



スタティック NAT とダイナミック NAT 変換の設定

この章の内容は、次のとおりです。

- [ネットワーク アドレス変換の概要, 1 ページ](#)
- [スタティック NAT に関する情報, 2 ページ](#)
- [ダイナミック NAT の概要, 4 ページ](#)
- [タイムアウト メカニズム, 5 ページ](#)
- [NAT の内部アドレスおよび外部アドレス, 6 ページ](#)
- [ダイナミック NAT のプールのサポート, 6 ページ](#)
- [スタティックおよびダイナミック Twice NAT の概要, 7 ページ](#)
- [スタティック NAT のライセンス要件, 8 ページ](#)
- [スタティック NAT の注意事項および制約事項, 8 ページ](#)
- [ダイナミック NAT に関する制約事項, 9 ページ](#)
- [ダイナミック Twice NAT の注意事項および制約事項, 10 ページ](#)
- [スタティック NAT の設定, 11 ページ](#)
- [ダイナミック NAT の設定, 18 ページ](#)

ネットワーク アドレス変換の概要

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 インターネットワークをイネーブルにします。NAT はデバイス (通常、2つのネットワークを接続するもの) で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの (グローバルに一意のアドレスではなく) プライベート IP アドレスを正規の IP アドレスに変換します。NAT は、ネットワーク全体に対して 1つの IP 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、1つのIPアドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

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の間の出ルータに設定されます。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 IP アドレスをグローバルで一意の IP 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 はグローバルで一意の宛先 IP アドレスをローカル IP アドレスに変換します。出力点が複数存在する場合、個々の点で設定された NAT は、同一の変換テーブルを持っていなければなりません。

NAT は RFC 1631 に記述されています。

スタティック NAT に関する情報

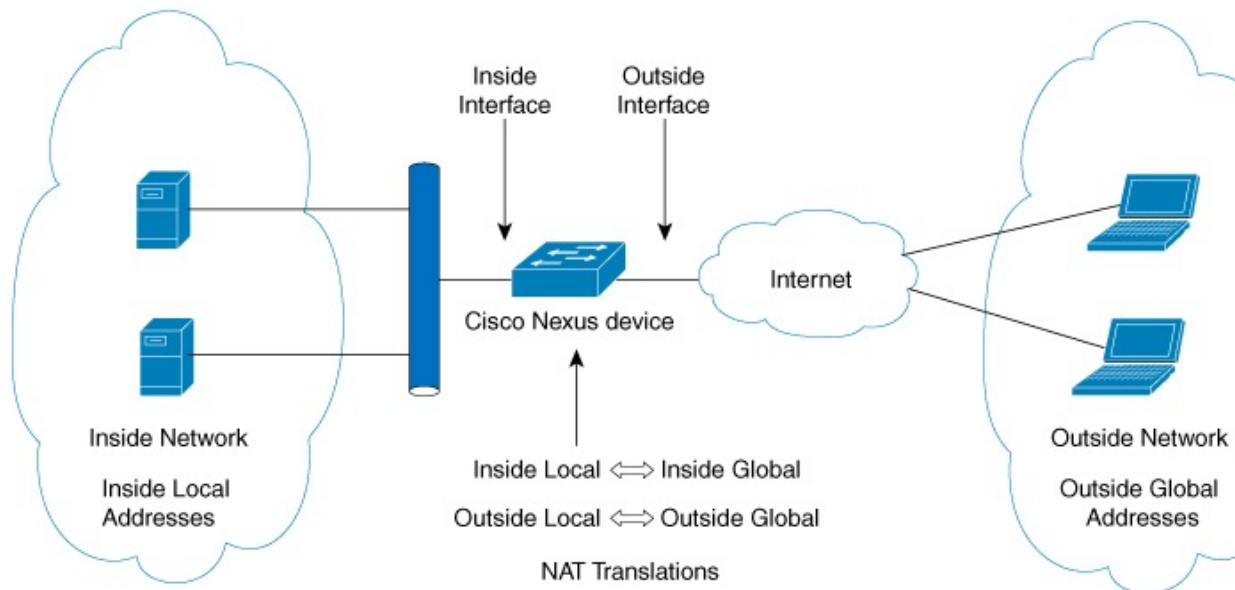
スタティック ネットワーク アドレス変換 (NAT) を使用すると、ユーザは内部ローカルアドレスから外部グローバルアドレスへの1対1変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへのIPアドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィックフローに影響を与えずに NAT 設定で NAT 変換を追加または削除できることを意味します。

スタティック NAT では、プライベートアドレスからパブリックアドレスへの固定変換が作成されます。スタティック NAT では1対1ベースでアドレスが割り当てられるため、プライベートアドレスと同じ数のパブリックアドレスが必要です。スタティック NAT では、パブリックアドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます (そのトラフィックを許可するアクセスリストがある場合)。

ダイナミック NAT およびポートアドレス変換 (PAT) では、各ホストは後続する変換ごとに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT の主な違いは、スタティック NAT ではリモートホストが変換済みのホストへの接続を開始でき (それを許可するアクセスリストがある場合)、ダイナミック NAT では開始できないという点です。

次の図に、一般的なスタティック NAT のシナリオを示します。変換は常にアクティブであるため、変換対象ホストとリモートホストの両方で接続を生成でき、マップアドレスは **static** コマンドによって静的に割り当てられます。

図 1: スタティック NAT



次に、スタティック NAT を理解するのに役立つ主な用語を示します。

- NAT の内部インターフェイス：プライベート ネットワークに面するレイヤ 3 インターフェイス。
- NAT の外部インターフェイス：パブリック ネットワークに面するレイヤ 3 インターフェイス。
- ローカルアドレス：ネットワークの内部（プライベート）部分に表示される任意のアドレス。
- グローバルアドレス：ネットワークの外部（パブリック）部分に表示される任意のアドレス。
- 正規の IP アドレス：Network Information Center (NIC) やサービス プロバイダーにより割り当てられたアドレス。
- 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。このアドレスは正規の IP アドレスである必要はありません。
- 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。これは、内部ネットワークのルーティング可能なアドレス空間から割り当てられるため、正規のアドレスである必要はありません。

- 内部グローバルアドレス：1 つ以上の内部ローカル IP アドレスを外部に対して表すために使用できる正規の IP アドレス。
- 外部グローバルアドレス：ホスト所有者が外部ネットワーク上のホストに割り当てた IP アドレス。このアドレスは、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た正規のアドレスです。

ダイナミック NAT の概要

ダイナミック ネットワーク アドレス 変換 (NAT) は、実 IP アドレスのグループを宛先ネットワーク上でルーティング可能なマッピングされた IP アドレスに変換します。ダイナミック NAT では、未登録および登録 IP アドレス間の 1 対 1 のマッピングを確立しますが、マッピングは通信時に利用可能な登録済みの IP アドレスに応じて変えることができます。

ダイナミック NAT の設定は、自動的に内部ネットワークと外部ネットワーク間またはインターネット間のファイアウォールを作成します。ダイナミック NAT は、スタブ ドメイン内で生じる接続のみを許可します。外部ネットワーク デバイスは、デバイスが通信を開始しない限り、ネットワークのデバイスに接続できません。

ダイナミック NAT 変換は、変換が必要なトラフィックをデバイスが受信するまで、NAT 変換テーブルには存在しません。ダイナミック変換は、新しいエントリのスペースを作成するために使用されないときに、クリアまたはタイムアウトされます。通常、NAT 変換エントリは、TCAM (Ternary Content Addressable Memory) エントリが制限されている場合はクリアされます。ダイナミック NAT 変換のデフォルトの最小タイムアウトは 30 分です。Cisco NX-OS リリース 6.0(2)A1(1e) では、**ip nat translation sampling-timeout** コマンドでのサンプリングタイムアウトの最小値は、30 分から 15 分に短縮されました。

ダイナミック NAT 変換のタイムアウトには、サンプリングタイムアウト値と TCP または UDP タイムアウト値の両方が含まれます。サンプリングタイムアウトは、デバイスがダイナミック変換のアクティビティのチェックをする時間を指定します。デフォルト値は、12 時間です。他のすべてのタイムアウトは、サンプルタイムアウトがタイムアウトになった後にのみ開始されます。サンプリングタイムアウト後、デバイスはこの変換に適合するパケットを検査します。チェックは、TCP または UDP タイムアウト期間中に発生します。TCP または UDP タイムアウト期間中にパケットがなければ、変換はクリアされます。アクティビティが変換で検出されると、チェックがすぐに停止され、サンプリングタイムアウト期間が開始されます。

この新しいサンプリングタイムアウト期間を待機した後、デバイスはダイナミック変換のアクティビティを再度チェックします。アクティビティのチェック中に TCAM は、CPU にダイナミック NAT 変換と一致するパケットのコピーを送信します。コントロールプレーンポリシング (CoPP) が下限しきい値で設定される場合、TCP または UDP パケットは CPU に到達しない可能性があり、CPU は NAT 変換の非アクティブとしてこれを考慮します。

ダイナミック NAT は、ポートアドレス変換 (PAT) およびアクセスコントロールリスト (ACL) をサポートします。オーバーロードとしても知られている PAT は、異なるポートを使用することにより、単一の登録済み IP アドレスに複数の未登録の IP アドレスをマッピングするダイナミック NAT の一形態です。NAT 設定は、同一または異なる ACL を使用して複数のダイナミック NAT

変換することができます。ただし、特定の ACL では、1つのインターフェイスのみしか指定することができません。

タイムアウトメカニズム

ダイナミック NAT 変換は作成された後、特に TCAM エントリの数が限られているため、新しい変換を作成できるように使用時にクリアする必要があります。Cisco NX-OS リリース 6.0(2)A4(1) では、**syn-timeout** および **finrst-timeout** のサポートが追加されます。次の NAT 変換のタイムアウトタイマーはスイッチでサポートされています。

- **syn-timeout** : SYN 要求を送信しますが、SYN-ACK 応答を受信しない TCP データのパケットタイムアウト値。

タイムアウト値の範囲は、1 ~ 172800 秒です。デフォルト値は 60 秒です。

- **finrst-timeout** : RST または FIN パケットを受信することによって、接続が終了されるときのフローエントリのタイムアウト値。RST および FIN パケットの両方の動作を設定するには、同じキーワードを使用します。

- 接続の確立後、RST パケットを受信すると、SYN --> SYN-ACK --> RST で、設定されたタイムアウト値の後にフローが期限切れとなります。
- 接続の確立後、FIN パケットを受信すると、SYN --> SYN-ACK --> FIN で、finrst タイマーが起動します。
- FIN-ACK が相手側から届いた場合は、変換エントリはすぐにクリアされ、それ以外の場合は、タイムアウト値が完了した後にクリアされます。



(注) ダイナミック プール ベースの設定が使用され、FIN-ACK が受信された場合は、変換エントリはクリアされません。

タイムアウト値の範囲は、1 ~ 172800 秒です。デフォルト値は 60 秒です。

- **finrst-timeout** : 接続が 3 ウェイ ハンドシェイク (SYN、SYN-ACK、ACK) の後に確立された TCP 変換のタイムアウト値。接続の確立後、アクティブ フローが発生しなければ、変換は設定されたタイムアウト値ごとに期限切れとなります。このタイムアウト値は、サンプリングタイムアウト値が完了した後に開始されます。

タイムアウト値の範囲は、サンプリングタイムアウトを含む、60 ~ 172800 秒です。

- **udp-timeout** : すべての NAT UDP パケットのタイムアウト値。

タイムアウト値の範囲は、サンプリングタイムアウトを含む、60 ~ 172800 秒です。

- **timeout** : ダイナミック NAT 変換のタイムアウト値。

タイムアウト値の範囲は、サンプリングタイムアウトを含む、60 ~ 172800 秒です。

- **sampling-timeout** : デバイスがダイナミック変換のアクティビティをチェックをする時間。

タイムアウト値の範囲は、900 ～ 172800 秒です。

finrst-timeout、**udp-timeout**、および **timeout** 値のタイマーは、**ip nat translation sampling-timeout** コマンドで設定されているタイムアウトの期限が切れた後にトリガーされます。

SYN、FIN および RST タイマーは、ダイナミック プールベース NAT には使用されません。

NAT の内部アドレスおよび外部アドレス

NAT の内部は、変換する必要がある組織が所有するネットワークを指します。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、NAT の外側は、スタブネットワークが接続するネットワークを指します。これらは一般に、組織の制御下にはありません。外部ネットワーク内のホストを変換の対象にすることができ、これらのホストも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。

- ローカルアドレス：ネットワークの内部に表示されるローカル IP アドレス。
- グローバルアドレス：ネットワークの外部に表示されるグローバル IP アドレス。
- 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、Internet Network Information Center (InterNIC) やサービスプロバイダーにより割り当てられた正規の 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 アドレスを表現した正規の IP アドレス（InterNIC 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。アドレスは必ずしも正規ではありません。アドレスは、内部でルート可能なアドレス空間から割り当てられます。
- 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。

ダイナミック NAT のプールのサポート

Cisco NX-OS リリース 6.0(2)A3(1) には、ダイナミック NAT のプールのサポートが導入されています。ダイナミック NAT は、新しい変換のプールからグローバルアドレスを動的に割り当てるために使用できるグローバルアドレスのプールを設定できます。アドレスは、セッションが期限切れまたはクローズされた後にプールに戻されます。これは、要件に基づいてアドレスをより効率的に活用します。

PAT のサポートは、グローバルアドレス プールの使用を含みます。また、IP アドレスの使用を最適化します。PAT は、ポート番号を使用して一度に 1 つの IP アドレスを使います。ポートが該当グループで使用できない場合や、複数の IP アドレスが設定されている場合は、PAT は次の IP アドレスに移動して最初の送信元ポートを再び割り当てようとします。このプロセスは、PAT が使用できるポートと IP アドレスがなくなるまで続きます。

ダイナミック NAT および PAT では、各ホストは後続する変換ごとに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT の主な違いは、スタティック NAT ではリモートホストが変換済みのホストへの接続を開始でき（それを許可するアクセスリストがある場合）、ダイナミック NAT では開始できないという点です。

スタティックおよびダイナミック Twice NAT の概要

送信元 IP アドレスと宛先 IP アドレスの両方が、ネットワーク アドレス変換 (NAT) デバイスを通過する単一パケットとして変換されると、Twice NAT と呼ばれます。Twice NAT は、スタティックおよびダイナミック変換でサポートされます。

Twice NAT は、変換グループの一部として、2 つの NAT 変換（1 つの内部および 1 つの外部）を設定することができます。これらの変換は、NAT デバイスを通して流れるように単一のパケットに適用できます。グループの一部として、2 つの変換を追加すると、個々の変換と組み合わせ変換の両方が有効になります。

NAT の内部変換では、パケットが内部から外部へ流れる際に、送信元 IP アドレスとポート番号を変更します。パケットが外部から内部に戻る際に、宛先の IP アドレスとポート番号を変更します。NAT の外部変換では、パケットが外部から内部に流れる際に、送信元 IP アドレスとポート番号を変更し、パケットが内部から外部に戻る際に、宛先 IP アドレスとポート番号を変更します。

Twice NAT を使用しない場合、変換ルールのうちの 1 つだけがパケット、送信元 IP アドレスとポート番号または宛先 IP アドレスとポート番号のいずれかに適用されます。

同じグループに属するスタティック NAT 変換は、Twice NAT 設定と見なされます。スタティック設定が、設定されたグループ ID を持っていない場合は、Twice NAT 設定では動作しません。グループ ID によって識別される単一のグループに属するすべての内部および外部 NAT 変換は、Twice NAT 変換を形成するようになっています。

ダイナミック Twice NAT 変換は、事前定義された **ip nat pool** または **interface overload** 設定から動的に送信元 IP アドレスとポート番号の情報を選択します。パケット フィルタリングは、ACL の設定によって実行され、ソース変換が、ダイナミック NAT ルールの使用によって実行できるように、トラフィックはダイナミック NAT 変換ルールの方向性から生成する必要があります。

ダイナミック Twice NAT は、変換グループの一部として、2 つの NAT 変換（1 つの内部および 1 つの外部）を設定することができます。1 つの変換はダイナミックである必要があり、他の変換はスタティックである必要があります。これら 2 つの変換が変換グループの一部の場合、両方の変換は、内部から外部または外部から内部のいずれかの NAT デバイスを通過するときに単一のパケットに適用できます。

スタティック NAT のライセンス要件

次の表に、スタティック NAT のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	<p>スタティック NAT には、LAN Base ライセンスおよび Algo Boost ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。</p> <p>(注) レイヤ 3 インターフェイスをイネーブルにするため、LAN Base Services ライセンスがスイッチにインストールされていることを確認します。</p>

スタティック NAT の注意事項および制約事項

スタティック NAT 設定時の注意事項および制約事項は、次のとおりです。

- NAT は、スタティック NAT とダイナミック NAT の両方を含む最大 1024 の変換がサポートされています。
- Cisco Nexus デバイスは、次のインターフェイス タイプ上の NAT をサポートします。
 - スイッチ仮想インターフェイス (SVI)
 - ルーテッドポート
 - レイヤ 3 ポート チャネル
- NAT はデフォルトの仮想ルーティングおよびフォワーディング (VRF) テーブルのみでサポートされます。
- NAT は、IPv4 ユニキャストだけでサポートされています。
- Cisco Nexus デバイスは、次をサポートしません。
 - ソフトウェアの変換。すべての変換はハードウェアで行われます。
 - アプリケーション層の変換。レイヤ 4 およびその他の組み込み IP は変換されません (FTP、ICMP の障害、IPSec、HTTPS など)。
 - インターフェイス上で同時に設定された NAT および VLAN アクセス コントロール リスト (VACL)。
 - フラグメント化された IP パケットの PAT 変換。

- ソフトウェア転送パケットの NAT 変換。たとえば、IP オプションを持つパケットは NAT 変換されません。
- 出力 ACL は元のパケットに適用され、NAT 変換済みパケットには適用されません。
- デフォルトでは、NAT は 256 TCAM エントリで最大 127 の変換まで実行できます。より多くの NAT 変換が必要な場合は、他のエリア内の TCAM リージョン割り当てを減らしてから、**hardware profile tcam region nat** コマンドを使用して NAT TCAM リージョンを増やす必要があります。
- HSRP および VRRP は、NAT の内部アドレスでサポートされ NAT の外部アドレスではサポートされません。
- ワープモード遅延パフォーマンスは、外部から内部ドメインに着信するパケットではサポートされません。
- IP アドレスがスタティック NAT 変換または PAT 変換に使用される場合、他の目的には使用できません。たとえば、インターフェイスに割り当ててはできません。
- スタティック NAT の場合は、外部グローバル IP アドレスが外部インターフェイス IP アドレスと異なる必要があります。
- 変換された IP が、外部インターフェイスサブネットの一部である場合、NAT の外部インターフェイスで **ip local-proxy-arp** コマンドを使用します。
- NAT 統計情報は利用できません。
- (100 を超える) 多数の変換を設定する場合、変換を設定してから NAT インターフェイスを設定する方が迅速に設定できます。
- 次の機能のうち 1 つだけが一度にインターフェイスで有効にできます。これらの機能の 2 つ以上がインターフェイスで有効になっている場合、最後に有効になっている機能のみが動作します。
 - NAT
 - DHCP リレー
 - VACL

ダイナミック NAT に関する制約事項

次の制限はダイナミック ネットワーク アドレス変換 (NAT) に適用されます。

- フラグメント化されたパケットはサポートされません。
- アプリケーションレイヤゲートウェイ (ALG) 変換はサポートされません。アプリケーションレベルゲートウェイとしても知られている ALG は、アプリケーションパケットのペイロード内の IP アドレス情報を変換するアプリケーションです。

- NAT と仮想アクセス コントロール リスト (ACL) は、インターフェイスで同時にサポートされていません。インターフェイスで NAT または仮想 ACL のいずれかを設定することができます。
- 出力 ACL は、変換されたパケットには適用されません。
- デフォルト以外の Virtual Routing and Forwarding (VRF) インスタンスはサポートされません。
- MIB はサポートされていません。
- Cisco Data Center Network Manager (DCNM) はサポートされません。
- 複数のグローバル仮想デバイス コンテキスト (VDC) は、Cisco Nexus デバイスではサポートされていません。
- ダイナミック NAT 変換は、アクティブおよびスタンバイ デバイスと同期されません。
- ステートフル NAT はサポートされません。ただし、NAT と Hot Standby Router Protocol (HSRP) は共存できます。
-
- タイムアウト値は、設定されているタイムアウト + 119 秒になります。
- 通常、NAT の ICMP フローは、設定されたサンプリングタイムアウトと変換タイムアウトの期限後にタイムアウトになります。ただし、スイッチに存在する NAT の ICMP フローがアイドル状態になると、サンプリングタイムアウトの期限が設定された直後にタイムアウトになります。
- 変換された IP が、外部インターフェイスサブネットの一部である場合、NAT の外部インターフェイスで **ip local-proxy-arp** コマンドを使用します。
- Cisco Nexus 3548 シリーズスイッチで新しい変換を作成すると、フローは、変換がハードウェアでプログラムされるまでソフトウェア転送され、これには数秒かかります。この間、内部グローバルアドレスの変換エントリはありません。そのため、リターントラフィックはドロップされます。この制限を克服するには、ループバックインターフェイスを作成し、NAT プールに属する IP アドレスを指定します。

ダイナミック Twice NAT の注意事項および制約事項

ダイナミック Twice NAT を設定する場合は、次のガイドラインを参照してください。

- ダイナミック Twice NAT では、スタティック NAT のフローを作成する前にダイナミック NAT のフローが作成されない場合、ダイナミック Twice NAT のフローは正しく作成されません。
- 空の ACL が作成されると、**permit ip any any** のデフォルトのルールが設定されます。最初の ACL が空白な場合、NAT-ACL は、さらに ACL エントリと一致しません。
- サポートされている ICMP 変換またはフローエントリの最大数は、TCAM スペースの適切な利用のため、176 になっています。

- レイヤ3 インターフェイスで NAT を設定する場合、リロードした後または既存の NAT 変換をクリアした後、NAT 変換は学習されません。この問題のため、NAT、ACL に一致するトラフィックのドロップがあります。この問題が存在する場合は、NAT 設定を削除し、NAT 変換が学習されるように、インターフェイスで同様に再設定する必要があります。

スタティック NAT の設定

スタティック NAT のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# feature nat	デバイス上でスタティック NAT 機能をイネーブルにします。
ステップ 3	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

インターフェイスでのスタティック NAT の設定

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# interface type slot/port	設定す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 3	switch(config-if)# ip nat {inside outside}	内部または外部としてインターフェイスを指定します。

	コマンドまたはアクション	目的
		(注) マーク付きインターフェイスに到着したパケットだけが変換できます。
ステップ 4	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、スタティック NAT を使用して内部のインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# ip nat inside
```

内部送信元アドレスのスタティック NAT のイネーブル化

内部送信元変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。NAT は、内部ローカル IP アドレスを内部グローバル IP アドレスに変換します。リターントラフィックでは、宛先の内部グローバル IP アドレスが内部ローカル IP アドレスに変換されて戻されます。



- (注) Cisco Nexus デバイスが、内部送信元 IP アドレス (Src:ip1) を外部送信元 IP アドレス (newSrc:ip2) に変換するように設定されている場合、Cisco Nexus デバイスは内部宛先 IP アドレス (newDst: ip1) への外部宛先 IP アドレス (Dst: ip2) の変換を暗黙的に追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# ip nat inside source static local-ip-address global-ip-address [group group-id]	内部グローバルアドレスを内部ローカルアドレスに、またはその逆に (内部ローカルトラフィックを内部グローバルトラフィックに) 変換するようにスタティック NAT を設定します。
ステップ 3	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

	コマンドまたはアクション	目的
--	--------------	----

次に、内部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.1 5.5.5.5
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック NAT のイネーブル化

外部送信元変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。NAT は、外部グローバル IP アドレスを外部ローカル IP アドレスに変換します。リターントラフィックでは、宛先の外部ローカル IP アドレスが外部グローバル IP アドレスに変換されて戻されます。

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# ip nat outside source static <i>global-ip-address local-ip-address</i> [group group-id] [add-route]	外部グローバルアドレスを外部ローカルアドレスに、またはその逆に（外部ローカルトラフィックを外部グローバルトラフィックに）変換するようにスタティック NAT を設定します。
ステップ 3	switch(config)# copy running-config startup-config	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、外部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static 2.2.2.2 6.6.6.6
switch(config)# copy running-config startup-config
```

内部送信元アドレスのスタティック PAT の設定

ポートアドレス変換（PAT）を使用して、特定の内部ホストにサービスをマッピングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# ip nat inside source static { <i>inside-local-address outside-local-address</i> {tcp udp} <i>inside-local-address</i> { <i>local-tcp-port local-udp-port</i> } <i>inside-global-address {global-tcp-port </i> <i>global-udp-port}</i> } group group-id	スタティック NAT を内部ローカル ポート、内部グローバル ポートにマッピングします。
ステップ 3	switch(config)# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、UDP サービスを特定の内部送信元アドレスおよび UDP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static udp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック PAT の設定

ポート アドレス変換 (PAT) を使用して、サービスを特定の外部ホストにマッピングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# ip nat outside source static { <i>outside-global-address</i> <i>outside-local-address {tcp udp}</i> <i>outside-global-address {global-tcp-port </i> <i>global-udp-port}</i> ; <i>outside-local-address</i> { <i>global-tcp-port global-udp-port</i> } group <i>group-id add-route</i>	スタティック NAT を、外部グローバル ポート、外部ローカル ポートにマッピングします。

	コマンドまたはアクション	目的
ステップ 3	<code>switch(config)# copy running-config startup-config</code>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、TCP サービスを特定の外部送信元アドレスおよび TCP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static tcp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

スタティック Twice NAT の設定

同じグループ内のすべての変換は、スタティック Twice ネットワーク アドレス 変換 (NAT) ルールを作成する際に考慮されます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： <code>switch> enable</code>	特権 EXEC モードをイネーブルにします。 • 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： <code>switch# configure terminal</code>	特権 EXEC モードを開始します。
ステップ 3	ip nat inside source static <i>inside-local-ip-address</i> <i>inside-global-ip-address</i> [group <i>group-id</i>] 例： <code>switch(config)# ip nat inside</code> <code>source static 10.1.1.1</code> <code>192.168.34.4 group 4</code>	内部グローバル IP アドレスに対応する内部ローカル IP アドレスを変換するために、スタティック Twice NAT を設定します。 • group キーワードは、変換が属するグループを決定します。

	コマンドまたはアクション	目的
ステップ 4	<p>ip nat outside source static <i>outside-global-ip-address</i> <i>outside-local-ip-address</i>[group <i>group-id</i>] [add-route]</p> <p>例： switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4 add-route</p>	<p>外部ローカル IP アドレスに対応する外部グローバル IP アドレスを変換するために、スタティック Twice NAT を設定します。</p> <ul style="list-style-type: none"> • group キーワードは、変換が属するグループを決定します。
ステップ 5	<p>interface type number</p> <p>例： switch(config)# interface ethernet 1/2</p>	<p>インターフェイスを設定し、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。</p>
ステップ 6	<p>ip address ip-address mask</p> <p>例： switch(config-if)# ip address 10.2.4.1 255.255.255.0</p>	<p>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。</p>
ステップ 7	<p>ip nat inside</p> <p>例： switch(config-if)# ip nat inside</p>	<p>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。</p>
ステップ 8	<p>exit</p> <p>例： switch(config-if)# exit</p>	<p>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。</p>
ステップ 9	<p>interface type number</p> <p>例： switch(config)# interface ethernet 1/1</p>	<p>インターフェイスを設定し、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。</p>
ステップ 10	<p>ip address ip-address mask</p> <p>例： switch(config-if)# ip address 10.5.7.9 255.255.255.0</p>	<p>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。</p>
ステップ 11	<p>ipnatoutside</p> <p>例： switch(config-if)# ip nat outside</p>	<p>NAT の対象である外部ネットワークにインターフェイスを接続します。</p>
ステップ 12	<p>end</p> <p>例： switch(config-if)# end</p>	<p>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。</p>

スタティック NAT および PAT の設定例

次に、スタティック NAT の設定例を示します。

```
ip nat inside source static 103.1.1.1 11.3.1.1
ip nat inside source static 139.1.1.1 11.39.1.1
ip nat inside source static 141.1.1.1 11.41.1.1
ip nat inside source static 149.1.1.1 95.1.1.1
ip nat inside source static 149.2.1.1 96.1.1.1
ip nat outside source static 95.3.1.1 95.4.1.1
ip nat outside source static 96.3.1.1 96.4.1.1
ip nat outside source static 102.1.2.1 51.1.2.1
ip nat outside source static 104.1.1.1 51.3.1.1
ip nat outside source static 140.1.1.1 51.40.1.1
```

次に、スタティック PAT の設定例を示します。

```
ip nat inside source static tcp 10.11.1.1 1 210.11.1.1 101
ip nat inside source static tcp 10.11.1.1 2 210.11.1.1 201
ip nat inside source static tcp 10.11.1.1 3 210.11.1.1 301
ip nat inside source static tcp 10.11.1.1 4 210.11.1.1 401
ip nat inside source static tcp 10.11.1.1 5 210.11.1.1 501
ip nat inside source static tcp 10.11.1.1 6 210.11.1.1 601
ip nat inside source static tcp 10.11.1.1 7 210.11.1.1 701
ip nat inside source static tcp 10.11.1.1 8 210.11.1.1 801
ip nat inside source static tcp 10.11.1.1 9 210.11.1.1 901
ip nat inside source static tcp 10.11.1.1 10 210.11.1.1 1001
ip nat inside source static tcp 10.11.1.1 11 210.11.1.1 1101
ip nat inside source static tcp 10.11.1.1 12 210.11.1.1 1201
```

例：スタティック Twice NAT の設定

次の例は、内部送信元および外部送信元のスタティック Twice NAT 設定を設定する方法を示しています。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4
Switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4
Switch(config)# interface ethernet 1/2
Switch(config-if)# ip address 10.2.4.1 255.255.255.0
Switch(config-if)# ip nat inside
switch(config-if)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 10.5.7.9 255.255.255.0
switch(config-if)# ip nat outside
Switch(config-if)# end
```

スタティック NAT の設定の確認

スタティック NAT の設定を表示するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# show ip nat translations	内部グローバル、内部ローカル、外部ローカル、および外部グローバルの各 IP アドレスを示します。

次に、スタティック NAT の設定を表示する例を示します。

```
switch# show ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
any ---                ---                20.4.4.40         220.2.2.20
tcp ---                ---                23.1.1.133:333   210.3.3.33:555
any 160.200.1.140     10.1.1.40         ---                ---
any 160.200.1.140     10.1.1.40         20.4.4.40         220.2.2.20
tcp 172.9.9.142:777   12.2.2.42:444    ---                ---
tcp 172.9.9.142:777   12.2.2.42:444    23.1.1.133:333   210.3.3.33:555
```

ダイナミック NAT の設定

ダイナミック変換および変換タイムアウトの設定

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 モードをイネーブルにします。 • 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 access-list access-list-name 例： Switch(config)# ip access-list acl1	アクセス リストを定義し、アクセス リスト 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 4	permit <i>protocol source source-wildcardany</i> 例： Switch(config-acl)# permit ip 10.111.11.0/24 any	条件に一致したトラフィックを許可する IP アクセスリストの条件を設定します。
ステップ 5	deny <i>protocol source source-wildcardany</i> 例： Switch(config-acl)# deny udp 10.111.11.100/32 any	ネットワークの入力からのパケットを拒否する IP アクセスリストの条件を設定します。 拒否ルールはと許可ルールして扱われ、拒否ルールに記載された条件に一致するパケットは NAT 変換されずに転送されます。
ステップ 6	exit 例： Switch(config-acl)# exit	アクセスリスト 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 7	ipnatinside <i>source list access-list-name interface type number overload</i> 例： Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload	手順 3 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 8	interface <i>type number</i> 例： Switch(config)# interface ethernet 1/4	インターフェイスを設定し、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 <i>address ip-address mask</i> 例： Switch(config-if)# ip address 10.111.11.39 255.255.255.0	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 10	ipnat <i>inside</i> 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 11	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。

	コマンドまたはアクション	目的
ステップ 12	interface <i>typenumber</i> 例： Switch(config)# interface ethernet 1/1	インターフェイスを設定し、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 13	ipaddress <i>ip-addressmask</i> 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 14	ipnat <i>outside</i> 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 15	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 16	ipnat <i>translationtcp-timeoutseconds</i> 例： Switch(config)# ip nat translation tcp-timeout 50000	TCP ベースのダイナミック NAT エントリのタイムアウト値を指定します。 <ul style="list-style-type: none"> 設定されたタイムアウトの上限に達すると、動的に作成された NAT 変換がクリアされます。すべての設定されたタイムアウトは、ip nat translation sampling-timeout コマンドで設定されているタイムアウトの期限が切れた後にトリガーされます。
ステップ 17	ipnat <i>translationmax-entries[all-host]number-of-entries</i> 例： Switch(config)# ip nat translation max-entries 300	ダイナミック NAT 変換の最大数を指定します。エントリの数は、1 ~ 1023 を指定できます。

	コマンドまたはアクション	目的
ステップ 18	<p>ipnattranslationudp-timeoutseconds</p> <p>例： Switch(config)# ip nat translation udp-timeout 45000</p>	<p>UDP ベースのダイナミック NAT エントリのタイムアウト値を指定します。</p> <ul style="list-style-type: none"> 設定されたタイムアウトの上限に達すると、動的に作成された NAT 変換がクリアされます。すべての設定されたタイムアウトは、ip nat translation sampling-timeout コマンドで設定されているタイムアウトの期限が切れた後にトリガーされます。
ステップ 19	<p>ipnattranslationtimeoutseconds</p> <p>例： switch(config)# ip nat translation timeout 13000</p>	<p>ダイナミック NAT 変換のタイムアウト値を指定します。</p>
ステップ 20	<p>ipnattranslationsyn-timeout {seconds never}</p> <p>例： switch(config)# ip nat translation syn-timeout 20</p>	<p>SYN 要求を送信するが SYN-ACK 応答を受信しない TCP データのパケットタイムアウト値を指定します。</p> <p>タイムアウト値の範囲は、1 ~ 172800 秒です。デフォルト値は 60 秒です。</p> <p>never キーワードは、SYN タイマーが実行されないことを指定します。</p>
ステップ 21	<p>ipnattranslationfinrst-timeout {seconds never}</p> <p>例： switch(config)# ip nat translation finrst-timeout 30</p>	<p>終了 (FIN) またはリセット (RST) パケットを受信することで接続が終了される場合のフロー エントリのタイムアウト値を指定します。RST および FIN パケットの両方の動作を設定するには、同じキーワードを使用します。</p>

	コマンドまたはアクション	目的
		タイムアウト値の範囲は、1 ~ 172800 秒です。デフォルト値は 60 秒です。 never キーワードは、FIN または RST タイマーが実行されないことを指定します。
ステップ 22	end 例： Switch(config)# end	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。

ダイナミック NAT プールの設定

単一の **ip nat pool** コマンドで IP アドレスの範囲を定義することにより、または **ip nat pool** および **address** コマンドを使用することにより NAT プールを作成できます

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# feature nat	デバイスで NAT 機能をイネーブルにします。
ステップ 3	switch(config)# ip nat pool <i>pool-name</i> [<i>startip endip</i>] { prefix <i>prefix-length</i> netmask <i>network-mask</i> }	グローバル IP のアドレスの範囲の NAT プールを作成します。IP アドレスは、プレフィクス長またはネットワーク マスクを使用してフィルタリングされます。
ステップ 4	switch(config-ipnat-pool)# address <i>startip endip</i>	(任意) グローバル IP アドレスの範囲が、プールの作成中に指定されていない場合は指定します。
ステップ 5	switch(config)# no ip nat pool <i>pool-name</i>	(任意) 指定された NAT プールを削除します。

この例では、プレフィクス長を使用した NAT プールの作成方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
switch(config)#
```

この例では、ネットワーク マスクを使用した NAT プールの作成方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
switch(config)#
```

この例では、**ip nat pool** および **address** コマンドを使用した NAT プールの作成およびグローバル IP アドレスの範囲の定義方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool7 netmask 255.255.0.0
switch(config-ipnat-pool)# address 40.1.1.1 40.1.1.5
switch(config-ipnat-pool)#
```

この例では、NAT プールの削除方法を示します。

```
switch# configure terminal
switch(config)# no ip nat pool pool4
switch(config)#
```

送信元リストの設定

内部インターフェイスと外部インターフェイスの IP アドレスの送信元リストを設定できます。

はじめる前に

プールの送信元リストを設定する前に、プールの設定を確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch# ip nat inside source list <i>list-name pool pool-name [overload]</i>	(任意) オーバーロードの有無にかかわらずプールを使用した NAT 内部送信元リストを作成します。
ステップ 3	switch# ip nat outside source list <i>list-name pool pool-name [add-route]</i>	(任意) オーバーロードをかけずにプールを使用した NAT 外部送信元リストを作成します。

この例では、オーバーロードをかけずにプールを使用した NAT 内部送信元リストを作成する方法を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list1 pool pool1
switch(config)#
```

この例では、オーバーロードをかけてプールを使用した NAT 内部送信元リストを作成する方法を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list2 pool pool2 overload
switch(config)#
```

この例では、オーバーロードをかけずにプールを使用した NAT 外部送信元リストを作成する方法を示します。

```
switch# configure terminal
switch(config)# ip nat outside source list list3 pool pool3
switch(config)#
```

内部送信元アドレスのダイナミック Twice NAT の設定

内部送信元アドレス変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。内部送信元アドレスのダイナミック Twice NAT を設定できます。

はじめる前に

スイッチ上で NAT がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# ip nat outside source static <i>outside-global-ip-address</i> <i>outside-local-ip-address</i> [tcp udp] <i>outside-global-ip-address</i> <i>outside-global-port</i> <i>outside-local-ip-address</i> <i>outside-local-port</i> [group <i>group-id</i>] [add-route] [dynamic]	外部グローバルアドレスを内部ローカルアドレスに変換する、または内部ローカルトラフィックを内部グローバルトラフィックに変換するようにスタティック NAT を設定します。 group キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# ip nat inside source list <i>access-list-name</i> [interface <i>type slot/port</i> overload pool <i>pool-name</i>] [group <i>group-id</i>] [dynamic]	オーバーロードの有無にかかわらずプールを使用した NAT 内部送信元リストを作成することにより、ダイナミック送信元変換を確立します。

	コマンドまたはアクション	目的
		group キーワードは、変換が属するグループを決定します。
ステップ 4	<code>switch(config)# ip nat pool pool-name [startip endip] {prefix prefix-length netmask network-mask}</code>	グローバル IP のアドレスの範囲の NAT プールを作成します。IP アドレスは、プレフィクス長またはネットワーク マスクを使用してフィルタリングされます。
ステップ 5	<code>switch(config)# interface type slot/port</code>	インターフェイスを設定し、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	<code>switch(config-if)# ip nat outside</code>	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 7	<code>switch(config-if)# exit</code>	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 8	<code>switch(config)# interface type slot/port</code>	インターフェイスを設定し、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	<code>switch(config-if)# ip nat inside</code>	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。

次に、内部送信元アドレスのダイナミック Twice NAT を設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip nat outside source static 2.2.2.2 4.4.4.4 group 20 dynamic
switch(config)# ip nat inside source list acl_1 pool pool_1 overload group 20 dynamic
switch(config)# ip nat pool pool_1 3.3.3.3 3.3.3.10 prefix-length 24
switch(config)# interface Ethernet1/8
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/15
switch(config-if)# ip nat inside
```

外部送信元アドレスのダイナミック Twice NAT の設定

外部送信元アドレス変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。外部送信元アドレスのダイナミック Twice NAT を設定できます。

はじめる前に

スイッチ上で NAT がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	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	switch(config)# ip nat inside source static <i>inside-local-ip-address inside-global-ip-address</i> [tcp udp] <i>inside-local-ip-address local-port inside-global-ip-address global-port</i> [group <i>group-id</i>] [dynamic]	内部グローバルアドレスを内部ローカルアドレスに変換する、または内部ローカルトラフィックを内部グローバルトラフィックに変換するようにスタティック NAT を設定します。 group キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# ip nat outside source list <i>access-list-name</i> [interface <i>type slot/port</i> pool <i>pool-name</i>] [group <i>group-id</i>] [add-route] [dynamic]	プールを使用した NAT 外部送信元リストを作成することにより、ダイナミック送信元変換を確立します。
ステップ 4	switch(config)# ip nat pool <i>pool-name</i> [<i>startip endip</i>] { prefix <i>prefix-length</i> netmask <i>network-mask</i> }	グローバル IP のアドレスの範囲の NAT プールを作成します。IP アドレスは、プレフィクス長またはネットワーク マスクを使用してフィルタリングされます。
ステップ 5	switch(config)# interface <i>type slot/port</i>	インターフェイスを設定し、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	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 7	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 8	switch(config)# interface <i>type slot/port</i>	インターフェイスを設定し、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	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。

次に、外部送信元アドレスのダイナミック Twice NAT を設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip nat inside source static 7.7.7.7 5.5.5.5 group 30 dynamic
switch(config)# ip nat outside source list acl_2 pool pool_2 group 30 dynamic
switch(config)# ip nat pool pool_2 4.4.4.4 4.4.4.10 prefix-length 24
switch(config)# interface Ethernet1/6
switch(config-if)# ip nat outside
switch(config-if)# exit
```

```
switch(config)# interface Ethernet1/11
switch(config-if)# ip nat inside
```

ダイナミック NAT 変換のクリア

ダイナミック変換をクリアするには、次の作業を実行します。

コマンド	目的
clear ip nat translation [all inside <i>global-ip-address local-ip-address</i> [outside <i>local-ip-address global-ip-address</i>] outside <i>local-ip-address global-ip-address</i>]	すべてまたは特定のダイナミック NAT 変換を削除します。

この例では、すべてのダイナミック変換をクリアする方法を示します。

```
switch# clear ip nat translation all
```

この例では、内部および外部アドレスのダイナミック変換をクリアする方法を示します。

```
switch# clear ip nat translation inside 2.2.2.2 4.4.4.4 outside 5.5.5.5 7.7.7.7
```

ダイナミック NAT の設定の確認

ダイナミック NAT の設定を表示するには、次の作業を行います。

コマンド	目的
show ip nat translations	ダイナミック変換を含むアクティブなネットワーク アドレス変換 (NAT) を表示します。 エントリがいつ生成され、いつ使用されたかを含む各変換テーブルエントリの追加情報が表示されます。
show run nat	NAT の設定を表示します。

この例では、NAT の実行コンフィギュレーションを表示する方法を示します。

```
switch# show run nat

!Command: show running-config nat
!Time: Wed Apr 23 11:17:43 2014

version 6.0(2)A3(1)
feature nat

ip nat inside source list list1 pool pool1
ip nat inside source list list2 pool pool2 overload
ip nat inside source list list7 pool pool7 overload
ip nat outside source list list3 pool pool3
ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
ip nat pool pool2 10.1.1.1 10.1.1.2 netmask 255.0.255.0
```

例：ダイナミック変換および変換タイムアウトの設定

```
ip nat pool pool3 30.1.1.1 30.1.1.8 prefix-length 24
ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
ip nat pool pool7 netmask 255.255.0.0
  address 40.1.1.1 40.1.1.5
```

この例では、アクティブ NAT 変換を表示する方法を示します。

オーバーロードをかけた内部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local      Outside local     Outside global
icmp 20.1.1.3:64762     10.1.1.2:133     20.1.1.1:0       20.1.1.1:0
icmp 20.1.1.3:64763     10.1.1.2:134     20.1.1.1:0       20.1.1.1:0
```

オーバーロードをかけない外部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local      Outside local     Outside global
any  ---              ---              177.7.1.1:0      77.7.1.64:0
any  ---              ---              40.146.1.1:0     40.46.1.64:0
any  ---              ---              10.4.146.1:0     10.4.46.64:0
```

例：ダイナミック変換および変換タイムアウトの設定

次の例では、アクセスリストを指定して、ダイナミック オーバーロード ネットワーク アドレス 変換 (NAT) を設定する方法を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip access-list acl1
Switch(config-acl)# permit ip 10.111.11.0/24 any
Switch(config-acl)# deny udp 10.111.11.100/32 any
Switch(config-acl)# exit
Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload
Switch(config)# interface ethernet 1/4
Switch(config-if)# ip address 10.111.11.39 255.255.255.0
Switch(config-if)# ip nat inside
Switch(config-if)# exit
Switch(config)# interface ethernet 1/1
Switch(config-if)# ip address 172.16.232.182 255.255.255.240
Switch(config-if)# ip nat outside
Switch(config-if)# exit
Switch(config)# ip nat translation tcp-timeout 50000
Switch(config)# ip nat translation max-entries 300
Switch(config)# ip nat translation udp-timeout 45000
Switch(config)# ip nat translation timeout 13000
Switch(config)# end
```

VRF 対応 NAT に関する情報

VRF 対応 NAT 機能は、VRF (virtual routing and forwarding instances) のアドレス空間を理解し、パケットを変換するスイッチをイネーブルにします。イネーブルにするにより、NAT 機能が 2 つの VRF 間で使用されている重複するアドレス空間のトラフィックを変換できるようになります。

VRF 対応 NAT は、スタティック NAT とダイナミック NAT 設定でサポートされます。トラフィックが、デフォルト以外の VRF (内部) から同じデフォルト以外の VRF (外部) に流れるように設定されている場合、IP NAT コマンドの `match-in-vrf` オプションを指定する必要があります。

トラフィックが、デフォルト以外の VRF（内部）からデフォルトの VRF（外部）に流れるように設定されている場合、IP NAT コマンドの `match-in-vrf` オプションは指定することはできません。

1 つの `non-default-vrf` から別の `non-default-vrf` へ流れるトラフィックは変換されません。（たとえば、`vrfA` を `vrfB` に）。

VRF 対応 NAT の設定

はじめる前に

スイッチ上で NAT がイネーブルであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	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	<code>switch(config)# [no] ip nat inside outside source list ACL_NAME [interface INTERFACE NAME overload] [pool POOL NAME overload] [group group-id] [dynamic] [vrf <vrf-name> [match-in-vrf]</code>	VRF 固有のダイナミック NAT を作成または削除します。 group キーワードは、変換が属するグループを決定します。
ステップ 3	<code>switch(config)# [no] ip nat inside outside source static LOCAL_IP GLOBAL_IP [tcp udp LOCAL_IP LOCAL_PORT GLOBAL_IP GLOBAL_PORT] [group group-id] [dynamic] [vrf <vrf-name> [match-in-vrf]</code>	VRF 固有のスタティック NAT を作成または削除します。 group キーワードは、変換が属するグループを決定します。
ステップ 4	<code>switch(config)# interface type slot/port [vrf <vrf-name ip nat inside outside</code>	VRF 対応 インターフェイスで NAT を <input type="checkbox"/> ネーブルにします。

`show run nat` コマンドの出力を参照してください。

```
#show run nat
...
feature nat
ip nat inside source static 1.1.1.1 1.1.1.100 vrf red match-in-vrf
ip nat outside source static 2.2.2.200 2.2.2.2 vrf red match-in-vrf add-route
ip nat inside source list nat-acl-in1 pool pool-in1 vrf red match-in-vrf overload
ip nat outside source list nat-acl-out1 pool pool-out1 vrf red match-in-vrf add-route
interface Ethernet1/3
 ip nat outside
interface Ethernet1/5
 ip nat inside

N3548#show ip nat translation verbose
Pro Inside global      Inside local      Outside local      Outside global
any 1.1.1.100          1.1.1.1           ---                ---
  Flags:0x800001 time-left(secs):-1 id:0 state:0x0 grp_id:0 vrf: red   Timer left (secs):
-1 syn (secs):-1 fin-rst (secs):-1
```

```
Outside Static with vrf 'red'
N3548#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
any ---                ---                2.2.2.2            2.2.2.200
  Flags:0xa00009 time-left(secs):-1 id:0 state:0x0 grp_id:0 vrf: red   Timer left (secs):
-1 syn (secs): -1 fin-rst (secs): -1
Dynamic Inside NAT entries
N3548#show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
udp 199.1.2.1:64542    141.1.1.11:63    102.1.1.11:63     102.1.1.11:63
  Flags:0x800082 time-left(secs):19 id:223 state:0x3 grp_id:0 vrf: red   Timer left
(secs): 19 syn (secs): -1 fin-rst (secs): 19
```