レイヤ 3 ネットワークアドレス変換

ネットワーク アドレス変換

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、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。これは、パケットが別のネットワークに転送される前に行われます。

NAT は、ネットワーク全体に対して 1 つのアドレスだけを外部にアドバタイズするように設定できます。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。

機能情報の確認

ご使用のソフトウェアリリースでは、このドキュメントで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、この章の最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/ に進みます。Cisco.com のアカウントは必要ありません。

NAT を設定する利点

NAT を設定すると、次の利点があります。

- NAT は 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）登録 IP アドレスをまだ所有していないサイトは、IP アドレスを取得する必要があります。このような場合、254 を超えるクライアントが存在するか、または計画されている場合、クラス 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。

- NAT はクライアント 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、または動的に 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。

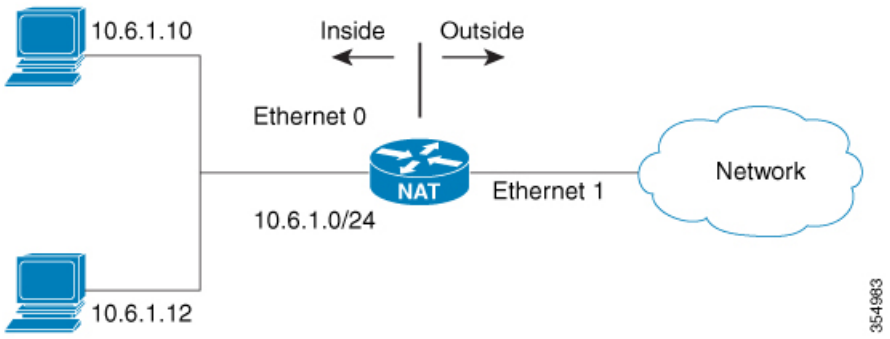
NAT の機能

NAT が設定されたデバイスには、少なくとも内部ネットワークに対して 1 つ、外部ネットワークに対して 1 つのインターフェイスがあります。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出口となる点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 はそのパケットを破棄し、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るため、全体的なスループットの性能が改善されます。性能の詳細については、「NAT の性能とスケール数 （11 ページ）」セクションを参照してください。

図 *1 : NAT*



NAT の用途

NAT は次のシナリオで使用できます。

- 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、グローバルに一意な IP アドレスに変換する必要があるのはこのドメインにある IP アドレスのごく一部のみです。また、これらのアドレスは再利用できます。

- 番号の付け直しを行う場合：

  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、組織が所有し変換が必要な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、ある空間（ローカルアドレス空間として知られている）内にアドレスを持ち、それが別の空間（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 つまたは複数の内部ローカル 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。
- 静的ポート変換：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静的変換：内部/外部ローカルアドレスの指定された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のアドレス/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 規則に基づいて、静的または動的に作成され得ます。
- 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。この設定で、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。

- 静的アドレス変換（静的 NAT）：ローカルアドレスとグローバルアドレスを 1 対 1 でマッピングします。
- 動的アドレス変換（動的 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）

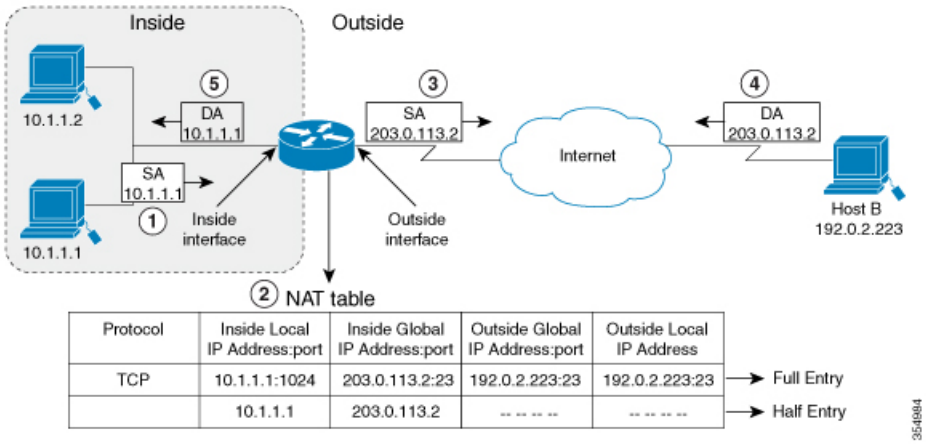
自分が属するネットワークの外部と通信するときに、未登録の IP アドレスをグローバルで一意な IP アドレスに変換できます。

静的または動的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。

- 静的変換は、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、静的変換が便利です。静的変換は、x セクションで説明されているように、静的 NAT 規則を設定して有効にできます。
- 動的変換は、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。動的変換は、動的 NAT 規則を設定することで有効にできます。マッピングは、設定されている規則を実行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制御リスト（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。動的変換は、「内部送信元アドレスの動的変換の設定 （14 ページ）」セクションで説明されているように動的規則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、上の図の内部送信元アドレス変換を示しています。

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横取りし、パケットを変換しようとします。

   一致する NAT 規則の有無に基づいて、次のシナリオが考えられます。

   - 一致する静的変換規則が存在する場合、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、パケットは動的変換規則に対して照合され、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。
   - 一致する規則がない場合、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、たとえ一致する規則があってもパケットは破棄されます。

（注） 動的変換に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. 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信されます。NATモジュールはこのパケットを横取りし、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

ネットワークの外部から内部に移動する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、「重複するネットワークの変換の設定 （20ページ）」セクションで説明します。

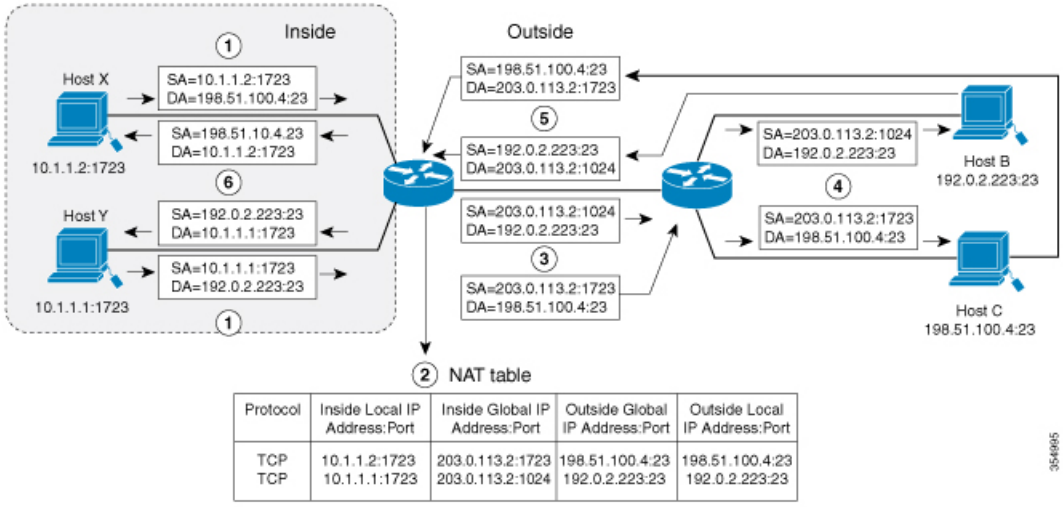
ポートアドレス変換

デバイスで、多くのローカルアドレスに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のアドレスを節約できます。このタイプのNAT設定は、オーバーロードまたはポートアドレス変換（PAT）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。ただし、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横取りし、パケットの変換を試みます。

   一致する NAT 規則の有無に基づいて、次のシナリオが考えられます。

   - 一致する静的変換規則が存在する場合はその規則が優先され、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、パケットは動的変換規則に対して照合され、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。
   - 一致する規則がない場合、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、一致する規則があってもパケットは破棄されます。
   - これは PAT 設定であるため、トランスポートの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。

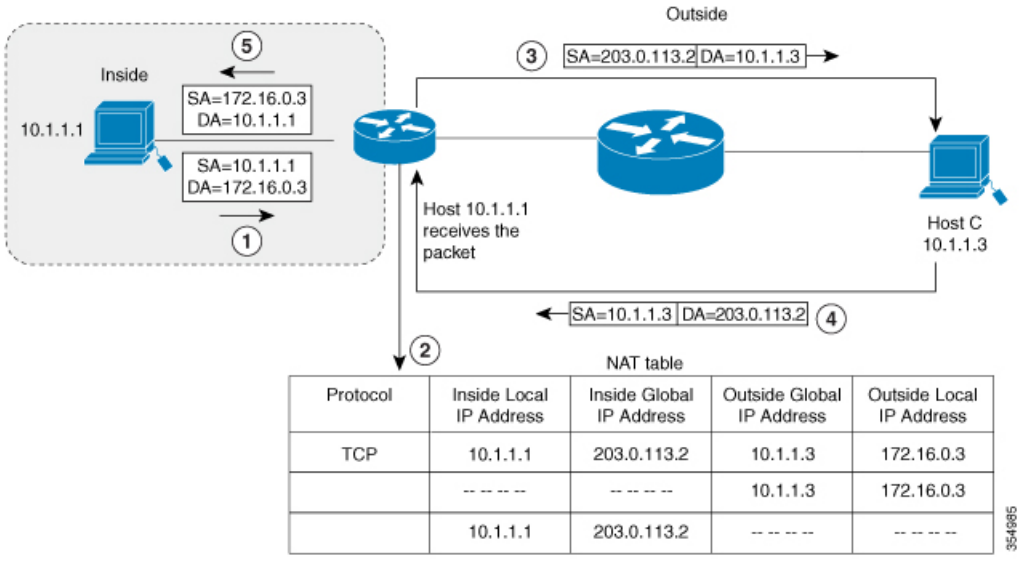
ホスト 10.1.1.1 および 10.1.1.2 はパケットを受信し、通信を続行します。デバイスは、受信する各パケットについて手順 2 ～ 5 を実行します。

重複ネットワーク

使用する IP アドレスが正当でない、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には 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、ネットワークの重複が発生します。

次の図は重複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）。そのように重複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にはNATデバイスを使用して遠隔にある対向のアドレス（10.1.1.3）を内部から見た別のアドレスに変換する必要があります。

図 *4 : NAT* による重複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。重複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、重複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

- 一部の NAT の動作については、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
- 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、理想的な設定では 192 に制限されています。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 規則は、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、特定の規則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。
- 動的に作成された NAT フローは、アクティブでない状態が一定期間続くと失効します。そのアクティビティを追跡できる NAT フローの数は 192 に制限されています。
- 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。
- 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 と PBR は同じ TCAM スペースを共有し、共存できません。
- ルートマップを用いた NAT はサポートされていないため、NAT 設定はルートマップを使用せずに行う必要があります。
- NAT はマルチキャストパケットではサポートされません。

NAT の性能とスケール数

ハードウェアでサポートされる双方向 NAT フローの最大数は 192 に制限されています。

アドレスのみの変換

（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（AOT）機能は、トランスポートの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方式では、ハードウェア変換を実行するために 384 個の 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 1 つまたは複数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。既存の動的フローは、**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、単純な内部静的規則および内部動的規則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。単純な静的規則のタイプは **ip nat inside source static** *local-ip global-ip* で、動的規則のタイプは **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静的変換の設定

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静的変換を設定します。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、静的変換が便利です。

手順の概要

1. **enable**
2. **configure terminal**
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
     ```

4. **interface** *type number*
5. **ip address** *ip-address mask* **[secondary]**
6. **ip nat inside**
7. **exit**

8. **interface** *type number*
9. **ip address** *ip-address mask* **[secondary]**
10. **ip nat outside**
11. **end**

手順の詳細

	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 アドレス間の静的変換を設定します。
		内部ローカル アドレスと内部グローバル アドレス間の静的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 アドレス間の静的変換を設定します。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変換されません。

ステップ 4	**interface** *type number* 例： `Switch(config)# interface GigabitEthernet 1/0/1`	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。

	コマンドまたはアクション	目的
ステップ 7	**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、グローバル設定モードに戻ります。
ステップ 8	**interface** *type number* 例： `Switch(config)# interface GigabitEthernet 1/0/2`	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動的変換の設定

動的変換は、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。動的変換は、動的NAT規則を設定することで有効にできます。マッピングは、設定されている規則を実行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、動的変換が便利です。動的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解放できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* **netmask** *netmask* | **prefix-length** *prefix-length*
4. **access-list** *access-list-number* **permit** *source [source-wildcard]*
5. **ip nat inside source list** *access-list-number* **pool** *name*
6. **interface** *type number*
7. **ip address** *ip-address mask*
8. **ip nat inside**

9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask*
12. **ip nat outside**
13. **end**

手順の詳細

	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、動的送信元変換を設定します。
ステップ 6	**interface** *type number* 例： `Switch(config)# interface GigabitEthernet 1/0/1`	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： `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。

	コマンドまたはアクション	目的
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 GigabitEthernet 1/0/2`	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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat pool** *name start-ip end-ip* **netmask** *netmask* | **prefix-length** *prefix-length*
4. **access-list** *access-list-number* **permit** *source [source-wildcard]*
5. **ip nat inside source list** *access-list-number* **pool** *name* **overload**
6. **interface** *type number*
7. **ip address** *ip-address mask* **[secondary]**
8. **ip nat inside**
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask* **[secondary]**
12. **ip nat outside**
13. **end**

手順の詳細

	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-208 192.168.202.129 192.168.202.158 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）。許可する範囲が広すぎるアクセス 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、動的送信元変換を設定します。
ステップ 6	**interface** *type number* 例： `Switch(config)# interface GigabitEthernet 1/0/1`	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。

	コマンドまたはアクション	目的
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、グローバル設定モードに戻ります。
ステップ 10	**interface** *type number* 例： `Switch(config)# interface GigabitEthernet 1/0/2`	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 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）」セクション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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static network** *local-ip global-ip* [**no-payload**]}
4. **ip nat inside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* [**overload**] | **static** {**tcp** | **udp**} *local-ip local-port global-ip global-port* [**no-payload**]}
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**]}
6. **ip nat outside source** {**list** {*access-list-number* | *access-list-name*} **pool** *pool-name* | **static** *local-ip global-ip* [**no-payload**]}
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**]}
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**]}

9. **exit**
10. **show ip nat translations** [**verbose**]

手順の詳細

	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** | **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`	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。
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**]}	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。

	コマンドまたはアクション	目的
	例： `Device(config)# ip nat outside source static tcp 10.1.1.1 20000 192.168.1.1 20000 no-payload`	
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。
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。

重複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、静的変換を使用して、これらのホストやルータと通信する必要がある場合は、重複するネットワークの静的変換を設定します。

（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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *local-ip global-ip*
4. **ip nat outside source static** *local-ip global-ip*
5. **interface** *type number*
6. **ip address** *ip-address mask*
7. **ip nat inside**
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask*

11. **ip nat outside**
12. **end**

手順の詳細

	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 アドレス間の静的変換を設定します。
ステップ 4	**ip nat outside source static** *local-ip global-ip* 例： `Switch(config)# ip nat outside source static 172.16.0.3 10.1.1.3`	外部ローカル アドレスと外部グローバル アドレス間の静的変換を設定します。
ステップ 5	**interface** *type number* 例： `Switch(config)# interface GigabitEthernet 1/0/1`	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 コンフィギュレーション 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 GigabitEthernet 1/0/2`	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 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、動的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、アクティブでない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、x セクション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。

- 動的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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat translation** *seconds*
4. **ip nat translation udp-timeout** *seconds*
5. **ip nat translation tcp-timeout** *seconds*
6. **ip nat translation finrst-timeout** *seconds*
7. **ip nat translation icmp-timeout** *seconds*
8. **ip nat translation syn-timeout** *seconds*
9. **end**

手順の詳細

	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： `Switch(config)# ip nat translation tcp-timeout 2500`	（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。
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。

	コマンドまたはアクション	目的
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。

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、次のものがあります。

- HTTP
- TFTP
- Telnet
- Archie
- Finger
- ネットワーク タイム プロトコル（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）
- リモートコピー（rcp）

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

- 静的規則と動的規則の両方が設定されている場合は、規則に指定されているローカルアドレスが重複していないことを確認してください。このような重複の可能性がある場合は、静的規則が使用するアドレスを動的規則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重複もなくす必要があります。重複していると、望ましくない動作が生じることがあります。
- NAT 規則に関連付けられている ACL では、**permit ip any any** などの範囲の広い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 規則でアドレス プールを共有しないでください。
- 静的 NAT と動的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 対応インターフェイスを通過する ALG パケットは、パケットが変換されるかどうかに関係なく、CPU にパントされます。そのため、NAT トラフィック専用のインターフェイスを使用することをお勧めします。NAT 変換する必要がない他のタイプのトラフィックにはすべて、別のインターフェイスを使用します。

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より早く 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、Cisco.com の「Verifying NAT Operation and Basic NAT Troubleshooting」を参照してください。

ネットワークアドレス変換の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能説明
Cisco IOS XE Cupertino 17.7.1	レイヤ 3 ネットワークアドレス変換（Cisco Catalyst IE9300 高耐久性シリーズ スイッチ）	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 はデバイス上で動作し、通常は 2 つのネットワークを同時に接続して、パケットが一方のネットワークに転送される前に、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ティング可能アドレスに変換します。 この機能のサポートは、次のスイッチモデルで導入されました。 • IE-9310-26S2C-A • IE-9320-26S2C-A

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。