VoIP における NAT

内容

概要

このドキュメントでは、CUBE (Cisco Unified Border Element) として動作しているルータでの

NAT（ネットワークアドレス変換）動作、CME または CUCME（Cisco Unified Cummunication Manager Express）、ゲートウェイおよび CUSP（Cisco Unified SIP Proxy）について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SIP（Session Initiation Protocol）
- Voice over Internet Protocol
- ルーティング プロトコル

使用するコンポーネント

このドキュメントの情報は、次に基づくものです。

- 任意の IOS バージョン 12.4T 以上。
- 任意の CME バージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

ネットワーク アドレス変換は、異なるアドレス空間を使用してネットワーク間を行き来するパケットの IP アドレスを変換する一般的な手法です。このドキュメントの目的は、NAT を再確認することではありません。シスコの VoIP ネットワークで使用される NAT の包括的な評価を行います。 さらに、範囲は MS 音声テクノロジーを構成するコンポーネントに限定しています。

- NAT は基本的に、パケット内の IP アドレスを異なる IP アドレスに置き換えます。
- プライベート サブネットの複数のホストが単一のパブリック IP アドレスを*共有（つまり、単一のパブリック IP アドレスのように表示）してインターネットにアクセスできるようにします。*
- 通常、NAT の設定は、内部ホストの IP アドレスのみを変更します。
- NAT は双方向です。A が内部インターフェイスの B に変換されると、外部インターフェイスに到達している B は A に変換されます。
- RFC1631

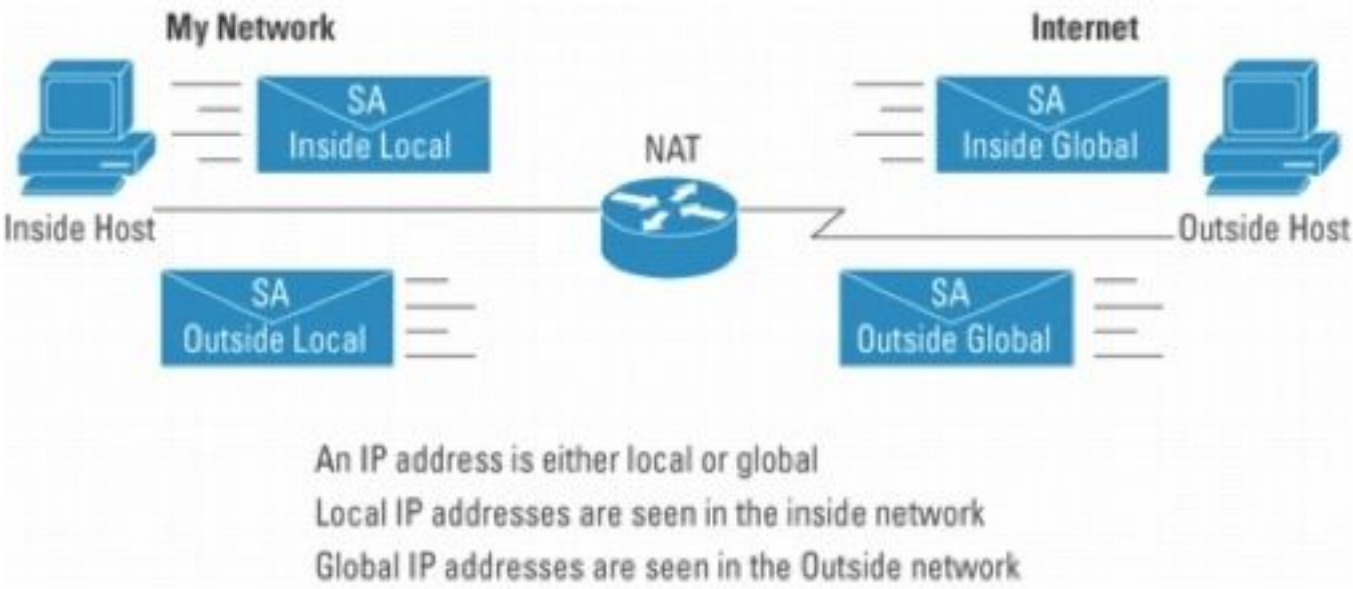

図 1：

注:NATは、プライベートアドレス空間を使用してIPパケットをネットワークにルーティングする際の補助手段と考えると役立つ場合があります。つまり、NAT はルーティングできないアドレスをルーティング可能にします。

図 2 は、次の図で参照されるトポロジを示しています。

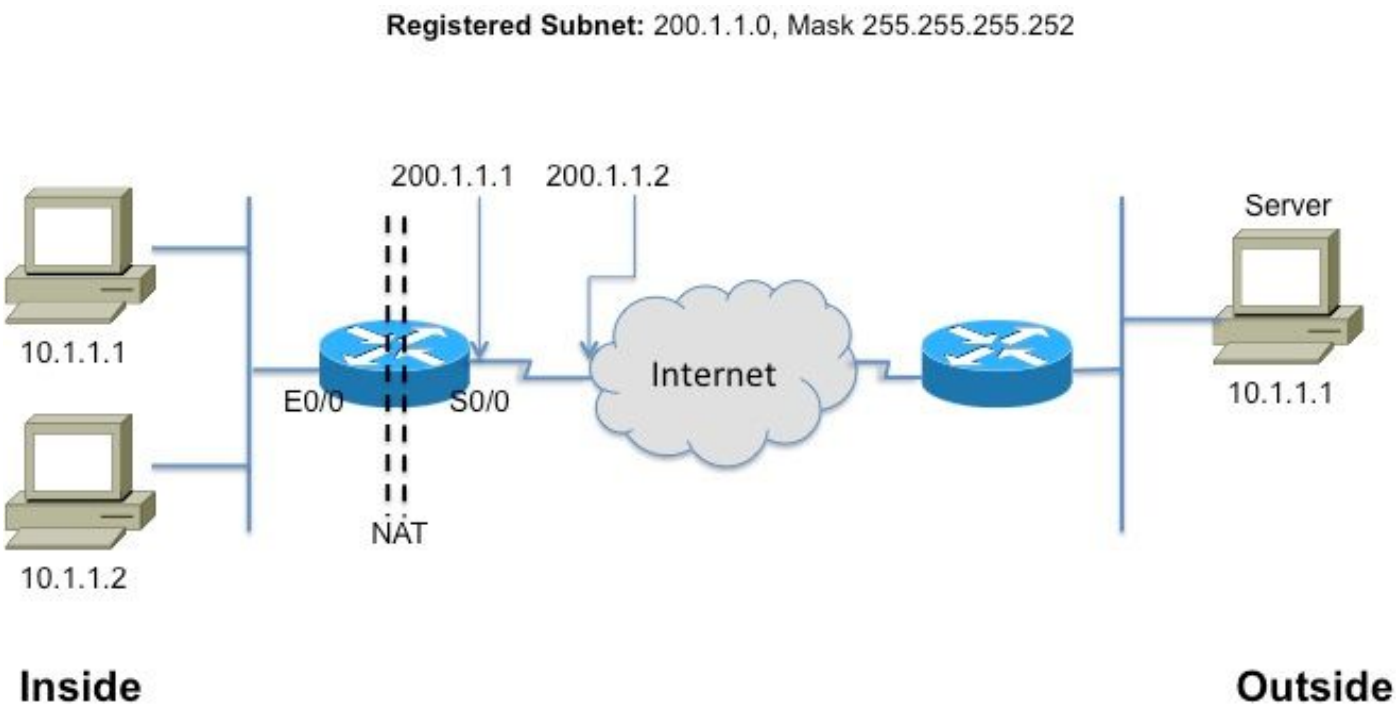

図 2

この用語集は、NAT の

- **内部ローカル アドレスについて理解し説明するための基礎となります：内部ネットワークのホストに割り当てられた IP アドレス。**通常、このアドレスはプライベートアドレス空間からのものです。
- **内部グローバルアドレス**:NICまたはサービスプロバイダーによって割り当てられるルーティ

ング可能なIPアドレスで、外部ネットワークへの1つ以上の内部ローカルIPアドレスを表します。

- **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：ホスト所有者によって、外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、グローバルにルーティング可能なアドレス、またはネットワーク空間から割り当てられます。

注:これらの用語を理解してください。NAT のメモやドキュメントはこれらを参照しています。

スタティック NAT

これは NAT の最もシンプルな形式で、各々の内部アドレスは静的に外部アドレスに変換されます（その逆も同様です）。

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

図 3

上記の変換のための設定の CLI は次のとおりです。

```
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 200.1.1.251 255.255.255.252
 ip nat outside < – 必須![2]
ip nat inside source static 10.1.1.2 200.1.1.2
ip nat inside source static 10.1.1.1 200.1.1.1
```

ダイナミック NAT

ダイナミック NAT では、各内部ホストはアドレス プールからのアドレスにマッピングされます

。

- 内部グローバル アドレス プールから IP アドレスを割り当てます。
- 新しいパケットが依然として別の内部ホストから到達し、それが NAT エントリを必用としますが、すべてのプール済み IP アドレスが使用されている場合は、ルータはパケットを単純に破棄します。
- 基本的に、内部グローバル アドレス プールは、インターネットを同時に使用する必要のある、同時ホストの最大数と同じくらいの大きさである必要があります。

次の CLI は、ダイナミック NAT の設定を示しています

```
ip nat pool fred 200.1.1.1 200.1.1.2 netmask 255.255.255.252
!
!
ip nat inside source list 1 pool fred
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
```

NAT オーバーロード (PAT)

(IP アドレスの) プールが、変換される必要のあるアドレスのセットより小さい場合、この機能が役立ちます。

- 1 つのみまたは少数の外部アドレスに NAT される複数の内部アドレス
- PAT (ポート アドレス変換) では、内部グローバル IP アドレスの一意な送信元ポート番号を使用して、変換を区別します。ポート番号は 16 ビットでエンコードされるため、合計数は理論上 IP アドレスごとに 65,536 と同じくらい高くなります。PAT は元の送信元ポートを維持しようとし、この送信元ポートがすでに割り当てられている場合、PAT は最初の使用可能なポート番号を見つけようとします。
- NATオーバーロードは65,000を超えるポートを使用できるため、多くの登録済みIPアドレスを必要とせずに拡張できます。多くの場合、必要なのは1つの外部グローバルIPアドレスだけです。

図 4 は PAT を示しています。

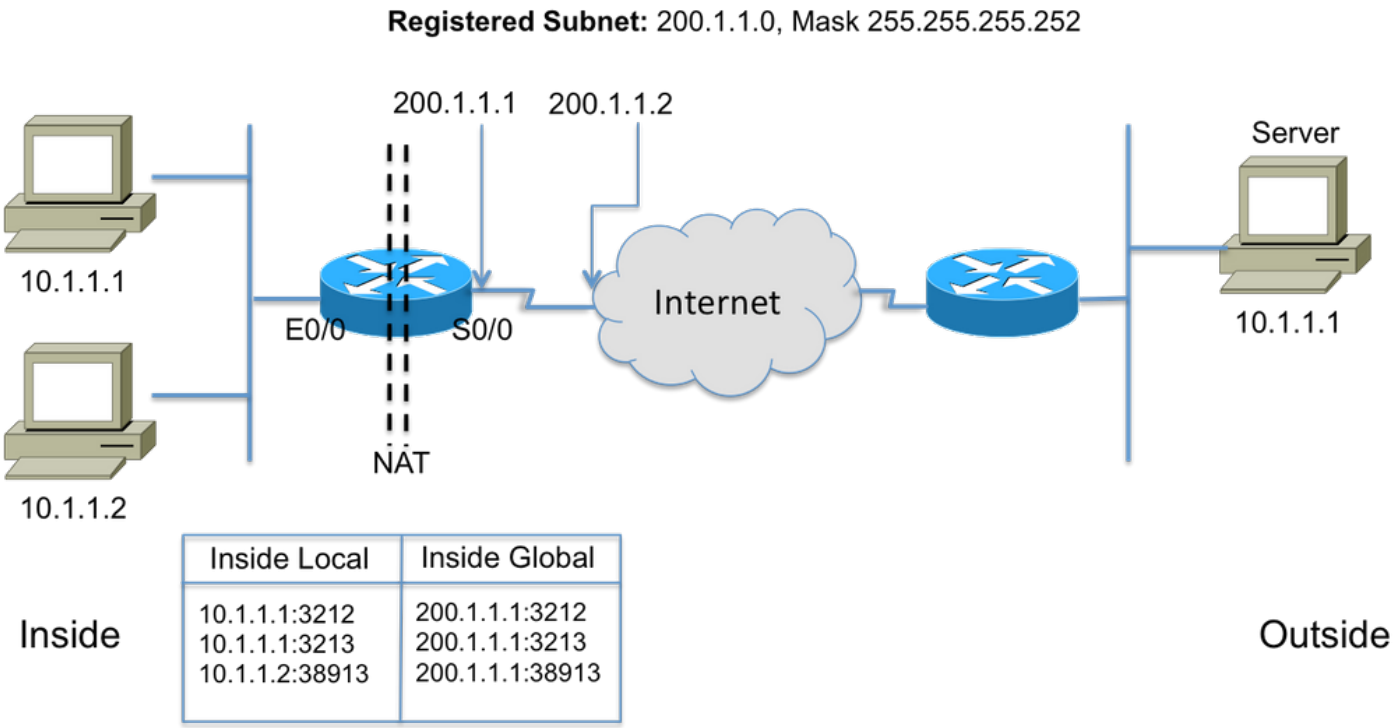

図 4

NAT コマンド オプション

シスコの NAT 導入は、オプションのホストが非常に多様です。少数については下記で示していますが、拡張の詳細な一覧については、「 http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html 」を参照してください。

- ポートによるスタティック変換 – 特定のポート宛ての着信パケット(例： SMTPサーバの場合はポート25)が特定のサーバに送信されます。
- ルート マップのサポート：フィルタ/ACL の設定での柔軟性
- より柔軟なプール設定：不連続なアドレスの範囲を許可します。
- ホスト番号保持：「ネットワーク」部分を変換し、「ホスト」部分を保持します。

NAT ピンホール

NAT 用語のピンホールは、<host IP port> および <global address, *global port*> *タプル間のマッピングを参照します。* これによって、NAT デバイスは受信メッセージの (*グローバル ポートとなる*) *宛先ポート番号を使用し、セッションを発信したホスト IP およびポートに宛先をマッピングし直すことができます。*ピンホールは不使用期間後にタイムアウトし、パブリック アドレスは NAT プールに戻されることに注意してください。

VoIP における NAT

では、VoIP ネットワークにおける NAT の問題や関心事項は何ですか。もちろん、これまでディスカッションしてきた (基本的な NAT と呼ばれる) NAT は IP パケットのヘッダー内の IP アドレスのみを変換し、チェックサムを再計算することを思い起こしてください。ですが、VoIP シグ

ナリングは、シグナリング メッセージの本文に組み込まれたアドレスを運びます。つまり、レイヤ 5 で発生することです。

図 5 は、組み込まれた IP アドレスが変換されないままにされている影響を示しています。コール シグナリングは正常に完了していますが、サービス プロバイダーの SIP プロキシは、コール エージェントにより送信されたメディアのアドレスにメディア パケット（RTP）をルーティングしようとするのに失敗しています。

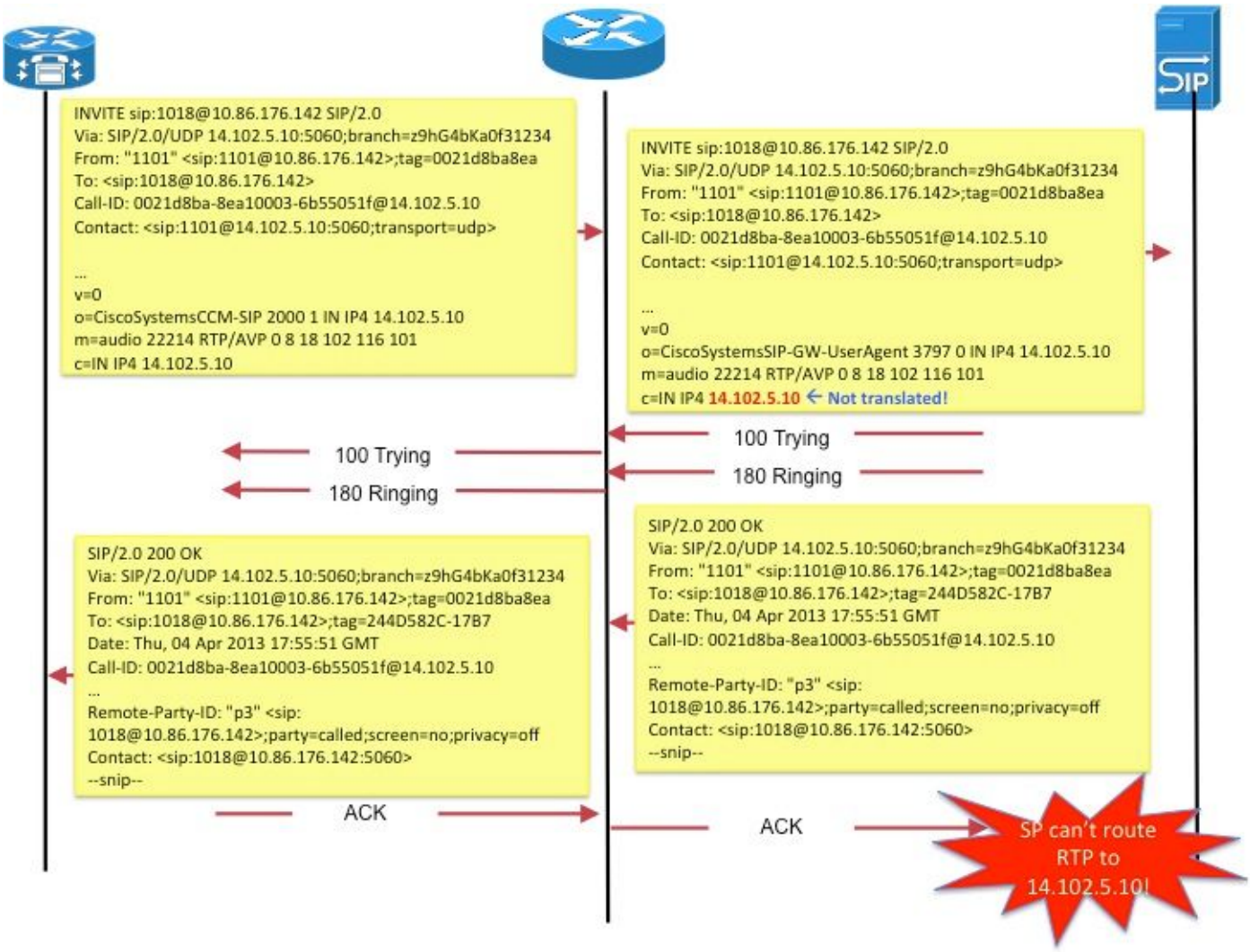

図 5：

もう 1 つの例は、SIP エンドポイントの SDP の [Contact:]フィールドの使用です。これは、エンドポイントが新しい要求のシグナリング メッセージを受信することを希望するアドレスに通信するために行います。

これらの問題は、アプリケーション レイヤ ゲートウェイ（ALG）という機能によって処理されます。

ALG

ALG は、（たとえば SIP）をサポートし、プロトコル パケット検査およびそれを介したトラフィックの「フィックスアップ」を行う、特定のアプリケーションで使用されるプロトコルを理解しています。さまざまなフィールドが SIP コール シグナリングに対してフィックスアップされる仕組みの詳細については、「http://www.voip-info.org/wiki/view/Routers+SIP+ALG」を参照してくだ

さい。

シスコのルータでは、ALG SIP のサポートは、標準の TCP ポート 5060 でデフォルトで有効にされています。SIP シグナリングに対して標準でないポートをサポートするためには、ALG を設定することができます。「http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html」を参照してください。

> **注意**:注意が必要です。さまざまな VoIP プロトコルに対して、組み込まれたどのフィールドが変換される必要があるかを詳述する RFC や他の標準はありません。その結果、実装は機器のベンダー間で異なり、相互運用性の問題（および TAC のケース）を招いてます。

ゲートウェイ

ゲートウェイは、定義上は、IP-to-IP デバイスではないため、NAT は適用されません。

CME

ドキュメントのこのセクションでは、CME とのコール シナリオを再確認し、なぜ NAT を使用する必要があるかを理解します。

シナリオ 1ローカル フォン

シナリオ 2 リモート フォン（パブリック IP アドレスを持つ）

シナリオ 3 リモート テレワーカー

> **注**：すべての場合、音声を流すためには、CMEのIPアドレスがルーティング可能である必要があります

Local

このシナリオ（図 6）では、コールに関連する 2 台の電話は、プライベート IP アドレスを持つ skinny フォンです。

図 6

注:同じCMEシステム内の別のSkinny電話機とのコールで接続されているSkinny電話機は、メディアパケットを別の電話機に直接送信することに注意してください。つまり、ローカル フォンどうしの RTP は、CME を通過しません。

したがってこの場合では、NAT は適用されないか必要とされません。

注:CMEは、コールに関係する2台の電話が両方ともskinnyと同じネットワークセグメント内にあるかどうかに基づいて、メディア(RTP)を直接実行する必要があるかどうかを判断します。そうでない場合は、CME は RTP パスに自身を挿入します。

ローカルとリモート

このシナリオ (図 7) では、CME は、電話からの RTP が CME で終了されるように RTP ストリームに自身を挿入します。CME は、他の電話へのストリームを再発信します。CME は、内部 (プライベート) ネットワークおよび外部ネットワーク両方の一員であり、その内部アドレスを内部の電話に、外部 (パブリック) アドレスを外部の電話に送信するため、ここでも NAT は不要です。

ただし、UDP/TCP ポートは (RTP だけでなくシグナリングも)、リモート IP フォンと CME 送信元 IP アドレス間でオープンである必要があることに注意してください。これは、ファイアウォールまたはその他のフィルタリング デバイスは、問題になっているポートを許可するように設定されるということです。

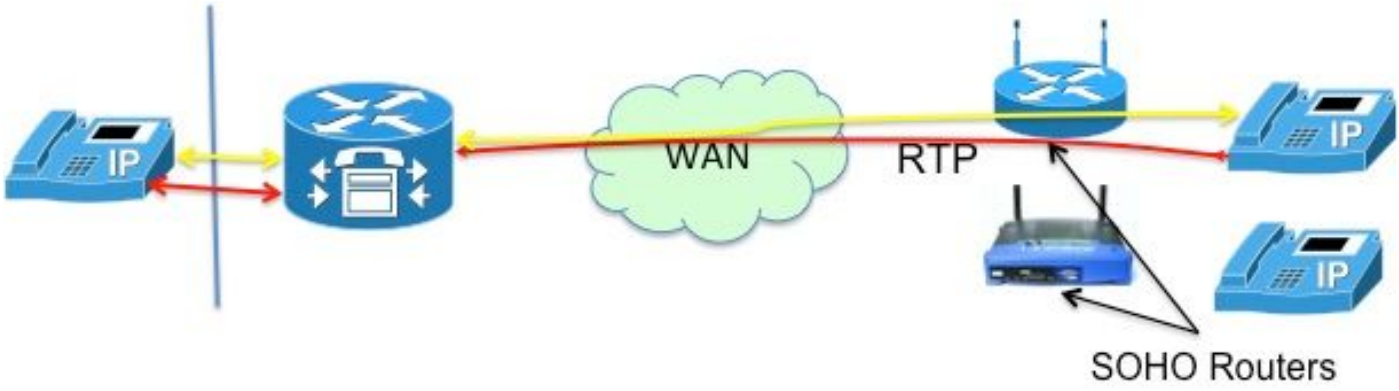

図 7

注:シグナリング[メッセージ]は常にCMで終端されることに注意してください

リモート テレワーカー

これは WAN を超えて CME に接続する IP フォンを参照し、CME ルータからリモートにあるオフィスを持つテレワーカーをサポートします。最も一般的な設計は、ルーティング可能な IP アドレスを持つ電話と、プライベート IP アドレスを持つ電話を必要とするものです。

パブリック (読み取り：ルーティング可能な) IP アドレスを持つリモート フォン

コールに関わる両方の電話がパブリックで、ルーティング可能な IP アドレスで設定されると、メディアは図 8 の電話間で直接フローできます。 したがって、再度、NAT は必要ではありません

。

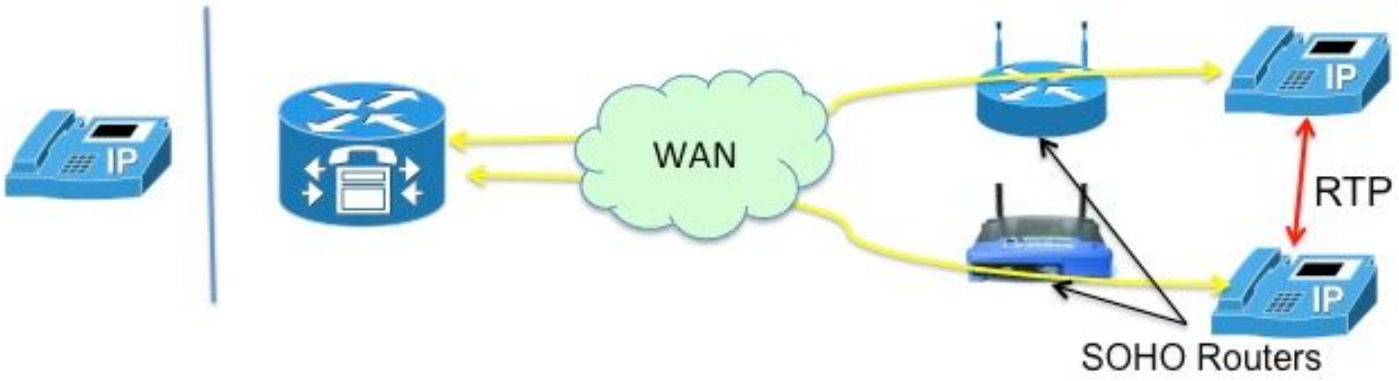

図 8

プライベート IP アドレスを持つリモート フォン

このシナリオでは、コールはプライベート IP アドレスで設定された skinny 電話間で信号が送信されます。 ホーム オフィス (SOHO) のルータは、一般に「SCCP 認識型」ではない傾向があります。つまり、SCCP メッセージに組み込まれた IP アドレスの変換ができません。これは、コールのセットアップ完了時に、電話は相互のプライベート IP アドレスで終了することを意味しています。 両方の電話がプライベートであるため、CME は、音声が電話間で直接フローするように、それらの間でコールに信号を送ります。ただし、次の回避策のいずれかを実行しない限り、片方向または無方向の音声が発生します(プライベートIPアドレスは定義上、インターネット上でルーティングできません)。

·SOHO ルータでスタティック ルートを設定する

·電話に IPsec VPN 接続を確立する

これを解決するより優れた方法は、「mtp」を設定することです。mtp コマンドによって、リモート フォンからのメディア (RTP) パケットが CME ルータを介してトランジットされるようになります (図 9) 。

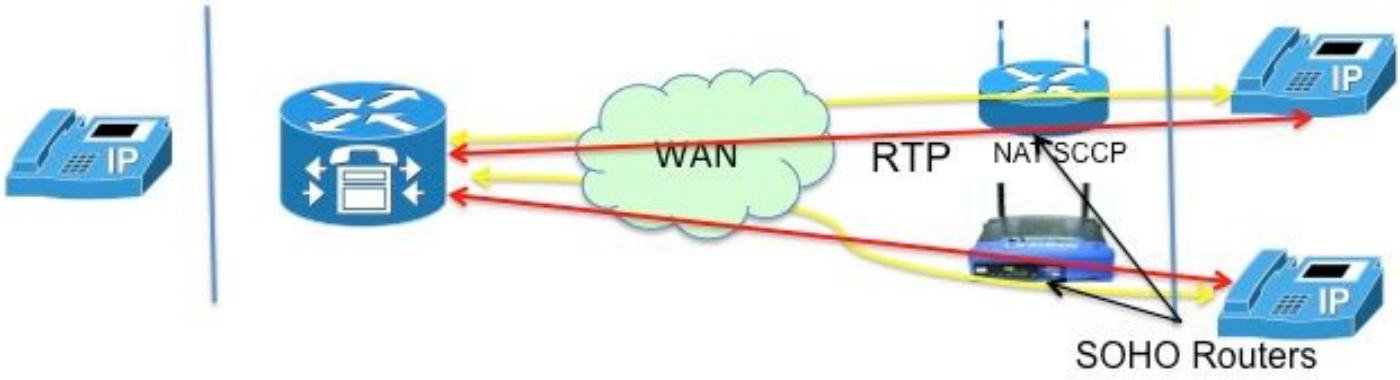

図 9

「mtp」ソリューションは、ファイアウォール ポートを開通した複雑さゆえに優れています。WAN を超えてフローするメディア パケットは、ファイアウォールによって遮断される場合があります。これはファイアウォールでポートを開く必要があるということですが、どのポートでしょうか。CME が音声をリレーしていれば、ファイアウォールは RTP パケットを通過させるように簡単に設定することができます。 CME ルータは、***特定の UDP ポート (2000) をメディア パケット用に使用します。***したがって、ポート 2000 へ、およびポート 2000 からパケットを許可す

るだけで、すべての RTP トラフィックが通過できます。

図 10 では mtp を設定する方法を示しています。

```
ephone 1

 mac 1111.2222.3333

 type 7965

 mtp

 button 1:1
```

図 10

mtp ですべてがうまくいくとは限りません。mtp が望ましくない場合がある状況があります。

- MTP は CPU 使用率を大きく上昇させます。
- マルチキャスト MOH は一般に、WAN を超えて転送できません。マルチキャスト MOH 機能は電話に対して MTP が有効にされているかどうかを確認し、有効にされている場合はその電話 L に MOH を送信しません。

マルチキャスト パケットを転送**できる WAN 設定があり、ファイアウォールを介して RTP パケットを許可できる場合は、MTP を使用しないように決定できます。**

リモート SIP フォン

SIP フォンが上述のシナリオで述べられなかったことに注意してください。これは、電話の 1 つが SIP フォンである場合、CME は音声パスに自身を挿入するという事実によるためです。つまり、NAT が不要な、上述されている local-to-remote のシナリオになります。

CUBE

CUBE は、すべてのセッションを終了し再発信して、NAT および PAT 機能を本質的に実行します。CUBE は、自身のアドレスを通信相手のエンドポイントのアドレスに代替し、効率的にこのエンドポイントのアドレスを非表示に（変換）します。

したがって、NAT は CUBE 機能では必要ありません。NAT が CUBE で必要な VoIP サービスのシナリオを、次のセクションで説明します。

ホスト型 NAT トラバーサル

ホスト型テレフォニー サービスの簡単なバックグラウンドがわかれば、この機能の原理を理解できます。

ホスト型テレフォニー サービスは、ほとんどの周辺機器がサービス プロバイダーの場所にある VoIP サービスの新しい形式です。これらは、基本的な NAT のみ（つまり L3/L4 での NAT）を実装するホーム ゲートウェイ（HGW）と連携します。たとえば、Verizon は自宅で FiOS サービスを提供する光ネットワーク ターミナル（ONT）をインストールします。音声コールは、ONT に組み込まれている SIP プロセスを使用して信号が送信されます。SIP シグナリングは、Verizon

のプライベート IP ネットワークを新しいソフト スイッチに作り直し、サービスと制御を提供して、他の FiOS のデジタル音声の顧客または従来の電話の顧客に対して音声通信を確立します。

ホスト型テレフォニー サービス用の主要プロバイダーの要件を次に示します。

- リモート NAT トラバーサル：NATおよびファイアウォール デバイス（"ALG" をリモートで実行）を活用するエンドポイントにクラス 5 のサービスを配布する能力（NAT レイヤ 3 のみを実行可能）
- Co-media のサポート：IP ネットワークにメディアをルートし直す意義がない、同じ場所に設置されたデバイス間でメディアを送信する能力
- 追加された設備はなく、CPE を追加する必要性はありません。

上述を前提とすると、このようなサービスを実装するのにどのようなオプションがありますか。

- HGW を高価な ALG に置き換える。
- セッション ボーダー コントローラ（SBC）を使用してパケットに組み込まれた SIP ヘッダーを変更する。これには、非常に安全な、フォールトトレラント設定の、SIP をサポートするネットワーク ホスト型キャリア グレード製品が含まれます。この解決策は NAT SBC を参照しています。

NAT SBC オプションは、上記のプロバイダー要件を満たしています。

NAT SBC

NAT SBC は次のように機能します（図 11）。

1. アクセス ルータは L3/L4 の IP アドレスのみを変換する
2. SIP メッセージ内の IP アドレスは変換されない
3. SBC NAT は組み込まれた IP アドレスを傍受し変換する。 SBC は **200.200.200.10** を宛先とする SIP パケットを確認する瞬間に、nat-sbc コードでキックします。
4. メディアは変換されず、電話 [5] 間で直接実行される。

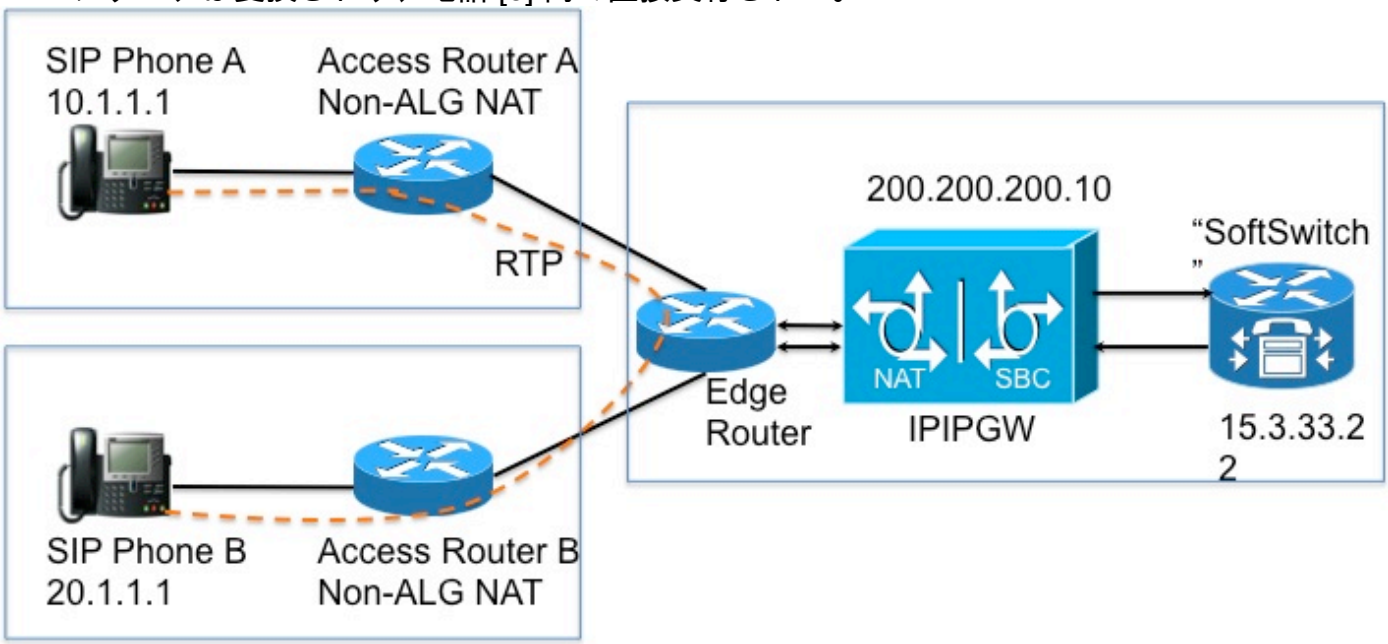

図 11

設計メモ

- IP アドレス 200.200.200.10（図 12）は、NAT SBC のどのインターフェイスにも割り当てされません。これは、SIP フォン A および SIP フォン B が、シグナリング メッセージを送信する「プロキシ」のアドレスとして設定されます。
- ホーム デバイスは、特定の SIP/SDP *アドレスのみ*のフィールド（例、Call-Id:,O= , Warning:headers & branch= parameter.maddr= and received= パラメータは特定のシナリオのみで処理）を変換しません。 これらのフィールドは認証を破るため、プロキシ認証と認証変換を除き、NAT SBC によって処理されます。
- ホーム デバイスが PAT を行うように設定されると、ユーザ エージェント（電話とプロキシ）は、対称シグナリング [6]、対称、およびアーリー メディア（early media）をサポートする必要があります。NAT SBC ルータの上書きポートを設定する必要があります。
- 対称シグナリング、対称メディア、およびアーリー メディアのサポートがない場合、中継ルータを PAT なしで設定する必要があり、上書きアドレスは NAT SBC に設定します。

コンフィギュレーション

一般的な NAT SBC の設定例は次のとおりです。

```
ip nat sip-sbc

  proxy 200.200.200.10 5060 15.3.33.22 5060 protocol udp

  call-id-pool call-id-pool

  session-timeout 300

  mode allow-flow-around

  override port

!

ip nat pool sbc1 15.3.33.61 15.3.33.69 netmask 255.255.0.0

ip nat pool sbc2 15.3.33.91 15.3.33.99 netmask 255.255.0.0

ip nat pool call-id-pool 1.1.1.1 1.1.255.254 netmask 255.255.0.0

ip nat pool outside-pool 200.200.200.100 200.200.200.200 netmask 255.255.255.0

ip nat inside source list 1 pool sbc1 overload

ip nat inside source list 2 pool sbc2

ip nat outside source list 3 pool outside-pool add-route

ip nat inside source list 4 pool call-id-pool

!

access-list 1 permit 10.1.1.0 0.0.0.255

access-list 1 permit 171.1.1.0 0.0.0.255

access-list 2 permit 20.1.1.0 0.0.0.255

access-list 2 permit 172.1.1.0 0.0.0.255

access-list 3 permit 15.4.0.0 0.0.255.255

access-list 3 permit 15.5.0.0 0.0.255.255
```

```
access-list 4 permit 10.1.0.0 0.0.255.255

access-list 4 permit 20.1.0.0 0.0.255.255
```

SBC NAT によるコール フロー

図 13 と図 14 では変換に関するコール フローを示します。次の点に注意する必要があります。

- 登録では、ソフト スイッチは 2 台の電話を次のようにメモします。
  --SIP フォン A – 15.3.33.62 2001

  --SIP フォン B – 15.3.33.62 2002

- このコール フローでは、SBC NAT は実質的にはメディア IP アドレスを変換しないままにします。

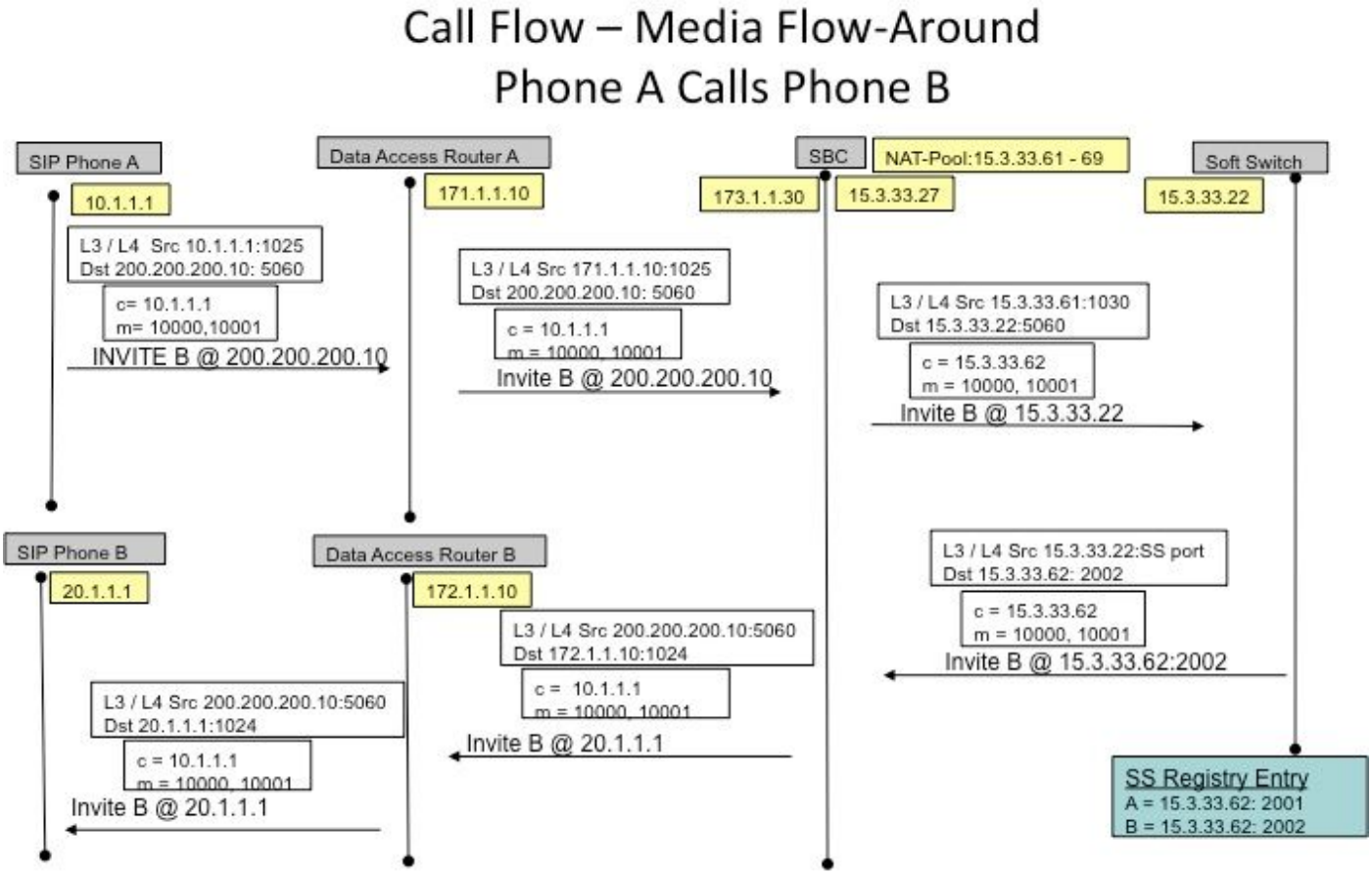

図 13

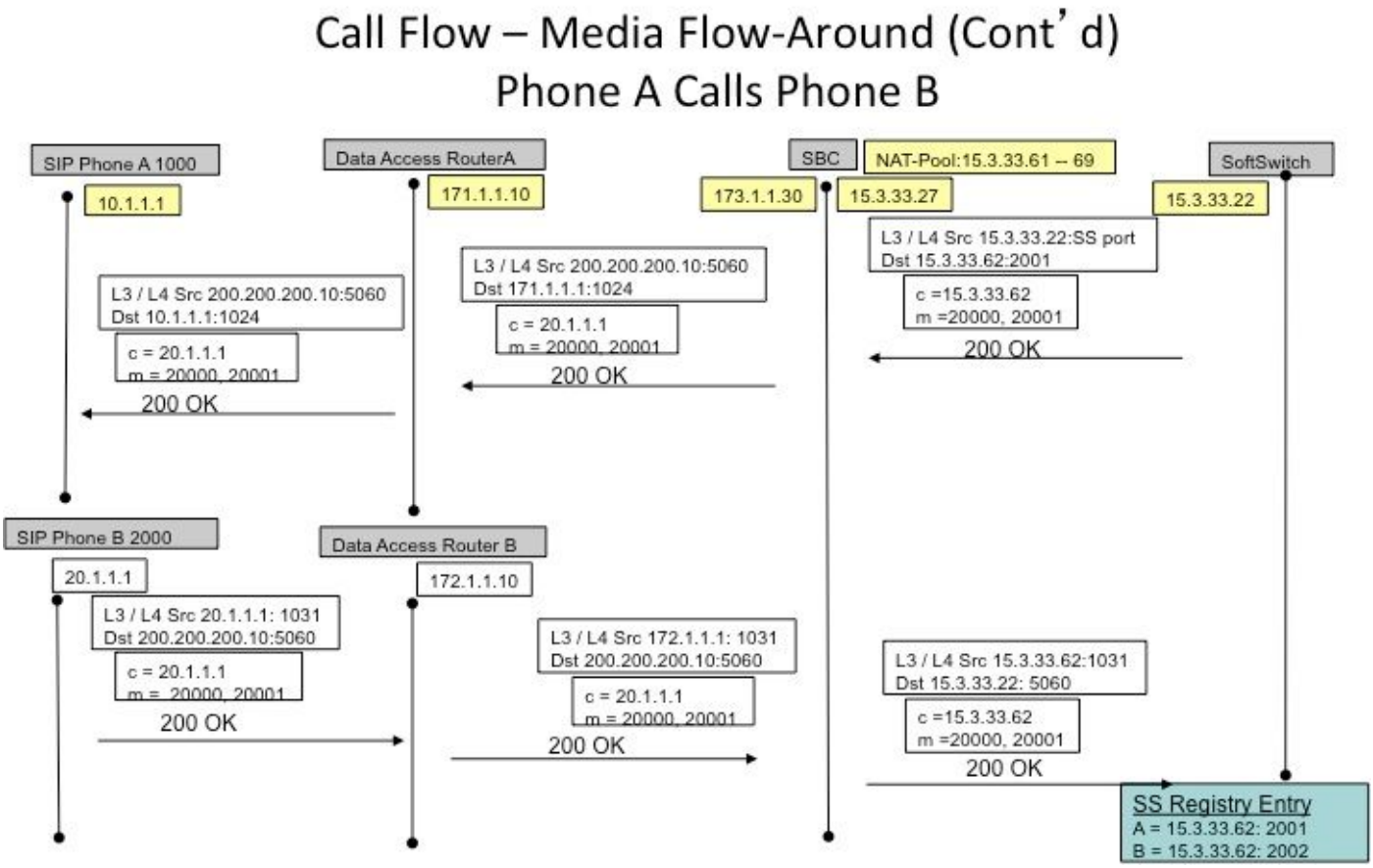

図 14

SIP 登録

以前のバージョン（SBC NATの）では、SIPエンドポイントはキープアライブパケットを送信して、SIP登録ピンホールを開いたままにしておく（着信コールなどのトラフィックをout->inフローに許可する）必要がありました。キープアライブパケットは、エンドポイントまたはレジストラ（ソフトスイッチ）によって送信された任意のSIPパケットである可能性があります。 最新のバージョンではこの必要性が取り除かれ、ピンホールを開けたままにするため、（ソフト スイッチとは対照的に）NAT-SBC 自体によるエンドポイントの頻繁な再登録が強制されています。

> **注：**期限切れの登録ピンホールの兆候は、コール シグナリングがランダムに失敗し、不明瞭である場合があります。

CUSP

CUSPは論理ネットワークという概念を持っています。論理ネットワークとは、同様に扱われるローカルインターフェイスの集合を指します(たとえば、 インターフェイス、ポート、トランスポート（リスニング用）ルーティングの目的で使用されます。論理ネットワークを CUSP で設定する場合、NAT を使用するように設定できます。設定されると、SIP ALG が自動的に有効になります。これは特定の論理ネットワークの場合に便利です。

トラブルシューティング

症状

一方向または両方向でコールが失敗するのは、明らかな症状である場合があります。より明らかでない症状には次があります。

- 片通話
- 転送が片通話になる
- 音声中断
- SIP 登録の損失

Show コマンドと debug コマンド

- `deb ip nat  [sip | skinny]`
- `show ip nat statistics`
- `show ip nat translations`

チェックするべき事柄

- 設定には **ip nat inside** または **ip nat outside** インターフェイス サブコマンドが含まれるようにします。これらのコマンドはインターフェイスで NAT を有効にし、内部/外部指定が重要です。
- スタティック NAT では、**ip nat source static コマンドは内部ローカルアドレスを最初に、内部グローバル IP アドレスを 2 番目にリストアップするようにします。**
- ダイナミック NAT では、任意の NAT 変換が発生する前に、内部ホストによって送信されるパケットと一致するように設定された ACL が、このホストのパケットに一致するようにします。たとえば、10.1.1.1 の内部ローカル アドレスが 200.1.1.1 に変換される必要がある場合は、ACL が 200.1.1.1 でなく送信元アドレス 10.1.1.1 に一致するようにします。
- PAT のないダイナミック NAT では、プールに十分な IP アドレスがあるようにします。十分なアドレスがないという症状には、ダイナミック変換の一覧内の NAT プールで定義された範囲のアドレスがすべて表示されるだけでなく、**show ip nat statistics コマンドの出力の 2 番目のミス カウンタで値が増大することがあります。**
- PAT では、**ip nat inside source list コマンドに overload オプションを追加することを忘れがちです。**それなしでも NAT は機能しますが、PAT は機能せず、ユーザのパケットが変換されていなかったり、ホストがインターネットにたどりつけなくなることが多くあります。
- おそらく NAT は正しく設定されていますが、ACL がインターフェイスの 1 つに存在し、パケットを破棄します。インターフェイスに入るパケットの NAT の前、および、インターフェイスを出るパケットのアドレス変換後に、IOS は ACL を処理することに注意してください。
- WAN に面するインターフェイスで "ip nat outside" を設定することを忘れないでください（外部アドレスが変換されていない場合も）。
- NAT が設定され次第、show ip nat translations は何も表示しなくなります。一度 ping し、もう一度確認します。
- NAT-SBC の内部および外部インターフェイスで **wireshark トレースをつかみます。**

シナリオ

複数のシナリオのデバッグ出力を次に示します。これらはほとんど説明を必要としません。

基本的な NAT

基本的な NAT の設定とデバッグ行を次に示します。

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Serial0/1/0
 description **Line to FRS**
 ip address 100.10.10.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 encapsulation ppp
ip nat inside source list 91 interface Serial0/1/0 overload
access-list 91 permit 10.1.1.1

R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 100.10.10.1:7     10.1.1.1:7         200.200.200.2:7    200.200.200.2:7
icmp 100.10.10.1:8     10.1.1.1:8         200.200.200.2:8    200.200.200.2:8

R1#ping 200.200.200.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.200.2, timeout is 2 seconds:
!!!!!
R1# sho log
000044: *Apr 17 00:13:00.027: NAT: s=10.1.1.1->100.10.10.1, d=200.200.200.2
[40]
000045: *Apr 17 00:13:00.027: NAT*: s=200.200.200.2, d=100.10.10.1->10.1.1.1
[40]
```

Debug line for NAT on Incoming packet

SIP ALG

debug ip nat sip からの出力行を示します。この場合、送信パケットに組み込まれている IP アドレスが変換されます。

```
ip nat inside source static 10.1.1.1 20.1.1.1
------------------------------------------------------------------------
Sent: INVITE sip:1018@10.86.176.142:5060 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.1:5060;branch=z9hG4bK23C1ED01
Remote-Party-ID: "3196" <sip:3196@10.1.1.1>;party=calling;screen=no;privacy=off
From: "3196" <sip:3196@10.1.1.1>;tag=A9F3DB34-EEE
To: <sip:1018@10.86.176.142>
Date: Tue, 23 Apr 2013 17:53:02 GMT
Call-ID: 7A3AC014-AB7511E2-BE6BB2A0-B6AF1B2B@10.1.1.1
--snip--
Contact: <sip:3196@10.1.1.1:5060>
--snip--
v=0
o=CiscoSystemsSIP-GW-UserAgent 9771 5845 IN IP4 10.1.1.1
s=SIP Call
c=IN IP4 10.1.1.1
t=0 0
m=audio 16384 RTP/AVP 18 100 101
c=IN IP4 10.1.1.1
--snip-
------------------------------------------------------------------------
068441: Apr 23 13:53:02.477: NAT: SIP: [0] processing INVITE message
068442: Apr 23 13:53:02.477: NAT: SIP: [0] register:0 door_created:0
--snip--
068447: Apr 23 13:53:02.477: NAT: SIP: [0] translated embedded address 10.1.1.1->20.1.1.1
068448: Apr 23 13:53:02.477: NAT: SIP: [0] register:0 door_created:0
068449: Apr 23 13:53:02.477: NAT: SIP: [0] register:0 door_created:0
068450: Apr 23 13:53:02.477: NAT: SIP: Contact header found
068451: Apr 23 13:53:02.477: NAT: SIP: Trying to find expires parameter
068452: Apr 23 13:53:02.477: NAT: SIP: [0] translated embedded address 10.1.1.1->20.1.1.1
068453: Apr 23 13:53:02.477: NAT: SIP: [0] register:0 door_created:0
068454: Apr 23 13:53:02.477: NAT: SIP: [0] message body found
068455: Apr 23 13:53:02.477: NAT: SIP: Media Lines present:1
068456: Apr 23 13:53:02.477: NAT: SIP: Translated m= (10.1.1.1, 16384) -> (20.1.1.1, 16384)
068457: Apr 23 13:53:02.477: NAT: SIP: old_sdp_len:307 new_sdp_len :307
068458: Apr 23 13:53:02.477: //158107/79BF74A6BE66/SIP/Msg/ccsipDisplayMsg:
```

参考資料

概要：

- http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html
- **分析：** http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml

VoIP と NAT

- https://supportforums.cisco.com/docs/DOC-5406
- http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-security/id-60290html

NAT 機能のマトリックス

- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919.shtml
- http://www.cisco.com/en/US/technologies/tk648/tk361/tk438/technologies_white_paper09186a00801af2b9.html
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919shtml

ホスト型 NAT トラバーサル：

- www.tmcnet.com/it/0804/FKagoor.htm

NAT SBC

- EDCS-611622
- EDCS-526070

ALG：

- http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-0s/iadnat-applvlgw.html
- http://www.voip-info.org/wiki/view/Routers+SIP+ALG
- http://www.commpartners.us/knowledge/attachments/voip-nat.pdf
- http://www.cisco.com/en/US/partner/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html

CME

- http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/srnd/design/guide/security.html#wp1077376
- http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc_cucm.html

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。