FAQを使用したネットワークアドレス変換(NAT)のトラブルシューティング

内容

概要

このドキュメントでは、ネットワークアドレス変換(NAT)ルータプロセスがどのように動作するかについて説明し、いくつかの一般的な質問に対する回答を示します。

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は通常、2つのネットワークを接続するときにルータ上で動作し、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。

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、そのアドレスの背後にある内部ネットワーク全体が効果的に隠され、セキュリティが強化されます。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 はどのように機能しますか。

A.基本的に、NATではルータなどの単一のデバイスがインターネット（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）の間のエージェントとして機能できます。つまり、ネットワークの外部にあるものに対してコンピュータのグループ全体を表すには、一意のIPアドレスが1つだけ必要になります。

Q. NAT の設定方法を教えてください。

A.従来の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)とルータ上の別のインターフェイス(NAT Inside)を作成し、パケットヘッダー（および必要に応じてペイロード）内のIPアドレスに一連の変換ルールを作成して、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』のセクションを参照してください。

Q. NATのCisco IOS®ソフトウェアとCisco適応型セキュリティアプライアンス(ASA)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は、Cisco ASAのNAT機能と基本的に異なることはありません。主な違いは、実装および設計要件でサポートされるトラフィックタイプが異なることです。Cisco ASAデバイスでのNATの設定の詳細については、『NATの設定例』を参照してください（サポートされているトラフィックタイプを含む）。

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。

A. Cisco Feature Navigatorツールを使用すると、機能(NAT)を識別し、このCisco IOSソフトウェア機能を使用できるリリースとハードウェアバージョンを確認できます。このツールを使用するには、『Cisco機能ナビゲータ』を参照してください。

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。

A. NATによってトランザクションが処理される順序は、パケットが内部ネットワークから外部ネットワークに移動するか、外部ネットワークから内部ネットワークに移動するかによって異なります。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。詳細は、『NATの処理順序』を参照してください。

Q. NATはパブリックワイヤレスLAN環境に導入できますか。

A.はい。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をサポートし、それらの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します。

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

。

A.はい。NATを使用すると、実ホスト間のロードバランスを調整する仮想ホストを内部ネットワーク上に確立できます。

Q. NAT 変換の数をレート制限することはできますか。

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。これにより、ユーザはNATアドレスの使用方法をより細かく制御できます。レート制限NAT変換機能を使用すると、ウイルス、ワーム、およびサービス拒否攻撃の影響を制限できます。

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。

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

- 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してproxy-arpを実行できます。この動作が望ましくない場合は、eno-aliaskeyword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 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。

A. NATセッションの制限は、ルータで使用可能なDRAMの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。ただし、プラットフォームの仕様を確認することもお勧めします。

Q. Cisco IOS NATでは、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 NATは、Cisco Express Forwarding(CEF)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をサポートしています。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
- その時点で実行されているその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.はい。送信元および宛先の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（ダイヤラインターフェイスを含む）に適用できます。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。Wireless Virtual Interface(WVI)は、NVRAMに書き込む時点では存在しません。そのため、リブート後、ルータはワイヤレス仮想インターフェイスのNAT設定を失います。

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。

A.はい。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 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。

A.はい。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。詳細については、前の質問「NATの設定方法」を参照してください。

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。

A.はい。これは、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 リストを使用すると実行できます。同じホスト上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て変換されないかのいずれかになります。

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して、どのIPデバイスが変換されるかを定義できます。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anyanynetworkを使用しないでください。スタティックNAT設定では、パケットがどのSTATICルール設定とも一致しない場合、パケットは変換なしで送信できます。

Q. PAT（オーバーロード）が設定されている場合、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、および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、元の要求と同じポート値を割り当てようとしますが、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探し、それをカンバセーションに割り当てます。

Q. PAT はどのように機能しますか。

A.PATは、1つのグローバルIPアドレスまたは複数のアドレスで動作します。

1つのIPアドレステーブルを持つ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がトラフィックタイプを認識しており、そのトラフィックタイプに使用可能な「特定のポート
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
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、セッションが続行さ
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
7	ポートが使用可能な場合はそれが割り当てられて、セッションが続行されます。
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。

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。

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
9 ミリ秒	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、セッションが続行
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
11	ポートが使用可能な場合は、そのポートが割り当てられ、セッションが続行されます。
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

Q. NAT IP プールとは何ですか。

A.NAT IPプールは、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、次のコンフィギュレーション コマンドを使用します。

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

例 1

次の例では、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ネットワークにアドレス指定された内部ホスト間の変換を行います。

```
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、一連の実ホスト間で分散される接続である仮想アドレスを定義することを目標としています。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. 設定できる NAT IP プール (ip nat pool "name") の最大数はいくつですか。

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可能なDRAMの量によって制限されます。 (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ビット以下である必要があります。12.4(11)T以降では、Cisco IOSによってCCE(Common Classification Engine)が導入されました。そこでは、NAT のプール数が 255 以下に制限されています。

Q. NATプールでルートマップとACLを比較する利点は何ですか。

A.ルートマップは、不要な外部ユーザが内部ユーザ/サーバに到達するのを防ぎます。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。詳細は、『ルートマップを使用した複数プールのNATサポート』を参照してください。

Q. NAT の観点から見た IP アドレスの「重複」とは何を意味しますか。

A. IPアドレスの重複は、相互接続を行う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いと、2つの口ケーションは接続できず、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、別の会社に割り当てられたプライベート

アドレス、またはRFC 1918で定義されたプライベートアドレスの範囲から取得できます。

プライベートIPアドレスはルーティングできず、外部への接続を許可するにはNAT変換が必要です。 このソリューションでは、外部から内部へのドメインネームシステム(DNS)の名前クエリ応答のインターセプト、外部アドレスの変換設定、および内部ホストに転送する前にDNS応答を修正する必要があります。 両方のネットワーク間の接続を必要とするユーザを解決するには、NATデバイスの両側にDNSサーバが必要です。

NATでは、DNSAandPTRrecordsの内容に対するアドレス変換を検査および実行できます。これについては、「重複ネットワークでのNATの使用」を参照してください。

Q. 静的 NAT 変換とは何ですか。

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のマッピングがあります。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、Port Address Translation（PAT；ポートアドレス変換）を実行する場所で発生します。

次の例は、スタティックNATの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。

```
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 10.1.10.1 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

Q. *NATOverloading*という用語は何を意味していますか。これはPATですか。

A.はい。NATオーバーロードはPATです。PATでは、1つ以上のアドレスの範囲を持つプールを使用するか、インターフェイスIPアドレスをポートと組み合わせて使用します。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アドレスと送信元/宛先ポートの情報を含む変換テーブルエントリで、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、*内部*（内部ローカル）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、通常は登録された）IPアドレスに変換するために使用されるCisco IOS NATの機能です。各変換の一意の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. 動的 NAT 変換とは何ですか。

A. ダイナミック NAT 変換では、ローカル アドレスとグローバル アドレスの間にダイナミック マッピングを設定できます。ダイナミックマッピングを行うには、変換す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のプールまたはインターフェイスIPアドレスを定義し、この2つを関連付けます。

Q. ALG とは何ですか。

A.ALGはアプリケーション層ゲートウェイ(ALG)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. 静的 NAT 変換と動的 NAT 変換を併用する構成は可能ですか。

A.はい。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用さ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は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を実行する場合、tracerouteはNATグローバルアドレスを表示する必要がありますか、それともNATローカルアドレスをリークする必要がありますか。

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 はどのようにしてポートを割り当てますか。

A. NATでは、フルレンジとポートマップという追加のポート機能が導入されています。

- 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。

詳細は、『PATの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。
- 対称ポートを使用すると、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どのように違いますか。

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際にフラグメント化されるか、廃棄される必要があります。If the Don't Fragment (DF) パケットのIPヘッダーに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る可能性があります。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、そのパケットは廃棄され、ICMPエラーメッセージは送信元に返されるネクストホップMTU値を示しま

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セグメンテーションは、エンドステーション上のアプリケーションがデータを送信するときに実行されます。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では、まず（TCP MSS値に基づいて）このデータを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に渡すことができます。その後、IPはIPヘッダーを追加して、リモートエンドホストにパケットを送信できます。TCPセグメントを持つIPパケットが、TCPホスト間のパス上の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できます。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に再構成でき、最初に送信された完全なTCPセグメントをTCPレイヤに渡すことができます。TCP レイヤは、伝送中に IP がパケットをフラグメント化し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。

A. virtual-reassemblyを無効にするため、NATは順序が入れ替わったIPフラグメント**のみをサポートします**。

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両方に同じデバッグCLIを使用します。**debug ip nat frag**。

Q. サポートされている NAT MIB はありますか。

A.いいえ。NAT MIBはサポートされておらず、CISCO-IETF-NAT-MIBもサポートされていません。

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に関係しますか。

A. 3ウェイハンドシェイクが完了せず、NATがTCPパケットを検出した場合、NATは60秒のタイマーを開始できます。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変換テーブルからNAT変換がタイムアウトするまでの時間を変更できますか。

A.はい。すべてのエントリまたは異なる種類の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付加する場合、LDAPを停止するにはどうすればよいのですか。

A. LDAPは、Search-Res-Entryタイプのメッセージを処理する際に、余分なバイト（LDAP検索結果）を追加するように設定されています。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10バイト分のデータが追加されると、パケットが生成され、ネットワーク内の最大伝送ユニット(MTU)を超えた場合、パケットは廃棄されます。この場合は、パケットを送受信するために、CLIno ip nat service append-ldap-search-rescommandコマンドを使用して、このLDAP動作をオフにすることをお勧めします。

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。

A. NAT-NVIなどの機能の内部グローバルIPアドレスのNAT設定ボックスで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持つin-to-out方向からのパケットには、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のルートを提供する一方で、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見つからない場合、これは設定エラーと見なされ、結果として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*キーワードを使用したACLはサポートされていますか。

A.ダイナミックNAT変換のためにCisco IOS NATを設定する場合、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キーワードを使用した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とCUCM 7のすべてのデフォルトの電話ロードは、SCCPv17をサポートしています。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。

NAT は、現在のところ 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、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以下にダウングレードする必要があります。CUCM6は、SCCP v16を使用している限り、どの電話ロード

でもNATの問題に遭遇しません。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 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。

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. 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。

A. RTPおよびRTCPのサービスプロバイダーPATポート割り当て拡張機能により、SIP、H.323、およびSkinny音声コールが保証されます。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、指定された範囲内のRFC-1889に準拠する番号に変換されます。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にPAT変換される可能性があります。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に変換することはできません。

Q. Session Initiation Protocol(SIP)とは何ですか。また、SIPパケットはNATを使用してルーティングできますか。

A. Session Initiation Protocol(SIP)は、ASCIIベースのアプリケーション層制御プロトコルで、2つ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、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）のホスト型 NAT トラバーサルサポートとは何ですか。

A. Cisco IOSのSBC用ホステッドNATトラバーサル機能を使用すると、Cisco IOS NAT SIP Application-Level Gateway(ALG)ルータがCisco Multiservice IP-to-IP Gateway上でSBCとして機能し、Voice over IP(VoIP)サービスの円滑な配信に役立ちます。

詳細については、『セッションボーダーコントローラ用のCisco IOSホストNATトラバーサルの設定』を参照してください。

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。

A. NATルータによって処理されるコールの数は、ボックスで使用可能なメモリの量とCPUの処理能力によって決まります。

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ていますか。

A. Cisco IOS-NATでは、H323のTCPセグメンテーションとSKINNYの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オーバーロード設定を使用する場合に注意する必要のある注意事項はありますか。

A.はい。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。内部デバイスはこの登録を定期的に送信し、NATはこのピンホール/関連付けをシグナリングメッセージ内の情報から更新します。

Q.音声環境でlear ip nat trans *コマンドまたはlear ip nat trans forcedcommandを使用すると、何か問題が発生しますか。

A.音声導入では、aclear ip nat trans *コマンドまたはaclear ip nat trans forcedcommandコマンドを発行してダイナミックNATを設定すると、ピンホール/アソシエーションが消去されるため、内部デバイスからの次の登録サイクルを待って、これを再度確立する必要があります。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 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。

A.いいえ。現在、同じ場所に配置される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 をサポートしていますか。

A.いいえ。UDP SIP ALG（ほとんどの導入で使用）は影響を受けないことに注意してください。

NAT と VRF/MPLS

Q. NATルータは、VRFとグローバルアドレス空間の同じアドレス空間で自分自身をサポートできますか。Currently, I receive this warning: *"% similar static entry (10.1.1.1 —> 10.2.2.2) already exists"*when I attempt to configure the this:

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED
```

A.レガシーNATでは、異なるVRFでのオーバーラッピングアドレス設定がサポートされています。match-in-vrfoptionを使用してoverlapping at ruleを設定し、その特定のVRF上のトラフィックに

対して同じVRF内でupip nat inside/outsideed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のオーバーラップするVRFスタティックNATエントリに対しては、match-in-vrfkeyword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。

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

Q.レガシーNATでは、VRF-Lite（VRFから別のVRFへのルート）はサポートされていますか。

A.いいえ。NVIを使用して、異なるVRF間でNATを実行する必要があります。レガシー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 Virtual Interfaceの略です。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間のルーティングには、NAT NVIを使用する必要がありますか。

A.シスコでは、VRFからグローバルNATへの変換(ip nat inside/out)、および同じVRF内のインターフェイス間にレガシー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 での TCP セグメンテーションはサポートされていますか。

A. NAT-NVIでは、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 をサポートしていますか。

A.いいえ。UDP SIP ALG（ほとんどの導入で使用）は影響を受けないことに注意してください。

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。

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を使用すると、複数のネットワークアドレス変換(NAT)を変換グループとして機能させることができます。IPアドレス情報の変換を必要とするトラフィックは、変換グループのメンバの1人が処理します。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。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. TCP セグメンテーションは SNAT でサポートされていますか。

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、NATがイネーブルになるとNATがサポートされます as-queuing .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した。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のv4からv6への変換です。プロトコル変換(NAT-PT)は、RFC 2765およびRFC 2766で定義されているIPv6-IPv4変換メカニズムであり、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します。

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

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 がサポートされていますか。

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 をサポートしていますか。

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 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、SXトレインのCatalyst 6500では使用できません。

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。

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ていません。

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。

A. 65xx/76xxプラットフォームでは、VRF対応NATはサポートされておらず、CLIはブロックされています。

注：仮想コンテキスト透過モードで動作するFWSMを利用すると、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 を実装するにはどうすればよいですか。

A. NATは、非登録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を有効にして、インターネットに接続します。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. 音声機能に NAT を実装するにはどうすればよいですか。

A.音声機能のNAT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組み込みメッセージをパケットに変換し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 を MPLS VPN と統合するにはどうすればよいですか。

A. NATとMPLS VPNの統合機能を使用すると、単一のデバイスに複数のMPLS VPNを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ても、NAT は、IP トラフィックを受信する MPLS VPN を区別できます。この機能拡張により、複数のMPLS VPNユーザがサービスを共有しながら、各MPLS VPNが互いに完全に分離されます。

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。

A. Network Address Translation（NAT；ネットワークアドレス変換）スタティックマッピングで設定され、ルータによって所有されているアドレスに対して、Address Resolution Protocol（ARP；アドレス解決プロトコル）クエリーがトリガーされると、NATは、ARPが指し示すインターフェイス上の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を実装する方法を教えてください。

A. NAT仮想インターフェイス(NVI)機能を使用すると、インターフェイスをNAT内部またはNAT外部のいずれかに設定する必要がなくなります。

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。

A. NATでは、2種類のロードバランシングが可能です。1組のサーバへのインバウンドでロードバランシングを行い、サーバへの負荷を分散できます。また、複数の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接続のためのCisco IOS NATロードバランシング』を参照してください。

Q. NATをIPSecと組み合わせて実装するにはどうすればよいのですか。

A.サポート対象は次のとおりです。 IP Security (IPSec) Encapsulating Security Payload (ESP) through NAT IPSec NAT Transparencyを使用します。

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透過機能により、NATとIPSec間の多くの既知の非互換性に対処する際に、IPSecトラフィックがネットワーク内のNATポイントまたはPATポイントを通過できるようになりました。

Q. NAT-PT を実装するにはどうすればよいですか。

A.NAT-PT(Network Address Translation—Protocol Translation)は、RFC 2765およびRFC 2766で定義されているIPv6-IPv4変換メカニズムで、IPv6専用デバイスとIPv4専用デバイスの間での通信を可能にします（その逆も可）。

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にNATを適用できます。マルチキャスト用のダイナミックNATが実行されている場合、ルートマップは使用できません。この場合は、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のCiscoルータでの動作』を参照してください。宛先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(MSRR)ソリューションでNATを使用します。

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。

A.SNATは、動的にマッピングされたNATセッションに対する継続的なサービスを可能にします。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に相談した後にのみ実施する必要があります。

次のシナリオではSNATが推奨されます。

- HSRPとは異なり、一部の機能が存在しないため、プライマリ/バックアップは推奨モードではありません。
- 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設計されていないため、次のテストは成功しないものと予想されます。

- トラフィックがある間にNATエントリがクリアされる場合。
- トラフィックがある間にインターフェイスパラメータ（IPアドレスの変更、shut/no-shutなど）が変更されたとき。
- SNAT specificclearorshowcommandsは適切に実行されるとはかぎらないため、推奨されません。SNAT relatedclearandshowcommandsの一部は次のとおりです。

```
clear ip snat sessions *
clear ip snat sessions
```

```
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>
```

- ユーザがエントリをクリアする場合は、**clear ip nat trans forcedorclear ip nat trans *コマンドを使用できます。エントリを表示する場合は、show ip nat translation、show ip nat translations verbose**、および**show ip nat** statscommandsコマンドを使用できます。*service* internalisが設定されている場合は、SNAT固有の情報も表示できます。
- バックアップルータでNAT変換がクリアされることは推奨されません。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は同じである必要があります。両方のルータで同じイメージを実行する必要があります。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はありますか。

A.はい。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. **permit ip any any** でNAT用のACLを使用すると、予期しない結果が生じる可能性があります。12.4(20)T以降では、NATはローカルに生成されたHSRPおよびルーティングプロトコルパケットが外部インターフェイスから送信された場合、それらのパケットと、NATルールに一致するローカルで暗号化されたパケットを変換できます。
3. NATの重複ネットワークがある場合は、**match-in-vrfkeyword**を使用します。異なるVRFのオーバーラップするVRFスタティックNATエントリに対して**match-in-vrfkeyword**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。

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf


Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

4. 同じアドレス範囲を持つNATプールは、**match-in**-vrfkeywordを使用しない限り、**異なるVRFで使用すること**はできません。以下に、いくつかの例を示します。

```
ip nat pool poolA 172.31.1.1 172.31.1.10 prefix-length 24
ip nat pool poolB 172.31.1.1 172.31.1.10 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:CLI設定は有効ですが、**match-in-vrf** キーワードを使用しない場合、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使用してISPのロードバランシングを展開する場合、ベストプラクティスは、ACL照合に対するインターフェイス照合で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

- テクニカル サポートとドキュメント – Cisco Systems

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。