

ネットワークアドレス変換 (NAT) に関する FAQ の確認

内容

[はじめに](#)

[NAT 全般](#)

[Q. NAT とは何ですか。](#)

[Q. NAT はどのように機能しますか。](#)

[Q. NAT の設定方法を教えてください。](#)

[Q. Cisco IOSソフトウェアとCisco PIXセキュリティアプライアンスでのNATの実装の主な違いは何ですか。](#)

[Q. Cisco IOS の NAT 機能はどの Cisco ルーティングハードウェアで利用できますか。ハードウェアを注文するにはどうすればよいですか。](#)

[Q. NAT の処理が行われるのはルーティングの前ですか、それとも後ですか。](#)

[Q. NAT を公衆無線 LAN 環境に導入できますか。](#)

[Q. NAT は、内部ネットワーク上のサーバーに対して TCP の負荷分散を行いますか。](#)

[Q. NAT 変換の数をレート制限することはできますか。](#)

[Q. NAT で使用される IP サブネットまたはアドレスの、ルーティングの学習または伝播の仕組みを教えてください。](#)

[Q. Cisco IOS の NAT 機能でサポートされる同時 NAT セッションの数はいくつですか。](#)

[Q. Cisco IOS の NAT 機能を使用すると、どのようなルーティング性能を期待できますか。](#)

[Q. サブインターフェイスに Cisco IOS の NAT 機能を適用できますか。](#)

[Q. Cisco IOS の NAT 機能と Hot Standby Router Protocol \(HSRP \) を組み合わせることで ISP に冗長リンクを提供できますか。](#)

[Q. Cisco IOS の NAT 機能は、フレームリレー インターフェイスでのインバウンド変換に対応していますか。また、イーサネット側でのアウトバウンド変換をサポートしますか。](#)

[Q. 1 台の NAT 対応ルータで、一部のユーザーには NAT を適用し、他のユーザーにはそれまでどおり各自に IP アドレスを適用するような設定を、同じイーサネット インターフェイス上でできますか。](#)

[Q. PAT \(オーバーロード変換 \) を設定する場合、各内部グローバル IP アドレスに対して最大いくつの変換を作成できますか。](#)

[Q. PAT はどのように機能しますか。](#)

[Q. NAT IP プールとは何ですか。](#)

[Q. 設定可能な NAT IP プールの最大数は何ですか \(ip nat pool \) 。](#)

[Q. NAT プールでルートマップと ACL を使用する利点には、どのような違いがありますか。](#)

[Q. NAT における IP アドレスの重複とは何ですか。](#)

[Q. 静的 NAT 変換とは何ですか。](#)

[Q. NAT オーバーロードとは何ですか。これは PAT ですか。](#)

[Q. 動的 NAT 変換とは何ですか。](#)

[Q. ALG とは何ですか。](#)

[Q. 静的 NAT 変換と動的 NAT 変換を併用する構成は可能ですか。](#)

[Q. NAT ルータを経由して traceroute を実行すると、traceroute によって NAT グローバルアドレスが表示されるのですか。それとも、NAT ローカルアドレスがリークされるのですか。](#)

[Q. PAT はどのようにしてポートを割り当てますか。](#)

Q. IP フラグメンテーションと TCP セグメンテーションはどのように違いますか。

Q. NAT は IP フラグメンテーションおよび TCP セグメンテーションのアウトオブオーダーに対応していますか。

Q. IP フラグメンテーションと TCP セグメンテーションをデバッグするにはどうすればよいですか。

Q. サポートされている NAT MIB はありますか。

Q. TCP タイムアウトとはどのような事象ですか。また、NAT の TCP タイマーとはどのような関連がありますか。

Q. NAT変換がタイムアウトするまでの時間をNAT変換テーブルから変更できますか。

Q. Lightweight Directory Access Protocol (LDAP) で、各 LDAP 応答パケットに追加のバイトが付加されないようにする方法を教えてください。

Q. NAT ボックスで使用する内部グローバル IP または外部ローカル IP アドレスにはどのようなルートが推奨されますか。

Q. Cisco IOSのNATでは、logキーワードを使用するACLはサポートされていますか。

Voice-NAT

Q. NAT は、Cisco Unified Communications Manager (CUCM) V7 に付属している Skinny Client Control Protocol (SCCP) v17 をサポートしていますか。

Q. NAT はどのバージョンの CUCM、SCCP、ファームウェアロードをサポートしていますか。

Q. サービスプロバイダーが提供する RTP および RTCP 用の PAT ポート割り当て拡張とはどのようなものですか。

Q. Session Initiation Protocol (SIP) とは何ですか。SIP パケットは NAT で処理できますか。

Q. セッション ボーダー コントローラ (SBC) のホスト型 NAT トラバースサポートとは何ですか。

Q. ルータのメモリおよび CPU は SIP、Skinny、H323 のコールをいくつまで NAT で処理できますか。

Q. NATルータでは、SkinnyパケットとH323パケットのTCPセグメンテーションはサポートされていますか。

Q. 音声環境で NAT のオーバーロード設定を使用する際に注意することはありますか。

Q. 音声環境で clear ip nat trans * コマンドまたは clear ip nat transforce コマンドを発行することで起きる、既知の問題はありますか。

Q. NAT は音声ソリューションの併存環境をサポートしていますか。

Q. NVI は Skinny ALG、H323 ALG、TCP SIP ALG をサポートしていますか。

NAT と VRF/MPLS

Q. NATルータでは、グローバルアドレス空間でNATが実行されると同時に、VRF内の同じアドレス空間でのNATもサポートされるのですか。現在、これを設定しようとすると、「% similar static entry (10.1.1.1 -> 10.210.2.2) already exists」という警告が表示されます。

Q. レガシー NAT は VRF-Lite (特定の VRF から別の VRF への NAT) をサポートしていますか。

NAT NVI

Q. NAT NVI とは何ですか。

Q. グローバルのインターフェイスとVRFのインターフェイスの間でNATを行う場合、NAT NVIを使用する必要がありますか。

Q. NAT-NVI での TCP セグメンテーションはサポートされていますか。

Q. NVI は Skinny ALG、H323 ALG、TCP SIP ALG をサポートしていますか。

Q. TCP セグメンテーションは SNAT でサポートされていますか。

SNAT

Q. ステートフル NAT (SNAT) とは何ですか。

Q. TCP セグメンテーションは SNAT でサポートされていますか。

Q. SNATは非対称ルーティングをサポートしていますか。

NAT-PT (v6 から v4)

Q. NAT-PT とは何ですか。

[Q. NAT-PT は Cisco Express Forwarding \(CEF\) パスでサポートされていますか。](#)

[Q. NAT-PT ではどの ALG がサポートされていますか。](#)

[Q. ASR 1004 は NAT-PT をサポートしていますか。](#)

[プラットフォーム依存の Cisco 7300/7600/6k](#)

[Q. Catalyst 6500 の SX トレインでステートフル NAT \(SNAT\) を使用できますか。](#)

[Q. VRF 対応 NAT は 6000 系のハードウェアでサポートされていますか。](#)

[Q. 7600 シリーズおよび Cat6000 シリーズは VRF 対応 NAT をサポートしていますか。](#)

[プラットフォーム依存の Cisco 850](#)

[Q. Cisco 850 のリリース 12.4T では Skinny NAT ALG がサポートされますか。](#)

[NAT の導入](#)

[Q. NAT を実装するにはどうすればよいですか。](#)

[Q. 音声機能に NAT を実装するにはどうすればよいですか。](#)

[Q. NAT を MPLS VPN と統合するにはどうすればよいですか。](#)

[Q. NAT スタティックマッピングは、HSRP による高可用性をサポートしていますか。](#)

[Q. NAT NVI を実装するにはどうすればよいのですか。](#)

[Q. NAT を使用した負荷分散を実装するにはどうすればよいですか。](#)

[Q. IPSec と組み合わせて NAT を実装するにはどうすればよいのですか。](#)

[Q. NAT-PT を実装するにはどうすればよいですか。](#)

[Q. マルチキャスト NAT を実装するにはどうすればよいですか。](#)

[Q. ステートフル NAT \(SNAT\) を実装するにはどうすればよいですか。](#)

[NAT のベストプラクティス](#)

[Q. NAT のベストプラクティスはありますか。](#)

[関連情報](#)

はじめに

このドキュメントでは、ネットワークアドレス変換 (NAT) に関してよく寄せられる質問について説明します。

NAT 全般

Q. NAT とは何ですか。

A. 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。登録されていない IP アドレスを使用したプライベート IP ネットワークがインターネットに接続できるようになります。NAT はルータ (通常、2 つのネットワークどうしを接続するもの) 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 アドレスを正規のアドレスに変換します。

この機能の一部として、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 NAT を設定できます。これにより、内部ネットワーク全体がそのアドレスに効果的に隠されるため、セキュリティが高まります。NAT には、セキュリティとアドレス保全の 2 つの機能があり、一般にリモート アクセス環境に実装されます。

Q.NAT の仕組み

A. ルータなどの単一のデバイスを、インターネット（またはパブリックネットワーク）とローカルネットワーク（またはプライベートネットワーク）を仲介するエージェントとして機能させるのが、NAT の基本的な仕組みです。これにより、そのデバイスが属するネットワークの外部に対しては、一意の IP アドレス 1 つでコンピュータのグループ全体を表せます。

Q.NAT はどのように設定しますか。

A. 従来の NAT を構成するには、ルータ上に最低でも 1 つのインターフェイス（NAT 外部）を作成し、さらにそれとは別のインターフェイス（NAT 内部）を作成した上で、パケットヘッダー（および必要に応じてペイロード）の IP アドレスを変換するためのルールセットを設定する必要があります。NAT 仮想インターフェイス（NVI）を設定するには、NAT が有効に設定された少なくとも 1 つのインターフェイスと、前述と同じルールのセットが必要です。

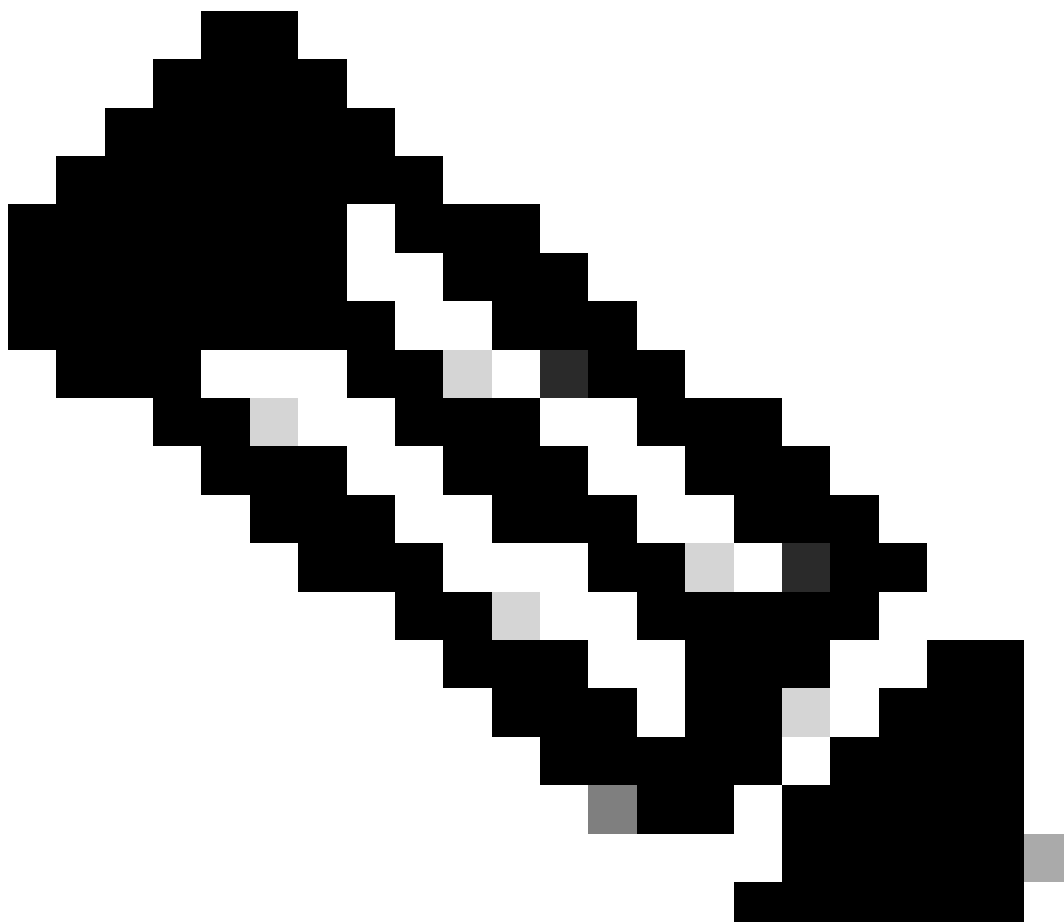
詳細については、『[Cisco IOS® IP アドレッシングサービス設定ガイド](#)』または『[NAT 仮想インターフェイスの設定](#)』を参照してください。

Q.Cisco IOS ソフトウェアと Cisco PIX セキュリティアプライアンスでの NAT の実装の主な違いは何ですか。

A. Cisco IOS ソフトウェアベースの NAT と、Cisco PIX セキュリティアプライアンスの NAT 機能には、基本的に違いはありません。主な違いは、実装でサポートされているトラフィックの種類などです。Cisco PIX デバイスでの NAT 設定の詳細については、NAT の設定例（サポートされているトラフィックのタイプを含む）を参照してください。

Q.どの Cisco ルーティング ハードウェアで Cisco IOS NAT を使用できますか。ハードウェアを注文するにはどうすればよいですか。

A. Cisco Feature Navigator ツールを使用すると、機能(NAT)を識別して、このCisco IOSソフトウェア機能が使用可能なリリースとハードウェアバージョンを調べることができます。このツールを使用するには、『Cisco Feature Navigator』を参照してください。



注：シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

Q.NAT はルーティングの前または後のどちらで行われますか。

A. NAT を利用してトランザクションが処理される順序は、パケットがネットワークの内部から外部に向かうか、逆に外部から内部に向かうかで異なります。内部から外部への変換はルーティングの後に行われ、外部から内部への変換はルーティングの前に行われます。詳細については、「NAT の処理順序」を参照してください。

Q.パブリック ワイヤレス LAN 環境に NAT を展開できますか。

A. あります。NAT スタティック IP サポート機能は、スタティック IP アドレスを持つユーザがパブリック ワイヤレス LAN 環境で IP セッションを確立できるようにサポートします。

Q.NAT は、内部ネットワークのサーバに対して TCP ロードバランシングを行いますか。

A. あります。NAT を使用して、複数の実ホストの間でのロード シェアリングを調整する仮想ホストを内部ネットワークに設定することができます。

Q.NAT 変換の数をレート制限できますか。

A. あります。レート制限 NAT 変換機能によって、ルータ上で同時に処理される NAT の数を制限できます。これにより、ユーザが NAT アドレスの使用方法をより詳細に管理できるようになるだけでなく、NAT 変換のレート制限機能を使用して、ウイルスやワーム、サービス拒絶攻撃の影響を制限できるようになります。

Q.NAT によって使用される IP サブネットまたはアドレスについてのルーティングは、どのように学習または伝達されますか。

A. NAT によって作成された IP アドレスのルーティングは、次の場合に学習が行われます。

- 内部グローバルアドレスプールが、ネクストホップ ルータのサブネットから取得される場合。
- スタティック ルート エントリがネクストホップ ルータで設定されて、ルーティング ネットワーク内に再配布される場合。

内部グローバルアドレスがローカルインターフェイスと一致すると、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、ルータはこれらのアドレスに対するプロキシARPを実行できます。この動作が望ましくない場合は、no-alias キーワードを使用します。

NAT プールを設定するとき、add-route オプションを使用して自動ルート注入を行うことができます。

Q.Cisco IOS NAT では何個の同時 NAT セッションがサポートされますか。

A. NAT セッションの上限数は、ルータに搭載されている DRAM の使用可能量によって制限されます。各 NAT 変換は、約 312 バイトの DRAM を消費します。その結果、10,000 変換 (一般に 1 つのルータで処理されるより多い数) では約 3 MB が消費されます。そのため、標準的なルーティング ハードウェアは、数千の NAT 変換をサポートするのに十分なメモリを備えています。

Q.Cisco IOS NAT ではどのようなルーティング パフォーマンスを期待できますか。

A. Cisco IOS の NAT 機能では、Cisco Express Forwarding スイッチング、ファストスイッチング、プロセススイッチングがサポートされます。12.4T リリース以降では、ファスト スイッチング パスはサポートされなくなります。Cat6k プラットフォームでは、スイッチングの順序は Netflow (HW スイッチング パス)、CEF、プロセス パスです。

パフォーマンスは、いくつかの要因によって異なります。

- アプリケーションの種類とそのトラフィックの種類
- IP アドレスが組み込みかどうか

- 複数のメッセージの交換と検査
- 必要な送信元ポート
- 変換の数
- 同時に動作している他のアプリケーション
- ハードウェアおよびプロセッサの種類

Q.Cisco IOS NAT をサブインターフェイスに適用できますか。

A. あります。送信元および送信先 NAT 変換は、IP アドレスを持つ任意のインターフェイスまたはサブインターフェイスに適用できます (ダイヤラ インターフェイスなど)。NAT をワイヤレス仮想インターフェイスに設定することはできません。ワイヤレス仮想インターフェイスは、NVRAM への書き込みの時点では存在しません。したがって、再起動すると、ルータはワイヤレス仮想インターフェイスでの NAT の設定を失います。

Q.Cisco IOS NAT でホットスタンバイ ルータ プロトコル (HSRP) を使用して ISP に冗長リンクを提供できますか。

A. あります。NAT は HSRP の冗長性を提供します。ただし、SNAT (ステートフル NAT) とは異なります。NAT での HSRP はステートレス システムです。障害が発生した場合、現在のセッションは維持されません。スタティック NAT の設定時に (パケットがどの STATIC ルール設定とも一致しない場合)、パケットは変換されずに送信されます。

Q.Cisco IOS NAT は、フレーム リレー インターフェイスでのインバウンド変換をサポートしますか。また、イーサネット側でのアウトバウンド変換をサポートしますか。

A. あります。NAT の場合、カプセル化は問題ではありません。インターフェイスに IP アドレスがあり、インターフェイスが NAT 内部または NAT 外部であれば、NAT を行うことができます。NAT が機能するには、内部と外部が必要です。NVI を使用する場合は、NAT 対応のインターフェイスが少なくとも 1 つ必要です。詳細は、「NAT を設定するにはどうすればよいのですか」の項を参照してください。

Q.単一の NAT 対応ルータで、一部のユーザは NAT を使用し、同じイーサネット インターフェイス上の他のユーザは、引き続き固有の IP アドレスを使用することができますか。

A. あります。これは、NAT を必要とするホストまたはネットワークの設定が記述されているアクセス リストを使用して実現できます。

アクセス リスト、拡張アクセス リスト、およびルート マップを使用して、IP デバイスが変換されるルールを定義することができます。ネットワークアドレスと適切なサブネットマスクを常に指定する必要があります。ネットワークアドレスまたはサブネットマスクの代わりにキーワード any を使用しないでください。スタティック NAT では、パケットがどの STATIC ルール設定とも一

致しない場合、パケットは変換されずに送信されます。

Q.PAT 用に設定するとき (オーバーロード)、内部グローバル IP アドレスごとに作成できる変換の最大数はいくつですか。

A.PAT (オーバーロード) は、グローバルIPアドレスごとに、使用可能なポートを0 ~ 511、512 ~ 1023、1024 ~ 65535の3つの範囲に分割します。PAT は、各 UDP または TCP セッションに一意の送信元ポートを割り当てます。PAT は、元の要求と同じ値のポートを割り当てようとしませんが、元の送信元ポートがすでに使用されている場合は、特定のポート範囲を先頭からスキャンして、最初に使用できるポートをカンバセーションに割り当てます。12.2S コード ベースは例外です。12.2S コード ベースは異なるポート ロジックを使用しており、ポートの予約はありません。

Q.PAT はどのように動作しますか。

A. PAT は 1 つのグローバル IP アドレスで機能する場合と、複数のアドレスで機能する場合があります。

1 つの IP アドレスを使用する PAT

条件	説明
1	NAT/PAT は、トラフィックを調べて、変換ルールと照合します。
2	ルールが PAT の設定と一致します。
3	PATは、トラフィックタイプに関する情報を持っていて、そのトラフィックタイプで使われる「特定のポートまたはネゴシエートするポートのセット」が存在する場合、それらのポートを除外し、一意のIDを割り当てません。
4	特別なポート要件のないセッションが発信接続を試みた場合、PAT は IP の送信元アドレスを変換し、発信した送信元ポート (たとえば 433) の使用可能性を調べます。 注 : Transmission Control Protocol (TCP ; 伝送制御プロトコル) および User Datagram Protocol (UDP ; ユーザデータグラムプロトコル) の場合、範囲は 1 ~ 511、512 ~ 1023、1024 ~ 65535 です。Internet Control Message Protocol (ICMP) の場合、最初のグループは 0 から始まります。
5	要求された送信元ポートが使用可能な場合、PAT は送信元ポートを割り当て、セッションが継続されます。
6	要求された送信元ポートが使用可能ではない場合、PAT は関連するグループの最初から検索を始めます (TCP または UDP アプリケーションの場合は 1 から開始し、ICMP の場合は 0 から開始します)。
7	ポートが使用可能な場合はそれが割り当てられて、セッションが継続されます。
8	使用可能なポートがない場合、パケットは破棄されます。

複数の IP アドレスを使用する PAT

条件	説明
----	----

1-7	最初の 7 つの条件は、単一 IP アドレスと同じです。
8	最初の IP アドレスの関連グループに使用可能なポートがない場合、NAT はプールの次の IP アドレスに進み、要求された元の送信元ポートの割り当てを試みます。
9	要求された送信元ポートが使用可能な場合、NAT は送信元ポートを割り当て、セッションが継続されます。
10	要求された送信元ポートが使用可能ではない場合、NAT は関連するグループの最初から検索を始めます (TCP または UDP アプリケーションの場合は 1 から開始し、ICMP の場合は 0 から開始します) 。
11	ポートが使用可能な場合はそれが割り当てられて、セッションが継続されます。
12	使用可能なポートがなく、プールで別の IP アドレスを使用できない場合、パケットは破棄されます。

Q.NAT IP プールとは何ですか。

A. NAT IP プールとは、必要に応じて割り当てられる NAT 変換用の IP アドレス範囲のことです。プールを定義するには、次のコンフィギュレーション コマンドを使用します。

<#root>

```
ip nat pool <name> <start-ip> <end-ip>
    {netmask <netmask> | prefix-length <prefix-length>}
    [type {rotary}]
```

例 1

次の例では、内部ホストのアドレスが192.168.1.0または192.168.2.0ネットワークからグローバルに一意な10.69.233.208/28ネットワークに変換されています。

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
ip address 10.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

例 2

この例の目標は、一連の実ホスト間に接続を分散する仮想アドレスを定義することです。このプールは実ホストのアドレスを定義します。アクセス リストは仮想アドレスを定義します。変換が

まだ存在しない場合、シリアル インターフェイス 0 (外部インターフェイス) からの TCP パケットのうち、アクセス リストと一致する宛先を持つものは、このプールに含まれるアドレスに変換されます。

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1
```

Q.設定可能なNAT IPプールの最大数は何ですか(ip nat pool <name>)。

A. 実際に使用するときには、設定可能な IP プールの最大数は個々のルータで使用できる DRAM の量によって上限が変わります。(Cisco はプール サイズを 255 に設定することを推奨します)。各プールは16ビット以下にする必要があります。12.4(11)T以降では、Cisco IOSにCCE(Common Classification Engine)が導入されています。そこでは、NAT のプール数が 255 以下に制限されています。12.2S コード ベースでは、最大プール数の制限はありません。

Q.NAT プールでのルート マップと ACL の利点は何ですか。

A. ルートマップは望ましくない外部ユーザーが内部のユーザーやサーバーにアクセスするのを防ぎます。また、ルールに基づいて単一の内部 IP アドレスを別の内部グローバル アドレスにマップする機能もあります。詳細については、『ルート マップを使用する複数プールの NAT サポート』を参照してください。

Q.NATのコンテキストでIPアドレスの重複とは何ですか。

A. IPアドレスの重複とは、相互接続を行おうとする2つの場所が、同じIPアドレス方式を使用している状況を指します。これは珍しいことではなく、企業の合併や買収の際によく発生します。特別なサポートがなければ、2つの場所は接続できず、セッションを確立できません。重複するIPアドレスは、別の会社に割り当てられたパブリックアドレスや、別の会社に割り当てられたプライベートアドレス、あるいは[RFC 1918](#)で定義されているプライベートアドレスという場合もあります

プライベート IP アドレスはルーティング不可能であり、外界に接続するには NAT 変換が必要です。これを解決するには、外部から内部へのドメイン ネーム システム (DNS) 名前クエリ応答をインターセプトし、外部アドレスの変換を設定して、DNS 応答を再構成してから内部のホストに転送する必要があります。両方のネットワーク間を接続するには、NAT デバイスの両側に DNS サーバが必要です。

「オーバーラップしているネットワークでの NAT の使用」で示されているように、NAT は DNS の A レコードと PTR レコードの内容を調べてアドレス変換を行うことができます。

Q.スタティック NAT 変換とはどのようなことですか。

A. 静的 NAT 変換は、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。ユーザは、ポート レベルでスタティック アドレス変換を設定し、残りの IP アドレスを他の変換に使用することもできます。これは通常、ポート アドレス変換 (PAT) を実行している場所で行われます。

次の例は、スタティック NAT で外部から内部への変換を許可するようにルートマップを設定する方法を示しています。

<#root>

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 10.1.10.128 0.0.0.127

route-map R1 permit 10
match ip address ACL-A
```

Q.NATオーバーロードとは何ですか。これはPATですか。

A. あります。NAT オーバーロードは、1 つ以上の一連のアドレスが含まれているプールを使用するか、またはポートとインターフェイス IP アドレスの組み合わせを使用する PAT です。オーバーロードでは完全に拡張された変換が作成されます。これは IP アドレスおよび送信元ポートと送信先ポートの情報を含む変換テーブル エントリであり、一般に PAT またはオーバーロードと呼ばれます。

PAT (またはオーバーロード) は Cisco IOS NAT の機能であり、内部 (内部ローカル) のプライベートアドレスを 1 つ以上の外部 (内部グローバル、通常は登録済み) の IP アドレスに変換するために使用されます。各変換の一意的送信元ポート番号が、カンバセーションの区別に使用されます。

Q.ダイナミック NAT 変換とはどのようなことですか。

A. 動的 NAT 変換では、ユーザはローカルアドレスとグローバルアドレスの間でダイナミック マッピングを確立できます。ダイナミック マッピングを実現するには、変換されるローカル アドレスと、グローバル アドレスの割り当て元となるアドレスまたはインターフェイス IP アドレスのプールを定義して、この 2 つを関連付けます。

Q.ALG とは何ですか。

A. ALG とはアプリケーション層ゲートウェイ (ALG) のことです。NAT は、アプリケーション データ ストリームで送信元 IP アドレスおよび送信先 IP アドレスの両方またはいずれかが送信さ

れない Transmission Control Protocol/User Datagram Protocol (TCP/UDP) トラフィックで、変換サービスを実行します。

このようなプロトコルとしては、FTP、HTTP、SKINNY、H232、DNS、RAS、SIP、TFTP、telnet、archie、finger、NTP、NFS、rlogin、rsh、rcp などがあります。IP アドレス情報をペイロードに埋め込む特定のプロトコルには、アプリケーション レベル ゲートウェイ (ALG) のサポートが必要です。

詳細については、『NAT でのアプリケーション レベル ゲートウェイの使用』を参照してください。

Q.スタティックとダイナミック両方の NAT 変換を使用する設定を作成できますか。

A. あります。ただし、同じ IP アドレスを、NAT スタティック設定と NAT ダイナミック設定プールの両方に使用することはできません。すべてのパブリック IP アドレスは一意である必要があります。スタティック変換で使われるグローバル アドレスは、同じグローバル アドレスを含むダイナミックプールで自動的に除外されないことに注意してください。ダイナミックプールは、スタティック エントリによって割り当てられるアドレスを除外して作成する必要があります。詳細については、『スタティック NAT とダイナミック NAT の同時設定』を参照してください。

Q.NAT ルータを経由して traceroute を実行すると、traceroute によって NAT グローバル アドレスが表示されますか。それとも、NAT ローカル アドレスがリークしますか。

A. 外部からの traceroute は、常にグローバル アドレスを返す必要があります。

Q.PAT によるポートの割り当てはどのように行われますか。

A. NAT では、フルレンジとポートマップというポート機能が追加されています。

- 全範囲では、NAT はデフォルトのポート範囲に関係なくすべてのポートを使用できます。
- ポートマップでは、NAT はユーザ定義のポート範囲を特定のアプリケーションに予約できます。

詳細については、『[PAT に対するユーザ定義の送信元ポート範囲](#)』を参照してください。

12.4(20)T2 以降の NAT には、L3/L4 のポート ランダム化および対称ポートが導入されています。

- ポートのランダム化により、NAT は送信元ポート要求に対して任意のグローバル ポートをランダムに選択できます。
- 対称ポートにより、NAT は独立したポイントをサポートできます。

Q.IP フラグメンテーションと TCP セグメンテーションは何が違いますか。

A. IPフラグメンテーションはレイヤ3(IP)で発生し、TCPセグメンテーションはレイヤ4(TCP)で発生します。IPフラグメンテーションは、インターフェイスの最大伝送ユニット(MTU)より大きいパケットがそのインターフェイスから送信されるときに発生します。これらのパケットは、インターフェイスから送信されるときに、フラグメント化されるか、廃棄される必要があります。パケットのIPヘッダーにフラグメントなし(DF)ビットが設定されていない場合、パケットはフラグメント化されます。パケットのIPヘッダーにDFビットが設定されている場合、パケットは廃棄され、ネクストホップのMTU値を示すICMPエラーメッセージが送信元に返されます。IPパケットのすべてのフラグメントは、IPヘッダーに同じIDが定義されています。そのため、最終的な受信者は、フラグメントを再構成することによって、元のIPパケットを再現できます。詳細については、『[GREおよびIPSecによるIPフラグメンテーション、MTU、MSS、およびPMTUDの問題の解決](#)』を参照してください。

TCPのセグメンテーションは、エンドステーションのアプリケーションがデータを送信するときに発生します。アプリケーションデータは、TCPが送信に最適であると考えられるサイズのチャンクに分割されます。TCPからIPに渡されるこのデータの単位が、セグメントと呼ばれます。TCPセグメントは、IPデータグラムで送信されます。これらのIPデータグラムは、ネットワークを通過する際に通り抜けられない低いMTUのリンクがあると、IPフラグメント化されます。

TCPは、最初にこのデータを(TCP MSS値に基づいて)TCPセグメントにセグメント化し、TCPヘッダーを追加して、このTCPセグメントをIPに渡します。次に、IPプロトコルはIPヘッダーを追加して、パケットをリモートエンドホストに送信します。TCPセグメントを含むIPパケットが、TCPホスト間のパス上にある発信インターフェイスのIP MTUよりも大きい場合、IPはIP/TCPパケットをフラグメント化して収まるようにします。これらのIPパケットフラグメントは、IPレイヤによってリモートホスト上で再構成され、(最初に送信された)完全なTCPセグメントがTCPレイヤに渡されます。TCP層は、転送中にIPによってパケットがフラグメント化されたことを認識しません。NATはIPフラグメントをサポートしますが、TCPセグメントはサポートしません。

Q.NATは、IPフラグメンテーションとTCPセグメンテーションの順序の間違いをサポートしますか。

A. NATを有効にするとip virtual-reassemblyが設定されるため、IPフラグメントのアウトオブオーダーにのみ対応できます。

Q.IPフラグメンテーションとTCPセグメンテーションをデバッグするにはどうすればよいですか。

A. NATでは、IPフラグメンテーションとTCPセグメンテーションのデバッグに、同じデバッグCLIコマンドdebug ip nat fragを使用します。

Q.サポートされるNAT MIBはありますか。

A. いいえ。CISCO-IETF-NAT-MIBも含め、サポートされているNAT MIBはありません。

Q.TCPタイムアウトとは何ですか。また、NAT TCPタイマーとはどのように関係しますか。

A. 3ウェイハンドシェイクが完了していないのに、NATでTCPパケットが検出された場合は、60秒のタイマーが開始されます。3ウェイハンドシェイクが完了すると、NATはNATエントリに対してデフォルトで24時間のタイマーを使用します。エンドホストがRESETを送信した場合、NATはデフォルトのタイマーを24時間から60秒に変更します。FINの場合は、NATはFINとFIN-ACKを受信した時点でデフォルトのタイマーを24時間から60秒に変更します。

Q.NAT変換がタイムアウトするまでの時間をNAT変換テーブルから変更できますか。

A. あります。すべてのエントリ、または異なるタイプのNAT変換 (udp-timeout、 dns-timeout、 tcp-timeout、 finrst-timeout、 icmp-timeout、 pptp-timeout、 syn-timeout、 port-timeout、 arp-ping-timeoutなど) のNATタイムアウト値を変更できます。

Q.Lightweight Directory Access Protocol (LDAP) が各 LDAP 応答パケットに余分なバイトを追加するのを止めるにはどうすればよいですか。

A. LDAP 設定では、Search-Res-Entry タイプのメッセージを処理する際に、追加のバイト (LDAP の検索結果) が付加されます。LDAP は、10バイトの検索結果を各 LDAP 応答パケットに追加します。この余分な10バイトのデータが原因で、パケットがネットワークの最大伝送ユニット (MTU) を超えると、パケットは破棄されます。このような場合は、パケットが送受信されるように、CLI の `no ip nat service append-ldap-search-res` コマンドを使用してLDAPのこの動作をオフにすることをお勧めします。

Q.NAT ボックスでの内部グローバル/外部ローカルの IP アドレスにはどのようなルートが推奨されますか。

A. NAT 機能が設定されているボックスでは、NAT-NVI などの機能に対応した内部グローバル IP アドレスのルートを指定する必要があります。同様に、外部ローカルIPアドレスのルートも NATボックスで指定する必要があります。この場合、外部スタティックルールを使用したinからout方向のパケットには、この種のルートが必要です。このようなシナリオでは、IG/OLのルートを指定する際に、ネクストホップIPアドレスも設定する必要があります。ネクストホップ設定がない場合は、設定エラーと見なされ、未定義の動作が発生します。

NVI-NAT は出力機能パスにだけ存在します。NAT-NVI で直接接続されたサブネットがある場合、またはボックスで外部 NAT 変換ルールが設定されている場合、これらのシナリオでは、ダミーのネクストホップ IP アドレスおよびネクストホップに関連付けられた ARP を提供する必要があります。これは、基盤となるインフラストラクチャが変換のためパケットを NAT に渡すために必要です。

Q.Cisco IOSのNATでは、logキーワードを使用するACLはサポートされていますか。

A. Cisco IOS の NAT 機能でダイナミック NAT 変換を設定すると、変換可能なパケットを識別するために ACL が使用されます。現在のNATアーキテクチャでは、log キーワードを使用するACLはサポートされていません。

Voice-NAT

Q. NAT は、Cisco Unified Communications Manager (CUCM) V7 に付属している Skinny Client Control Protocol (SCCP) v17 をサポートしていますか。

A. CUCM 7およびCUCM 7のすべてのデフォルトの電話ロードでは、SCCPv17がサポートされています。使用される SCCP のバージョンは、電話登録の時点で CUCM と電話に共通する最も高いバージョン番号によって決まります。

このドキュメントが作成された時点では、NATはまだSCCP v17をサポートしていません。SCCP v17のNATサポートが実装されるまでは、SCCP v16がネゴシエートされるように、ファームウェアをバージョン8-3-5以前にダウングレードする必要があります。CUCM6では、SCCP v16を使用している限り、どの電話ロードでもNAT問題は発生しません。現在、Cisco IOS は SCCP バージョン 17 をサポートしていません。

Q.NAT ではどの CUCM/SCCP/ファームウェア ロード バージョンがサポートされていますか。

A. NAT は CUCM バージョン 6.x 以前のリリースをサポートしています。これらの CUCM バージョンは、SCCP v15 (またはそれ以前) をサポートするデフォルトの 8.3.x (またはそれ以前の) 電話ファームウェア ロードでリリースされます。

NAT は、CUCM バージョン 7.x 以降のリリースをサポートしていません。これらの CUCM バージョンは、SCCP v17 (またはそれ以降) をサポートするデフォルトの 8.4.x 電話ファームウェア ロードでリリースされます。

CUCM 7.x 以降を使用する場合は、NAT によるサポートが得られるように、電話機では SCCP v15 以前のバージョンのファームウェア ロードが使用される必要があります。そのため、CUCM TFTP サーバには、古いバージョンのファームウェア ロードをインストールする必要があります。

Q.RTP と RTCP のサービス プロバイダー PAT ポート割り当て機能拡張とは何ですか。

A. サービスプロバイダーが提供する RTP および RTCP 機能への PAT ポート割り当て拡張は、SIP、H.323、Skinny の各プロトコルによる音声コールを保証する機能です。RTP ストリームに使用されるポート番号は偶数のポート番号で、RTCP ストリームはその次の奇数のポート番号です。ポート番号は、RFC-1889 で指定された範囲内の番号に準拠するように変換されます。範囲内のポート番号を持つコールは、この範囲内の別のポート番号へのPAT変換を行います。同様に、この範囲外のポート番号に対するPAT変換では、特定の範囲内の番号への変換は行われません。

Q.Session Initiation Protocol (SIP) とは何ですか。SIP パケットは NAT に対応していますか。

A. Session Initiation Protocol (SIP) は、アプリケーション層の ASCII ベースの制御プロトコルで

あり、2つ以上のエンドポイント間でコールを確立、維持、および終了するために使用できます。SIPは、インターネット技術特別調査委員会 (IETF) が開発した、IPを介したマルチメディア会議用の代替プロトコルです。Cisco SIPの実装では、サポートされるシスコプラットフォームがIPネットワークを介した音声コールおよびマルチメディアコールの確立を通知します。

SIPパケットはNATに対応しています。

Q.セッションボーダーコントローラ (SBC) のホスト NAT トラバーサルのサポートとは何ですか。

A. Cisco IOS の SBC 用ホスト型 NAT トラバーサル機能を使用することで、Cisco IOS NAT SIP アプリケーションレベルゲートウェイ (ALG) ルータを Cisco マルチサービス IP-to-IP ゲートウェイ上で SBC として機能させることができ、Voice over IP (VoIP) サービスを円滑に配信できます。

詳細は、『[Session Border Controller の Cisco IOS ホスト NAT トラバーサル](#)』を参照してください。

Q.ルータのメモリと CPU ではいくつの SIP、Skinny、H323 コールを NAT で処理できますか。

A. NAT ルータで処理されるコールの数は、NAT ボックスのメモリの空き容量と CPU の処理能力によって異なります。

Q.NATルータは、SkinnyおよびH323パケットのTCPセグメンテーションをサポートしますか。

A. Cisco IOS-NATでは、12.4メインラインでH323のTCPセグメンテーションがサポートされており、12.4(6)T以降のSKINNYではTCPセグメンテーションがサポートされています。

Q. 音声環境で NAT のオーバーロード設定を使用する際に注意することはありますか。

A. あります。NAT オーバーロードの設定と音声の導入がある場合、登録メッセージが NAT を通過するようにして、この内部デバイスに到達するように外側から内側への関連付けを作成する必要があります。内部デバイスは定期的にこの登録を送信し、NAT は通知メッセージ内の情報からこのピンホール/関連付けを更新します。

Q. 音声環境で clear ip nat trans * コマンドまたは clear ip nat trans force コマンドを発行することで起きる、既知の問題はありますか。

A. 音声環境では、clear ip nat trans * コマンドまたはclear ip nat trans forced コマンドを実行するときに、ダイナミックNATが設定されている場合には、ピンホール/関連付けがクリアされるため、内部デバイスからの次の登録サイクルによってこれが再確立されるのを待つ必要があります。音声の導入ではこれらのコマンドを使用しないことをお勧めします。

Q.NAT では音声と同じ場所に配置されるソリューションをサポートされますか。

A. いいえ。現時点では併存ソリューションはサポートされていません。NATを使用した次の展開（同じボックス）は、CME/DSP-Farm/SCCP/H323という同じ場所に配置されたソリューションと見なされます。

Q.NVI は Skinny ALG、H323 ALG、TCP SIP ALG をサポートしますか。

A. いいえ。ただし、UDP SIP ALG（ほとんどの環境で使用）には影響はありません。

NAT と VRF/MPLS

Q. NATルータでは、グローバルアドレス空間でNATが実行されるのと同時に、VRF内の同じアドレス空間でのNATもサポートされるのですか。現在、これを設定しようとする、「% similar static entry (10.1.1.1 —> 10.210.2.2) already exists」という警告が表示されます。

```
<#root>
```

```
72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2
```

```
72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED
```

A. 従来のNATでは、異なるVRFでのアドレス設定の重複がサポートされています。match-in-vrf オプションを使用してルールでオーバーラップを設定し、その特定のVRFのトラフィックに対して同じVRFでip nat inside/outsideを設定する必要があります。オーバーラップのサポートには、グローバルルーティングテーブルは含まれません。

異なるVRFのオーバーラップしているVRFスタティックNATエントリに対してmatch-in-vrfキーワードを追加する必要があります。ただし、グローバルアドレスとVRF NATアドレスをオーバーラップすることはできません。

```
<#root>
```

```
72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf
```

```
72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf
```

Q.レガシー NAT は VRF-Lite (VRF から異なる VRF への NAT) をサポートしますか。

A. いいえ。異なる VRF 間の NAT 処理には NVI を使用する必要があります。従来の NAT を使用して、VRF からグローバルへの NAT または同じ VRF 内での NAT を実行できます。

NAT NVI

Q. NAT NVI とは何ですか。

A. NVI は NAT 仮想インターフェイスの略称です。2 つの異なる VRF 間で NAT を行うことができます。このソリューションは、Network Address Translation on a Stick の代わりに使用する必要があります。

Q. グローバルのインターフェイスと VRF のインターフェイスの間で NAT を行う場合、NAT NVI を使用する必要がありますか。

A. シスコではグローバル NAT に対する VRF (ip nat inside/out) と、同じ VRF 内のインターフェイス間でレガシー NAT を使用することを推奨しています。NVI は、異なる VRF 間の NAT に使用されます。

Q. NAT-NVI の TCP セグメンテーションはサポートされますか。

A. NAT-NVI での TCP セグメンテーションはサポートされていません。

Q. NVI は Skinny ALG、H323 ALG、TCP SIP ALG をサポートしますか。

A. いいえ。ただし、UDP SIP ALG (ほとんどの環境で使用) には影響はありません。

Q. SNAT では TCP セグメンテーションはサポートされますか。

A. SNAT は TCP ALG (SIP、SKINNY、H323、DNS など) をサポートしていません。したがって、TCP セグメンテーションはサポートされません。ただし、UDP SIP と DNS はサポートされます。

SNAT

Q. ステートフル NAT (SNAT) とは何ですか。

A. SNAT では、2 つ以上のネットワーク アドレス トランスレータを 1 つの変換グループとして機能させることができます。変換グループの 1 つのメンバーが、IP アドレス情報の変換を必要とするトラフィックを処理します。さらに、アクティブなフローが発生するとバックアップ用トランスレータに通知します。バックアップ用トランスレータは、アクティブなトランスレータからの情報を使用して、重複する変換テーブル エントリを準備できます。これにより、アクティブなトランスレータで重大な障害が発生した場合は、バックアップに迅速に切り替えることができます。

す。変換のステートが先に定義されていたのと同じネットワーク アドレス変換が使用されるため、トラフィックのフローは継続します。

Q.SNAT では TCP セグメンテーションはサポートされますか。

A. SNAT は TCP ALG (SIP、SKINNY、H323、DNS など) をサポートしていません。したがって、TCP セグメンテーションはサポートされません。ただし、UDP SIP と DNS はサポートされます。

Q.SNATは非対称ルーティングをサポートしていますか。

A.非対称ルーティングでは、as-queuingをイネーブルにすることで、NATをサポートしています。デフォルトでは、as-queueing はイネーブルです。ただし、12.4(24)T 以降では as-queuing はサポートされなくなります。ユーザーは、パケットが適切にルーティングされること、および非対称ルーティングが正しく動作するように適切な遅延が追加されることを確認する必要があります。

NAT-PT (v6 から v4)

Q. NAT-PT とは何ですか。

A. NAT-PT は、NAT v4 を NAT v6 に変換する仕組みです。プロトコル変換(NAT-PT)は、[RFC 2765](#) および[RFC 2766](#) で定義されたIPv6-IPv4変換メカニズムです。これにより、IPv6専用デバイスとIPv4専用デバイスが相互に通信できるようになります。

Q.NAT-PT はシスコ エクスプレス フォワーディング (CEF) パスでサポートされますか。

A. NAT-PT は CEF パスではサポートされていません。

Q.NAT-PT ではどの ALG がサポートされますか。

A. NAT-PT は TFTP/FTP と DNS をサポートしています。NAT-PT では音声と SNAT はサポートされません。

Q.ASR 1004 は NAT-PT をサポートしますか。

A. アグリゲーション サービス ルータ (ASR) は NAT64 を使用します。

プラットフォーム依存の Cisco 7300/7600/6k

Q. Catalyst 6500 の SX トレインでステートフル NAT (SNAT) を使用できますか。

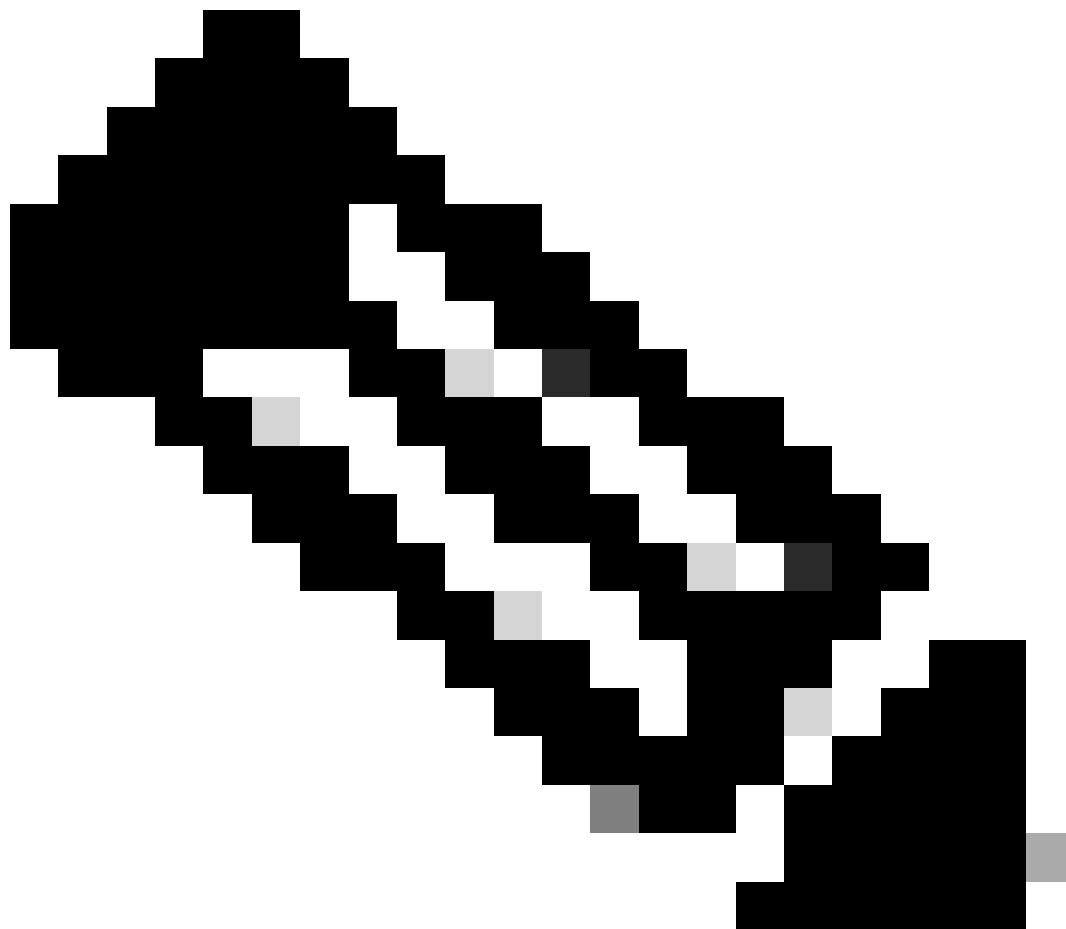
A. SNAT は Catalyst 6500 の SX トレインでは使用できません。

Q.VRF 対応の NAT は、6k 上のハードウェアでサポートされますか。

A. このプラットフォームのハードウェアでは、VRF 対応 NAT はサポートされていません。

Q.7600 および Cat6000 は、VRF 対応の NAT をサポートしますか。

A. 6500 系および 7600 系プラットフォームでは、VRF 対応 NAT はサポート対象外で、CLI はブロックされています。



注：FWSM を利用することで、仮想コンテキスト透過モードで動作する設計を実装できます。

プラットフォーム依存の Cisco 850

Q. Cisco 850 のリリース 12.4T では Skinny NAT ALG がサポートされますか。

A. いいえ。850 シリーズのリリース 12.4T では、Skinny NAT ALG はサポートされていません。

NAT の導入

Q. NAT を実装するにはどうすればよいですか。

A. NATは、未登録のIPアドレスを使用するプライベートIPインターネットワークがインターネットに接続できるようにします。NAT は、パケットが別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 (RFC1918) アドレスを正規にルーティング可能なアドレスに変換します。

Q.音声で NAT を実装するにはどうすればよいですか。

A. NAT の音声機能サポートにより、ネットワークアドレス変換 (NAT) が設定されたルータを通過する SIP 埋め込みメッセージを、変換でパケットに戻すことができます。音声パケットの変換には、アプリケーションレイヤゲートウェイ (ALG) が NAT とともに使用されます。

Q.NAT と MPLS VPN はどのように統合しますか。

A. NAT と MPLS VPN 機能との統合により、複数の MPLS VPN を単一のデバイスに設定して連携させることができます。MPLS VPN がすべて同じ IP アドレッシング スキームを使用している場合、NAT は、IP トラフィックを受信する MPLS VPN を区別できます。この拡張により、複数の MPLS VPN の顧客がサービスを共有しながら、各 MPLS VPN が互いに完全に分離していることが保証されます。

Q.NAT のスタティック マッピングはハイ アベイラビリティのための HSRP をサポートしますか。

A. ネットワークアドレス変換 (NAT) のスタティックマッピングが構成された、ルータが保持するアドレスに対して Address Resolution Protocol (ARP) クエリがトリガーされると、NAT は ARP が指すインターフェイスの BIA MAC アドレスで応答します。2 つのルータはそれぞれ、HSRP アクティブとスタンバイの役割を果たします。ルータの NAT 内部インターフェイスがイネーブルになり、グループに属するように設定される必要があります。

Q.NAT NVIはどのように実装しますか。

A. NAT 仮想インターフェイス (NVI) 機能により、インターフェイスを NAT の内部または外部のいずれかとして設定する必要がなくなりました。

Q.NAT でのロード バランシングはどのように実装しますか。

A. NATでは、2種類のロードバランシングを実行できます。1組のサーバへの着信のロードバランシングを行ってサーバへの負荷を分散できます。また、2つ以上のISPを経由するインターネットへのユーザトラフィックのロードバランシングを行うことができます。

アウトバウンドロードバランシングの詳細については、[『2つのISPの接続のためのCisco IOS』](#)

[NATのロードバランシング』](#)を参照してください。

Q.IPSecと組み合わせてNATを実装するにはどうすればよいのですか。

A. NAT および IPSec の NAT 透過性を利用した IP Security (IPSec) のカプセル化セキュリティペイロード (ESP) がサポートされています。

NAT を通じた IPsec ESP の機能により、オーバーロード モード、またはポート アドレス変換 (PAT) モードで設定された Cisco IOS NAT デバイス経由で、複数の同時 IPsec ESP トンネルまたは接続をサポートできるようになります。

IPSec NAT 透過機能は、NAT と IPSec の間にある多くの既知の非互換性を解決することにより、IPSec トラフィックがネットワーク上の NAT または PAT ポイントを通過し、送受信できるようにします。

Q.NAT-PT はどのように実装しますか。

A. NAT-PT(Network Address Translation—Protocol Translation)は、[RFC 2765](#)および[RFC 2766](#)で定義されたIPv6-IPv4変換メカニズムです。このメカニズムにより、IPv6専用デバイスとIPv4専用デバイスが相互に通信できるようになります。

Q.マルチキャスト NAT を実装するにはどうすればよいですか。

A. マルチキャストストリームの送信元 IP を NAT 処理することができます。マルチキャストのダイナミック NAT を行うときはルートマップは使用できず、アクセス リストだけがサポートされます。

詳細については、『マルチキャスト NAT はどのように Cisco ルータで機能するか』を参照してください。送信先のマルチキャスト グループは、マルチキャスト サービス リフレクション ソリューションを使用して NAT に対応します。

Q.ステートフル NAT (SNAT) はどのようにして実装しますか。

A. SNAT を利用すれば、ダイナミックマッピングによる NAT セッションを継続的に提供できます。スタティックに定義されたセッションが冗長性の恩恵を受けるのに SNAT は必要ありません。SNAT がない場合、ダイナミック NAT マッピングを使用するセッションは、重大な障害が発生した場合に深刻な影響を受け、再確立する必要があります。最小限の SNAT の設定のみがサポートされます。今後の導入は、現在の制限に関連する設計を検証するために、シスコアカウントチームと話し合った後でのみ実施する必要があります。

次のシナリオではSNATを推奨します。

- HSRP と比較して一部の機能がないためにプライマリ/バックアップが推奨されるモードでない場合。
- フェールオーバーのシナリオおよび 2 ルータのセットアップの場合。つまり、1 つのルータがクラッシュした場合、他のルータがシームレスに引き継ぎます (SNAT アーキテクチャは、インターフェイス フラップを処理するようには設計されていません)。

- 非対称ルーティング以外のシナリオがサポートされている場合。非対称ルーティングは、応答パケットでの遅延が、SNAT メッセージの交換に対する 2 つの SNAT ルータ間の遅延より大きい場合にのみ処理できます。

現在、SNATアーキテクチャはロバストネスを処理するようには設計されていないため、次のテストが成功するとは限りません。

- トラフィックがある間の NAT エントリのクリア。
- トラフィックがある間にインターフェイスパラメータを変更する (IPアドレスの変更、shut/no-shutなど)。
- SNAT 固有の clear または show コマンドは正常に実行されるとはかぎらないため、推奨されません。

SNATに関連するclearおよびshowコマンドの一部を次に示します。

```
<#root>

clear ip snat sessions *

clear ip snat sessions <ip address of the peer>

clear ip snat translation distributed *

clear ip snat translation peer < IP address of SNAT peer>

sh ip snat distributed verbose

sh ip snat peer < IP address of peer>
```

- エントリをクリアする場合は、clear ip nat trans forcedまたはclear ip nat trans *コマンドを使用できます。
- エントリを表示するには、< show ip nat translation 、 show ip nat translations verbose 、 およびshow ip nat stats コマンドを使用できます。service internalが設定されている場合は、SNAT固有の情報も表示されます。
- バックアップ ルータでの NAT 変換のクリアは推奨されません。NAT エントリのクリアは常にプライマリ SNAT ルータで行ってください。
- SNATはHAではないため、両方のルータの設定を同じにする必要があります。両方のルータで同じイメージが実行されている必要があります。また、両方の SNAT ルータで使用されている基盤となるプラットフォームが同じであることを確認します。

NAT のベスト プラクティス

Q. NAT のベストプラクティスがありますか。

A. あります。NAT のベストプラクティスは次のとおりです。

1. ダイナミックNATとスタティックNATの両方を使用する場合、ダイナミックNATのルールを設定するACLは、オーバーラップが発生しないようにスタティックローカルホストを除外する必要があります。
2. 予期しない結果になる可能性があるため、permit ip any any で NAT に対して ACL を使用するときは注意する必要があります。12.4(20)T以降では、ローカルに生成されたHSRPと外部インターフェイスに送信される場合のルーティングプロトコルパケット、およびNATルールに一致するローカルに暗号化されたパケットがNATによって変換されます。
3. NAT にオーバーラップしたネットワークがある場合は、match-in-vrf キーワードを使用します。

異なる VRF に対するオーバーラップした VRF スタティック NAT エントリには match-in-vrf キーワードを追加する必要がありますが、グローバル アドレスと VRF NAT アドレスをオーバーラップさせることはできません。

```
<#root>
```

```
Router(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf
```

```
<#root>
```

```
Router(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf
```

4. match-in-vrf キーワードを使用しない場合、同じアドレス範囲の NAT プールを異なる VRF で使用することはできません。

例 :

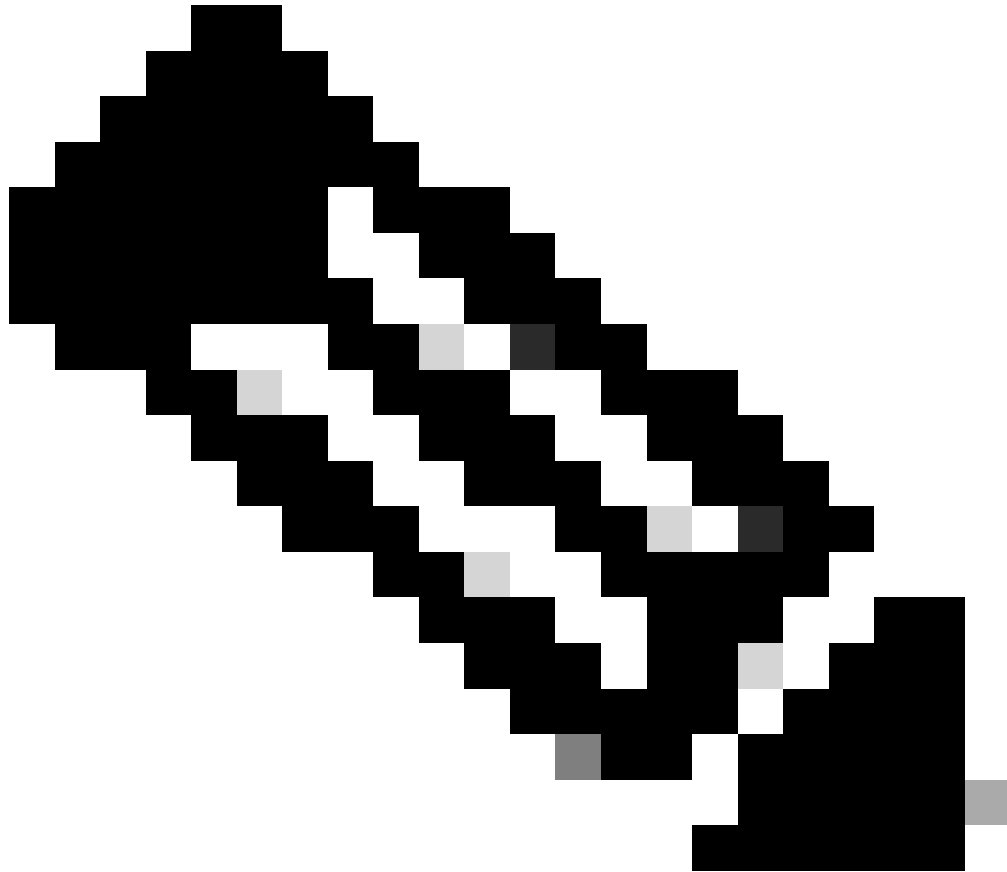
```
<#root>
```

```
ip nat pool poolA 1710.1.1.1 1710.1.1.10 prefix-length 24
```

```
ip nat pool poolB 1710.1.1.1 1710.1.1.10 prefix-length 24
```

```
ip nat inside source list 1 poolA vrf A match-in-vrf
```

```
ip nat inside source list 2 poolB vrf B match-in-vrf
```

注：有効なCLIが設定されていても、match-in-vrfキーワードを使用しなければ、その設定はサポートされません。

5. NAT インターフェイス オーバーロードのある ISP ロード バランシングを展開するときのベスト プラクティスは、ACL の照合よりインターフェイス一致のルートマップを使用することです。
6. プールマッピングを使用する場合は、2つの異なるマッピング (ACLまたはルートマップ) を使用して同じNATプールアドレスを共有しないでください。
7. フェールオーバーシナリオで2台の異なるルータに同じNATルールを展開する場合は、HSRPの冗長性を使用する必要があります。
8. スタティック NAT とダイナミック プールで同じ内部グローバル アドレスを定義しないでください。これを行うと、望ましくない結果を招くことがあります。

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。