スタティックおよびダイナミック NAT 変換の設定

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、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の間の出口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 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。出口点が複数存在する場合、個々の NAT は同じ変換テーブルを持っている必要があります。

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

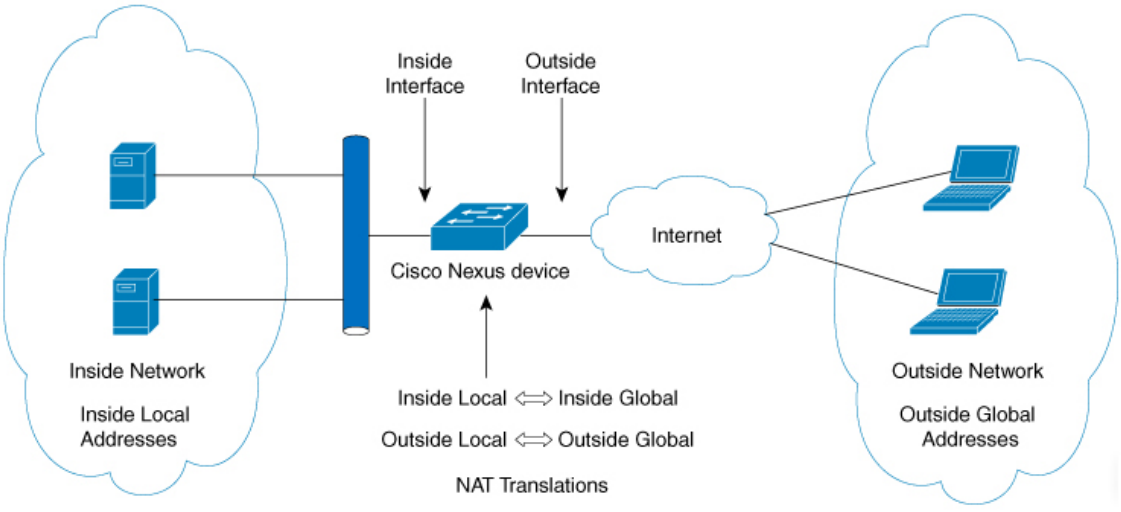
静的ネットワーク アドレス変換（NAT）を使用すると、ユーザは内部ローカル IP アドレスから内部グローバル IP アドレスへの 1 対 1 変換を構成することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 構成で NAT 変換を追加または削除できることを意味します。

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）。

静的または、ダイナミック NAT の主な違いは、ダイナミック NAT の場合、変換対象のトラフィックデバイスに受信するまでは、NAT 変換テーブルには変換エントリが存在しません。ダイナミック変換は、新しいエントリ用のスペースを確保するために使用されていない場合、クリアまたはタイムアウトされます。静的エントリは、トラフィックを受信するデバイスに関係なく、常に存在します。ただし、静的 NAT とダイナミック NATの両方で、各ホストは、オーバーロードなどのさまざまな構成に基づいて、後続の変換ごとに異なるアドレスまたはポートを使用できます。

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る 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）では、実際のアドレスのグループは、接続先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。またダイナミック NAT では、未登録の IP アドレスと登録済み IP アドレス間で一対一のマッピング確立しますが、通信時にプール内で利用可能な登録済みアドレスによって、マッピングは変化します。

ダイナミック NAT を設定自動Aすると、使用している内部ネットワークと外部ネットワークまたはインターネット間に、ファイウォールが構築されます。ダイナミックNATは、スタブドメイン内で発信された接続のみを許可します。外部ネットワーク上のデバイスは、接続を開始していない限り、ネットワーク内のデバイスに接続できません。

ダイナミック NAT の場合、変換対象のトラフィックデバイスに受信するまでは、NAT 変換テーブルには変換エントリが存在しません。ダイナミック変換は、新しいエントリ用のスペースを確保するために使用されていない場合、クリアまたはタイムアウトされます。通常、NAT 変換エントリはタイマーに基づいてクリアされます。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 3600 秒です。

（注） この項で説明している **ip nat translation sampling-timeout** コマンドはサポートされていません。統計情報はインストール済みの NAT ポリシーに 60 秒ごとに収集されます。これらの統計情報はフローがアクティブかまたはアクティブでないかを決定するために使用されます。

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。PAT（暗号化ともいう）、オーバーロードは未登録の複数の IP アドレスを、さまざまなポートを使うことによって、登録済みの単一の IP アドレスにマッピングするダイナミック NAT の 1 形態です。

タイムアウトメカニズム

ダイナミック NAT 変換を作成した後は、特に TCAM エントリの数が制限されている場合、新しい変換を作成できるように、使用していないものをクリアする必要があります。このリリースでは、syn-timeout および finrst-timeout がサポートされています。スイッチでは、次のNAT変換タイムアウトタイマーがサポートされています。

スイッチでは、次のNAT変換タイムアウトタイマーがサポートされています。

- syn-timeout：TCPデータのパケットタイムアウト値。SYNリクエストを送信後、SYN-ACK応答を受信するまでの最大待ち時間です。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 パケットの受信によって接続が終了したときのフローエントリのタイムアウト値。RSTパケットと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。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。

  接続が確立された後に SYN パケット（SYN >SYN-ACK >FIN）が受信されると、finrst タイマーが開始されます。

  相手側からFIN-ACKを受信すると、変換エントリはすぐにクリアされます。それ以外の場合は、タイムアウト値の完了後にクリアされます。

  接続が確立された後にRSTパケットを受信した場合（SYN>SYN-ACK>RST）、変換エントリはすぐにクリアされます。
- tcp-timeout：TCP 変換のタイムアウト値。3 ウェイ ハンドシェイク（SYN、SYN-ACK、ACK）の後に確立した接続の最大待ち時間です。接続が確立された後にアクティブ フローが発生しない場合、変換は設定されたタイム アウト値に従って期限切れになります。

  タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルトは、3600 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、60 ～ 172800 秒です。デフォルトは、3600 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、60 ～ 172800 秒です。デフォルトは、3600 秒です。

- icmp-timeout：ICMP パケットのタイムアウト値。

  タイムアウト値の範囲は、60 ～ 172800 秒です。デフォルトは、3600 秒です。

（注） 構成されたタイムアウトのないダイナミック エントリを作成すると、3600 秒のデフォルトのタイムアウトが使用されます。デフォルトのタイムアウト値を新しい値に変更した後に作成された変換エントリは、最新のタイムアウト値を取得します。

NAT の内部アドレスおよび外部アドレス

NAT 内部とは、変換を必要とす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 外部とは、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。通常、組織の管理下にはありません。外部ネットワーク内のホストを変換の対象にすることもできるため、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：ネットワークの内側部分に表示されるローカルな IP アドレスです。
- グローバル アドレス：ネットワークの外側部分に表示されるグローバルな IP アドレスです。
- 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、インターネット ネットワーク情報センター（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。必ずしも正規の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たものです。

ダイナミック NAT のプール サポート

Cisco NX-OS は、ダイナミック NAT のプールをサポートします。ダイナミック NAT を使用すると、グローバル アドレスのプールを設定して、新しい変換ごとにプールからグローバル アドレスを動的に割り当てることができます。アドレスは、セッションが期限切れになるか、閉じられた後にプールに返されます。これにより、要件に基づいてアドレスをより効率的に使用できます。

PAT のサポートには、グローバル アドレス プールの使用が含まれます。これにより、IP アドレスの使用率がさらに最適化されます。PAT は、ポート番号を使用して、一度に 1 つの IP アドレスを使い果たします。ポートが該当グループで見つけられなかった場合や、複数の IP アドレスが設定されている場合、PAT は次の IP アドレスに移動して、ユーザー定義プールに基づいて、（ソース ポートを無視するか、それを保存しようと試みて）割り当てを取得します。

ダイナミック NAT および PAT では、各ホストは変換するたび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。

静的およびダイナミック 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、IPv4 ユニキャストだけでサポートされています。
- 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 proxy-arp** コマンドを使用します。**add-route** キーワードを使用する場合は、**ip proxy-arp** を有効にする必要があります。
- Cisco Nexus デバイスは、次のインターフェイスタイプで NAT をサポートします。
  - スイッチ仮想インターフェイス（SVI）
  - 物理層レイヤ 3 インターフェイス
  - ポート チャンネル レイヤ 3 インターフェイス
- 非 TCP/UDP パケットは、常にソフトウェア変換されます。
- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- 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ることはできません。
- （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。
- Twice NAT はサポートされていません。

- NAT の内部ルールと外部ルールを同時に構成することはサポートされていません。
- IP NAT 内部または IP NAT 外部などの NAT 構成は、ループバック インターフェイスではサポートされていません。

ダイナミック NAT の制約事項

ダイナミックネットワークアドレス変換（NAT）には、次の制約事項が適用されます。

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- VXLANルーティングはCisco Nexusデバイスではサポートされません。
- フラグメント化されたパケットはサポートされません。
- アプリケーション層ゲートウェイ（ALG）変換はサポートされていません。ALG、またはアプリケーションレベル ゲートウェイは、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。
- 出力 ACL は、変換されたパケットには適用されません。
- MIB はサポートされていません。
- Cisco Data Center Network Manager（DCNM）はサポートされていません。
- Cisco Nexusデバイスでは、複数のグローバル仮想デバイスコンテキスト（VDC）はサポートされていません。
- ダイナミックNAT変換は、アクティブデバイス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はサポートされていません。ただし、NATとHot Standby Router Protocol（HSRP）は共存できます。
- のタイムアウト値は、設定されたタイムアウト+ 119秒までかかります。
- ダイナミックNATでは、プールのオーバーロードとインターフェイスのオーバーロードは外部NATではサポートされません。
- Cisco Nexus デバイスは、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）。
- [ip nat 内部（ip nat inside）] または [ip nat 外部（ip nat outside）] などの NAT 構成は、ループバック インターフェイスではサポートされていません。

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**	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 NAT の構成

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。 （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	（任意） switch(config)# **copy running-config startup-config**	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。

例

次に、内部からNATを構成する例を 2 つ示します。

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

```
switch# configure terminal
switch(config)# interface vlan 100
switch(config-if)# ip nat inside
```

次に、外部からNATを構成する例を 2 つ示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ip nat outside
```

```
switch# configure terminal
switch(config)# interface vlan 102
switch(config-if)# ip nat ouside
```

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、パケットの送信元アドレスは、内部インターフェイスから外部インターフェイスへ変換されます。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） 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、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Cisco Nexus デバイス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* [**vrf** *vrf-name*] [**match-in-vrf**] [**add-route**][**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ローカル

	コマンドまたはアクション	目的
		（local） 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	（任意） switch(config)# **copy running-config startup-config**	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。

例

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、接続先アドレスは内部インターフェイスから外部インターフェイスに変換されます。リターン トラフィックでは、宛先の外部グローバル IP アドレスが外部ローカル 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** *outsideGlobalIP outsideLocalIP* [**vrf** *vrf-name* [**match-in-vrf**] [**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。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	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。

例

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** {*inside-local-address inside-global-address* | {**tcp**| **udp**} *inside-local-address* {*local-tcp-port* | *local-udp-port*} *inside-global-address* {*global-tcp-port* | *global-udp-port*}} {**vrf** *vrf-name* {**match-in-vrf**} }	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	（任意） switch(config)# **copy running-config startup-config**	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。

例

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** {*outside-global-address outside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* | *global-udp-port*} *outside-local-address* {*global-tcp-port* | *global-udp-port*}} {**add-route**} {**vrf** *vrf-name* {**match-in-vrf**}}	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。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	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。

例

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
```

no-alias 設定の有効化と無効化

NAT デバイスは内部グローバル（IG）アドレスと外部ローカル（OL）アドレスを所有し、これらのアドレス宛ての ARP 要求に応答します。IG/OL アドレス サブネットがローカル インターフェイス サブネットと一致すると、NAT は IP エイリアスと ARP エントリをインストールします。この場合、デバイスは local-proxy-arp を使用して ARP 要求に応答します。

no-alias 機能は、アドレス範囲が外部インターフェイスの同じサブネットにある場合、特定の NAT プール アドレス範囲からのすべての変換された IP の ARP 要求に応答します。

NAT が設定されたインターフェイスで no-alias が有効になっている場合、外部インターフェイスはサブネット内の ARP 要求に応答しません。no-alias を無効にすると、外部インターフェイスと同じサブネット内の IP に対する ARP 要求が処理されます。

（注） この機能をサポートしていない古いリリースにダウングレードすると、*no-alias* オプションの設定が削除されることがあります。

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)# **show run nat**	NAT の設定を表示します。
ステップ 4	switch(config)# **show ip nat-alias**	エイリアスが作成されたかどうかの情報を表示します。 （注） デフォルトでは、エイリアスが作成されます。エイリアスを無効にするには、*no-alias* キーワードをコマンドに追加する必要があります。
ステップ 5	switch(config)# **clear ip nat-alias** *ip address/all*	エイリアス リストからエントリを削除します。特定のエントリを削除するには、削除する IP アドレスを指定する必要があります。すべてのエントリを削除するには、すべてのキーワードを使用します。

例

次に、すべてのインターフェイスの情報を表示する例を示します。

```
switch# configure terminal
switch(config)# show ip int b
IP Interface Status for VRF "default"(1)
Interface            IP Address      Interface Status
Lo0                  100.1.1.1       protocol-up/link-up/admin-up
Eth1/1               7.7.7.1         protocol-up/link-up/admin-up
Eth1/3               8.8.8.1         protocol-up/link-up/admin-up
```

次に、実行コンフィギュレーションの例を示します。

```
switch# configure terminal
switch(config)# show running-config nat
!Command: show running-config nat
!Running configuration last done at: Thu Aug 23 11:57:01 2018
!Time: Thu Aug 23 11:58:13 2018

version 9.2(2) Bios:version 07.64
feature nat
interface Ethernet1/1
  ip nat inside
```

```
interface Ethernet1/3
  ip nat outside
switch(config)#
```

この例は、エイリアスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#
```

次に、*show ip nat-alias* の出力例を示します。デフォルトでは、エイリアスが作成されます。

```
switch# configure terminal
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#
```

この例は、エイリアスを無効にする方法を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3 no-alias
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3 no-alias
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
7.7.7.2          Ethernet1/1
8.8.8.2          Ethernet1/3
switch(config)#

** None of the entry got appended as alias is disabled for above CLIs.
switch(config)#
```

この例は、エイリアスをクリアする方法を示します。エイリアス リストからエントリを削除するには、*clear ip nat-alias* を使用します。IP アドレスを指定して 1 つのエントリを削除することも、すべてのエイリアス エントリを削除することもできます。

```
switch# configure terminal
switch(config)# clear ip nat-alias address 7.7.7.2
switch(config)# show ip nat-alias
Alias Information for Context: default
Address         Interface
8.8.8.2          Ethernet1/3
switch(config)#
switch(config)# clear ip nat-alias all
switch(config)# show ip nat-alias
switch(config)#
```

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
```

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。

例

次に、スタティック NAT の設定を表示する例を示します。

```
switch# sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global

--- ---                ---                51.3.1.1           104.1.1.1
--- ---                ---                95.4.1.1           95.3.1.1
--- ---                ---                96.4.1.1           96.3.1.1
--- ---                ---                51.40.1.1          140.1.1.1
--- ---                ---                51.42.1.1          142.1.2.1
--- ---                ---                51.1.2.1           102.1.2.1
--- 11.1.1.1           101.1.1.1          ---                ---
--- 11.3.1.1           103.1.1.1          ---                ---
--- 11.39.1.1          139.1.1.1          ---                ---
```

```
--- 11.41.1.1          141.1.1.1          ---                ---
--- 95.1.1.1           149.1.1.1          ---                ---
--- 96.1.1.1           149.2.1.1          ---                ---
    130.1.1.1:590      30.1.1.100:5000    ---                ---
    130.2.1.1:590      30.2.1.100:5000    ---                ---
    130.3.1.1:590      30.3.1.100:5000    ---                ---
    130.4.1.1:590      30.4.1.100:5000    ---                ---
    130.1.1.1:591      30.1.1.101:5000    ---                ---
```

```
switch# sh ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
any ---                ---                22.1.1.3           22.1.1.2
    Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.130         11.1.1.3           ---                ---
    Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:0
any 11.1.1.133         11.1.1.33          ---                ---
    Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.133         11.1.1.33          22.1.1.3           22.1.1.2
    Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:0
tcp 10.1.1.100:64490   10.1.1.2:0         20.1.1.2:0         20.1.1.2:0
    Flags:0x82 time-left(secs):43192 id:31 state:0x3 grp_id:0 vrf: default
N3550T-1#
```

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 モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
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。
ステップ 4	**permit** *protocol source source-wildcard* **any** 例：	条件に一致するトラフィックを許可する条件をIPアクセスリストに設定します。

	コマンドまたはアクション	目的
	`Switch(config-acl)# permit ip 10.111.11.0/24 any`	
ステップ 5	**deny** *protocol source source-wildcard* **any** 例： `Switch(config-acl)# deny udp 10.111.11.100/32 any`	NAT 変換を拒否する条件を設定します。
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	**ip nat inside source list** *access-list-name* **interface** *type number* [**vrf** *vrf-name* [**match-in-vrf**] [**add-route**] [**overload**] 例： `Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload`	ステップ 3 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 8	**interface** *type number* 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 address** *ip-address mask* 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	**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。 （注） ループバック インターフェイスでは構成がサポートされていません。
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。
ステップ 12	**interface** *type number* 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。

	コマンドまたはアクション	目的
ステップ 13	**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 14	**ip nat outside** 例： `Switch(config-if)# ip nat outside`	インターフェイスを外部ネットワークに接続します。 （注） ループバック インターフェイスでは構成がサポートされていません。
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	**ip nat translation max-entries** *number-of-entries* 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 ー 1023 です。
ステップ 17	**ip nat translation timeout** *seconds* 例： `switch(config)# ip nat translation timeout 13000`	ダイナミック NAT 変換のタイムアウト値を指定します。
ステップ 18	**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

NAT プールは、単一の **ip nat pool** コマンドか、または **ip nat pool** と **address** コマンドを使用して、IP アドレスの範囲を定義することで作成できます。

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。

	コマンドまたはアクション	目的
ステップ 2	switch (config)# **feature nat**	デバイスの NAT 機能をイネーブルにします。
ステップ 3	switch (config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィッ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	（任意） switch (config-ipnat-pool)# **address** *startip endip*	グローバル IP アドレスの範囲を指定します（プールの作成時に指定していなかった場合）。
ステップ 5	（任意） switch (config)# **no ip nat pool** *pool-name*	指定した NAT プールを削除します。

例

次に、プレフィックス長を使用して NAT プールを作成する例を示します。

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

次に、ネットワークマスクを使用して NAT プールを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.255.255.0
switch(config)#
```

この例では **ip nat pool** と **address** コマンドを使用してNAT プールを作成し、グローバル IP アドレスの範囲を定義します。

```
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)#
```

次の例は、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。

始める前に

プールの送信元リストを設定する前に、必ずプールを設定してください。

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	（任意） switch# **ip nat inside source list** *list-name* **pool** *pool-name* [**overload**]	オーバーロードの有無にかかわらず、プールを使用して NAT 内部送信元リストを作成します。
ステップ 3	（任意） switch# **ip nat outside source list** *list-name* **pool** *pool-name* [**add-route**]	オーバーロードなしでプールを使用して NAT 外部送信元リストを作成します。

例

次に、オーバーロードのないプールを使用してNAT内部送信元リストを作成する例を示します。

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

次に、オーバーロードのあるプールを使用してNAT内部送信元リストを作成する例を示します。

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

次に、オーバーロードのないプールを使用してNAT外部送信元リストを作成する例を示します。

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

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** *global-ip-address local-ip-address* [**outside** *local-ip-address global-ip-address*] | **outside** *local-ip-address global-ip-address*]	すべてまたは特定のダイナミックNAT変換を削除します。

例

次に、すべてのダイナミック変換をクリアする例を示します。

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

次に、内部アドレスと外部アドレスのダイナミック変換をクリアする例を示します。

```
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	アクティブなネットワーク アドレス変換（NAT）変換を表示します。 エントリが作成および使用された日時など、各変換テーブル エントリの追加情報を表示します。
show run nat	NAT の設定を表示します。
show ip nat max	アクティブなネットワーク アドレス変換（NAT）の最大値を表示します。
show ip nat statistics	NAT 統計情報をモニタします。

例

次に、IP NAT 最大値を表示する例を示します。

```
switch# show ip nat max

IP NAT Max values
====================
Max Dyn Translations:80
Max all-host:0
```

```
No.Static:0
No.Dyn:1
No.Dyn-ICMP:1
====================
Switch(config)#
```

次に、NAT 統計情報を表示する例を示します。

```
switch# show ip nat statistics

IP NAT Statistics
==================================================
Stats Collected since: Mon Feb 24 18:27:34 2020
--------------------------------------------------
Total active translations: 1
No.Static: 0
No.Dyn:    1
No.Dyn-ICMP:   1
--------------------------------------------------
Total expired Translations: 0
SYN timer expired:          0
FIN-RST timer expired:      0
Inactive timer expired:     0
--------------------------------------------------
Total Hits:  2                  Total Misses:  2
In-Out Hits: 0                  In-Out Misses: 2
Out-In Hits: 2                  Out-In Misses: 0
--------------------------------------------------
Total SW Translated Packets: 2
In-Out SW Translated: 2
Out-In SW Translated: 0
--------------------------------------------------
Total SW Dropped Packets: 0
In-Out SW Dropped: 0
Out-In SW Dropped: 0

Address alloc. failure drop:      0
Port alloc.  failure drop:        0
Dyn. Translation max limit drop:  0
ICMP max limit drop:              0
Allhost max limit drop:           0
--------------------------------------------------
Total TCP session established: 0
Total TCP session closed:      0
--------------------------------------------------
NAT Inside Interfaces:  1
Ethernet1/34

NAT Outside Interfaces: 1
Ethernet1/32
--------------------------------------------------
Inside source list:
++++++++++++++++++++

Access list: T2
RefCount: 1
Pool: T2     Overload
Total addresses: 10
Allocated: 1    percentage: 10%
Missed: 0


Outside source list:
```

```
++++++++++++++++++++
------------------------------------------------------
======================================================
Switch(config)#
Switch(config)#


**No.Dyn-ICMP  field is to display the no of icmp dynamic translations , its a subset
of  "No.Dyn" field.
```

（注） Cisco NX-OS リリース 10.2（3u）以降では、**No.Dyn-ICMP** フィールドは **No.Dyn** フィールドのサブセットであり、ICMP ダイナミック変換の数が表示されます。

次に、NAT の実行コンフィギュレーションを表示する例を示します。

```
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
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
```

次に、アクティブな NAT 変換を表示する例を示します。

オーバーロードのある内部プール

```
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
```

オーバーロードのない外部プール

```
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

次に、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）を設定する例を示します。

```
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 max-entries 300
Switch(config)# ip nat translation timeout 13000
Switch(config)# end
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。