

NAT64の説明と設定

内容

[概要](#)

[前提条件](#)

[NAT64が必要な理由](#)

[IPv4とIPv6間の通信を可能にするにはどうすればよいのですか。](#)

[NAT64変換のタイプ](#)

[シナリオ 1：IPv6ネットワーク内のホストからIPv4サーバ（IPv4ネットワーク内）と通信する場合](#)

[ステートフルNAT64の場合のパケットフロー](#)

[NAT64の設定ガイド](#)

[NAT 46ルータの設定](#)

[NAT64の詳細の確認](#)

[シナリオ 2：IPv4専用クライアントからIPv6専用サーバへのトラフィック開始](#)

[NAT46の設定ガイド](#)

[NAT 46ルータの設定](#)

[NAT46の確認](#)

[翻訳シナリオとその適用可能性](#)

[NAT64の実装時に問題が発生した場合に備えた重要なトラブルシューティングコマンド](#)

概要

NAT64は、IPv4からIPv6への移行とIPv4 ~ IPv6の共存のためのメカニズムです。NAT64は、DNS64とともに、IPv6専用クライアントがIPv4専用サーバとの通信を開始できるようにすることを主な目的としています。NAT64は、静的または手動バインディングを使用してIPv6専用サーバとの通信を開始するIPv4専用にもです。このドキュメントでは、両方のシナリオについて説明しました。

前提条件

IPv6およびNATに関する基礎知識

NAT64が必要な理由

- 最近のほとんどのIPデバイスはIPv6対応ですが、古いデバイスの多くはIPv4専用です。これらのデバイスをIPv6ネットワーク経由で接続する方法が必要です。
- 上位層にIPv4アドレスを組み込む古いアプリケーションの中には、しばらくの間存在し続けることが予想され、IPv6に適応する必要があります。
- IPv4アドレスが使用できなくなると、IPv6アドレスが新しいデバイスに割り当てられます。ただし、インターネット上の到達可能なコンテンツの大部分はまだIPv4であり、これらの新しいデバイスはそのコンテンツに到達する必要があります。
- 数年が経過すると、反対のことが適用されます。コンテンツの大部分はIPv6ですが、残りの

IPv4専用デバイスの数はIPv6に到達する必要があります。

- IPv4専用デバイスは、最小限のユーザ認識またはユーザ認識のないIPv6専用デバイスと通信する必要があります。

IPv4とIPv6間の通信を可能にするにはどうすればよいのですか。

IPv6はIPv4と下位互換性がないため、次の3つのクラスのいずれかに分類される移行メカニズムが必要です。

- **デュアルスタックインターフェイス:** IPv4とIPv6の共存に対する最も簡単なソリューション（相互運用性ではない）は、インターフェイスを「バイリンガル」にすることです。これにより、IPv4からIPv4デバイスに、IPv6からIPv6デバイスに話すことができます。使用するバージョンは、デバイスから受信するパケットのバージョンによって異なります。また、デバイスのアドレスを問い合わせるときにDNSが提供するアドレスのタイプによっても異なります。デュアルスタックはIPv4からIPv6への移行を意図したものでしたが、IPv4が枯渇する前に移行が完了すると想定されていました。これは起こっていないので、デュアルスタッキングはより複雑になります。IPv4アドレスが十分に使用できない場合、すべてのインターフェイスにIPv4アドレスとIPv6アドレスの両方を割り当てるにはどうすればよいのですか。
- **トンネル:** トンネルも共存に関するもので、相互運用性ではありません。この機能により、あるバージョンのデバイスやサイトが、他のバージョンのネットワークセグメント（インターネットを含む）を経由して通信できるようになります。したがって、2つのIPv4デバイスまたはサイトがIPv4パケットをIPv6ネットワークで交換でき、2つのIPv6デバイスまたはサイトがIPv4ネットワークでIPv6パケットを交換できます。
- **翻訳者:** トランスレータは、あるバージョンのパケットのヘッダーを別のバージョンのヘッダーに変更することによって、IPv4デバイスとIPv6デバイス間の相互運用性を作成します。

#Likeその他の移行方法では、変換は長期戦略ではなく、最終的な目標はネイティブIPv6である必要があります。ただし、変換には、トンネリングよりも大きく2つの利点があります。

- 変換は、IPv6への段階的でシームレスな移行を実現します。
- コンテンツプロバイダーは、IPv6インターネットユーザに透過的にサービスを提供できます。

NAT64変換のタイプ

ステートレスNAT64

ステートレスNAT64では、状態は保持されません。つまり、すべてのIPv6ユーザに専用のIPv4アドレスが必要になります。IPv4枯渇フェーズなので、このモードのNAT64を採用するのは非常に困難です。少数のIPv6アドレス(NAT46)がある場合にステートレスNAT64を使用する唯一の利点です。

ステートフルNAT64

ステートフルNAT64では、状態は維持されます。1つのIPアドレスは、ポート番号が異なるすべてのプライベートユーザに使用されます。上の図では、パブリックIPv4サーバにアクセスするために、そのLAN内のすべてのIPv6ユーザに対して、1つのIPv4アドレスが異なるポート番号で使用されます。

ステートフルNAT64変換とステートレスNAT64変換の違いについての詳細は、次のとおりです。

ステートレスNAT64

1:1変換

IPv4アドレスの保存なし

エンドツーエンドアドレスの透過性と拡張性を保証

変換に状態またはバインドが作成されていません

IPv4変換可能なIPv6アドレスの割り当てが必要(必須)
IPv6ホストに対して手動またはDHCPv6ベースのアドレス割り当てが必要

ステートフルNAT64

1:N変換

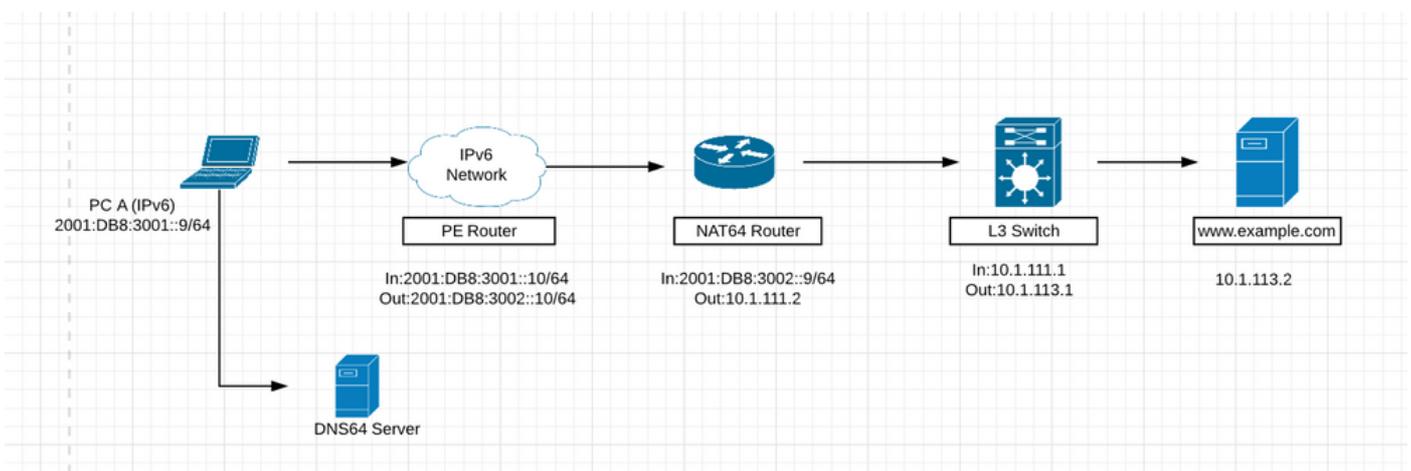
IPv4アドレスを節約する

アドレスのオーバーロードを使用するため、エンドツーエンドのアドレス透過性が欠ける状態またはバインドは、一意の変換ごとに作成します

IPv6アドレス割り当ての特性に関する要件がない任意のモードのIPv6アドレス割り当てviz.手動、DHCPv6、SLAAC

- このドキュメントでは、IPv6ホストがIPv4サーバと通信する際のLAB演習を使用したステートフルNAT64を示しました。また、IPv4ホストがIPv6サーバに到達するステートレスNAT64を実証しました。このシナリオはNAT46とも呼ばれます。

シナリオ 1 : IPv6ネットワーク内のホストからIPv4サーバ (IPv4ネットワーク内) と通信する場合



- 上の図では、IPv6ネットワーク内のホストが、IPv4ネットワーク内のip 10.1.113.2を持つWebサーバ(www.example.com)に到達しようとしています。
- IPv6ネットワークのホストからIPv4アドレス(10.1.113.2)に直接pingを実行すると、デバイスはIPv6アドレスのみを認識するため、このIPv4アドレスを認識しません。したがって、パケットはホストでドロップされます。
- 同様に、IPv4ネットワークからIPv6アドレスにpingを実行すると、デバイスはそのipを認識せず、デフォルトでIPv4ネットワーク専用設定されているため、エラーが発生します。
- また、IPv4パケットはIPv6専用ネットワークを経由してルーティングされることも、逆にルーティングされることもありません。したがって、エッジデバイス上のパケットを要件に応じてIPv4またはIPv6に変換するために、変換が必要になります。

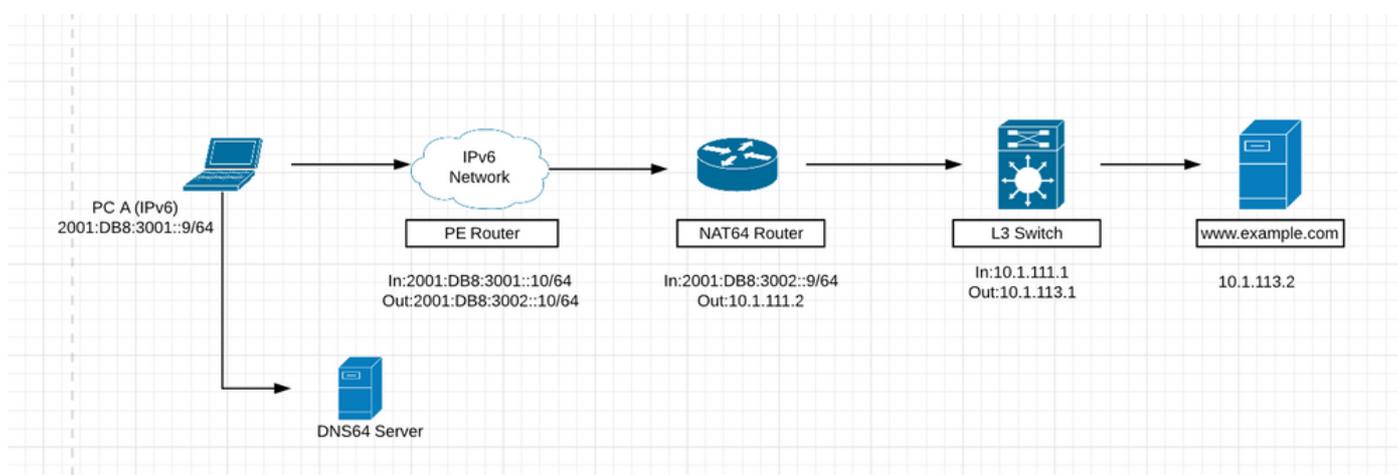
NAT64には3つの主要コンポーネントがあります

- NAT64プレフィクス** : IPv6専用ネットワーク上でパケットを送信するために、変換されたIPv4アドレスで使用される/32、/40、/48、/56、/64、または/96プレフィクス。NAT64プレフィクスは、ネットワーク固有のプレフィクス(NSP)または既知のプレフィクス(WKP)にするこ

とができます。NSPは組織によって割り当てられ、通常は組織のIPv6プレフィクスからのサブネットです。NAT64のWKPは64:ff9b::/96です。NSPが指定または設定されていない場合、NAT64はWKPを使用して、変換されたIPv4アドレスをプリペンドします。NAT64プレフィクスは、Pref64::/nとも呼ばれます。

- **DNS64サーバ**：DNS64サーバは、IPv6 AAAAレコードの通常のDNSサーバとして機能しますが、AAAAレコードが使用できない場合は、IPv4 Aレコードの検索も試行します。Aレコードが見つかった場合、DNS64はNAT64プレフィックスを使用してIPv4 AレコードをIPv6 AAAAレコードに変換します。これにより、IPv6専用ホストはIPv6を使用してサーバと通信できるという印象を受けます。
- **NAT64ルータ**：NAT64ルータは、IPv6専用ネットワークとIPv4専用ネットワーク間の変換を実行しながら、NAT64プレフィックスをIPv6専用ネットワークにアドバタイズします。

ステートフルNAT64の場合のパケットフロー



1. IPv6ネットワークに存在する上記の図のホストが、IPv4専用サーバであるWebサーバ www.example.com (10.1.113.2)と通信するとします。
2. この通信を可能にするには、IPv6ネットワークにDNS64サーバをインストールし、ipv4要求のDNSを理解して解決する必要があります。
3. DNS64サーバは、IPv6 AAAAレコードの通常のDNSサーバとして機能しますが、AAAAレコードが使用できない場合は、IPv4 Aレコードの検索も試みます。Aレコードが見つかった場合、DNS64はNAT64プレフィックスを使用してIPv4 AレコードをIPv6 AAAAレコードに変換します。これにより、IPv6専用ホストはIPv6を使用してサーバと通信できるという印象を受けます。
4. www.example.comに対するDNS解決要求がDNS64サーバに送信されます。このWebサイトサーバはIPv4アドレスに属しているため、最初にIPv6 AAAAレコードテーブルを検索しますが、IPv6 AAAAレコードは見つかりません。その後、IPv4データベースを検索し、このWebサイトに一致するIPv4アドレスを見つけます。これで、DNS64サーバはこのIPv4アドレスを16進数に変換し、NAT64プレフィックスをプリペンドして、このIPv4アドレスをIPv6アドレスに変換します。これにより、IPv6ホストはIPv6を使用してWebサーバと通信できるという印象を受けます。
5. パケットは、IPv6専用ネットワークで、IPv4アドレスの16進値に付加されたNAT64プレフィックスを使用してNAT64を実行するデバイスにルーティングされます。
6. NAT64ルータは、IPv6専用ネットワークとIPv4専用ネットワーク間の変換を実行しながら、

NAT64プレフィックスをIPv6専用ネットワークにアドバタイズします。

7.パケットがNAT64変換を行うデバイスにヒットすると、パケットはNat64用に設定したACLと照合されます。パケットがこのACLと一致すると、NAT64を使用してパケットはさらに変換されません。

8.ステートフルNAT64は、設定されたアクセスコントロールリスト(ACL)およびプレフィックスリストを使用して、NAT64状態の作成を許可されるIPv6開始トラフィックフローをフィルタリングします。IPv6ホストとIPv4アドレス間のマッピングの動的割り当てはこの方向でのみ行えるため、IPv6パケットのフィルタリングはIPv6からIPv4への方向で行われます。ステートフルNAT64は、PAT設定を使用したIPv4からIPv6へのパケットフローのエンドポイント依存フィルタリングをサポートします。

9.ステートフルNAT64 PAT設定では、パケットフローはIPv6レルムから発信され、NAT64ステートテーブルに状態情報を作成する必要があります。以前に作成された状態を持たないIPv4側からのパケットは廃棄されます。エンドポイントに依存しないフィルタリングは、スタティックなネットワークアドレス変換(NAT)および非PAT設定でサポートされます。

最初のIPv6パケットは、ステートフルプレフィックスに設定された自動ルーティング設定に基づいて、NAT仮想インターフェイス(NVI)にルーティングされます。ステートフルNAT64は、一連のルックアップを実行して、IPv6パケットがアクセスコントロールリスト(ACL)ルックアップに基づいて設定されたマッピングのいずれかに一致するかどうかを判別します。マッピングに基づいて、IPv4アドレス(およびポート)がIPv6宛先アドレスに関連付けられます。

IPv6パケットは変換され、IPv4パケットは次の方法で形成されます。

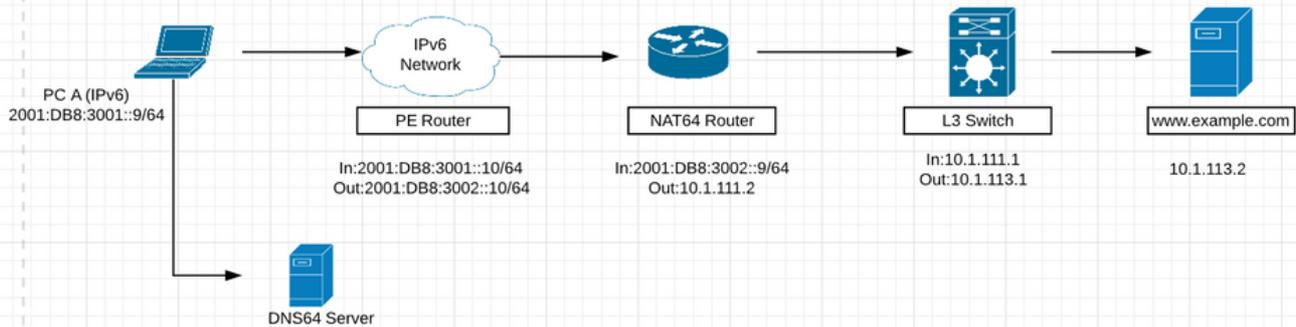
1. IPv6アドレスからプレフィックスを削除して、宛先IPv4アドレスを抽出します。送信元アドレスは、割り当てられたIPv4アドレス(およびポート)に置き換えられます。
2. 残りのフィールドはIPv6からIPv4に変換され、有効なIPv4パケットが形成されます。

10.新しいNAT64変換がセッションデータベースとバインドデータベースに作成されます。プールとポートデータベースは、設定に応じて更新されます。

11. IPv6パケットフローのリターントラフィックと後続のトラフィックは、このセッションデータベースエントリを変換に使用します。

- NAT64が機能するには、ipv6ネットワーク内のインターフェイスのipv6アドレスへの到達可能性がipv6から存在し、到達可能性もNAT64ルータからサーバのipv4アドレスへの到達可能性である必要があります。

NAT64の設定ガイド



ステップ1: ホストAは、サーバwww.example.comと通信するIPv6専用ホストです。これにより、DNSクエリ(AAAA:www.example.com)をDNS64サーバに送信します。DNS64は、このプロセスの主要コンポーネントです。DNS64サーバは、IPv6とIPv4の両方のDNSサーバです。クライアントは、IPv4サーバにIPv6アドレスを使用して到達できるという錯覚を抱きます。

ホストAがDNSクエリ(AAAA:www.example.com)をDNS64サーバに送信します。ホストAに関する限り、これはIPv6サーバの通常のDNS AAAAクエリです。

ステップ2: DNS64サーバは、ホストAからDNS AAAAクエリを受信します。ドメイン名を解決するために、DNS64サーバはwww.example.comのDNS AAAA権威サーバにクエリを送信します。

ステップ3: IPv6 DNS AAAA権威サーバは、www.example.comのAAAAリソースレコードを持っていないことを示す応答を返します。

ステップ4: AAAAクエリに対する空の応答（名前エラー）を受信すると、DNS64サーバがAクエリ(A:www.example.com)をIPv4 DNS A権威サーバに送信します。

ステップ5: IPv4 DNS権威サーバは、www.example.comに対するAリソースレコードを持ち、サーバのIPv4アドレスを持つ応答(A:www.example.com 10.1.113.2)。

手順6: DNS64サーバは、DNS A権威サーバからIPv4アドレスを受信し、そのアドレスをNAT64プレフィックス2800:1503:2000:1:1::/96でプリフィックスしてAAAAレコードを合成し、IPv4アドレスを16進数0a01:711010100000000000200000002ホストAがwww.example.comサーバに到達するための宛先IPv6アドレスとして使用します。

ステップ8: 合成されたAAAAレコードは、ホストAに対して完全に透過的です。ホストAに対しては、www.example.comがIPv6ネットワークおよびインターネットを介して到達可能であるかのように見えます。ホストAは、次の情報を使用してIPv6パケットをwww.example.comに送信するために必要なアドレス情報を取得できます。

- IPv6宛先アドレス：2800:1503:2000:1:1::0a01:71102
- IPv6送信元アドレス：2001:DB8:3001::9

ステップ9: NAT64ルータは、NAT64対応インターフェイスでホストAから送信されたIPv6パケットを受信します。着信パケットと設定済みACLを照合します。一致が見つからない場合、パケットは通常のIPv6ルーティングを使用して変換されずに転送されます。一致が見つかった場合、パケットは次の変換を行います。

- IPv6ヘッダーがIPv4ヘッダーに変換されます。
- IPv6宛先アドレスは、IPv6ステートフルNAT64プレフィックス2800:1503:2000:1:1::/96を削

除することによって、IPv4アドレスに変換されます。IPv6アドレス0a01:7102の下位32ビットは、ドット付き10進数のIPv4アドレス10.1.113.2として表されます。

- IPv6送信元アドレスは、設定されたIPv4アドレスプールを使用してIPv4アドレスに変換されます。NAT64の設定によっては、1:1アドレス変換を使用するか、IPv4アドレスのオーバーロードを使用します。これはIPv4のNATに似ています。このシナリオでは、ホストAの送信元IPv6アドレスが50.50.50.50 IPv4アドレスに変換されます。
- ステートフルNAT64 IPアドレス変換状態は、送信元アドレスと宛先アドレスの両方に対して作成されます。これらの状態は、パケットで最初に変換が実行されたときに作成されます。この状態は、フロー内の後続のパケットに対して維持されます。状態は、トラフィックと状態メンテナンスタイマーが期限切れになると終了します。

```
HUB-BR-1#sh nat64 translations
Proto  Original IPv4      Translated IPv4
       Translated IPv6  Original IPv6
-----
icmp   10.1.113.2:2654   [2800:1503:2000:1:1:0:a01:7102]:2654
       50.50.50.50:2654 [2001:db8:3001::9]:2654
Total number of translations: 1
```

ステップ10:NAT64変換の後、変換されたIPv4パケットは通常のIPv4ルートルックアッププロセスを使用して転送されます。このシナリオでは、パケットの転送にIPv4宛先アドレス10.1.113.2が使用されます。

ステップ11:www.example.comサーバは10.1.113.2の応答を返します。これは最終的にNAT64ルータによって受信されます。

ステップ12:NAT64ルータは、NAT64対応インターフェイスの1つでwww.example.comサーバからIPv4パケットを受信します。ルータはIPv4パケットを調べて、IPv4宛先アドレスにNAT64変換状態が存在するかどうかを判別します。変換状態が存在しない場合、パケットは廃棄されます。IPv4宛先アドレスの変換状態が存在する場合、NAT64ルータは次のタスクを実行します。

- IPv4ヘッダーがIPv6ヘッダーに変換されます。
- IPv4送信元アドレスは、既存のNAT64変換状態を使用してIPv6送信元アドレスに変換されます。このシナリオでは、送信元アドレスがIPv4アドレス10.1.113.2からIPv6アドレス2800:1503:2000:1:1:0:a01:7102に変換されます。宛先アドレスは、IPv4アドレス50.50.50.50から2001:DB8:3001::9に変換されます。

ステップ13:変換後、IPv6パケットは通常のIPv6ルートルックアッププロセスを使用して転送されます。

NAT 46ルータの設定

1.IPv6対応インターフェイス :

```
HUB-BR-1#sh run int gig0/0/1
Building configuration...

Current configuration : 131 bytes
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 nat64 enable
 cdp enable
 ipv6 address 2001:DB8:3002::9/64
end
```

2. IPv4側インターフェイス :

```
HUB-BR-1#sh run int gig0/0/0
Building configuration...

Current configuration : 119 bytes
!
interface GigabitEthernet0/0/0
 ip address 10.1.111.2 255.255.255.0
 negotiation auto
 nat64 enable
 cdp enable
end
```

3. ipv6トラフィックに一致するACLの作成

```
HUB-BR-1#sh ipv6 access-list nat64acl
IPv6 access list nat64acl
    permit ipv6 2001:DB8:3001::/64 any sequence 10
HUB-BR-1#
```

4. NAT64 IPv6とIPv4のアドレスマッピングを有効にします。

#nat64 prefix stateful 2800:1503:2000:1:1::/96 →サーバIPはこのipv6 ipアドレスにマッピングされます。ここで任意のipv6ネットワークアドレスを設定できますが、このipv6ネットワークアドレスはipv6ネットワークから到達可能である必要があります。また、DNS64サーバには、このipv6ネットワークアドレスとサーバipv4アドレスのマッピングが必要です。

5. #nat64 v4 pool pool1 50.50.50.50 50.50.50.50 →パケットがipv4ネットワークに入る間、元のipv6送信元アドレスがこのプールのipsに変換されます。
6. #nat64 v6v4 list nat64acl pool pool1 overload →これにより、nat64aclに一致するipv6アドレスがプールからipv4アドレスに変換されます
7. 10.1.113.2の16進数値は0a01:7102です。この設定が完了したら、PC Aから2800:1503:2000:1:1::0a01:7102アドレスにpingを実行します。

```
#ping 2800:1503:2000:1:1::0a01:7102
```

NAT64の詳細の確認

```
#show nat64
```

```
HUB-BR-1#sh nat64 translations
Proto  Original IPv4      Translated IPv4
       Translated IPv6  Original IPv6
-----
icmp   10.1.113.2:7749   [2800:1503:2000:1:1:0:a01:7102]:7749
       50.50.50.50:7749 [2001:db8:3001::9]:7749
Total number of translations: 1
```

```
#show nat64
```

```
HUB-BR-1#sh nat64 statistics
NAT64 Statistics

Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Sessions found: 33
Sessions created: 4
Expired translations: 4
Global Stats:
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 18
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 20
    MAP-T: 0

Interface Statistics
GigabitEthernet0/0/0 (IPv4 configured, IPv6 not configured):
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 15
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 0
    MAP-T: 0
  Packets dropped: 5
GigabitEthernet0/0/1 (IPv4 not configured, IPv6 configured):
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 0
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 20
    MAP-T: 0
  Packets dropped: 0
Dynamic Mapping Statistics
v6v4
  access-list nat64acl pool pool1 refcount 1
  pool pool1:
    start 50.50.50.50 end 50.50.50.50
    total addresses 1, allocated 1 (100%)
    address exhaustion packet count 0
Limit Statistics
```

シナリオ 2 : IPv4専用クライアントからIPv6専用サーバへのトラフィック開始

ドレスに追加することによって、IPv6アドレスに変換されます。これにより、IPv6送信元アドレス2800:1503:2000:1:1::0a01:7102になります(0a01:7102は10.1.113.2の16進数に相当します)。

ステップ6: 変換後、IPv6パケットは通常のIPv6ルーティングプロセスを使用してルーティングされます。パケットは最終的に2001:DB8:3001::9のwww.examplev6.comサーバにルーティングされます。

ステップ7: サーバwww.examplev6.comはホストA宛てのパケットで応答します。

ステップ8: NAT64ルータは、IPv6サーバから送信されたIPv6パケットをNAT64対応インターフェイスで受信し、次のタスクを実行します。

- IPv6ヘッダーがIPv4ヘッダーに変換されます。
- IPv6送信元アドレスは、ステートフル変換テーブルを使用して50.50.50.50に変換されます。
- IPv6宛先アドレスは、IPv6ステートフルNAT64プレフィクス2800:1503:2000:1:1::/96を削除してIPv4アドレスに変換されます。IPv6アドレスの下位32ビットである0a01:7102は、ドット付き11111110進数0IP0IP0IP0IP0IP0IP0IP4アドレス4アドレス0000000000002002000000002002000000000000000000000000

ステップ9: 変換後、NAT64ルータは通常のIPv4ルーティングプロセスを使用してパケットを10.1.113.2に転送します。

- 前のシナリオと同様に、ステートフルNAT64を使用して、IPv4専用クライアントとIPv6専用サーバの間で透過的な通信が確立されます。設定は、ステップ1で説明したstatic mappingコマンドを除いて類似しています。

NAT 46ルータの設定

1. IPv4側インターフェイス:

```
HUB-BR-1#sh run int gig0/0/0
Building configuration...

Current configuration : 137 bytes
!
interface GigabitEthernet0/0/0
 ip address 10.1.111.2 255.255.255.0
 ip ospf 1 area 0
 negotiation auto
 nat64 enable
 cdp enable
end
```

2. IPv6対応インターフェイス:

```
HUB-BR-1#sh run int gig0/0/1
Building configuration...

Current configuration : 131 bytes
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 nat64 enable
 cdp enable
 ipv6 address 2001:DB8:3002::9/64
end
```

3. IPv4からIPv6にトラフィックを正常に変換するためにルータに必要なその他の設定 :

```
nat64 prefix stateful 2800:1503:2000:1:1::/96
nat64 v6v4 static 2001:DB8:3001::9 50.50.50.50
```

設定が成功したら、IPv4ホストから50.50.50.50にpingします。

```
#ping 50.50.50.50
```

NAT46の確認

```
#show nat64
```

```
HUB-BR-1#sh nat64 translations

Proto  Original IPv4      Translated IPv4
       Translated IPv6  Original IPv6
-----
illegal ---
       50.50.50.50    2001:db8:3001::9
icmp   10.1.113.2:11     [2800:1503:2000:1:1:0:a01:7102]:11
       50.50.50.50:11 [2001:db8:3001::9]:11

Total number of translations: 2
```

```
#show nat46
```

```

HUB-BR-1#sh nat64 statistics
NAT64 Statistics

Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Sessions found: 9967
Sessions created: 14
Expired translations: 14
Global Stats:
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 4990
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 4992
    MAP-T: 0

Interface Statistics
GigabitEthernet0/0/0 (IPv4 configured, IPv6 not configured):
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 1947
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 0
    MAP-T: 0
  Packets dropped: 58
GigabitEthernet0/0/1 (IPv4 not configured, IPv6 configured):
  Packets translated (IPv4 -> IPv6)
    Stateless: 0
    Stateful: 0
    MAP-T: 0
  Packets translated (IPv6 -> IPv4)
    Stateless: 0
    Stateful: 1947
    MAP-T: 0
  Packets dropped: 0
Dynamic Mapping Statistics
  v6v4
Limit Statistics

```

翻訳シナリオとその適用可能性

IPv6/IPv4変換のシナリオ

- シナリオ 1 : IPv4インターネットへのIPv6ネットワーク
- シナリオ 2 : IPv4インターネットからIPv6ネットワーク
- シナリオ 3 : IPv6インターネットからIPv4ネットワーク
- シナリオ 4 : IPv6インターネットへのIPv4ネットワーク
- シナリオ 5 : IPv4ネットワークへのIPv6ネットワーク
- シナリオ 6 : IPv4ネットワークからIPv6ネットワークへ
- シナリオ 7 : IPv6インターネットからIPv4インターネットへ
- シナリオ 8 : IPv4インターネットからIPv6インターネットへ

適用性

- ・ IPv6と既存のIPv4コンテンツの両方に透過的にアクセス可能
- ・ IPv6ホストおよびネットワークから開始
- ・ IPv4ユーザとIPv6ユーザの両方に透過的にサービス可能
- ・ IPv4ホストおよびネットワークから開始
- ・ 既存のIPv4専用ネットワーク内のサーバで、IPv6ホストおよびネットワークから開始

近い将来、実行可能な事例ではない。このシナリオは

IPv4ネットワークとIPv6ネットワークの両方が同じ組織

上記と同じ

スループットが低下する

無制限のIPv6アドレス変換を処理する実行可能な変換

NAT64の実装時に問題が発生した場合に備えた重要なトラブルシューティングコマンド

```
#show platform hardware qfp active statistics drop(nat64)
```

```
#show running-config | include nat64 IOS
```

```
#show platform hardware qfp active feature nat64 datapath statistics
```

```
#show platform hardware qfp active feature nat64 datapath pool (pool is configured properly)
```

```
#show platform hardware qfp active feature nat64 datapath map(pool to mapping config)
```

```
#show platform software object-manager F0 pending-ack-update()
```