Network Address Translation（NAT; ネットワーク アドレス変換）に関する FAQ

目次

概要

このドキュメントでは、Network Address Translation（NAT; ネットワーク アドレス変換）に関する FAQ の一部に回答しています。

NAT 全般

Q. NAT とは何ですか。

A. Network Address Translation（NAT; ネットワーク アドレス変換）は、IP アドレスの節約を目的として設計されています。 未登録の IP アドレスを使用するプライベート IP ネットワークからインターネットに接続できるようになります。 NAT は通常、2 つのネットワークを接続するルータ上で動作し、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（グローバルに一意ではない）アドレスを正規のアドレスに変換します。

NAT はそ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設定できます。 これにより、セキュリティを強化し、そのアドレスの背後にある内部ネットワーク全体を効果的に隠すことができます。 NAT ではセキュリティとアドレス節約という二重の機能が提供され、一般的にリモート アクセス環境で実装されます。

Q. NAT の動作の仕組みはどのようになっているのですか。

A. 基本的には、ネットワーク アドレス変換では、ルータなどの単一デバイスがインターネット（つまり「パブリック ネットワーク」）とローカル（つまり「プライベート」）ネットワークと

の間のエージェントの役割を果たします。つまり、ネットワーク外部に対してコンピュータのグループ全体を表すのに、ただ 1 つの一意な IP アドレスがあればよいということになります。

Q. NAT を設定するにはどうすればよいのですか。

A. 従来からの NAT を設定するには、ルータ上に少なくとも 1 つのインターフェイス (NAT Outside) と、さらにもう 1 つのインターフェイス (NAT Inside) を実装する必要があります。また、パケット ヘッダの IP アドレス (および必要に応じてペイロード) を解釈するために、一連のルールを定義する必要があります。 Nat Virtual Interface (NVI) を設定するには、NAT に対応したインターフェイスが少なくとも 1 つ必要です。また、前の説明と同じように、一連のルールを設定する必要があります。

詳細は、『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. NAT の Cisco IOS ® ソフトウェアと Cisco PIX セキュリティ アプライアンス モデル 実装間の主な違いとは何か。

A. Cisco IOS ソフトウェア ベースの NAT と Cisco PIX セキュリティ アプライアンスでの NAT 機能の間には、基本的な違いはありません。 主な相違点としては、それぞれの実装でサポートされているトラフィック タイプが異なります。 Cisco PIX デバイスでの NAT の設定 (サポートされるトラフィック タイプなど) についての詳細は、『Cisco PIX 500 シリーズ セキュリティ アプライアンス』および『NAT 設定例』を参照してください。

Q. Cisco IOS NAT が利用可能な Cisco のルーティング ハードウェアはどれですか。 また、その注文はどうすればよいですか。

A. シスコの Feature Navigator ツールを使用すると、Cisco IOS ソフトウェアの機能 (NAT) を利用できるかどうか、およびどのリリースおよびハードウェアのバージョンが対応しているかを確認できます。 このツールを利用するには、『Cisco Feature Navigator』を参照してください。

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 を使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 Inside のネットワークから Outside ネットワークへ送信されるのか、それとも Outside のネットワークから Inside のネットワークへ送信されるのかによって異なります。 Inside から Outside への変換はルーティング後に行われ、Outside から Inside への変換はルーティング前に行われます。 詳細は、『NAT の処理順序』を参照してください。

Q. NAT は、パブリックな無線 LAN 環境にも導入できますか。

A. はい。 NAT - 固定 IP サポート機能によって、固定 IP を使用するユーザをサポートできるため、パブリックな無線 LAN 環境でも IP セッションを確立できます。

Q. NAT では、内部ネットワークに関係するサーバの TCP ロードバランシングは行われるのですか。

A. はい。 NAT を使用することで、ネットワーク内部に仮想ホストを確立できるため、実ホスト間の負荷を分散させることができます。 詳細は、『TCP ロードバランシングの使用によるサーバ

過負荷の回避』を参照してください。

Q. NAT による変換数をレート制限できますか。

A. はい。 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。 NAT アドレスの使用に関して、より精度の高い制御が可能になるだけでなく、レート制限 NAT 変換機能を使用することによって、ウィルスやワーム、サービス拒否攻撃による悪影響を抑制できます。

Q. ルーティングはどのように NAT によって使用するアドレスか IP サブネットのために学習されるか、または伝搬されますか。

A. NAT により作成された IP アドレスに関するルーティングが学習されるのは、次の条件が満たされた場合です。

- Inside 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得られる。
- ネクストホップ ルータでスタティック ルート エントリが設定され、ルーティング ネットワーク内で再配布される。

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き、NAT は IP エイリアスと ARP エントリを設定します。この場合、ルータはそれらのアドレスに対して、**プロキシ ARP** として機能します。 この動作が不都合な場合には、**no-alias** キーワードを使用します。

NAT プールが構成されているときは、**add-route** オプションを使用することによって、自動ルート インジェクションを利用できます。

Q. Cisco IOS の NAT では、同時 NAT セッションはいくつサポートされているのですか。

A. NAT セッションの上限は、ルータで使用できるメモリの量により制限されます。 NAT 変換が行われるたびに、DRAM で約 312 バイトが消費されます。 その結果、10,000 回の変換で約 3 MB が消費されます (通常 1 台のルータで処理されるよりも多い)。 したがって、一般的なルーティング ハードウェアは、数千回の NAT 変換をサポートするのに十分なメモリを搭載しています。

Q. Cisco IOS NAT を使用する場合、どのような種類のルーティング パフォーマンスが期待できますか。

A. Cisco IOS の NAT では、Cisco Express Forwarding (CEF; Cisco エクスプレス フォワーディング) スイッチング、ファースト スイッチング、およびプロセス スイッチングがサポートされています。 12.4T リリース以降では、ファースト スイッチング パスは利用できません。 Cat6k プラットフォームでは、スイッチング方式として、Netflow (ハードウェアによるスイッチング パス)、CEF、プロセス パスを利用できます。

パフォーマンスは、次のようないくつかの要因により決まります。

- アプリケーションの種類およびそのトラフィックの種類
- IP アドレスが埋め込まれているかどうか
- 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
- その時点で稼動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 はサブインターフェイスに適用できますか。

A. はい。（ダイヤラ インターフェイスを含む）IP アドレスを持つすべてのインターフェイスまたはサブインターフェイスに、送信元/宛先 NAT 変換を適用できます。 ワイヤレス仮想インターフェイスでは、NAT は設定できません。 NVRAM に書き込みが行われている時点では、ワイヤレス仮想インターフェイスは存在しません。 そのため、ルータのワイヤレス仮想インターフェイスに NAT が設定されていても、再起動されると失われてしまいます。

Q. Cisco IOS NAT を Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）と併用して、ISP に対する冗長リンクを提供できますか。

A. はい。 NAT では、HSRP の冗長化が提供されています。 ただし、Stateful NAT（SNAT; ステートフル NAT）とは異なるものです。 HSRP を使用した NAT は、ステートレス システムです。 障害が発生した場合には、現在のセッションは維持されません。 スタティック NAT が設定されているときは、（パケットがどのスタティック NAT のルール設定とも一致しない場合には）パケットは変換されずに送信されます。

Q. Cisco IOS の NAT では、フレームリレー インターフェイスでの着信側変換がサポートされていますか。 イーサネット側での発信変換はサポートされていますか。

A. はい。 カプセル化は NAT では問題にはなりません。 インターフェイスに IP アドレスが存在しており、そのインターフェイスが NAT Inside または NAT Outside であれば、NAT を設定できます。 NAT が機能するには、Inside と Outside が存在する必要があります。 NVI を使用する場合は、NAT に対応したインターフェイスが少なくとも 1 つは必要です。 NAT をどのように設定するか参照して下さいか。 詳細については。

Q. 1 台の NAT 対応ルータを使用して、一部のユーザには NAT を使用させ、同じイーサネット インターフェイス上のその他のユーザには引き続き独自の IP アドレスを使用させることは可能ですか。

A. はい。 それには、NAT を必要とするホストまたはネットワークのセットを記述するアクセス リストを使用します。 同じホストのすべてのセッションは変換されるか、またはルータを通過し変換されないか、そのどちらかになります。

アクセス リスト、拡張アクセス リスト、およびルート マップを使用すると、IP デバイスが変換される「*ルール*」を定義できます。 必ず、ネットワーク アドレスと適切なサブネット マスクを指定します。 キーワード **any** は、ネットワーク アドレスまたはサブネット マスクの場所では使用しないでください（詳細は、『NAT に関する FAQ、ベスト プラクティス、および導入ガイド』を参照）。 スタティック NAT を設定した場合には、どの STATIC ルール設定とも一致しないパケットについては、変換されずにそのまま送信されます。

Q. PAT（オーバーロード）を設定する場合、各 Inside グローバル IP アドレスごとに作成可能な変換の最大数は何ですか。

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 では、各 UDP または TCP セッションに、一意の送信元ポートが割り当てられます。 PAT は、元の要求と同じポート値の割り当てを試みます。ただし、元の送信元ポートがすでに使用されている場合は、特定のポート範囲の先頭からスキャンを開始して、使用可能な最初のポートを見つけ、それをカンバセーションに割り当てます。 12.2S のコード ベースには、例外が存在します。 12.2S のコード ベースでは異なるポート ロジックが使用されており、ポートは予約されません。

Q. PAT はどのように動作するのですか。

A. PAT は、IP アドレスが 1 つの場合でも、複数の場合でも動作します。

IP アドレスが 1 つの PAT の場合：

条件	説明
1	NAT/PAT はトラフィックを検査して、変換ルールとの照合を行います。
2	ルールが、ある PAT 設定に一致します。
3	PAT はトラフィック タイプに関する情報を持っているか、またそのトラフィック タイプは、使用するポートに関して、「ポートの特定のセット、またはネゴシエートするポート」を持っているかどうかを調べ、それらのポートを除外し、一意の ID を割り当てないようにします。
4	特別なポートの要件のないセッションが接続を試みると、PAT は発信元 IP アドレスを変換し、発信元ポート（たとえば 433）が使用できるかどうかをチェックします。 **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）では、以下の範囲になります。 1-511、512-1023、1024-65535。 Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）では、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である場合、PAT によってその送信元ポートが割り当てられ、セッションが継続します。
6	要求された送信元ポートが使用できない場合、PAT は関連するグループの先頭から検索を開始します（TCP または UDP アプリケーションでは 1 から始まり、ICMP では 0 から始まります）。
7	あるポートが使用できる場合、そのポートが割り当てられ、セッションが継続します。
8	使用できるポートがない場合、パケットは廃棄されます。

IP アドレスが複数である PAT の場合：

条件	説明
1-7	最初の 7 つの状況は IP アドレスが 1 つの場合と同様です。
8	1 つ目の IP アドレスの関連グループで使用できるポートがない場合、NAT はプール内の次の IP アドレスに移行し、要求された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である場合、NAT によってその送信元ポートが割り当てられ、セッションが継続します。
10	要求された送信元ポートが使用できない場合、NAT は関連するグループの先頭から検索を開始します（TCP または UDP アプリケーションでは 1 から始まり、ICMP では 0 から始まります）。
11	あるポートが使用できる場合、そのポートが割り当てられ、セッションが継続します。
12	使用できるポートがない場合、プール内で別の IP アドレスが使用可能でない限り、パケットは廃棄されます。

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 NAT 変換に割り当てられる IP アドレスの範囲です。 プールを定義するには、次のような設定コマンドが使用されます。

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 192.168.1.0 または 192.168.2.0 のネットワークを、グローバルに一意な 10.69.233.208/28 のネットワークに変換しています。

```
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

次の例では、仮想アドレスを定義することによって、接続を一連の実ホストに分散させています。 プールでは、実ホストのアドレスを定義します。 アクセス リストでは、仮想アドレスを定義します。 変換が存在しない場合には、シリアル インターフェイス 0（外部インターフェイス）か

ら送信される TCP パケットでは、送信先がアクセス リストと一致するものについては、プールに定義された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. 実際には、設定可能な IP プールの最大数は、特定のルータで使用されている使用可能なメモリの量により制限されます（シスコでは、プールのサイズは 255 に設定することを強く推奨します）。 各プールは 16 ビットを超えてはなりません。 12.4(11)T 以降では、IOS には Common Classification Engine（CCE）が導入されました。 このエンジンでは、NAT の最大プール数は 255 に制限されています。 12.2S のコード ベースには、最大プール数の制限はありません。

Q. NAT プールで ACL を使用するのではなく、ルートマップを使用する利点は何ですか。

A. ルートマップは、不適格な外部ユーザによって、内部ユーザ/サーバがアクセスされないように保護します。 また、ルールに基づいて、1 つの内部 IP アドレスを異なる複数の内部グローバル 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 における IP アドレス「重複」とは何ですか。

A. IP アドレス重複とは、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 つの場所は接続されず、セッションも確立できません。 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、Outside の世界へ接続するには NAT 変換が必要です。 解決策には、Outside から Inside への Domain Name System（DNS; ドメイン ネーム システム）の名前クエリの応答を代行受信し、Outside アドレス用の変換をセットアップして、DNS 応答を Inside ホストに転送する前に修正することが含まれます。 両方のネットワークを接続しようとするユーザを解決するには、NAT デバイスの両側に DNS サーバを使用する必要があります。

『*重複ネットワークでの NAT の使用*』で説明されているように、NAT は、DNS「*A*」および「PTR」レコードのコンテンツに対するアドレス変換を検査し、実行することができます。

Q. スタティック NAT 変換とは何ですか。

A. スタティック NAT 変換では、ローカル アドレスとグローバル アドレスの間に 1 対 1 のマッピ

ングが用意されます。 ユーザは、スタティック アドレス変換をポート レベルに設定することもでき、他の変換用に残りの IP アドレスを使用することができます。 通常、これは Port Address Translation (PAT; ポート アドレス変換) を実行している場合に発生します。

次の例は、スタティック NAT によって外部から内部への変換を実行できるように、ルートマップを設定する方法を示しています。

```
ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 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。 PAT と同じ意味ですか。

A. はい。 NAT オーバーロードは、PAT です。つまり、1 つまたは複数のアドレスの範囲が定義された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 アドレスを組み合わせて使用します。 オーバーロードを使用するときには、全面的な拡張変換を実装します。 つまり、PAT またはオーバーロードと呼ばれる、IP アドレスと送信元/宛先ポート情報を含む変換テーブルのエントリを定義します。

PAT (またはオーバーロード) は、Cisco IOS の NAT の 1 つの機能で、*internal* (Inside ローカル) プライベート アドレスを 1 つまたは複数の *Outside* (通常は登録された Inside グローバル) IP アドレスに変換するために使用できます。 各変換では、カンバセーションを区別するために、一意の送信元ポート番号が使用されます。

Q. ダイナミック NAT 変換とは何ですか。

A. ダイナミック NAT 変換では、ユーザがローカル アドレスとグローバル アドレスの間にダイナミック マッピングを確立できます。 変換されるローカル アドレスおよびグローバル アドレスが割り当てられるアドレスのプールまたはインターフェイスの IP アドレスを定義し、その 2 つを関連付けることによって、ダイナミック マッピングが実行されます。

Q. ALG とは何ですか。

A. ALG とは、Application Layer Gateway (ALC; アプリケーション レイヤ ゲートウェイ) の意味です。 NAT では、アプリケーション データ ストリームで送信元/宛先 IP アドレスを搬送しない任意の Transmission Control Protocol/User Datagram Protocol (TCP/UDP) 上で変換サービスが実行されます。

該当する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。 ペイロードに IP アドレスが埋め込まれた特殊なプロトコルについては、Application Level Gateway (ALG) によるサポートが必要になります。

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 変換を使用した設定を構築できますか。

A. はい。 ただし、スタティック NAT の設定またはダイナミック NAT に設定されるプールで、同じ IP アドレスは使用できません。 また、すべてのパブリック IP アドレスが一意である必要が

あります。 ただし、スタティック変換で使用されるグローバル アドレスは、それらのグローバル アドレスを含むダイナミック プールからは自動的には排除されません。 ダイナミック プールは、スタティック エントリとは排他的になるように割り当てる必要があります。 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 ルータ経由で traceroute を実行した場合、NAT グローバル アドレスが出力されますか。それとも、NAT ローカル アドレスが出力されますか。

A. Outside から traceroute を実行すると、常にグローバル アドレスが返されます。

Q. PAT では、どのような仕組みでポートが割り当てられるのですか。

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

- フルレンジ機能によって、デフォルトのポート範囲設定に関わらず、すべてのポートを使用できます。
- ポートマッピング機能によって、特定のアプリケーションに対して、ユーザ定義されたポート範囲を予約できます。

詳細は、『PAT におけるユーザ定義発信元ポート範囲の使用』を参照してください。

12.4(20)T2 以降では、L3/L4 ランダム ポートおよび対称型ポートが導入されています。

- ランダム ポートによって、発信元ポートの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。
- 対称型ポートによって、*エンドポイントの独立性*をサポートできます。

詳細は、『 ネットワーク アドレス変換の内部構造の分析』を参照してください。

Q. IP フラグメンテーションと TCP セグメンテーションの違いは何ですか。

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 Maximum Transmission Unit (MTU; 最大伝送ユニット) より大きなパケットが送信されたときに発生します。 これらのパケットについては、インターフェイスから送出されるときにフラグメント化されるか、または廃棄される必要があります。 パケットの IP ヘッダに Don't Fragment (DF; フラグメントなし) ビットが設定されていなければ、パケットはフラグメント化されます。 パケットの IP ヘッダに DF ビットが設定されている場合には、パケットはドロップされ、ネクストホップ MTU 値を指示する ICMP エラー メッセージが送信側に返されます。 IP パケットのすべてのフラグメントは、IP ヘッダに同じ ID が定義されています。そのため、最終的な受信側では、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。 詳細は、『GRE および IPsec による IP フラグメンテーション、MTU、および PMTUD に関する問題の解決』を参照してください。

TCP セグメンテーションは、端末上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 によって最適と判断されるサイズに分割されて送信されます。 この TCP から IP に渡されるデータの構成単位のことをセグメントと呼びます。 TCP セグメントは、IP データグラムとして送信されます。 これらの IP データグラムは、ネットワークを通過するときにさらに IP フラグメントに分割されるため、分割されない場合よりも低い MTU のリンクを利用できます。

TCP では、最初に (TCP MSS 値に基づいて) このデータを TCP セグメントに送信します。さら

に TCP ヘッダを追加して、この TCP セグメントを IP に渡します。 次に、IP では、パケットをリモートのエンド ホストに送信するために、 IP ヘッダを追加します。 TCP セグメントを伴った IP パケットのサイズが、TCP ホスト間のパス上にある発信インターフェイスの IP の MTU より大きくなる場合には、 MTU に合わせて IP/TCP パケットはフラグメント化されます。 これらの IP パケットのフラグメントは、IP レイヤによって、リモート ホスト上で再構成されます。その結果、 (最初に送信された状態に) 再現された TCP セグメントが、TCP レイヤに引き渡されます。 TCP レイヤでは、パケットが通過中にフラグメント化されていても通常と同じように処理できます。

NAT では、IP フラグメントはサポートされますが、TCP セグメントはサポートされません。

Q. NAT では、パケット順序が入れ替わった IP フラグメント、および TCP セグメントはサポートされますか。

A. NAT では、ip virtual-reassembly によって、パケット順序が入れ替わった IP フラグメントだけがサポートされています。

Q. IP フラグメンテーションおよび TCP セグメンテーションをデバッグする方法はありますか。

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. NAT MIB はサポートされていますか。

A. いいえ。 そこに CISCO-IETF-NAT-MIB を含むサポートされた NAT 無し MIB で。

Q. *TCP タイムアウト*とは何ですか。また、NAT の TCP タイマーとはどのような関係にありますか。

A. スリーウェイ ハンドシェイクが完了していないときに、NAT がパケットを検出した場合は、60 秒のタイマーが開始されます。 スリーウェイ ハンドシェイクが完了しているときは、NAT エントリには、24 時間のタイマーがデフォルトで使用されます。 エンド ホストが RESET を送信した場合には、NAT はデフォルト タイマーを 24 時間から 60 秒に変更します。 FIN の場合は、FIN および FIN-ACK を受信したときに、デフォルト 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. はい。 すべてのエントリの NAT タイムアウト値を変更できます。または、異なる種類の NAT 変換について個別に変更できます (upd-timeout、dns-timeout、tcp-timeout、finrst-timeout、icmp-timeout、pptp-timeout、syn-timeout、port-timeout、および arp-ping-timeout) 。

Q. Lightweight Directory Access Protocol (LDAP) では、LDAP 応答パケットごとに余分なバイトが追加されてしまいます。どうすれば追加されないようにできますか。

A. LDAP を設定すると、Search-Res-Entry タイプのメッセージを処理する間に、余分なバイト

（LDAP による検索結果）が追加されます。 LDAP では、LDAP 応答パケットごとに、それぞれ 10 バイトの検索結果が添付されます。 この 10 バイト分が追加されたことによって、パケットがネットワークの MTU を超過してしまった場合には、パケットはドロップされます。 このようなケースに関しては、シスコでは、パケットの送受信を優先するために、CLI **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推奨しています。

Q. NAT ボックスの Inside Global/Outside Local IP アドレスに関するルート 推奨事項とは何か。

A. ルートは NAT-NVI のような機能の Inside Global IP アドレスのための NAT によって設定されるボックスで規定 されなければなりません。 同様に、ルートはまた Outside Local IP アドレスのための NAT ボックスで規定 する必要があります。 この場合、外部静的なルールを使用して方向へののからのどのパケットでもこの種類のルートを必要とします。 そのようなシナリオでは、ルートを IG/OL に提供している間、ネクスト ホップ IP アドレスがまた設定する必要がある。 ネクスト ホップ 設定が抜けている場合、これは設定 エラーとみなされ、未定義動作という結果に終ります。

NVI-NAT は出力 機能 パスだけにあります。 NAT-NVI の接続されたサブネットかボックスで設定される外部 NAT 変換規則が直接ある場合それらのシナリオで、ネクスト ホップにダミー ネクスト ホップ IP アドレスおよびまた関連する ARP を提供する必要があります。 これは基礎的なインフラストラクチャのために必要変換のための NAT にパケットを渡すためにです。

Q. Cisco IOS NAT は「ログ」キーワードの ACL をサポートしますか。

A. ダイナミック NAT 変換を行うために Cisco IOS NAT を設定する場合、変換可能なパケットを判別するために ACL が使用されます。 現在の NAT アーキテクチャでは、「log」キーワードを使用した ACL はサポートされていません。

音声と NAT

Q. NAT では、Cisco Unified Communications Manager（CUCM）V7 に付属している Skinny Client Control Protocol（SCCP）v17 はサポートされますか。

A. CUCM 7 と 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。 SCCP のバージョンについては、電話を登録した時点での CUCM と電話に共通する最も高いバージョン番号が使用されます。

NAT では、現在のところ SCCP v17 はサポートされていません。 SCCP v17 のサポートが実装されるまでは、SCCP v16 を利用する必要があるため、ファームウェアを 8-3-5 以前のバージョンにダウングレードする必要があります。 CUCM6 の場合は、SCCP v16 が利用されている限りは、どの電話ロードにおいても NAT で問題が生じることはありません。 現在、Cisco IOS では、SCCP バージョン 17 はサポートされていません。

Q. NAT によってサポートされているのは、どのバージョンの CUCM /SCCP/ファームウェア ロードですか。

A. NAT では、CUCM バージョン 6.x 以前のリリースがサポートされています。 これらのバージョンの CUCM には、SCCP v15（以前）をサポートしたデフォルトの 8.3.x（以前のバージョン）の電話ファームウェア ロードが付属しています。

NAT では、CUCM バージョン 7.x 以降のリリースについてはサポートされません。 それらのバージョンの CUCM には、SCCP v17（以降）をサポートしたデフォルトの 8.4.x の電話ファームウェア ロードが付属しています。

CUCM 7.x 以降が使用される場合は、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。

次のリンクをご確認いただければ、SCCP v15 以前のバージョンをサポートするファームウェア ロード 8.3.x では NAT を利用できますが、SCCP v17 をサポートするファームウェア ロード 8.4.x では NAT を利用できないことが明らかになります。

http://third-gen-phones.gforge.cisco.com/twiki/prod/bin/view/Thirdgenphones/CCMLoadNumberAndCodeNameDecoderRing

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. 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の機能によって、SIP、H.323、および Skinny の音声コールにおける動作を保証します。 RTP ストリームに使用されるポート番号が偶数のポート番号で、RTCP ストリームがそれに続く奇数のポート番号になるようにします。 ポート番号は、RFC-1889 に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が含まれたコールでは、この範囲内の別のポート番号への PAT 変換が行われます。 同様に、この範囲外のポート番号の PAT 変換では、対象の範囲内の番号への変換は行われません。

詳細は、『RTP と RTCP のサービス プロバイダー PAT ポート割当機能拡張』を参照してください。

Q. Session Initiation Protocol（SIP; セッション開始プロトコル）とは何ですか。また、SIP パケットは NAT に対応していますか。

A. Session Initiation Protocol（SIP; セッション開始プロトコル）は、ASCII ベースのアプリケーション層制御プロトコルであり、2 点間およびそれ以上のエンドポイント間のコールの確立、維持、および終了に使用できます。 SIP は、IP を介したマルチメディア会議のために Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって開発された代替プロトコルです。 Cisco SIP の実装では、サポート対象の Cisco プラットフォームによる 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 コールの確立が実現されます。

SIP パケットは NAT に対応しています。

Q. Session Border Controller（SBC）のホスト NAT トラバーサル サポートとは何ですか。

A. SBC の Cisco IOS ホスト NAT トラバーサル機能では、Cisco IOS NAT SIP Application-Level Gateway（ALG）ルータが Cisco Multiservice IP-to-IP Gateway 上で SBC として動作するようにします。これによって、Voice over IP（VoIP）サービスを円滑に提供できるようになります。

詳細については、『Session Border Controller の Cisco IOS ホスト NAT トラバーサル』および『

Cisco IOS Session Border Controller を使用した、SIP コールの SP ホスト NAT トラバーサル』を参照してください。

Q. NAT を使用するときに、ルータのメモリおよび CPU で処理可能な SIP、Skinny、および H323 のコール数はどの程度ですか。

A. NAT ルータによって処理されるコールの数は、利用可能なメモリの量や CPU の処理能力によって異なります。

Q. NAT ルータでは、Skinny および H323 での TCP セグメンテーションはサポートされますか。

A. IOS-NAT では、12.4 メインラインにおいて H323 の TCP セグメンテーションがサポートされています。また、Skinny については、12.4(6)T 以降でサポートされています。

Q. 音声環境において、NAT オーバーロード設定を使用する際に、注意すべきことは何かあるでしょうか。

A. はい。 音声を利用する環境で NAT オーバーロードを設定するときには、NAT を動作させるために、登録メッセージが必要になります。また、この内部デバイスにアクセスできるように、out から in 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、この登録メッセージを定期的に送信します。また、NAT は、シグナリング メッセージによる情報を利用して、このピンホール/関連付けを随時更新します。

Q. 音声環境において、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ことによって発生する問題が何か存在しますか。

A. 音声環境で 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てしまうため、次回の登録サイクルで内部デバイスによる再確立が行われるまで待機しなければなりません。 シスコでは、音声環境ではこれらのコマンドを使用しないことを推奨しています。

Q. NAT では、共存型の音声ソリューションはサポートされますか。

A. いいえ。 現在のところ、共存型のソリューションはサポートされません。 CME/DSP-Farm/SCCP/H323 については、（同一ボックスに）NAT を使用して導入した場合には、共存型ソリューションと見なされます。

Q. NVI では、Skinny ALG、H323 ALG、および TCP SIP ALG はサポートされますか。

A. いいえ。 ほとんどの導入では UDP SIP ALG が使用されているため、特にメリットがないことに注意してください。

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じように、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。 次のような

設定を行おうとしたときに、 *「%の同じような静的エントリ (1.1.1.1 ------次を設定するように試みる時 > 22.2.2.2) 既に」存在 します*: `72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED`

A. 従来からの NAT では、異なる複数の VRF に対して、オーバーラップするアドレスを設定できます。 それには、match-in-vrf オプションによってルールを定義し、オーバーラップを設定する必要があります。また、特定の VRF によって処理されるトラフィックについては、同じ VRF に 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。

異なる複数の VRF スタティック NAT エントリをオーバーラッピングするには、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 アドレスはオーバーラッピングできません。

```
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf 72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```

Q. 従来からの NAT では、VRF-Lite (VRF から異なる VRF への NAT 変換) はサポートされますか。

A. いいえ。 異なる VRF 間で NAT を実行したい場合には、NVI を使用する必要があります。 従来からの NAT を使用して、VRF と グローバルとの間、または同一 VRF の内部で NAT を実行できます。

NAT NVI

Q. NAT NVI とは何ですか。

A. NVI とは、NAT Virtual Interface (NAT 仮想インターフェイス) の意味です。 NVI を使用することで、2 つの異なる VRF の間で NAT 変換を実行できます。 このソリューションは、「On a Stick」接続でのネットワーク アドレス変換の代わりに使用されます。

Q. グローバル側にあるインターフェイスと VRF 側にあるインターフェイスとの間で NAT を実行するときに、NAT NVI を使用できますか。

A. シスコでは、VRF とグローバル NAT、および同一 VRF 内のインターフェイス間では、従来からの NAT を使用することを推奨しています。 NVI は、異なる VRF 間での NAT に使用します。

Q. NAT - NVI では、TCP セグメンテーションはサポートされますか。

A. NAT - NVI では、TCP はサポートされません。

Q. NVI では、Skinny ALG、H323 ALG、および TCP SIP ALG はサポートされますか。

A. いいえ。 ほとんどの導入では UDP SIP ALG が使用されているため、特にメリットがないことに注意してください。

Q. SNAT を使用するときに、TCP セグメンテーションはサポートされますか。

A. SNAT は、いずれの TCP ALG についても（SIP、SKINNY、H323、または DNS など）サポートしていません。 そのため、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 はサポートされています。

SNAT

Q. Stateful NAT（SNAT; ステートフル NAT）とは何ですか。

A. SNAT を使用することにより、2 つ以上のアドレス変換を、変換グループとして機能させることができます。 変換グループのメンバの 1 つが、IP アドレス情報の変換が必要な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生じたときに、バックアップ変換プロセスに通知します。 バックアップ変換プロセスでは、アクティブな変換プロセスから送信された情報を使用して、変換テーブルのエントリを複製する準備を行います。 そのため、アクティブな変換プロセスが重大なエラーによって実行不能になった場合でも、トラフィックを即座にバックアップに切り替えることができます。 同じネットワーク アドレス変換と、エラー前に定義されていた変換の状態が使用されるため、トラフィック フローは継続されます。 詳細は、『Cisco Stateful NAT の使用による IP 復元力の強化』を参照してください。

Q. SNAT を使用するときに、TCP セグメンテーションはサポートされますか。

A. SNAT は、いずれの TCP ALG についても（SIP、SKINNY、H323、または DNS など）サポートしていません。 そのため、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 はサポートされています。

Q. 非対称ルーティングでは、SNAT はサポートされますか。

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によって、NAT をサポートします。 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 はサポートされていません。 そのため、非対称ルーティングが正しく動作するように、パケットが正しくルーティングされており、適切な遅延が追加されていることを確認する必要があります。

NAT-PT（v6 - v4 変換）

Q. NAT-PT とは何ですか。

A. NAT-PT は、NAT に使用される v4 - v6 変換サービスです。 プロトコル変換（NAT-PT）によって、RFC 2765 および RFC 2766 で定義された IPv6-IPv4 変換メカニズムが提供されるため、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。 この機能に関する詳細については IPv6 のための NAT-PT を設定することを参照して下さい

Q. NAT-PT は Cisco Express Forwarding（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ません。

Q. NAT-PT では、どの ALG がサポートされますか。

A. NAT-PT では、TFTP/FTP と DNS がサポートされます。 NAT-PT では、音声および SNAT に

ついて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. 集約 サービス ルータ（ASR）は NAT64 を使用します。 NAT64 の設定に関する詳細については、ステートレス NAT64 のためのルーティング ネットワークの設定を参照して下さい。

特定プラットフォーム（Cisco 7300/7600/6k）に関する質問

Q. SX トレインの Catalyst 6500 では、Stateful NAT (SNAT) を利用できますか。

A. SNAT は、SX トレインの Catalyst 6500 ではご利用になれません。

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

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

Q. 7600 および Cat6000 では、VRF 対応 NAT はサポートされますか。

A. 65xx/76xx プラットフォームでは、VRF 対応 NAT はサポートされないため、CLI はブロックされます。

注: 仮想コンテキスト透過モードで実行される FWSW を利用することによって設計を実装できます。

特定プラットフォーム（Cisco 850）に関する質問

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

A. いいえ。 850 シリーズでは、12.4T の Skinny NAT ALG はサポートされません。

NAT の導入

Q. NAT を導入するには、どのようにすればよいのですか。

A. NAT では、インターネットに接続するために、未登録の IP アドレスを使用するプライベート IP のインターネットワークをイネーブルにします。 NAT は、パケットが他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、正規のルーティング可能なアドレスに変換します。

NAT の導入についての詳細は、『NAT の設定による IP アドレスの変換』を参照してください。

Q. 音声とともに使用される NAT は、どのように導入すればよいのですか。

A. 音声機能をサポートした NAT によって、SIP に埋め込まれたメッセージが、NAT によってパケットが変換されるように構成されたルータを通過できるようになります。 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）が使用されます。

音声とともに使用される NAT についての詳細は、『NAT による ALG のサポート』を参照してください。

Q. NAT と MPLS VPN は、どのように統合すればよいのですか。

A. NAT に MPLS VPN の機能を統合することによって、複数の MPLS VPN が 1 つのデバイス上で協調して動作するように構成できます。 NAT を利用することによって、複数の MPLS VPN で同じ IP アドレッシング スキームが使用されている場合でも、IP トラフィックを受信できるようになります。 このような機能強化によって、複数の MPLS VPN を利用するユーザは、それぞれの MPLS VPN の独立性を確保しながら、同時にサービスを共有できるようになります。

Q. NAT のスタティック マッピングでは、ハイ アベイラビリティのための HSRP はサポートされていますか。

A. NAT スタティック マッピングを使用して設定された、ルータによって所有されるアドレスに対して、Address Resolution Protocol（ARP; アドレス解決プロトコル）キューがトリガされるときに、NAT は インターフェイス上の ARP がポイントしている BIA MAC アドレスを使用して応答します。 2 つのルータは、それぞれ HSRP アクティブおよびスタンバイとして動作します。 それぞれのインターフェイスの NAT Inside をイネーブルにし、グループに属するように設定する必要があります。

Q. NAT NVI はどのように導入すればよいのですか。

A. NAT Virtual Interface（NVI）機能によって、インターフェイスを NAT Inside または NAT Outside のどちらかに設定する必要がなくなります。 NAT NVI の詳細については、「NAT 仮想インターフェイスの設定」を参照してください。

Q. NAT でロードバランシングを導入するには、どのようにすればよいのですか。

A. NAT では、2 種類のロードバランシングの導入が考えられます。 まず、サーバの負荷を分散させるために、一連のサーバに着信するデータに対してロードバランシングを適用できます。また、2 つ以上の ISP を利用している場合に、インターネットに発信されるユーザ トラフィックに対してロードバランシングを適用できます。

着信側のロードバランシングについての詳細は、「TCP ロードバランシングの使用によるサーバ過負荷の回避」を参照してください。

発信側のロードバランシングについての詳細は、『2 つの ISP の接続のための IOS NAT のロードバランシング』を参照してください。

Q. IPSec と NAT を同時に利用するには、どのようにすればよいのですか。

A. NAT および IPSec NAT 透過を通して、IP Sec ESP（IP Security Encapsulating Security Payload）がサポートされます。

NAT による IPSec ESP のサポート機能では、オーバーロードまたは PAT モードに設定された Cisco IOS NAT デバイスを通して、複数の IPSec ESP トンネルまたは接続の同時使用をサポートできます。

IPSec NAT 透過機能が導入されたことによって、NAT と IPSec の間に数多く存在した既知の非

互換性が解決されたため、IPSec トラフィックがネットワークの NAT または PAT ポイントを通過できるようになりました。

Q. NAT-PT を導入するには、どのようにすればよいのですか。

A. NAT-PT (Network Address Translation—Protocol Translation) は、RFC 2765 および RFC 2766 で定義された IPv6-IPv4 変換メカニズムによって、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します。

NAT-PT の導入と設定についての詳細は、『NAT-PT for IPv6 の実装』を参照してください。

Q. マルチキャスト NAT を導入するには、どのようにすればよいのですか。

A. マルチキャスト ストリームであっても、発信元 IP に NAT を適用できます。 マルチキャストにダイナミック NAT を適用するときは、ルートマップは使用できません。この場合、アクセスリストだけがサポートされます。

詳細は、『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。 宛先マルチキャスト グループの NAT については、Multicast Service Reflection ソリューションを使用します。

Q. ステートフル NAT (SNAT) は、どのようにして導入すればよいのですか。

A. SNAT を使用することで、ダイナミックにマップされた NAT セッションで、持続的なサービスが可能になります。 SNAT が不要なスタティックに定義されるセッションの場合でも、導入することによって冗長性というメリットが得られます。 SNAT が導入されていない環境では、重大なエラーが生じたときに、ダイナミック NAT マッピングを使用するセッションが中断してしまうため、セッションを再確立しなければなりません。 現在、SNAT に関しては、最低限の設定だけがサポートされます。 実際に導入される場合には、現在の制限事項が十分に考慮されているかを検証するために、事前にシスコ アカウント チームにご連絡していただく必要があります。

次のようなシナリオでは、SNAT のご使用をお奨めします。

- SNAT のホワイトペーパー『 Cisco Stateful NAT の使用による IP 復元力の強化』で説明されている HSRP モード。
- HSRP と比較した場合に、いくつかの機能が不足しているため、プライマリ/バックアップ モードが望ましくない。
- フェールオーバーを導入する予定があり、2 台のルータが構成される。 つまり、1 台のルータがクラッシュしても、別のルータにシームレスに引き継がれるようにする場合 (SNAT は、インターフェイスのフラップを処理するようには設計されていない) 。
- 非対称ではないルーティングをサポートする予定がある。 応答パケットの遅延が、2 台の SNAT ルータ間で SNAT メッセージを交換する時間より長くなる場合にだけ、非対称ルーティングを処理できる。

現在のところ、SNAT のアーキテクチャは、ロバストネスを処理するようには設計されていません。 そのため、次のようなテストの実行が成功するとはかぎりません。

- トラフィックが存在する間に、NAT エントリをクリアする。
- トラフィックが存在する間に、(IP アドレスの変更、shut/no-shut などの) インターフェイス パラメータを変更する。
- SNAT 固有の **clear** または **show** コマンドについては、正しく実行されるとはかぎらないため

、使用を推奨しない。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。 **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>**

- エントリをクリアしたい場合には、clear ip nat trans forced または clear ip nat trans ? コマンドを使用できる。エントリを表示したい場合には、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る。 *service internal* が設定されている場合にも、同じように SNAT 固有の情報が表示される。
- バックアップ ルータで NAT 変換をクリアすることは推奨されない。 NAT エントリは常にプライマリ SNAT ルータでクリアする。
- SNAT は HA ではない。 そのため、両方のルータの設定が同一である必要がある。 また、両方のルータでは、同じイメージが実行されている必要がある。 さらに、両方の SNAT ルータに使用されている基本プラットフォームが同じでなければならない。

NAT のベスト プラクティス

Q. NAT にはベスト プラクティスがありますか。

A. はい。 次に NAT のベスト プラクティスを示します。

1. ダイナミックおよびスタティック NAT を両方使用するときは、ダイナミック NAT のルールを定義した ACL では、オーバーラップを避けるために、スタティック ホストを除外します。
2. permit ip any any を設定した NAT で ACL を使用すると、予期しない動作をする場合があるため注意が必要です。 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出されるルーティング プロトコル パケット、さらに NAT ルールに一致する、ローカルに暗号化されたパケットも変換されます。
3. オーバーラッピング ネットワークで NAT を使用するときには、match-in-vrf キーワードを使用します。異なる複数の VRF でオーバーラップする 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 アドレスではオーバーラップできません。 `Router(config)#` **`ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf`** `Router(config)#` **`ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf`**
4. 同じアドレス範囲が定義された NAT プールは、match-in-vrf キーワードを使用しないかぎり、異なる複数の VRF には使用できません。次に、例を示します。 **ip nat pool poolA 171.1.1.1 171.1.1.10 prefix-length 24 ip nat pool poolB 171.1.1.1 171.1.1.10 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 が実行されていても、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 インターフェイスのオーバーロードを利用するときに、ISP のロードバランシングを導入する場合は、ACL マッチングで一致したインターフェイスで、ルートマップを使用するのがベスト プラクティスです。
6. プール マッピングを使用するときには、同じ NAT プールのアドレスを共有に、2 つの異なるマッピング (ACL またはルートマップ) を使用しないように注意してください。
7. フェールオーバーを導入したいときに、2 つの異なるルータに同じ NAT ルールを導入する場合は、HSRP による冗長性を使用してください。
8. スタティック NAT およびダイナミックプールの同じ内部グローバルアドレスを定義しないで下さい。 この操作は望ましくない結果をもたらす場合があります。

関連情報

- IP ルーティング テクノロジーに関するサポート ページ (英語)
- テクニカルサポートとドキュメント - Cisco Systems