VoIP の NAT

目次

概要

この資料は CUBE（Cisco Unified Border Element）として動作しているルータで NAT（ネットワークアドレス変換）動作を、CME または CUCME（Express Cummunication Cisco Unified マネージャ）、ゲートウェイおよび先端（Cisco Unified SIP Proxy）記述したものです。

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 IP（インターネット プロトコル）
- ルーティング プロトコル

使用するコンポーネント

この文書に記載されている情報は基づいています

- IOSバージョン 12.4T 以上に。
- 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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

異なるアドレス スペースを使用してネットワークの間で流れるパケットの IP アドレスを変換する広く使われた手法はネットワーク アドレス変換（NAT）あります。 この資料の目的は NAT を検討することではないです。 むしろ、この資料は Cisco の VOIPネットワークで使用されるように NAT の広範囲 の 評価を提供することを向けます。 なお、スコープは MS 音声 テクノロジーを構成するコンポーネントに制限されます。

- NAT は別の IP アドレスと基本的にパケット内の IP アドレスを取り替えます
- インターネットにアクセスするために（すなわちのように現われて下さい）単一 パブリック IPアドレスを*共有する*私用 サブネットの有効マルチプルホスト。
- 通常、NAT 設定変更内部ホストの IP アドレスだけ
- NAT は A に A が内部インターフェイスの B に変換されれば双方向、outside インターフェイスで着く B 変換されますです!
- RFC1631

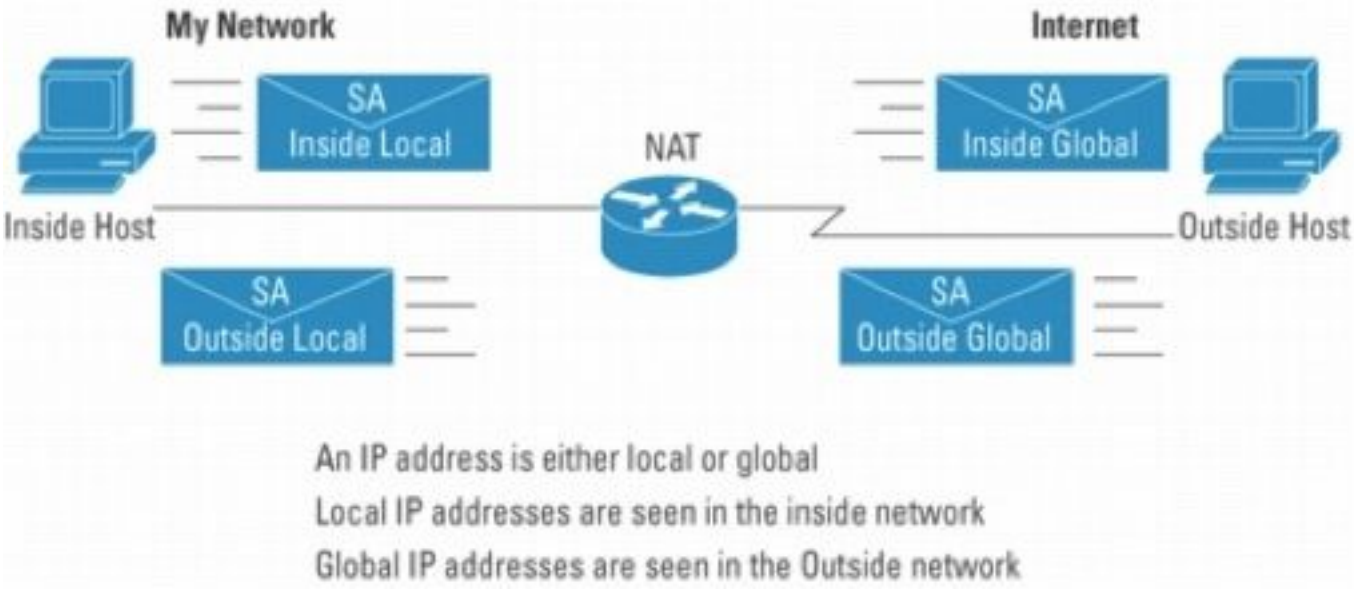

Figure 1

注: それはプライベートアドレス空間を使用してネットワークにおよびから IP パケットをルーティングするために援助として NAT を捉えるのを助けるかもしれません。 すなわち、NAT はルーティングが不可能なアドレスをルーティング可能にさせます

図 2 続く実例で参照されるトポロジーを示します。

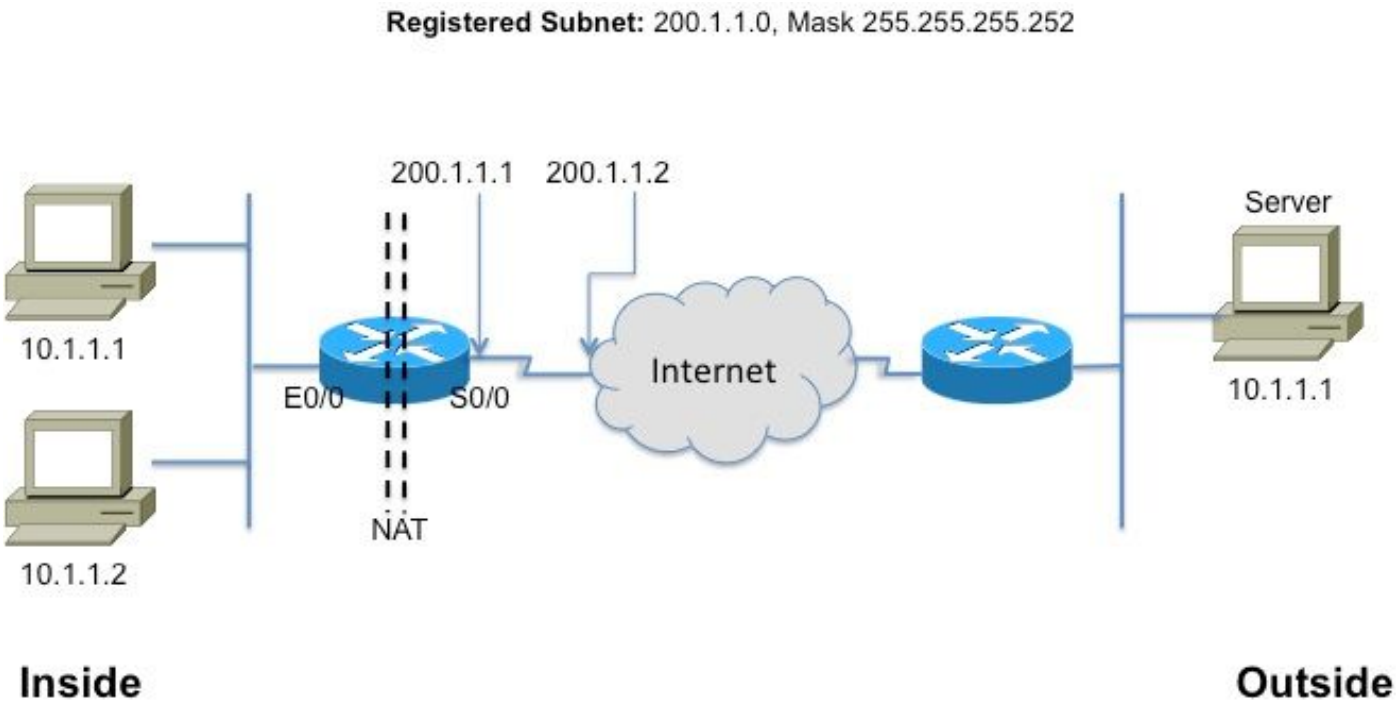

図 2

この用語集は基本的 NAT を理解し、記述するためにです

- **内部ローカルアドレス**：内部ネットワーク上のホストに割り当てられた IP アドレス。 通常、アドレスはプライベートアドレス空間からあります。
- **内部グローバルアドレス**—外界に 1つ以上の Inside Local IP アドレスを表す NIC か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IPアドレス。
- **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はなく、内部で経路指定可能なアドレス空間から割り当てられます。
- **外部グローバル アドレス**：外部ネットワーク上のホストにホストの所有者により割り当てられる IP アドレス。 このアドレスは、グローバルに経路指定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: これらの用語と快適になって下さい。 NAT のメモかドキュメントはそれらを示して確実です

スタティック NAT

これが外部アドレスに NAT の最も簡単な形式、各内部アドレスで静的に変換されるである（またその逆にも）。

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への CLI は次の通りです

interface Ethernet0/0

ip address 10.1.1.3 255.255.255.0

ip nat inside

!!

interface Serial0/0

IP アドレス 200.1.1.251 255.255.255.252

ip nat outside <---- 必須! [2]

ip nat inside ソース スタティック 10.1.1.2 200.1.1.2

ip nat inside ソース スタティック 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の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のプールから IP アドレスを割り当てます。
- 新しいパケットが更に別の内部ホストから、NAT エントリを着き、すべてのプーリングされた IP アドレスが使用中必要とするがなら場合、ルータはパケットを単に廃棄します。
- 基本的に、内部グローバルアドレスのプールはとインターネットを同時に利用する必要がある同時ホストの最大数大きい必要があります

次の CLI はダイナミック NAT を設定することを説明します

```
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 overload 設定（PAT）

（IP アドレス）のプールがアドレスのセットより小さいとき変換される必要があるこの機能は役立ちます。

- 複数の内部アドレスは外部アドレスただ 1 つまたは少数のにネットワークアドレス交換しました
- PAT （ポート アドレス変換）は変換の間で区別するのに Inside Global IP アドレスの固有 の送信元ポート番号を使用します。 ポート番号が 16 ビットで符号化されるので、総数は論理上 IP アドレスごとに 65,536 高い可能性があります。 PAT はこの送信元ポートが既に割り当てられた PAT 最初の利用可能なポート数を見つけるように試みればである場合オリジナルソースポートを維持するように試みます
- NAT overload 設定は 65,000 以上のポートをできま、多くの登録済みの IP アドレスを必要としないでよくスケーリングするようにそれが—多くの場合し使用、1 Outside Global IP アドレスだけ必要とします。

図 4 PAT を説明します。

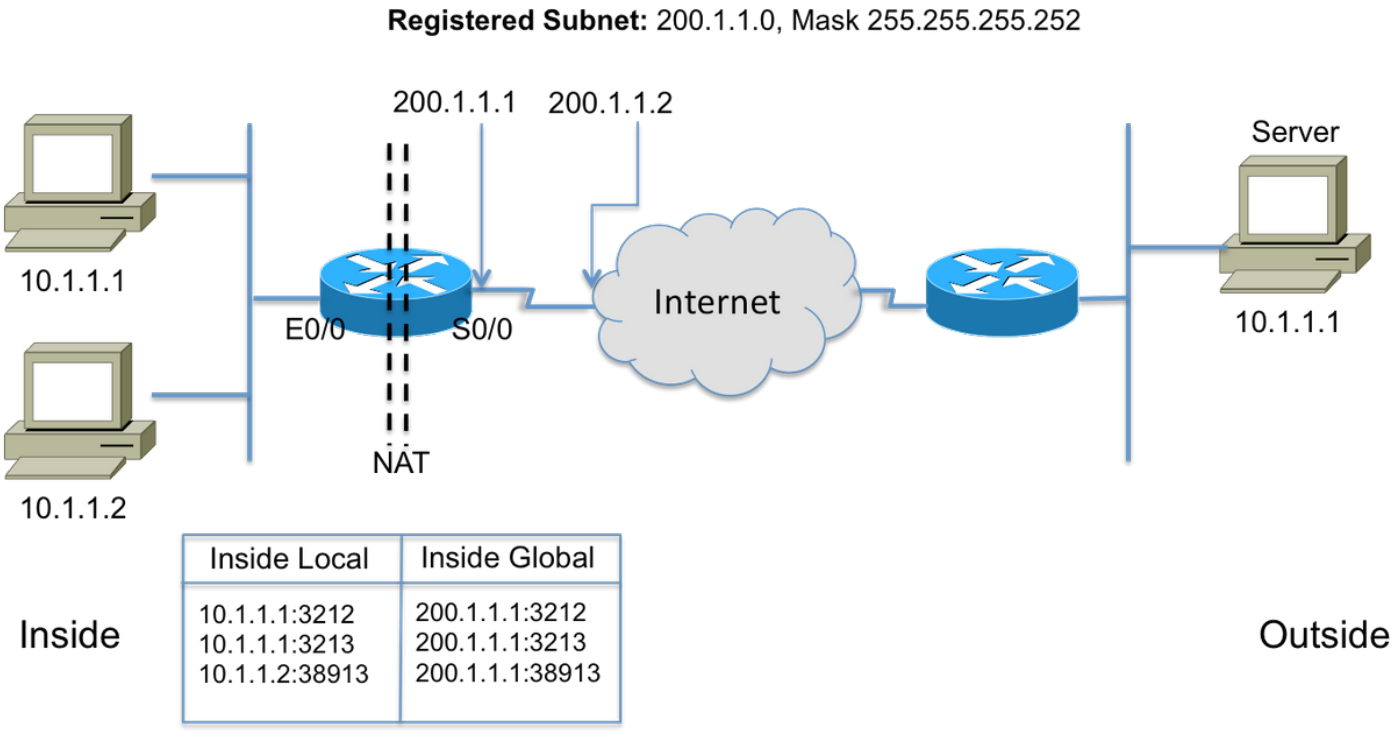

図 4

Nat コマンド オプション

Cisco NAT 実装はオプションの多くと非常に多用途です。 少数は下記にリストされていますが、機能拡張の完全なリストの詳細については http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html を示します。

- ポートが付いているスタティック トランスレーション–特定のポート（例えばポート 25、なぜなら SMTP サーバ）に当たった 着信パケットは特定のサーバに送信 しました。
- ルート マップのためのサポート-フィルター/ACL の設定の柔軟性
- 不連続アドレス範囲を許可するより適用範囲が広いプール設定。

- ホスト番号保持- 「ネットワーク」部品を変換して下さい、「ホスト」部品を保って下さい。

NAT ピンホール

NAT 語調のピンホールは <host IP、port> および <global アドレス間のマッピングを、*グローバル な* port> タプル示します。 それは NAT デバイスが（*グローバル な* ポートである）着信メッセージの宛先ポート番号 セッションを起こしたポートおよびホストIPアドレスに戻って宛先をマッピング するのに使用するようにします。 ピンホールが不使用の期間以降に時間を計り、パブリックアドレスが NATプールに返されることに注意することは重要です。

VoIP の NAT

このように、VOIPネットワークの NAT の問題および問題は何ですか。 それで、これまでのところ（losely 基本 NAT として referredto）変換する IPパケットヘッダーの IP アドレスだけを論議した再呼び出しし、*チェックサムを計算し直しますその NAT を、当然、VoIP シグナリングはシグナルメッセージの本文で*組み込まれるアドレスを運びますが。 すなわち、レイヤ5 で

図 5 組み込み IP アドレスを未翻訳に残す効果を説明します。 呼出し シグナリングは成功した完了しまが、サービスプロバイダーの SIP プロキシは失敗しま Call Agent によって送信 されるメディア アドレスにメディア（RTP）パケットをルーティングすることを試みます!

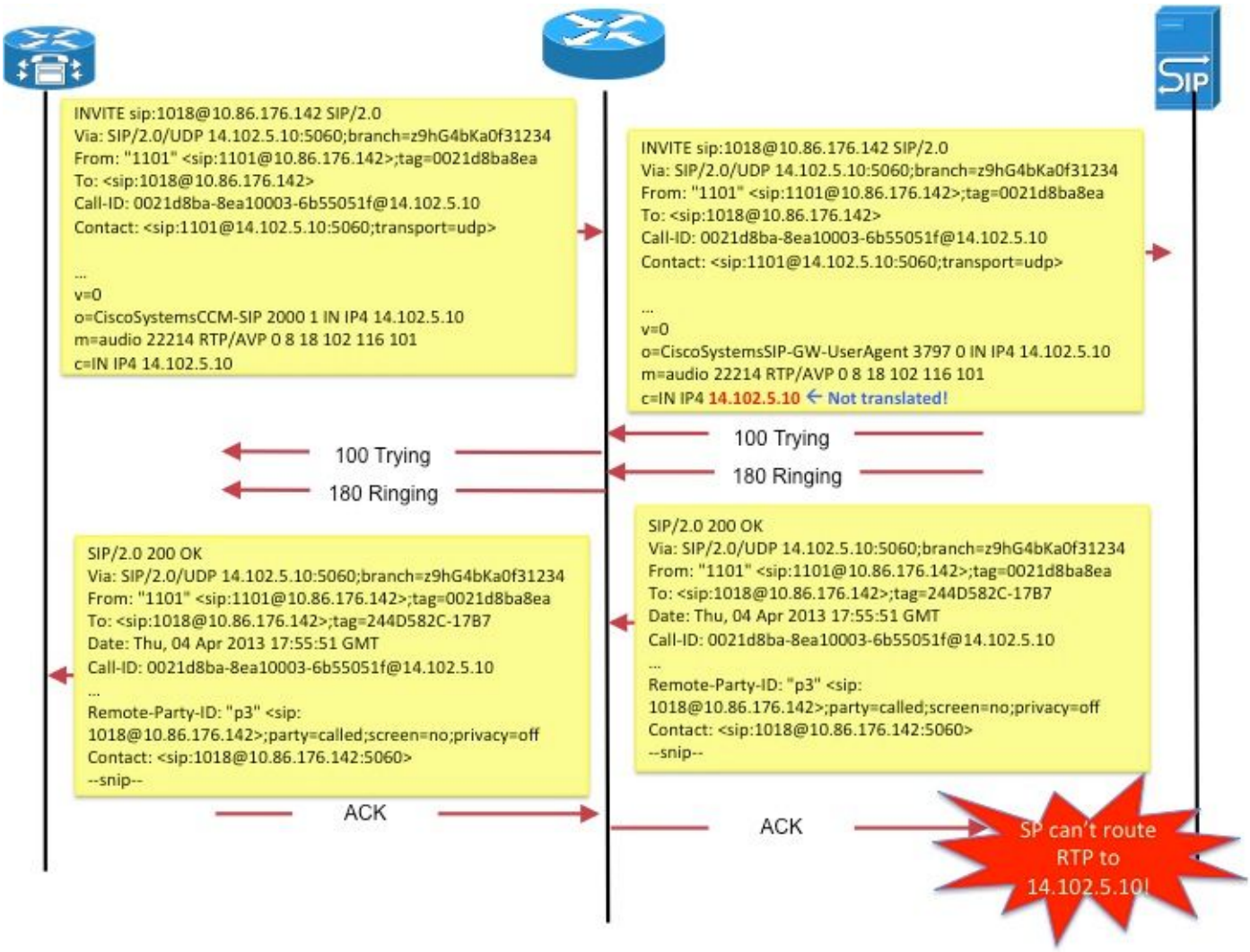

図 5：

もう一つの例は SIP エンドポイントの***連絡先***の使用です*:* エンドポイントが New 要求のためのシグナルメッセージを受け取ることを望むアドレスを伝える SDP のフィールド。

これらの問題はアプリケーション層ゲートウェイ（ALG）と呼ばれる機能によって当たります。

ALG

ALG は（例えば SIP）サポートし、それによってトラフィックのプロトコル パケット点検および「フィックスアップ」をする特定のアプリケーションによって使用されるプロトコルを理解します。 よい説明に関してはさまざまなフィールドが SIP 呼出し シグナリングのために固定どのようにのであるか、http://www.voip-info.org/wiki/view/Routers+SIP+ALG を参照して下さい。

on Cisco ルータは標準 TCPポート 5060 で、ALG SIP のためのサポート、デフォルトで、有効になります。 SIP シグナリングのための標準外ポートをサポートするために ALG を設定することは可能性のあるです。 http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html を参照して下さい。

> **注意**： 用心して下さい! RFC または組み込みフィールドがさまざまな VoIP プロトコルのために変換する必要がある綴り他の規格がありません。 その結果、実装は相互運用問題変わります（および TAC ケース）に終って、機器 の ベンダー間で。

ゲートウェイ

ゲートウェイ以来、IP-to-IP で はない デバイスは、NAT です適用されない定義上ではありません。

CME

NAT がなぜ使用する必要があるか理解する CME のドキュメントリビュー コール シナリオのこのセクション。

シナリオ 1.地域電話

シナリオ 2.リモートフォン（公共 IP アドレスと）

シナリオ 3.リモート 在宅勤務者

> **注:** いずれの場合も、フローするオーディオのために CME IP アドレスは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（6）図は、コールに関連する 2 台の電話私用 IP アドレスのスキニー 電話です。

図 6

注: そのスキニー 電話接続される同じ CME システムは他の電話にメディア パケットを直接送信するの別のスキニー 電話によってコールで覚えていて下さい; 地域電話への地域電話のためのすなわち RTP は CME をフローしません。

従って、NAT は適用されないまたはこの場合必要とされてです。

注: CME はコールに関連する 2 台の電話はスキニーおよび同じネットワークセグメントにであるかどうかメディア (RTP ことを) 直接または基づかないもしかどうか判別します。さもなければ、CME は RTP パスでそれ自身を挿入します。

遠隔へのローカル

このシナリオ (7) 図は RTP ストリームに、CME 電話からの RTP が CME で終わることそれ自身をそのような物挿入します。 CME は他の電話の方のストリームを再作成します。 CME が内部 (私用) ネットワークおよび外部ネットワーク両方で置かれたりおよび外部電話に内部電話への内部アドレスおよび外部 (パブリック) アドレスを送信 するので、NAT がここに必要となりません。

しかし注意して下さい、それは UDP/TCP ポート (シグナリング、また RTP) リモートIP 電話と CME ソース IP アドレス間で開く必要があります。 これは疑わしいポートを可能にするためにファイアウォールか他のフィルタリング デバイスが設定されることを意味します。

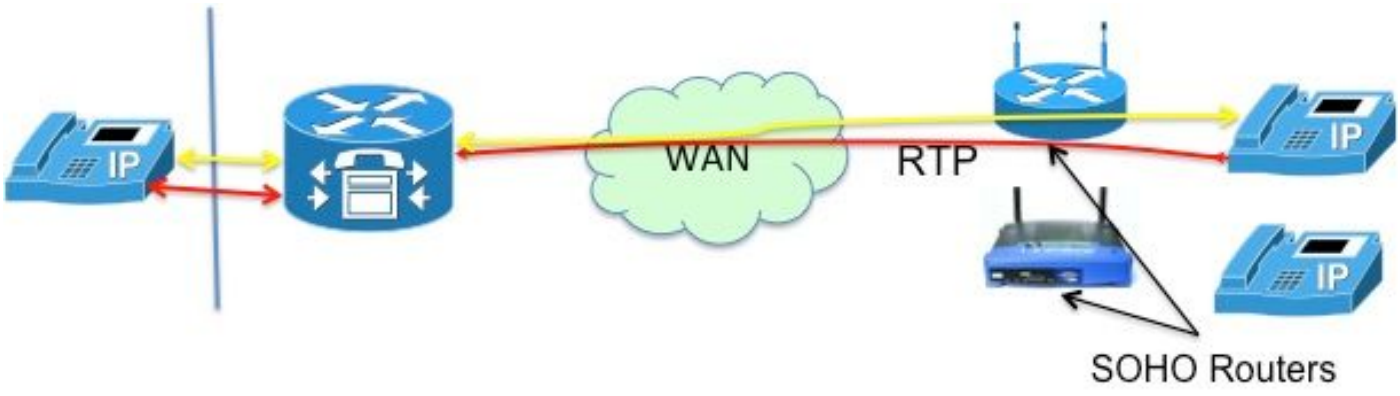

図 7

注: 信号を送って[メッセージ]常に CM で終了されることに注目して下さい

リモート在宅勤務者

これは CME ルータからリモートであるオフィスを持っている在宅勤務者をサポートするために WAN 上の CME に接続する IP 電話を示します。 もっとも一般的な設計はルーティング可能 な IP アドレスと電話および私用 IP アドレスと電話を含むそれらです。

パブリックが付いているリモートフォン (読まれる: ルーティング可能 な) IP アドレス

コールに関連する電話が両方とも公共、ルーティング可能 な IP アドレスで設定されれば、メディアは電話の間で直接 8) 計算しますフローできます。 従って、もう一度、NAT のための必要無し!

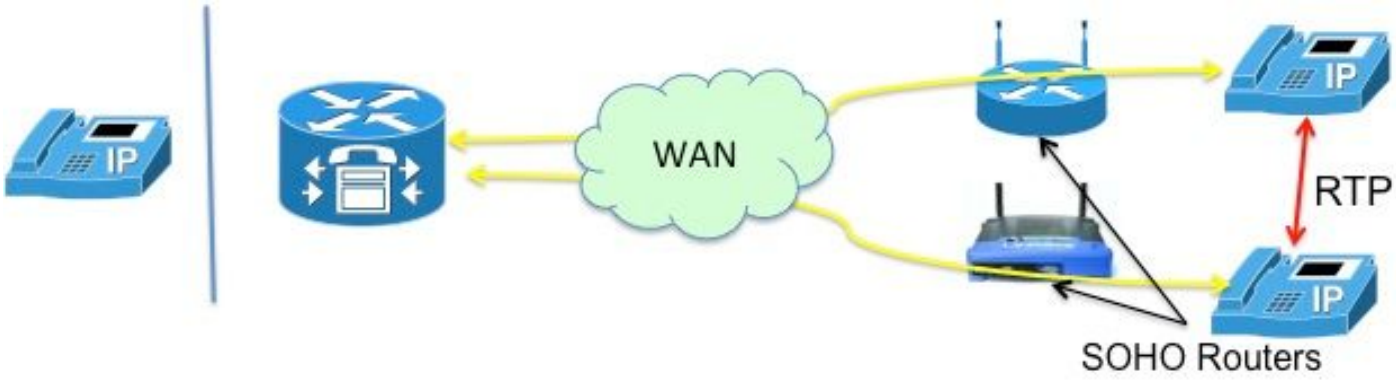

図 8

プライベート IP アドレスのリモートフォン

このシナリオでは、コールは私用 IP アドレスで設定されるスキニー 電話の間で信号を送られます。 家庭内オフィス (SOHO) ルータは、一般に、「わかっている」SCCP でなくがちです。 SCCP メッセージで組み込まれる IP アドレスの変換のすなわちできない。 これは、コールセットアップ 完了に、電話が互いのプライベート IP アドレスで終ることを意味します。 電話が両方とも私用であるので、CME はその間でオーディオが電話の間で直接フローすることコールにそのような物信号を送ります。 しかしこれは一方向または非方法オーディオという結果に、次のいずれかの回避策設定されていなければ、(私用 IP アドレス以来、定義上では、インターネットのにルーティングされるはできません!) 終ります-

- SOHOルータの設定スタティック・ルート
- 電話への IPSec VPN 接続を確立して下さい

これを解決するよりよい方法は「mtp」を設定することです。 mtp コマンドはリモートフォンからのメディア (RTP) パケットが CME ルータ (9) 図を通って通過するようにします。

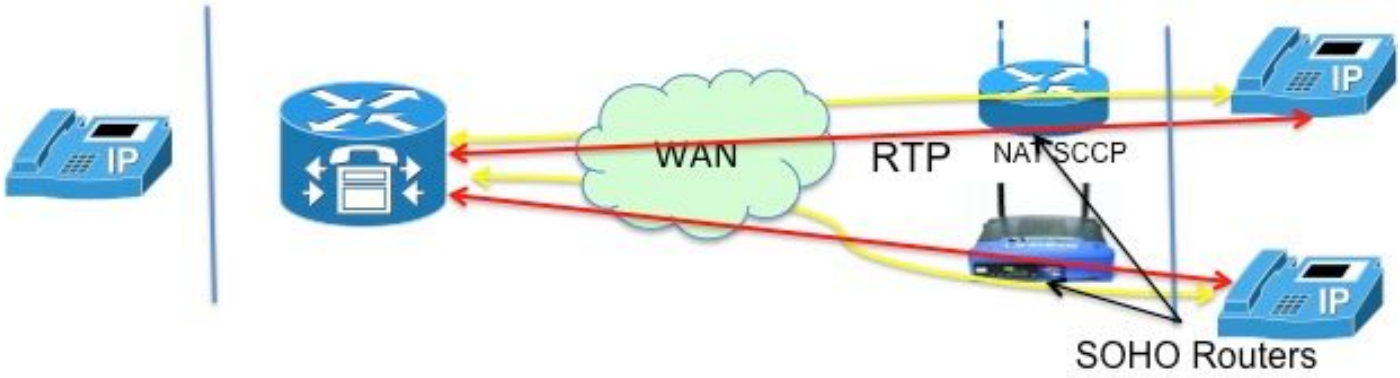

図 9

「mtp」ソリューションはファイアウォール ポートを開くことの複雑な状況が理由でよりよいです。 WAN に流れるメディア パケットはファイアウォールによって妨げられるかもしれません。 これはファイアウォールの開港を必要とする、どれことを意味しますか。 オーディオを中継で送っていて RTP パケットを渡すために CME がファイアウォールは容易に設定することができます。 CME ルータはメディア パケットのために***仕様*** UDP port(2000!) を使用します。 このように、ちょうどポート 2000 に出入するパケットを許可することを、すべての RTP トラフィックは通過させることができます。

図 10 mtp を設定する方法を説明します。

```
ephone 1

 MAC 1111.2222.3333

  7965

 mtp

  1:1
```

図 10

すべては mtp とすばらしくないです。 mtp が好ましくないかもしれない状況があります

- MTP は CPU稼働率で穏やかではないです
- マルチキャスト MOH は WAN にその phoneL に MTP が電話のために有効に なるかどうか、そして見るマルチキャスト MOH 機能チェックあれば、送信 しません MOH を一般に転送することができません。

従って、マルチキャスト パケットを転送**でき**、ファイアウォールによって RTP パケットを許可することができる WAN設定があれば MTP を使用しないことにすることができます。

リモート SIP 電話

SIP 電話が上記のシナリオで述べられなかったことに注目して下さい。 これは、CME は音声経路にそれ自身を挿入するというファクトが理由で電話の 1 つが SIP Phone ならそうなったものです。 これはそれから NAT が必要とならないか先に解説されているローカルにリモート シナリオになります。

CUBE

CUBE はそれとして本来 NAT および PAT 機能を終了し、再作成しますすべてのセッションを行います。 従って CUBE はと伝えるあらゆるエンドポイントのアドレスの自身のアドレスを置換しま、効果的に (変換) そのエンドポイントのアドレスを隠します。

従って、CUBE 機能と NAT が必要となりません。 NAT が CUBE で必要となる VOIPサービス シナリオが次の セクションに記述されているようにあります。

ホストされた NAT 走査

ホストされたテレフォニーサービスの簡潔なバックグラウンドはこの機能のための理論的根拠の理解を助けます。

ホストされたテレフォニーサービスはサービスプロバイダーの位置のギヤ常駐するのほとんど VOIPサービスの New 形式です。 それらは基本的な NAT だけ (L3/L4 のすなわち NAT) 実装されているホームゲートウェイ (HGW) を使用します。 例えば Verizon はホームの 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 に構築される SIP プロセスを使用して信号を送られます。 SIP シグナリングは他の FiOS デジタル音声 顧客に音声通信を確立するためにサービスおよび制御を提供するまたは従来の電話 顧客への Verizon の私用 IPネットワークになされます新しいソフト スイッチへの。

ホストされたテレフォニーサービスのためのキー プロバイダ必要条件の間で含んで下さい、

- リモート NAT 走査: (NAT レイヤ3 しかしないことができる NAT!) およびファイアウォール デバイスを利用するエンドポイントにクラス 5 サービスを提供する機能 (「ALG」をリモートですることによって!)
- 共同メディア サポート: IPネットワークにメディアを戻す理にかなっていない同じ場所に配置されたデバイス間のメディアを送信 する機能
- 追加された機器無し、CPE を追加する必要を省きます。

上を与えられて、どんなオプションがそのようなサービスを設定するためにありますか。

- 高い ALG と HGW を取り替えて下さい、
- セッション ボーダー コントローラ (SBC) をパケットのための組み込み SIP ヘッダを修正するのに使用して下さい。 これは非常にセキュアの、フォールト トレラント 設定で SIP をサポートするネットワーク ホストの、搬送波グレード製品を含みます。 このソリューションは参照された NAT SBC です。

NAT SBC オプションは上記リストに記載されているプロバイダ必要条件を満たします。

NAT SBC

次の通り NAT SBC 作業 (図 11)

1. アクセスルータは L3/L4 IP アドレスだけ変換します
2. 変換されない SIP メッセージの IP アドレス
3. SBC NAT は組み込みIPアドレスを代行受信し、変換します。 SBC が 200.200.200.10 に向かう SIP パケットをそれ見る時点は NAT sbc コードを作動させます。

4. メディアは直接変換されないし、phones[5] の間で行きます

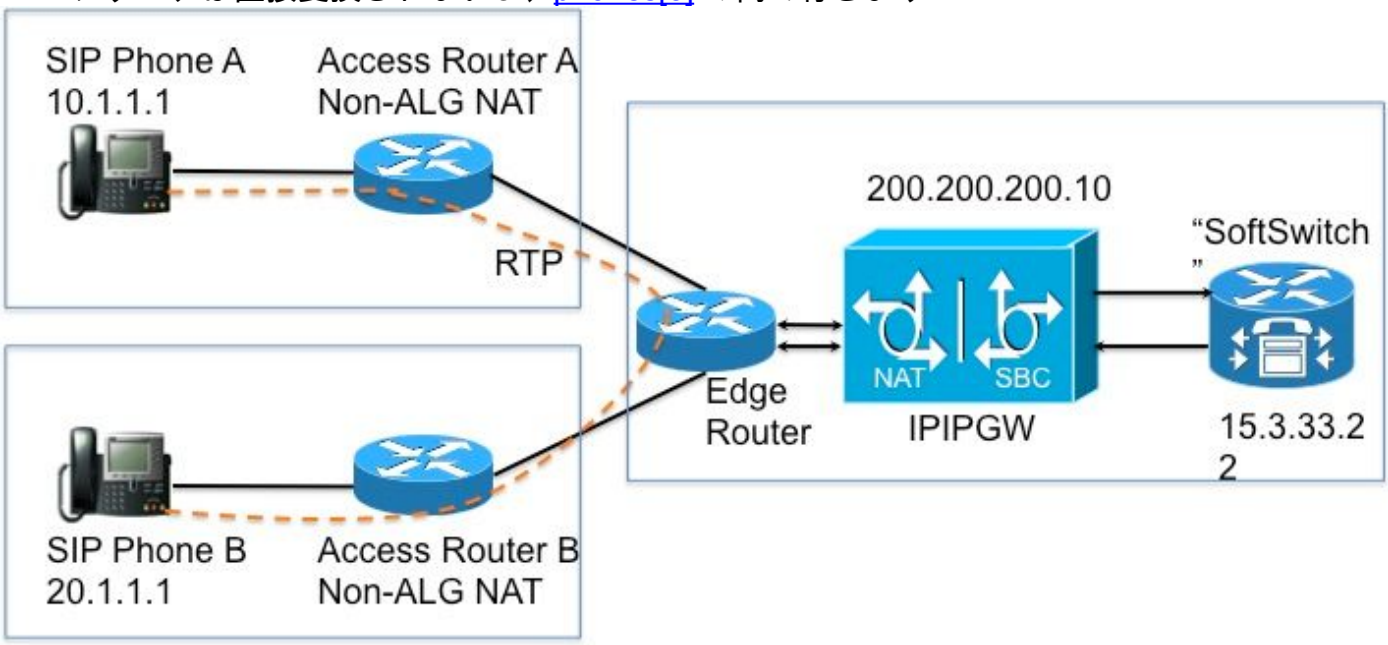

図 11

設計メモ

- IP アドレス 200.200.200.10 は NAT SBC のあらゆるインターフェイスに（図 12）割り当てられません。 それはへの「プロキシ」のアドレスでどの SIP Phone A および SIP Phone B 送信シグナルメッセージか設定されます。
- ホーム デバイスはある特定の SIP/SDP アドレス*だけ*フィールド（例えば呼び出しID を変換しません: 、警告する O=: ヘッダ及び branch= パラメータ。 maddr= および received= パラメータはただ。ある特定の場合処理されました）。 これらのフィールドはプロキシ許可および許可 変換を除いて NAT SBC によってこれらが認証を壊すので、処理されます。
- PAT をするためにホーム デバイスが設定される場合ユーザ エージェントは（電話およびプロキシ）対称 signaling[6] および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 ルータの上書きする ポートを設定して下さい。
- 対称 シグナリングおよび対称およびアーリー メディア（early media）のためのサポートがない時、中間ルータは PAT なしで設定する必要があり、上書きする アドレスは NAT SBC で設定する必要があります。

設定

典型的な NAT SBC のための設定 例は続きます。

```
IP NAT  sbc

  200.200.200.10 5060 15.3.33.22 5060  UDP

  ID   ID

   300
```

```
!

ip nat pool sbc1 15.3.33.61 15.3.33.69  255.255.0.0

ip nat pool sbc2 15.3.33.91 15.3.33.99  255.255.0.0

ip nat pool  ID  1.1.1.1 1.1.255.254  255.255.0.0

ip nat pool  200.200.200.100 200.200.200.200  255.255.255.0

ip nat inside source list 1  sbc1

ip nat inside source list 2  sbc2

ip nat outside source list 3

ip nat inside source list 4   ID

!

access-list 1  10.1.1.0 0.0.0.255

access-list 1  171.1.1.0 0.0.0.255

access-list 2  20.1.1.0 0.0.0.255

access-list 2  172.1.1.0 0.0.0.255

access-list 3  15.4.0.0 0.0.255.255

access-list 3  15.5.0.0 0.0.255.255

access-list 4  10.1.0.0 0.0.255.255

access-list 4  20.1.0.0 0.0.255.255
```

SBC NAT とのコールフロー

図 13 および図 14 変換の点ではコールフローを説明して下さい。 次のポイントは注目されるはずです

- 登録に、ソフト スイッチは 2 台の電話の下でように注意します
  -- SIP Phone A – 15.3.33.62 2001

  -- SIP Phone B – 15.3.33.62 2002
- このコールフローでは、SBC NAT は効果的にメディア IP アドレスを未翻訳に去ります。

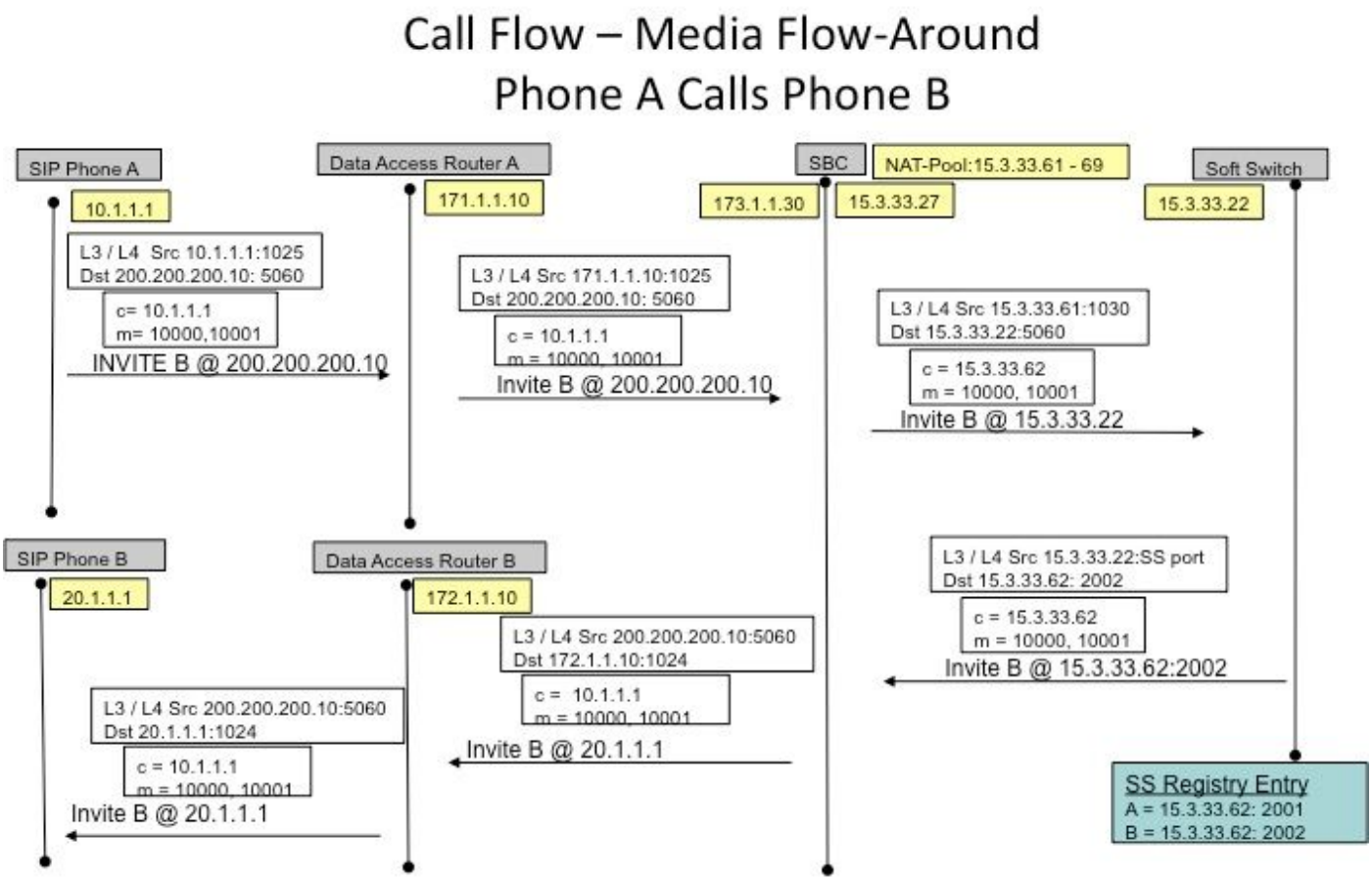
Call Flow – Media Flow-Around
Phone A Calls Phone B
SIP Phone A
10.1.1.1
Data Access Router A
171.1.1.10
SBC
NAT-Pool:15.3.33.61 - 69
173.1.1.30
15.3.33.27
Soft Switch
15.3.33.22
L3 / L4 Src 10.1.1.1:1025
Dst 200.200.200.10: 5060
c= 10.1.1.1
m= 10000,10001
INVITE B @ 200.200.200.10
L3 / L4 Src 171.1.1.10:1025
Dst 200.200.200.10: 5060
c = 10.1.1.1
m = 10000, 10001
Invite B @ 200.200.200.10
L3 / L4 Src 15.3.33.61:1030
Dst 15.3.33.22:5060
c = 15.3.33.62
m = 10000, 10001
Invite B @ 15.3.33.22
SIP Phone B
20.1.1.1
Data Access Router B
172.1.1.10
L3 / L4 Src 15.3.33.22:SS port
Dst 15.3.33.62: 2002
c = 15.3.33.62
m = 10000, 10001
Invite B @ 15.3.33.62:2002
L3 / L4 Src 200.200.200.10:5060
Dst 172.1.1.10:1024
c = 10.1.1.1
m = 10000, 10001
Invite B @ 20.1.1.1
L3 / L4 Src 200.200.200.10:5060
Dst 20.1.1.1:1024
c = 10.1.1.1
m = 10000, 10001
Invite B @ 20.1.1.1
SS Registry Entry
A = 15.3.33.62: 2001
B = 15.3.33.62: 2002

図 13

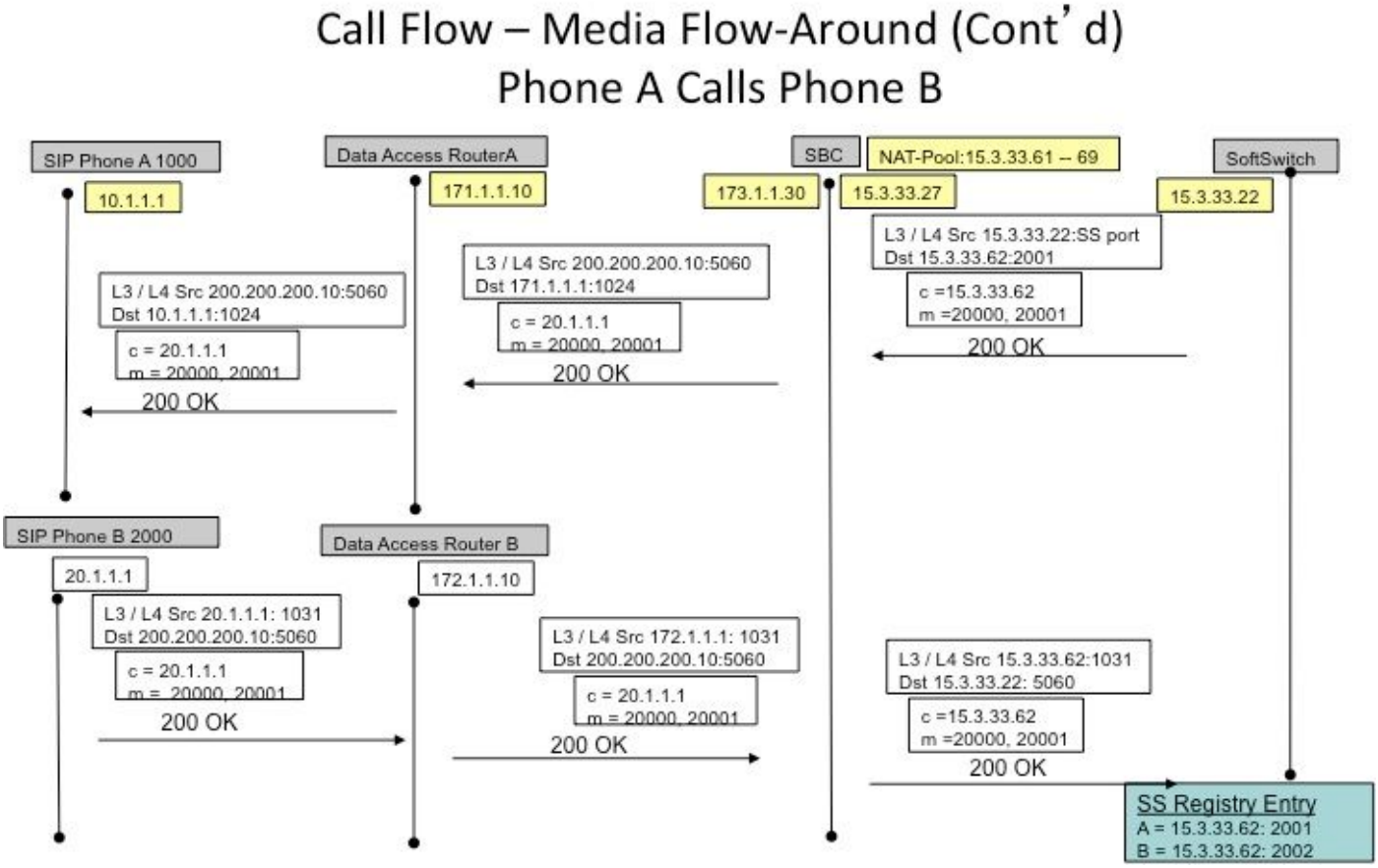
Call Flow – Media Flow-Around (Cont'd)
Phone A Calls Phone B
SIP Phone A 1000
10.1.1.1
Data Access RouterA
171.1.1.10
SBC
NAT-Pool:15.3.33.61 -- 69
173.1.1.30
15.3.33.27
SoftSwitch
15.3.33.22
L3 / L4 Src 15.3.33.22:SS port
Dst 15.3.33.62:2001
c =15.3.33.62
m =20000, 20001
200 OK
L3 / L4 Src 200.200.200.10:5060
Dst 171.1.1.1:1024
c = 20.1.1.1
m = 20000, 20001
200 OK
L3 / L4 Src 200.200.200.10:5060
Dst 10.1.1.1:1024
c = 20.1.1.1
m = 20000, 20001
200 OK
SIP Phone B 2000
20.1.1.1
Data Access Router B
172.1.1.10
L3 / L4 Src 172.1.1.1: 1031
Dst 200.200.200.10:5060
c = 20.1.1.1
m = 20000, 20001
200 OK
L3 / L4 Src 15.3.33.62:1031
Dst 15.3.33.22: 5060
c =15.3.33.62
m =20000, 20001
200 OK
L3 / L4 Src 20.1.1.1: 1031
Dst 200.200.200.10:5060
c = 20.1.1.1
m = 20000, 20001
200 OK
SS Registry Entry
A = 15.3.33.62: 2001
B = 15.3.33.62: 2002

図 14

SIP 登録

（SBC NAT）の以前のバージョンでは、SIP エンドポイントは SIP 登録ピンホールを開いた保存するためにキープアライブ パケットを送信しなければなりませんでした（out->in トラフィックがフローするようにするため例えばインバウンドコール）。 キープアライブ パケットはエンドポイントかレジストラ（ソフト スイッチ）が送信 した SIP パケットである可能性があります。 最近のバージョンは頻繁に再登録するようにエンドポイントを強制していて NAT-SBC 自体がこれのための必要を、（ソフト スイッチに対して）ピンホールを保存するために開きます取り除きます。

> **注:** 期限切れの登録ピンホールの現象はランダム 呼出し シグナリング失敗と曖昧、である場合もあります。

先端

先端に（例えばインターフェイス、ポート、受信のための転送する）ありますルーティング目的で同様に扱われるローカルインターフェイスの収集を示すロジカルネットワークの概念が。 先端のロジカルネットワークを設定するとき、NAT を使用するためにそれを設定できます。 設定されて、SIP ALG は自動的に有効に なります。 これは役立ちます時ある特定のロジカルネットワーク。

トラブルシューティング

症状

明らかな現象はコールが 1 または両方向に失敗することであるかもしれません。 より少なく明らかな現象は含むかもしれません

- 単方向音声
- 転送の単方向音声
- 非方法オーディオ
- 損失 SIP 登録

Show およびdebug コマンド

- `deb IP NAT [ | ]`
- `show ip nat statistics`
- `show ip nat translations`

チェックするべき事柄

- 設定が **ip nat inside** か **ip nat outside** インターフェイス サブコマンドが含まれているようにして下さい。 これらのコマンドはインターフェイスの NAT を有効に し、内部/外部指定は重要です。

- スタティック NAT に関しては、**IP NAT source static コマンドが**内部ローカルアドレスおよび Inside Global IP アドレスを二番目に最初にリストするようにして下さい。
- ダイナミック NAT に関しては、あらゆる NAT 変換の前のホストのパケットが、発生したことパケットを一致するために設定された ACL が一致する 内部ホストによって送信 したことを確認して下さい。 たとえば 200.1.1.1 への 10.1.1.1 の内部ローカルアドレスが変換されたら、その ACL 一致送信元アドレス 10.1.1.1 を、ない 200.1.1.1 確認して下さい。
- PAT のないダイナミック NAT に関しては、プールに十分な IP アドレスがあることを確認して下さい。 十分なアドレスを持っていないことの徴候はダイナミック変換のリストの NATプールで定義される **show ip nat statistics コマンド**出力の第 2 失敗カウンターで成長する値が含まれていましたり、また範囲のすべてのアドレスを見ます。
- PAT に関しては、**ip nat inside source list コマンドに過負荷** オプションを追加することを忘れていることは容易です。 変換されないそれ、NAT 作業、しかし PAT なしでインターネットに接続できないことはユーザのパケットおよびホストに終って、頻繁に。
- 多分 NAT は、インターフェイスの 1 つで存在 する ACL 正しく設定されパケットを廃棄します。 ことに IOSプロセス ACL 前にインターフェイスに入るパケットのためのおよびインターフェイスを終了するパケットのためのアドレスを変換した後 NAT 注目して下さい。
- インターフェイスの「ip nat outside」を設定することを忘れないで WAN に直面し (外部アドレスを変換しません) !
- NAT が設定されるとすぐ、show ip nat translations は何も示しません。 一度 ping し、次に再度チェックして下さい。
- NAT-SBC の inside および outside インターフェイスの **wireshark トレースを**つかんで下さい

シナリオ

幾つかのシナリオのためのデバッグ 出力は下記に示されています。 それらは大抵自ら明らかです !

基本的な NAT

基本 NAT のための設定およびデバッグ行は下記に示されています。

```
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 一ロからの出力行は示されています。 この場合、アウトゴーイングパケットの組み込みIPアドレスは変換されます。

```
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

[Overview] :

- http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html
- **構造分析:** 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 および NAT

- DOC-5406
- http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-security/id-60290.html

NAT 機能マトリクス

- 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_note09186a0080b17919.shtml

ホストされた NAT 走査:

- 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