ネットワーク アドレス変換の設定

Network Address Translation（NAT）

ネットワーク アドレス変換（NAT）は、IP アドレスの節約を目的として設計されています。NAT によって、未登録 IP アドレスを使用するプライベート IP ネットワークをインターネットに接続できます。NAT はデバイス（通常、2 つのネットワークを接続するもの）上で動作し、別のネットワークにパケットを転送する前に、内部ネットワークのプライベート（グローバルに一意ではない）アドレスをグローバルにルート可能なアドレスに変換します。

NAT では、外部にアドバタイズするアドレスをネットワーク全体で 1 つだけにする機能を備えています。この機能により、そのアドレスの後ろにある内部ネットワーク全体を効果的に隠すことができ、セキュリティが強化されます。NAT には、セキュリティおよびアドレス節約の二重の機能性があり、一般的にリモート アクセス環境で実装されます。

NAT は、エンタープライズ エッジでも使用され、内部ユーザーのインターネットへのアクセスを許可し、メール サーバーなど内部デバイスへのインターネット アクセスを許可します。

Cisco Catalyst 9300 シリーズ スイッチはスタックをサポートしており、NAT はスタック設定でサポートされます。

NAT の設定の利点

- IP が枯渇する問題を解決します。

  組織が NAT を使用すると、既存のネットワークを持っていてインターネットにアクセスする必要がある場合に、IP アドレスが枯渇する問題を解決できます。ネットワーク インフォメーションセンター（NIC）に登録された IP アドレスをまだ持っていないサイトは、IP アドレスを取得する必要があります。255 以上のクライアントが存在する、またはそのような環境を予定している場合は、Class B アドレスの不足が深刻な問題になります。NAT はこのような問題に対応するために、隠された数千の内部アドレスを、取得の容易な Class C アドレスの範囲にマップします。

- クライアント IP アドレスを外部ネットワークから隠すことで、セキュリティ レイヤも提供します。

  内部ネットワークのクライアントの IP アドレスをすでに登録しているサイトでも、ハッカーがクライアントを直接攻撃できないように、これらのアドレスをインターネットから隠すことができます。クライアントアドレスを隠すことにより、セキュリティがさらに強化されます。NAT により LAN 管理者は、インターネット割り当て番号局の予備プールを利用して、Class A アドレスを自由に拡張することができます。Class A アドレスの拡張は組織内で行われ、LAN またはインターネット インターフェイスでアドレッシングの変更に配慮する必要はありません。

- Cisco ソフトウェアは、選択的、またはダイナミックに NAT を実行できます。この柔軟性により、ネットワーク管理者は RFC 1918 アドレスまたは登録したアドレスを使用することができます。

- NAT は、IP アドレスの簡略化や節約のためにさまざまなデバイス上で使用できるように設計されています。また、NAT により、変換に使用できる内部ホストを選択することもできます。

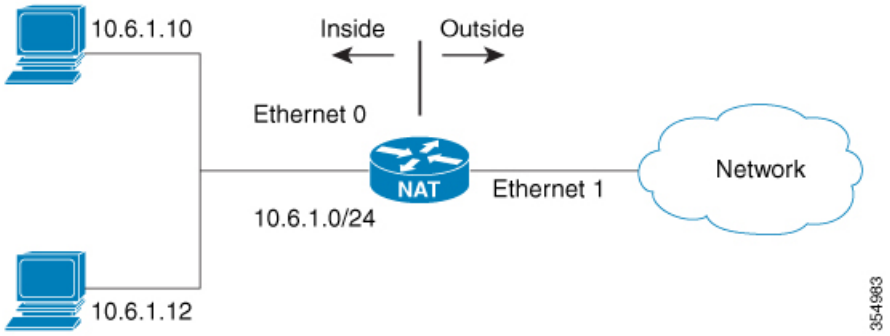
- NAT は、NAT を設定する若干のデバイス以外には、何ら変更を加えずに設定できるという大きな利点があります。

NAT の機能

NAT が設定されたデバイスには、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。標準的な環境では、NAT はスタブ ドメインとバックボーン間の出口デバイスに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元 アドレスをグローバルで一意の アドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルに一意な宛先アドレスをローカルアドレスに変換します。複数の内部ネットワークをデバイスに接続でき、同様にデバイスから外部ネットワークへと複数の終了ポイントが存在する場合があります。アドレスが足りなくなって、パケットにアドレスを割り当てられなくなった場合、NAT はそのパケットをドロップし、Internet Control Message Protocol（ICMP）ホスト到達不能パケットをその接続先に送信します。

変換および転送は、ハードウェアのスイッチング プレーンで実行され、全体的なスループットのパフォーマンスが改善されます。パフォーマンスの詳細については、「NAT のパフォーマンスとスケール数」を参照してください。

図 *1 : NAT*



NAT の用途

NAT は次のような場合に使用できます。

- ホストのごく少数しかグローバルな一意の IP アドレスを持っていない状況でインターネットに接続する場合。

  NAT はスタブ ドメイン（内部ネットワーク）と、インターネットなどのパブリック ネットワーク（外部ネットワーク）との境界にあるデバイス上に設定されます。NAT はパケットを外部ネットワークに送信する前に、内部のローカル アドレスをグローバルに一意の IP アドレスに変換します。接続性の問題への解決策として NAT が役立つのは、スタブ ドメイン内の比較的少数のホストが同時にドメインの外部と通信する場合のみです。この場合、外部との通信が必要なときに、このドメインにある IP アドレスのごく一部をグローバルに一意な IP アドレスに変換する必要があります。また、これらのアドレスは再利用できます。

- 番号付け直し：

  内部アドレスの変更には相当の工数がかかるため、変更する代わりに NAT を使用して変換することができます。

NAT の内部アドレスおよび外部アドレス

NAT において、内部という用語は、変換が必要な組織が所有するネットワークを表します。NAT が設定されている場合、このネットワーク内のホストは、別の空間（グローバル アドレス空間として知られている）にあるものとしてネットワークの外側に現れる 1 つ空間（ローカル アドレス空間として知られている）内のアドレスを持つことになります。

同様に、外部という用語は、スタブ ネットワークの接続先で、通常、その組織の制御下にはないネットワークを表します。外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストはローカル アドレスとグローバル アドレスを持つことができます。

NAT では、次の定義が使用されます。

- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは、多くの場合、NIC やサービス プロバイダーにより割り当てられたルート可能な IP アドレスではありません。
- 内部グローバル アドレス：外部に向けて、1 つ以上の内部ローカル IP アドレスを表すグローバルなルート可能な IP アドレス（NIC またはサービス プロバイダーにより割り当てられたもの）。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。必ずしもルート可能な IP アドレスでありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 外部グローバルアドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられます。
- 内部送信元アドレス変換：内部ローカル アドレスを内部グローバル アドレスに変換します。
- 外部送信元アドレス変換：外部グローバル アドレスを外部ローカル アドレスに変換します。
- スタティック ポート変換：内部/外部ローカルアドレスの IP アドレスとポート番号を、対応する内部/外部グローバル アドレスの IP アドレスとポート番号に変換します。
- 特定のサブネットのスタティック変換：指定された内部/外部ローカル アドレスの範囲のサブネットを対応する内部/外部グローバル アドレスに変換します。
- ハーフ エントリ：ローカルおよびグローバル アドレス/ポート間のマッピングを表し、NAT モジュールの変換データベースで維持されます。ハーフ エントリは、設定されている NAT ルールに基づいて、静的または動的に作成できます。

- フル エントリ/フロー エントリ：特定のセッションに対応する一意のフローを表します。ローカルからグローバルへのマッピングに加えて、指定したフローを完全修飾する接続先情報も維持されます。フル エントリは常に動的に作成されて NAT モジュールの変換データベースで維持されます。

NAT のタイプ

ネットワーク全体を表す 1 つのアドレスのみを外部にアドバタイズするように NAT を設定できます。これにより、内部ネットワークを外部から効果的に隠すことができるため、セキュリティがさらに強化されます。

NAT には次のタイプがあります。

- スタティック アドレス変換（スタティック NAT）：ローカル アドレスとグローバル アドレスを 1 対 1 マッピングします。
- ダイナミック アドレス変換（ダイナミック NAT）：未登録の IP アドレスを、登録済み IP アドレスのプールから取得した登録済み IP アドレスにマップします。
- オーバーロード/PAT：複数の未登録 IP アドレスを、複数の異なるレイヤ 4 ポートを使用して、1 つの登録済み IP アドレスにマップ（多対 1）します。この方法は、ポート アドレス変換（PAT）とも呼ばれます。オーバーロードを使用することにより、使用できる正規のグローバル IP アドレスが 1 つのみでも、数千のユーザーをインターネットに接続することができます。

NAT による外部ネットワークへのパケットのルーティング（内部送信元アドレス変換）

自分が属するネットワークの外部と通信するときに、未登録の IP アドレスをグローバルで一意な IP アドレスに変換できます。

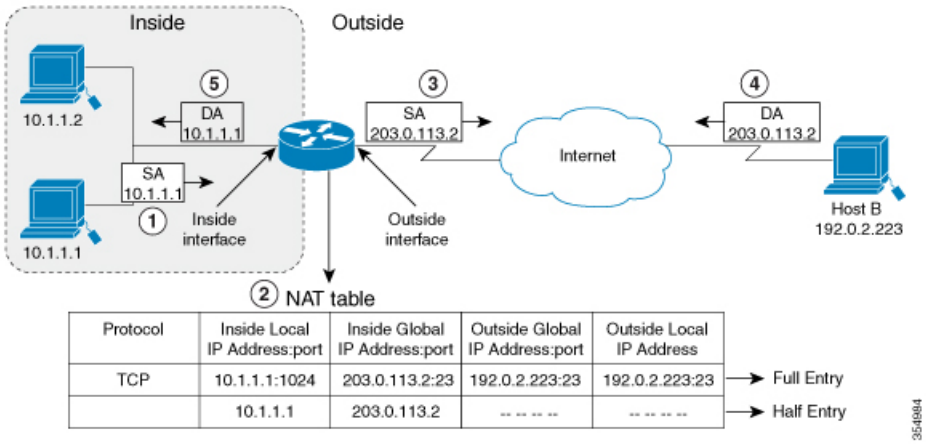
スタティックまたはダイナミック内部送信元アドレス変換は、次のようにして設定できます。

- スタティック変換は、内部ローカル アドレスと内部グローバル アドレスの間に 1 対 1 のマッピングを設定します。外部から固定アドレスを使って内部のホストにアクセスする必要がある場合には、スタティック変換が便利です。スタティック変換は、内部送信元アドレスのスタティック変換の設定 （13 ページ）で説明されているように、スタティック NAT ルールを設定して有効にできます。
- ダイナミック変換は、内部ローカル アドレスとグローバル アドレスのプールの間にマッピングを動的に設定します。ダイナミック変換は、ダイナミック NAT ルールを設定することで有効にできます。マッピングは、設定されているルールをランタイム時に評価した結果に基づいて設定されます。内部ローカルアドレスの指定には、標準と拡張の両方のアクセス コントロール リスト（ACL）を使用できます。内部グローバル アドレスはアドレ

スプールまたはインターフェイスから指定できます。ダイナミック変換は、内部送信元アドレスのダイナミック変換の設定 （14 ページ） のセクションで説明されているようにダイナミックルールを設定して有効にできます。

次の図には、ネットワーク内の送信元アドレスを、ネットワーク外の送信元アドレスに変換するデバイスが示されています。

図 *2 : NAT* 内部送信元変換



次のプロセスは、上の図に示す内部送信元アドレス変換について示します。

1. ホスト 10.1.1.1 のユーザーは、外部ネットワークのホスト B との接続を開きます。
2. NAT モジュールは、対応するパケットをインターセプトし、パケットを変換しようとします。

   一致する NAT ルールの有無に基づいて、次のシナリオが考えられます。

   - 一致するスタティック変換ルールが存在する場合、パケットは対応する内部グローバルアドレスに変換されます。存在しない場合、パケットはダイナミック変換ルールに対して照合され、一致した場合は対応する内部グローバルアドレスに変換されます。NAT モジュールは、変換したパケットに対応する完全修飾フローエントリを変換データベースに挿入します。これにより、このフローに対応するパケットの高速変換および転送が双方向で促進されます。
   - 一致するルールがない場合、パケットはアドレス変換を行わずに転送されます。
   - 有効な内部グローバルアドレスを取得できない場合は、たとえ一致するルールがあってもパケットはドロップされます。

（注） ダイナミック変換に ACL が使用される場合、NAT は ACL を評価し、特定の ACL で許可されているパケットのみが変換の対象になるようにします。

3. デバイスはホスト 10.1.1.1 の内部ローカル送信元アドレスを、この変換の内部グローバル アドレス 203.0.113.2 で置き換え、パケットを転送します。
4. 4. ホスト B はこのパケットを受信し、内部グローバル IP 宛先アドレス（DA）203.0.113.2 を使用して、ホスト 10.1.1.1 に応答します。
5. ホスト B からの応答パケットは、内部グローバル アドレスに送られます。NAT モジュールはこのパケットをインターセプトし、変換データベースにセットアップされているフロー エントリを使って対応する内部ローカル アドレスに変換し直します。

ホスト 10.1.1.1 はパケットを受信し、会話を続けます。デバイスは、受信する各パケットについて手順 2 ～ 5 を実行します。

外部送信元アドレス変換

ネットワークの内部から外部に移動する IP パケットの送信元アドレスを変換できます。通常、このタイプの変換は、重複しているネットワークを相互接続するために、内部送信元アドレスの変換と組み合わせて使用されます。

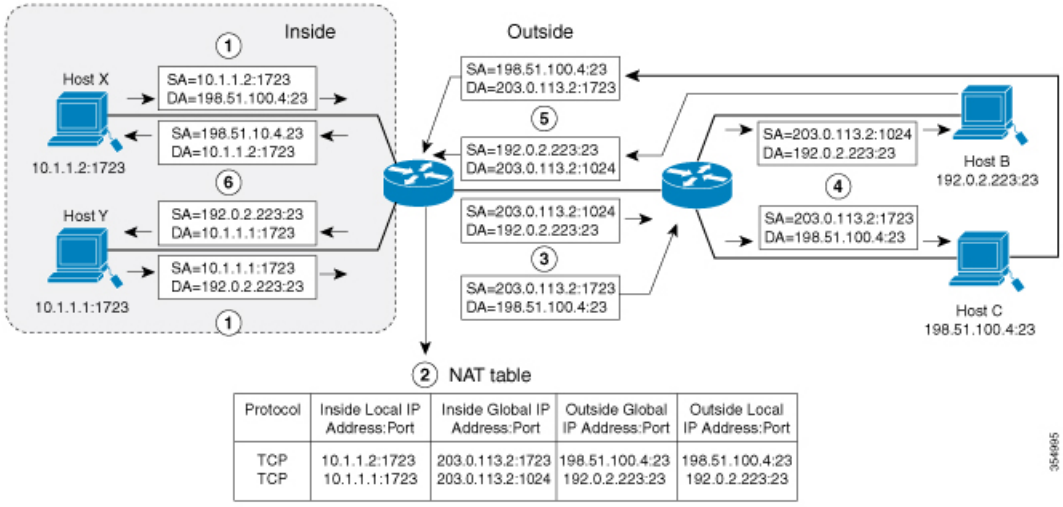
このプロセスについては、セクションで説明します。オーバーラップするネットワークの変換の設定 （20 ページ）

ポート アドレス変換（PAT）

デバイスが複数のローカル アドレスに対して 1 つのグローバル アドレスを使用できるようにすることで、内部グローバル アドレス プール内のアドレスを節約できます。このようなタイプの NAT の設定はオーバーロード、またはポート アドレス変換と呼ばれます。オーバーロードが設定されている場合、デバイスは、より高いレベルのプロトコルから十分な情報（たとえば、TCP または UDP ポート番号）を保持して、グローバル アドレスを正しいローカル アドレスに戻します。複数のローカル アドレスが 1 つのグローバル アドレスにマッピングされる場合、各内部ホストの TCP または UDP ポート番号によりローカル アドレスが区別されます。

次の図は、1 つの内部グローバル アドレスが複数の内部ローカル アドレスを表すときの NAT の動作を示しています。区別は、TCP ポート番号により行われます。

図 *3:* 内部グローバル アドレスをオーバーロードする *PAT/NAT*



このデバイスは、上の図に示すように、内部グローバルアドレスのオーバーロードで次の処理を行います。ホスト B およびホスト C はいずれも、アドレス 203.0.113.2 にある 1 つのホストと通信していると信じています。しかし、実際には、異なるホストと通信しています。区別にはポート番号が使用されます。つまり、多数の内部ホストは、複数のポート番号を使用して、内部グローバル IP アドレスを共有することができます。

1. ホスト 10.1.1.1:1723 のユーザはホスト B への接続を開き、ホスト 10.1.1.2:1723 のユーザはホスト C への接続を開きます。
2. NAT モジュールは、対応するパケットをインターセプトし、パケットの変換を試みます。

   一致する NAT ルールの有無に基づいて、次のシナリオが考えられます。

   - 一致するスタティック変換ルールが存在する場合はそのルールが優先され、パケットは対応するグローバルアドレスに変換されます。存在しない場合、パケットはダイナミック変換ルールに対して照合され、一致した場合は対応するグローバルアドレスに変換されます。NAT モジュールは、変換したパケットに対応する完全修飾フロー エントリを変換データベースに挿入し、このフローに対応するパケットの高速変換および転送を双方向で促進します。
   - 一致するルールがない場合、パケットはアドレス変換を行わずに転送されます。
   - 有効な内部グローバルアドレスを取得できない場合は、一致するルールがあってもパケットはドロップされます。
   - これは PAT 設定であるため、トランスポート ポートにより複数のフローを 1 つのグローバルアドレスに変換できます。（送信元アドレスに加えて送信元ポートも変換されるため、関連付けられているフローエントリは対応する変換マッピングを維持します。）

3. デバイスは、内部ローカル送信元アドレス/ポート 10.1.1.1/1723 および 10.1.1.2/1723 を対応する選択されたグローバル アドレス/ポート 203.0.113.2/1024 および 203.0.113.2/1723 にそれぞれ置き換えてパケットを転送します。
4. ホスト B はこのパケットを受信し、ポート 1024 で内部グローバル IP アドレス 203.0.113.2 を使用してホスト 10.1.1.1 に応答します。ホスト C はこのパケットを受信し、ポート 1723 で内部グローバル IP アドレス 203.0.113.2 を使用してホスト 10.1.1.2 に応答します。
5. デバイスは、内部グローバル IP アドレスを持つパケットを受信すると、内部グローバル アドレスとポート、および外部アドレスとポートをキーとして NAT テーブル検索を実行します。次に、アドレスを内部ローカル アドレス 10.1.1.1:1723/10.1.1.2:1723 に変換し、パケットをホスト 10.1.1.1 および 10.1.1.2 にそれぞれ転送します。

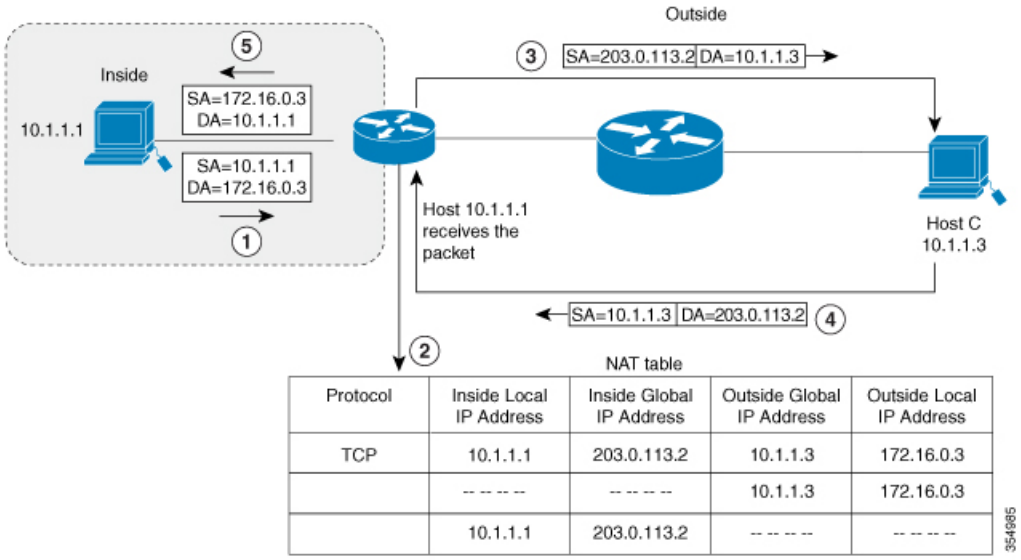
ホスト 10.1.1.1 および 10.1.1.2 はパケットを受信し、通信を続行します。デバイスは、受信する各パケットについて手順 2 ～ 5 を実行します。

オーバーラップ ネットワーク

使用する IP アドレスが合法でない、または正式に割り当てられていない場合、IP アドレスを変換するために NAT を使用します。すでに合法的に所有されインターネットまたは外部ネットワーク上のデバイスに割り当てられている IP アドレスを、独自のネットワーク上の別のデバイスに割り当てると、ネットワークのオーバーラッピングが発生します。

次の図はオーバーラップしたネットワークを示しています。内部ネットワークと外部ネットワークの両方のローカル IP アドレスが同じです（10.1.1.x）。1 台の NAT デバイスを使用している場合、リモート ピアのアドレス（10.1.1.3）を内部から見た別のアドレスに変換するには、そのようにオーバーラップしているアドレス空間の間のネットワーク接続を確立する必要があります。

図 *4: NAT* によるオーバーラップするアドレスの変換



内部ローカルアドレス（10.1.1.1）および外部グローバルアドレス（10.1.1.3）が同じサブネットにあることに注意してください。オーバーラップするアドレスを変換するために、まず、内部送信元アドレスの変換によって内部ローカル アドレスが 203.0.113.2 に変換され、NAT テーブルにハーフ エントリが作成されます。受信側では、外部送信元アドレスが 172.16.0.3 に変換され、ハーフ エントリがもう 1 つ作成されます。すべての変換を完了し、NAT テーブルがフル エントリで更新されます。

次の手順は、オーバーラップするアドレスをデバイスが変換する方法を示します。

1. ホスト 10.1.1.1 は 172.16.0.3 への接続を開きます。
2. NAT モジュールは、内部ローカル アドレスと内部グローバル アドレスを相互に、また外部グローバルアドレスと外部ローカルアドレスを相互にマップする変換マッピングをセットアップします。
3. 送信元アドレス（SA）は、内部グローバルアドレスで置き換えられ、宛先アドレス（DA）は外部グローバル アドレスで置き換えられます。
4. ホスト C はパケットを受信し、会話を続けます。
5. デバイスは NAT テーブルの検索を行い、DA を内部ローカル アドレスで、SA を外部ローカル アドレスで置き換えます。
6. この変換プロセスを使用して、パケットがホスト 10.1.1.1 により受信され、会話が続けられます。

NAT の制限事項

- NAT の動作によっては、ハードウェアデータプレーンで現在サポートされていません。比較的遅いソフトウェア データ プレーンで実行される動作は次のとおりです。
  - Internet Control Message Protocol（ICMP）パケットの変換。
  - アプリケーション レイヤ ゲートウェイ（ALG）処理を必要とするパケットの変換。
  - 内側と外側の両方で変換が必要なパケット。
- 理想的な設定のハードウェアで変換および転送できるセッションの最大数は、Cisco Catalyst 9500シリーズ スイッチでは 2500。変換が必要なその他のフローは、スループットを下げてソフトウェア データ プレーンで処理されます。

（注） 変換ごとに TCAM の 2 つのエントリが使用されます。

- 設定されている NAT ルールは、リソースの制約のためにハードウェアにプログラムできない場合があります。これにより、特定のルールに該当するパケットが変換されずに転送されることがあります。
- ALG のサポートは、FTP、TFTP、および ICMP プロトコルに現在制限されています。また、TCP SYN、TCP FIN、および TCP RST は ALG トラフィックの一部ではありませんが、ALG トラフィックの一部として処理されます。
- ダイナミックに作成された NAT フローは、非アクティブな状態が一定期間続くとエージアウトします。
- ポリシーベースルーティング（PBR）と NAT は、同じインターフェイスではサポートされていません。PBR と NAT は、異なるインターフェイス上に設定されている場合にのみ連携します。
- ポート チャネルは、NAT の設定でサポートされていません。
- NAT は、断片化されたパケットの変換をサポートしていません。
- Bidirectional Forwarding Detection（BFD）は、NAT 設定ではサポートされていません。
- NAT は、ステートフル スイッチオーバー（SSO）をサポートしていません。動的に作成された NAT の状態は、アクティブデバイスとスタンバイデバイスの間で同期されません。
- 等コスト マルチパス ルーティング（ECMP）は、NAT でサポートされていません。
- ルートマップを設定された NAT はサポートされていないため、ルートマップを使用せずに NAT 設定を行う必要があります。
- NAT ACL の明示的な拒否アクセス制御エントリ（ACE）はサポートされていません。明示的な許可 ACE のみがサポートされます。

NAT のパフォーマンスとスケール数

NAT モジュールは、転送情報と書き換え情報を使用して関連したハードウェアテーブルをプログラミングすることで、ハードウェアの変換と転送をラインレートで実行できます。NAT のスループットを向上させるために、NAT 重視のリソース割り当てスキームを設定できます。

より良いパフォーマンスとスケール数が NAT で得られるように SDM テンプレートを設定します。次を参照してください。 スイッチ データベース管理（SDM）テンプレートの設定 （23 ページ）

ハードウェアで使用可能な TCAM フローの最大数は 5000 です。

（注） アドレスのみの変換を使用すると、フローの処理が最適化され、NAT 機能のスケールが拡張されます。

アドレスのみの変換

アドレスのみの変換（AOT）機能は、トランスポートポートではなくアドレスフィールドのみを変換する必要がある状況で使用できます。そのような状況で AOT 機能を有効にすると、ハードウェアにおいてラインレートで変換および転送できるフローの数が大幅に増加します。この改善は、変換および転送に関連したさまざまなハードウェアリソースの使用を最適化することによって実現されます。一般的な NAT 集中型リソース割り当てスキームでは、ハードウェア変換を実行するために 5000の TCAM エントリが確保されます。その結果、ラインレートで変換および転送できるフローの数に厳密な上限が設定されます。AOT スキームでは、TCAM リソースの使用が高度に最適化されるため、TCAM テーブルでより多くのフローに対応できるようになり、ハードウェア変換および転送の規模が大幅に拡大します。AOT は、フローの大部分が単一または少数の宛先に送信される場合に非常に効果的です。そのような良好な条件下では、AOT により、特定のエンドポイントから発信されるすべてのフローのラインレート変換および転送が有効になる可能性があります。AOT 機能は、デフォルトでは無効になっています。**no ip nat create flow-entries** コマンドを使用して有効にできます。既存のダイナミックフローは、**clear ip nat translation** コマンドを使用してクリアできます。AOT 機能は、**ip nat create flow-entries** コマンドを使用して無効にできます。

アドレスのみの変換の制限事項

- AOT 機能は、単純な内部スタティックルールおよび内部ダイナミックルールに対応する変換シナリオでのみ正しく機能すると想定されています。単純なスタティックルールのタイプは **ip nat inside source static** *local-ip global-ip* で、ダイナミックルールのタイプは **ip nat inside source list** *access-list* **pool** *name* である必要があります。

- AOT が有効になっている場合、**show ip nat translation** コマンドを使用しても、変換および転送されるすべての NAT フローの可視性が実現することはありません。

NAT の設定

このセクションで説明するタスクを使用して、NAT を効果的に設定できます。設定によっては、複数の作業を実行する必要があります。

内部送信元アドレスのスタティック変換の設定

内部ローカル アドレスと内部グローバル アドレス間の 1 対 1 マッピングを可能にするには、内部送信元アドレスのスタティック変換を設定します。外部から固定アドレスを使って内部のホストにアクセスする必要がある場合には、スタティック変換が便利です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	要件に応じて次の 3 つのコマンドのいずれかを使用します。
	• **ip nat inside source static** *local-ip global-ip*
	`Switch(config)# ip nat inside source static 10.10.10.1 172.16.131.`
	• **ip nat inside source static** *protocol local-ip port global-ip port*
	`Switch(config)# ip nat inside source static tcp 10.10.10.1 1234 172.16.131.1 5467`
	• **ip nat inside source static network** *local-ip global-ip* { **prefix_len** *len* | **subnet** *subnet-mask*}
	`Switch(config)# ip nat inside source static network 10.10.10.1 172.16.131.1 prefix_len 24`
		内部ローカルアドレスと内部グローバルアドレス間のスタティック変換を設定します。
		内部ローカルアドレスと内部グローバルアドレス間のスタティック ポート変換を設定します。
		内部ローカルアドレスと内部グローバルアドレス間のスタティック変換を設定します。内部グローバルアドレスに変換するサブネットの範囲を指定できます。IP アドレスのホスト部分は変換されますが、IP のネットワーク部分は同じままになります。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Switch(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *ip-address mask* **[secondary]** 例： `Switch(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 6	**ip nat inside** 例： `Switch(config-if)# ip nat inside`	NAT の対象である内部ネットワークにインターフェイスを接続します。
ステップ 7	**exit** 例： `Switch(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 8	**interface** *type number* 例： `Switch(config)# interface gigabitethernet 0/0/0`	異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* **[secondary]** 例： `Switch(config-if)# ip address 172.31.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 10	**ip nat outside** 例： `Switch(config-if)# ip nat outside`	外部ネットワークにインターフェイスを接続します。
ステップ 11	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

内部送信元アドレスのダイナミック変換の設定

ダイナミック変換は、内部ローカル アドレスとグローバル アドレスのプールの間にマッピングを動的に設定します。ダイナミック変換は、ダイナミック NAT ルールを設定することで有効にできます。マッピングは、設定されているルールをランタイム時に評価した結果に基づいて設定されます。内部ローカル アドレスの指定には ACL を使用できます。また、内部グローバル アドレスは、アドレス プール、またはインターフェイスから指定できます。

プライベート ネットワークに存在する複数のユーザーがインターネットへのアクセスを必要としている場合には、ダイナミック変換が便利です。ダイナミックに設定されたプール IP アドレスは必要に応じて使用でき、インターネットへのアクセスが必要なくなったときは別のユーザーが使用できるようにリリースできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* | **prefix-length** *prefix-length* 例： `Switch(config)# ip nat pool net-208 172.16.233.208 172.16.233.223 prefix-length 28`	必要に応じて割り当てられるグローバル アドレスのプールを定義します。
ステップ 4	**access-list** *access-list-number* **permit** *source [source-wildcard]* 例： `Switch(config)# access-list 1 permit 192.168.34.0 0.0.0.255`	変換されるアドレスを許可する標準アクセス リストを定義します。
ステップ 5	**ip nat inside source list** *access-list-number* **pool** *name* 例： `Switch(config)# ip nat inside source list 1 pool net-208`	ステップ 4 で定義したアクセス リストを指定して、ダイナミック送信元変換を設定します。
ステップ 6	**interface** *type number* 例： `Switch(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *ip-address mask* 例： `Switch(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 8	**ip nat inside** 例：	NAT の対象である内部ネットワークにインターフェイスを接続します。

	コマンドまたはアクション	目的
	`Switch(config-if)# ip nat inside`	
ステップ 9	**exit** 例： `Switch(config-if)#exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Switch(config)# interface ethernet 0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* 例： `Switch(config-if)# ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 12	**ip nat outside** 例： `Switch(config-if)# ip nat outside`	外部ネットワークにインターフェイスを接続します。
ステップ 13	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

PAT の設定

グローバル アドレスのオーバーロードを使用して、内部ユーザにインターネットへのアクセスを許可し、内部グローバル アドレス プールのアドレスを節約するには、この作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip nat pool** *name start-ip end-ip* **netmask** *netmask* | **prefix-length** *prefix-length* 例： `Switch(config)# ip nat pool net-208 192.168.202.129 192.168.202.158 netmask 255.255.255.224`	必要に応じて割り当てられるグローバル アドレスのプールを定義します。
ステップ 4	**access-list** *access-list-number* **permit** *source [source-wildcard]* 例： `Switch(config)# access-list 1 permit 192.168.201.30 0.0.0.255`	変換されるアドレスを許可する標準アクセス リストを定義します。 アクセス リストは、変換されるアドレスだけを許可する必要があります（各アクセス リストの最後に暗黙の「deny all」ステートメントが存在することに注意してください）。許可が多すぎるアクセス リストを使用すると、予測困難な結果を招くことがあります。
ステップ 5	**ip nat inside source list** *access-list-number* **pool** *name* **overload** 例： `Switch(config)# ip nat inside source list 1 pool net-208 overload`	手順 4 で定義されたアクセス リストを指定して、ダイナミック送信元変換を設定します。
ステップ 6	**interface** *type number* 例： `Switch(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip address** *ip-address mask* **[secondary]** 例： `Switch(config-if)# ip address 192.168.201.1 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 8	**ip nat inside** 例： `Switch(config-if)# ip nat inside`	NAT の対象である内部ネットワークにインターフェイスを接続します。
ステップ 9	**exit** 例： `Switch(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 10	**interface** *type number* 例： `Switch(config)# interface ethernet 0`	異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**ip address** *ip-address mask* **[secondary]** 例： `Switch(config-if)# ip address 192.168.201.29 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 12	**ip nat outside** 例： `Switch(config-if)# ip nat outside`	外部ネットワークにインターフェイスを接続します。
ステップ 13	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

外部 IP アドレスのみの NAT の設定

デフォルトで NAT は、NAT でのアプリケーション レベル ゲートウェイの使用 （24 ページ）で説明されているように、パケットのペイロードに埋め込まれているアドレスを変換します。埋め込みアドレスを変換することが望ましくない場合は、外部の IP アドレスのみを変換するように NAT を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static network** *local-ip global-ip* [**no-payload**]} 例： `Device(config)# ip nat inside source static network 10.1.1.1 192.168.251.0/24 no-payload`	内部ホストデバイスでのネットワークパケット変換を無効化します。
ステップ 4	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** {**tcp** |	内部ホストデバイスでのポートパケット変換を無効化します。

	コマンドまたはアクション	目的
	udp} *local-ip local-port global-ip global-port* [**no-payload**]} 例： `Device(config)# ip nat inside source static tcp 10.1.1.1 2000 192.168.1.1 2000 no-payload`	
ステップ 5	**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** [**network**] *local-network-mask global-network-mask* [**no-payload**]} 例： `Device(config)# ip nat inside source static 10.1.1.1 192.168.1.1 no-payload`	内部ホストルータでのパケット変換を無効化します。
ステップ 6	**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* | **static** *local-ip global-ip* [**no-payload**]} 例： `Device(config)# ip nat outside source static 10.1.1.1 192.168.1.1 no-payload`	外部ホストルータでのパケット変換を無効化します。
ステップ 7	**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* | **static** {**tcp** | **udp**} *local-ip local-port global-ip global-port* [**no-payload**]} 例： `Device(config)# ip nat outside source static tcp 10.1.1.1 20000 192.168.1.1 20000 no-payload`	外部ホストデバイスでのポートパケット変換を無効化します。
ステップ 8	**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* | **static** [**network**] *local-network-mask global-network-mask* [**no-payload**]} 例： `Device(config)# ip nat outside source static network 10.1.1.1 192.168.251.0/24 no-payload`	外部ホストデバイスでのネットワークパケット変換を無効化します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show ip nat translations** [**verbose**] 例： `Device# show ip nat translations`	アクティブな NAT を表示します。

オーバーラップするネットワークの変換の設定

スタブ ネットワーク内の IP アドレスが別のネットワークに属する正式な IP アドレスであるときに、スタティック変換を使用して、これらのホストやルータと通信する必要がある場合は、オーバーラップするネットワークのスタティック変換を設定します。

（注） NAT 外部変換を成功させるためには、デバイスに外部ローカルアドレスのルートを設定する必要があります。ルートは手動で、または **ip nat outside source** {**static** | **list**} コマンドと関連付けられた **add-route** オプションを使用して設定できます。ルートの自動作成を有効にする **add-route** オプションを使用することを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	
ステップ 3	**ip nat inside source static** *local-ip global-ip* 例： `Switch(config)# ip nat inside source static 10.1.1.1 203.0.113.2`	内部ローカルアドレスと内部グローバルアドレス間のスタティック変換を設定します。
ステップ 4	**ip nat outside source static** *local-ip global-ip* 例：	外部ローカルアドレスと外部グローバルアドレス間のスタティック変換を設定します。

	コマンドまたはアクション	目的
	`Switch(config)# ip nat outside source static 172.16.0.3 10.1.1.3`	
ステップ 5	**interface** *type number* 例： `Switch(config)# interface ethernet 1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip address** *ip-address mask* 例： `Switch(config-if)# ip address 10.114.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 7	**ip nat inside** 例： `Switch(config-if)# ip nat inside`	内部と接続されることを示すマークをインターフェイスに付けます。
ステップ 8	**exit** 例： `Switch(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 9	**interface** *type number* 例： `Switch(config)# interface ethernet 0`	異なるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**ip address** *ip-address mask* 例： `Switch(config-if)#  ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 11	**ip nat outside** 例： `Switch(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 12	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

アドレス変換タイムアウトの設定

NAT の設定に基づき、アドレス変換のタイムアウトを設定できます。

デフォルトでは、ダイナミックに作成された変換エントリは、さまざまなリソースを効率的に利用できるようにするために、非アクティブな状態が一定時間続くとタイムアウトします。必要に応じて、タイムアウトのデフォルト値を変更できます。主な変換タイプに関連付けられているデフォルトのタイムアウト設定は、次のとおりです。

- 確立された TCP セッション：24 時間
- UDP フロー：5 分
- ICMP フロー：1 分

デフォルトのタイムアウト値は、ほとんどの展開シナリオでタイムアウト要件を満たすことができます。ただし、これらの値は必要に応じて調整/微調整できます。短いタイムアウト値を設定すると（60 秒未満）、CPU の使用率が高くなることがあるため推奨されません。詳細については、NAT の設定のベスト プラクティス （24 ページ）を参照してください。

この項で説明するタイムアウトは、設定に応じて変更できます。

- ダイナミック設定のためにグローバル IP アドレスを迅速に解放する必要がある場合は、**ip nat translation timeout** コマンドを使用して、デフォルトのタイムアウトよりもタイムアウトを短く設定してください。ただし、次の手順で指定するコマンドで設定した他のタイムアウトよりも長い時間にしてください。
- TCP セッションが両側から受け取る終了（FIN）パケットで正しく終了していない場合、またはリセット時に正しく終了しない場合は、**ip nat translation tcp-timeout** コマンドを使用してデフォルトの TCP タイムアウトを変更してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Switch> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat translation** *seconds* **例：** `Switch(config)# ip nat translation 300`	（任意）NAT 変換がタイムアウトになるまでの時間を変更します。 デフォルト タイムアウトは 24 時間です。これは、ハーフエントリのエージング タイムに適用されます。
ステップ 4	**ip nat translation udp-timeout** *seconds* **例：** `Switch(config)# ip nat translation udp-timeout 300`	（任意）UDP タイムアウト値を変更します。
ステップ 5	**ip nat translation tcp-timeout** *seconds* **例：**	（任意）TCP タイムアウト値を変更します。 デフォルトは 24 時間です。

	コマンドまたはアクション	目的
	`Switch(config)# ip nat translation tcp-timeout 2500`	
ステップ 6	**ip nat translation finrst-timeout** *seconds* 例： `Switch(config)# ip nat translation finrst-timeout 45`	（任意）Finish and Reset タイムアウト値を変更します。 finrst-timeout：TCP セッションが finish-in（FIN-IN）要求と finish-out（FIN-OUT）要求の両方を受信した後の、または TCP セッション リセット後のエージング タイム。
ステップ 7	**ip nat translation icmp-timeout** *seconds* 例： `Switch(config)# ip nat translation icmp-timeout 45`	（任意）ICMP タイムアウト値を変更します。
ステップ 8	**ip nat translation syn-timeout** *seconds* 例： `Switch(config)# ip nat translation syn-timeout 45`	（任意）同期（SYN）タイムアウト値を変更します。 同期タイムアウトまたはエージング タイムは、TCP セッションで SYN 要求が受信された場合にのみ使用されます。同期確認応答（SYNACK）要求が受信されると、タイムアウトが TCP タイムアウトに変更されます。
ステップ 9	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スイッチ データベース管理（SDM）テンプレートの設定

SDM テンプレートを使用し、NAT に合わせてシステム リソースを最適に設定します。

テンプレートを設定してシステムを再起動した後、**show sdm prefer** 特権 EXEC コマンドを使用して、新しいテンプレート設定を確認できます。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドにより、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

SDM テンプレートを設定して NAT の動作を最適にサポートするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer nat** 例： `Switch(config)# sdm prefer nat`	スイッチで使用する SDM テンプレートを指定します。 このテンプレートを利用するには、Network Advantage のライセンスが必要です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**write memory** 例： `Switch# write memory`	リロードする前に現在の構成を保存します。
ステップ 5	**reload** 例： `Switch# reload`	オペレーティング システムをリロードします。

NAT でのアプリケーション レベル ゲートウェイの使用

NAT は、アプリケーション データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP/UDP トラフィックにおいて変換サービスを実行します。送信元および宛先 IP アドレスを伝送しないプロトコルには、HTTP、TFTP、telnet、archie、finger、Network Time Protocol（NTP）、ネットワーク ファイル システム（NFS）、リモート ログイン（rlogin）、リモート シェル（rsh）protocol、およびリモート コピー（rcp）があります。

アドレス/ポート情報をペイロードで搬送するアプリケーションは、NAT アプリケーション レベル ゲートウェイ（ALG）により、NAT ドメイン全体で正しく機能できます。パケット ヘッダ内のアドレス/ポートの通常の変換に加えて、ALG はペイロードに存在するアドレス/ポートの変換も処理し、一時マッピングを設定します。

NAT の設定のベスト プラクティス

- スタティック ルールとダイナミック ルールの両方が設定されている場合は、ルールに指定されているローカル アドレスがオーバーラップしていないことを確認してください。こ

のようなオーバーラップの可能性がある場合は、スタティック ルールが使用するアドレスをダイナミック ルールに関連付けられている ACL で除外してください。同様に、グローバル アドレス間のオーバーラップもなくす必要があります。オーバーラップしていると、望ましくない動作が生じることがあります。

- NAT ルールに関連付けられている ACL では、**permit ip any any** などのあいまいなフィルタリングを使用しないでください。このようなフィルタリングは、必要のないパケットを変換することがあります。
- 複数の NAT ルールでアドレス プールを共有しないでください。
- スタティック NAT とダイナミック プールで同じ内部グローバル アドレスを定義しないでください。これを行うと、望ましくない結果を招くことがあります。
- NAT に関連付けられているデフォルトのタイムアウト値を変更する場合は、慎重に行ってください。タイムアウト値を短くすると、CPU の使用率が高くなることがあります。
- 変換エントリを手動でクリアする場合は、アプリケーション セッションが中断されることがあるため、慎重に行ってください。

NAT のトラブルシューティング

ここでは、NAT のトラブルシューティングと確認のための基本的な手順について説明します

- NAT で実現できることを明確に定義する。
- **show ip nat translation** コマンドで、正しい変換テーブルが存在していることを確認する。
- **show ip nat translation verbose** コマンドで、タイマーの値が正しく設定されていることを確認する。
- **show ip access-list** コマンドで、NAT の ACL 値をチェックする。
- **show ip nat statistics** コマンドで、NAT の全体的な設定をチェックする。
- **clear ip nat translation** コマンドで、タイマーの期限が切れる前に NAT 変換テーブルのエントリをクリアする。
- debug nat ip と debug nat ip detailed コマンドを使用して、NAT 設定をデバッグする。

NAT のトラブルシューティングの詳細については、を参照してください。 http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/8605-13.html

ネットワーク アドレス変換の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *1: NAT* の機能情報

機能名	リリース	機能情報
アドレスのみの変換のサポート	Cisco IOS XE Fuji 16.9.1	アドレスのみの変換（AOT）は、NAT でラインレートで変換および転送できる IP フローの数を増やすことを目的としています。AOT は、TCAMS などのハードウェアリソースの使用を最適化し、より多くのフローの処理を可能にします。
ネットワーク アドレス変換のサポート	Cisco IOS XE Gibraltar 16.10.1	この機能が導入されました。 ネットワーク アドレス変換（NAT）は、登録されていない IP アドレスを使用してインターネットへ接続するプライベート IP ネットワークを有効にします。NAT はデバイス（通常、2 つのネットワークを接続するもの）上で動作し、別のネットワークにパケットを転送する前に、内部ネットワークのプライベートアドレスをグローバルなルート可能なアドレスに変換します。

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。