズします。ブランチはデフォルトルートを受け取り、それを使用してすべての DIA トラフィックのハブに到達します。Cisco IOS XE SD-WAN デバイス は、すべての DIA トラフィックのインターネットゲートウェイとして機能します。

（注） デフォルトでは、NAT64 IPv4 プールアドレスと既知の NAT64 プレフィックスが OMP ルートとして受信されます。

OMP を介した NAT64 ルートのアドバタイズの詳細については、「OMP を介した NAT ルートのアドバタイズに関する情報」を参照してください。

図 *1 : OMP* を使用した *NAT* ルートのアドバタイズ



サービス側 NAT64

表 *4:* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイスのサービス側 NAT64	Cisco IOS XE SD-WAN リリース 16.12.1b Cisco vManage リリース 19.2.1	サービス側ネットワークアドレス変換（NAT）64 機能は、送信元 IPv6 アドレスを NAT プール内の使用可能な IPv4 アドレスに変換します。宛先 IPv6 アドレスは、IPv4 組み込み IPv6 アドレスであるため、宛先 IPv6 アドレスはサーバーの実際の IPv4 アドレスに変換されます。 サービス側 NAT64 により、IPv4 サーバーは IPv6 クライアントと通信できます。

サービス側 NAT64 に関する情報

IPv4 パブリックアドレス空間が減少し、よりルーティング可能なアドレスに対する必要性が高まる中、サービスプロバイダーと企業は IPv6 ネットワークの構築と展開を続けています。IPv4 インターネットはしばらく存続するため、IPv4 ネットワークと IPv6 ネットワーク間の通信は、シームレスなエンドユーザー エクスペリエンスにとって重要な要件です。

NAT IPv6 to IPv4（NAT64）テクノロジーは、IPv6 と IPv4 ネットワーク間の通信を容易にします。

サービス側 NAT64 機能は、送信側 IPv6 アドレスを NAT プール内の使用可能な IPv4 アドレスに変換します。宛先 IPv6 アドレスは、IPv4 組み込み IPv6 アドレスであるため、宛先 IPv6 アドレスはサーバーの実際の IPv4 アドレスに変換されます。

Cisco IOS XE SD-WAN デバイス は、IPv6 アドレスを IPv4 アドレスに、IPv4 アドレスを IPv6 アドレスに変換するためにステートフル NAT64 を使用します。NAT オーバーロードを使用したステートフル NAT64 は、IPv4 アドレスと IPv6 アドレス間の 1:*n* マッピングを提供します。

サービス側 NAT64 の仕組み

1. IPv6 クライアントが IPv4 サーバーへの接続を試みます。
2. IPv6 クライアントは、IPv6 AAAA レコード DNS クエリを作成します。これは、IPv4 アドレスに対する IPv6 クエリです。

   DNS64 サーバーは、IPv4 に埋め込まれた IPv6 アドレスで応答します。

   例：

   ```
   64:ff9b::c000:0201
   ```

これは、NAT64 の既知のプレフィックス（WKP）である 64:FF9B::/96 を使用します。WKP は、アドレスファミリ間のアルゴリズムマッピングに使用されます。

IPv4 埋め込み IPv6 アドレスは、可変長プレフィックス、埋め込み IPv4 アドレス、および可変長サフィックスで設定されます。最後の 32 ビットは、元の IPv4 アドレスの 16 進表現で、この例では 192.0.2.1 です。

3. IPv6 クライアントは、IPv4 サーバーへの接続を試みます。
4. IPv6 から IPv4 への変換が実行されます。

   送信元 IPv6 アドレスは、プール内の使用可能な IPv4 アドレスの 1 つに変換されます。

   宛先 IPv6 アドレスは、IPv4 組み込み IPv6 アドレスであるため、宛先 IPv6 アドレスはサーバーの実際の IPv4 アドレスに変換されます。

サービス側 NAT64 の利点

- インターネット上の IPv4 サーバーを使用したサービス VPN 内の IPv6 クライアント間の通信をサポート
- IPv6 および IPv4 ネットワークへのデュアルアクセスを維持するために、IPv6 アドレスから IPv4 アドレスへの変換を提供します。
- ステートフル NAT64 を使用する場合、既存の IPv4 ネットワーク インフラストラクチャをほとんどまたはまったく変更する必要がない
- IPv4 インターネットサービスにアクセスする IPv6 ユーザーにシームレスなインターネット エクスペリエンスを提供し、IPv4 のビジネス継続性を維持します。
- データポリシーを設定することなく、NAT64 の設定をサポート

サービス側 NAT64 の使用例

サポートされているトラフィックフローは、リモートサイト、データセンター、または別のブランチサイトにある IPv6 クライアントから、ローカル LAN 上の IPv4 クライアントまたはサーバーまでです。

（注） トラフィックの発信は常に、オーバーレイネットワークのトランスポート側（WAN）からサービス側（LAN）に行われます。

サービス側 NAT64 の前提条件

- ドメイン ネーム システム（DNS）トラフィックを機能させるには、別の DNS64 をインストールして稼働させる必要があります。

サービス側 NAT64 の制限事項

- トラフィックは常にリモートブランチサイトから発信され、ローカル LAN 上の IPv4 サーバーにアクセスする必要があります。
- トラフィックは、IPv4 サーバーからデータセンター内の IPv6 クライアントまたはリモートブランチサイトに発信できません。

サービス側 NAT64 の IPv4 アドレス制限事項

- 使用可能な IPv4 宛先 IP アドレスの詳細については、導入ガイドライン、RFC 6052、セクション 3.1 を参照してください。
- RFC 5735 のセクション 3 の展開ガイドラインに記載されているような、非グローバル IPv4 アドレスを表すために、既知のプレフィックス（WKP）を使用することはできません。

  たとえば、次の IPv4 プレフィックスは許可されていません。

  - 0.0.0.0/8
  - 10.0.0.0/8
  - 127.0.0.0/8
  - 169.254.0.0/16

- サービス側（LAN）でプライベート IPv4 アドレス範囲を使用することはできません。

サービス側 NAT64 の設定

次のセクションでは、サービス側 NAT64 の設定に関する情報を提供します。

機能テンプレートを使用したサービス側 NAT64 の有効化

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. [Cisco VPN Interface Ethernet] テンプレートを編集するには、**...** をクリックし、[Edit] をクリックします。

（注） [Cisco VPN Interface Ethernet] テンプレートは、サービス側のインターフェイスです。

4. [NAT] をクリックし、NAT64 に [IPv6] を選択します。
5. スコープを [Default] から [Global] に変更します。
6. [NAT64] フィールドで、[On] をクリックして NAT64 を有効にします。
7. [更新（Update）] をクリックします。

サービス側 NAT64 プールの設定

はじめる前に

1. NAT64 IPv4 プールを設定する前に、[Cisco VPN Interface Ethernet] テンプレートを使用してサービス側の NAT64 を有効にしておく必要があります。
2. 新しい [Cisco VPN] 機能を作成するか、既存の [Cisco VPN] 機能を編集します。[Cisco VPN] 機能テンプレートは、NAT64 を設定するサービス側 VPN に対応します。

サービス側 NAT64 プールの設定

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. [Cisco VPN] テンプレートを編集するには、テンプレートの横にある **...** をクリックし、[Edit] をクリックします。
4. [NAT] をクリックします。
5. [NAT64 v4 Pool] をクリックします。
6. [New NAT64 v4 Pool] をクリックします。
7. [NAT64 Pool name] フィールドで、プール名を指定します。

（注） プール名には番号を指定する必要があります。

8. [NAT 64 v4 Pool Range Start] フィールドで、プール範囲の開始の IPv4 アドレスを指定します。
9. [NAT 64 v4 Pool End Start]フィールドで、プール範囲の終了の IPv4 アドレスを指定します。
10. ドロップダウンリストから [Global] を選択します。

11. [On] をクリックして、[NAT 64 Overload] を有効にします。

（注） [NAT 64 Overload] はデフォルトで [Off] に設定されています。

12. [Add] をクリックします。

13. [Update] をクリックして、設定をデバイスにプッシュします。

CLI を使用したサービス側 NAT64 の設定

表 *5:* 機能の履歴

機能名	リリース情報	説明
NAT64 デバイスの IPv6 サポート	Cisco IOS XE SD-WAN リリース 16.12.1b	この機能は、Cisco IOS XE SD-WAN デバイスでの IPv4 と IPv6 間の通信を容易にする NAT64 をサポートします。

CLI を使用したサービス側 NAT64 の有効化

このセクションでは、サービス側の NAT64 を有効にするための CLI 設定の例を示します。

LAN インターフェイスでサービス側の NAT64 を有効にします。これは、Cisco vManage 上の [Service VPN] テンプレートに相当します。

IPv4 アプリケーション サーバーはローカル LAN サイトにあり、IPv6 クライアントはデータセンターまたは LAN のリモートサイトにあります。

```
Device# interface GigabitEthernet 5.104
nat64 enable
```

CLI を使用したサービス側 NAT64 プールの設定

このセクションでは、サービス側 NAT64 プールを設定するための CLI 設定の例を示します。

```
Device# nat64 v4 pool pool10 192.0.2.0 192.0.2.254
nat64 v6v4 list global-list_nat64 pool pool10 vrf 4 overload
```

サービス側 NAT64 の設定の確認

例：指定されたデバイスのルーティングテーブルに表示される内容

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

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
```

```
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP, Nd - Nat-Route DIA
Nd  64:FF9B::/96 [6/0]
     via Null0%default, directly connected
m   2001:DB8:AA:A::/64 [251/0]
     via 172.16.255.16%default, Sdwan-system-intf%default
C   2001:DB8:BB:A::/64 [0/0]
     via GigabitEthernet5.104, directly connected
L   2001:DB8:BB:A::1/128 [0/0]
     via GigabitEthernet5.104, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

この例では、NAT64 の既知のプレフィックス、`64:FF9B::/96` がサービス VPN の IPv6 ルーティングテーブルに表示されます。

次に、**show ip route vrf 4** コマンドの出力例を示します。

```
Device# show ip route vrf 4
Routing Table: 4
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

NAT64 IPv4 プールアドレスは、サービス VPN の IPv4 ルーティングテーブルの `nat inside` ルートとしてルーティングテーブルにインストールされます。

例：OMP のルーティングテーブルに表示される内容

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

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP
m   64:FF9B::/96 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
C   2001:DB8:AA:A::/64 [0/0]
     via GigabitEthernet5.104, directly connected
L   2001:DB8:AA:A::1/128 [0/0]
     via GigabitEthernet5.104, receive
m   2001:DB8:BB:A::/64 [251/0]
```

```
     via 172.16.255.15%default, Sdwan-system-intf%default
L    FF00::/8 [0/0]
     via Null0, receive
```

この例では、NAT64 の既知のプレフィックスである `64:FF9B::/96` がオーバーレイ管理プロトコル（OMP）ルートとして受信されます。

NAT64 IPv4 プールアドレスは、OMP ルートとして受信されます。

サービス側 NAT64 の設定例

この例は、サービス側 NAT64 の設定を示しています。

```
nat64 v4 pool 1-4 192.0.2.0 192.0.2.254
nat64 v6v4 list nat64-list pool 1-4 vrf 4 overload
!
interface GigabitEthernet5.104
 encapsulation dot1Q 104
 vrf forwarding 4
 ip address 10.1.19.15 10.255.255.255
 ip mtu 1496
 ip ospf network broadcast
 ip ospf 4 area 0
 nat64 enable
end
```

この例は、NAT64 プールの設定を示しています。

```
nat64 v4 pool 1-4 192.0.2.0 192.0.2.254
nat64 v6v4 list nat64-list pool 1-4 vrf 4 overload
!
interface GigabitEthernet5.104
 encapsulation dot1Q 104
 vrf forwarding 4
 ip address 10.1.19.15 10.255.255.255
 ip mtu 1496
 ip ospf network broadcast
 ip ospf 4 area 0
 nat64 enable
end
```

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。