NAT dans le VoIP

Contenu

Introduction

Ce document décrit le comportement NAT (de traduction d'adresses réseau) dans des Routeurs fonctionnant comme CUBE (Logiciel Cisco Unified Border Element), CME ou CUCME (Manager Express de Cisco Unified Cummunication), passerelles et TRANCHANT (Cisco Unified SIP Proxy).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SIP (protocole SIP)
- Voix sur ip (Internet Protocol)
- Protocoles de routage

Composants utilisés

Les informations dans ce document sont basées en fonction

- Toute version IOS 12.4T et en haut.
- Toute version de CME

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

La traduction d'adresses réseau est une technique utilisée généralement pour traduire des adresses IP sur les paquets qui circulent entre les réseaux utilisant les différents espaces d'adressage. Le but de ce document n'est pas de passer en revue NAT. En revanche, ce document vise à fournir un examen complet de NAT comme il est utilisé dans les réseaux VoIP de Cisco. En outre, la portée est limitée aux composants qui composent la technologie de Ms-Voix.

- NAT remplace fondamentalement l'adresse IP dans des paquets par une adresse IP différente
- Plusieurs hôtes d'enables dans un sous-réseau privé *pour partager* (c.-à-d. apparaissez comme) une adresse IP publique simple, pour accéder à l'Internet.
- Typiquement, modification de configurations NAT seulement l'adresse IP des hôtes internes
- NAT est bidirectionnel si A obtient traduit à B sur l'interface interne, B arrivant à l'interface extérieure obtiendra traduit à A !
- RFC1631

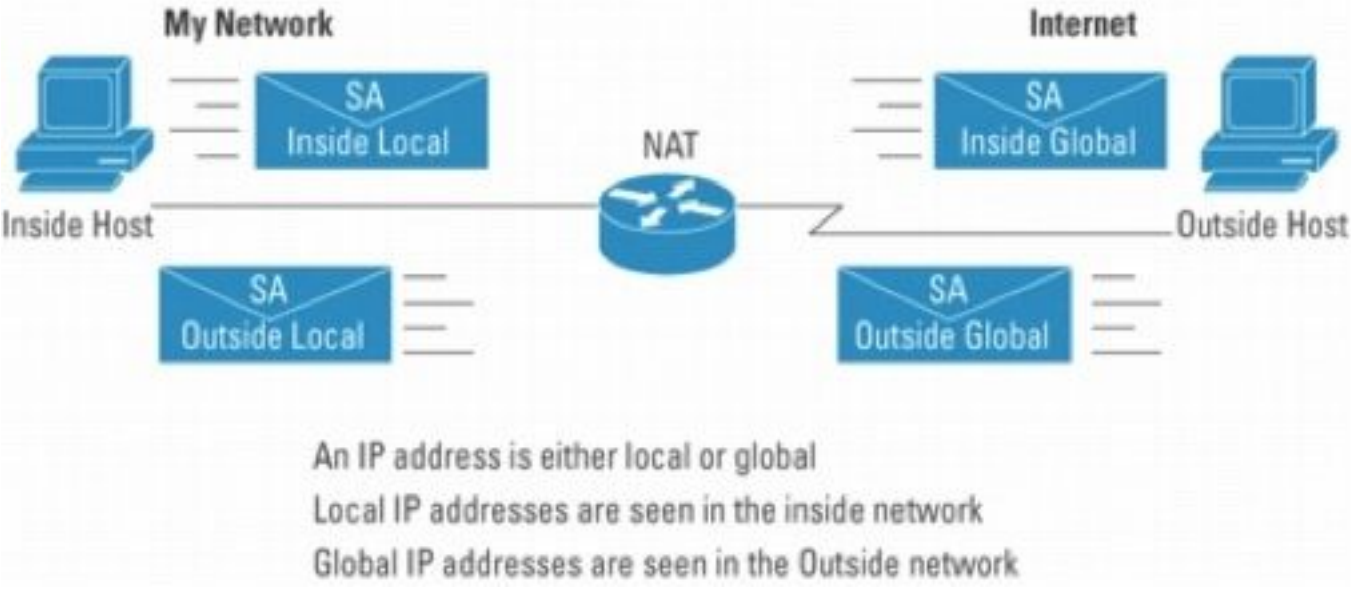

Figure 1

> Remarque: Il peut aider à penser à NAT comme aide pour conduire des paquets IP dans et hors des réseaux utilisant l'espace d'adressage privé. En d'autres termes, NAT fait des discours non-routable routable

La figure 2 affiche la topologie référencée dans les illustrations qui suivent.

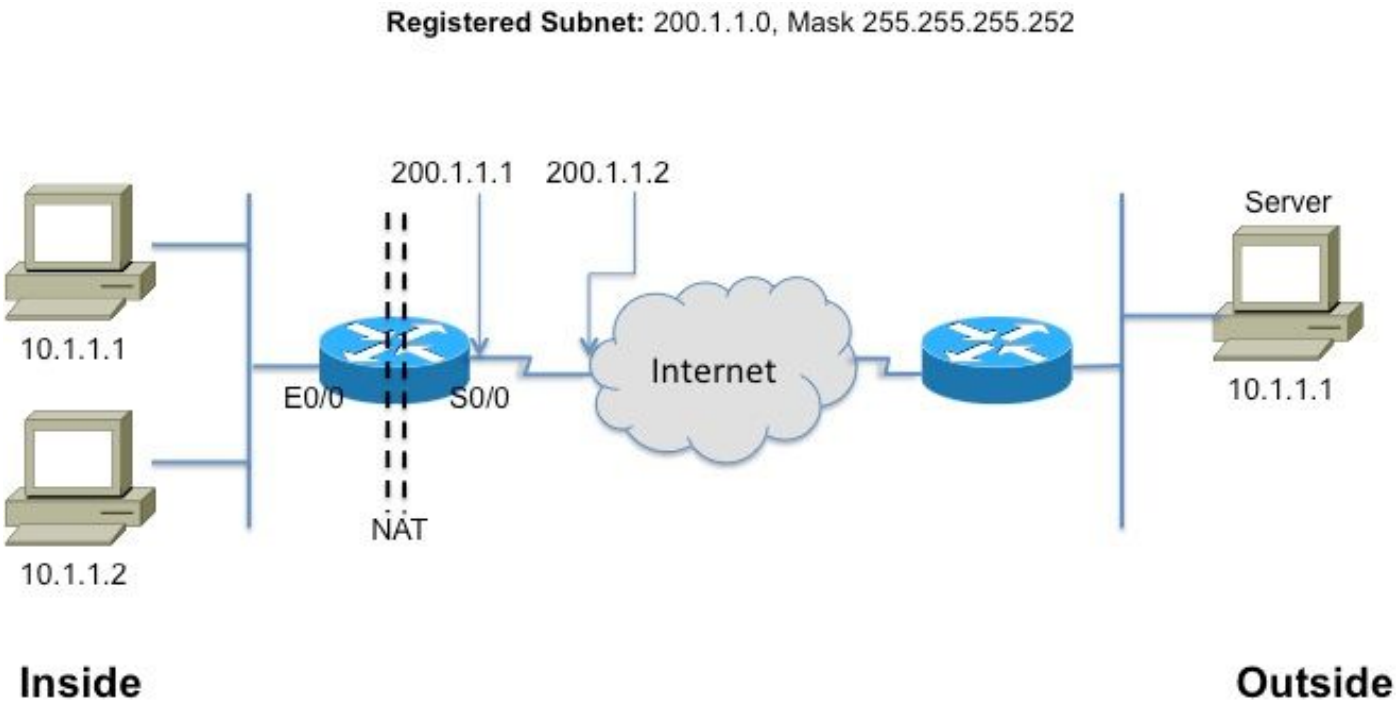

Figure 2

Ce glossaire est fondamental pour comprendre et décrire NAT

- **Adresse locale interne** - L'adresse IP assignée à un hôte sur le réseau interne. Typiquement, l'adresse est d'un espace d'adressage privé.
- **Adresse globale interne** — Une adresse IP routable assignée par le NIC ou le fournisseur de services qui représente un ou plusieurs adresses IP d'interne local au monde extérieur.
- **Adresse locale externe** - L'adresse IP d'un hôte externe comme elle apparaît au réseau interne. Pas nécessairement une adresse légitime, elle est allouée à partir d'un espace d'adresses routable à l'intérieur.
- **Adresse globale extérieure** - L'adresse IP assignée à un hôte sur le réseau externe par le propriétaire de l'hôte. L'adresse est allouée à partir d'une adresse routable globalement ou d'un espace réseau.

> Remarque: Obtenez confortable avec ces termes. N'importe quelle note ou documentation sur NAT est sûre de se rapporter à eux

NAT statique

C'est la forme la plus simple de NAT, où dans chaque adresse intérieure est statiquement traduite à une adresse d'extérieur (et vice versa).

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Figure 3

Le CLI à la configuration pour la traduction ci-dessus est comme suit

interface Ethernet0/0

IP address 10.1.1.3 255.255.255.0

ip nat à l'intérieur

!

interface Serial0/0

IP address 200.1.1.251 255.255.255.252

ip nat outside <-- Requis ! [2]

ip nat inside source 10.1.1.2 statique 200.1.1.2

ip nat inside source 10.1.1.1 statique 200.1.1.1

NAT dynamique

Dans NAT dynamique, chaque hôte interne est tracé à une adresse d'un groupe d'adresses.

- Alloue une adresse IP d'un groupe d'adresses globales internes.
- Si un nouveau paquet arrive d'encore un autre hôte interne, et il a besoin d'une entrée NAT, mais toutes les adresses IP mises en commun sont en service, le routeur jette simplement le paquet.
- Essentiellement, le groupe d'adresses globales internes doit être aussi grand que le nombre maximal d'hôtes simultanés qui doivent utiliser l'Internet en même temps

Le CLI suivant illustre configurer NAT dynamique

```
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
```

Surcharge NAT (PAT)

Quand le groupe (d'adresses IP) est plus petit que l'ensemble d'adresses qui doivent être traduites, cette caractéristique est livré dans pratique.

- Plusieurs adresses internes NATed seulement à une ou quelque adresses externes
- PAT (translation d'adresses d'adresse du port) utilise de seuls numéros de port de source sur l'adresse IP **globale d'**intérieur pour distinguer les traductions. Puisque le numéro de port est encodé dans 16 bits, le nombre total pourrait théoriquement être aussi élevé que 65,536 par adresse IP. PAT tentera de préserver le port de source d'origine, si ce port de source est déjà PAT alloué tentera de trouver le premier numéro de port disponible
- La surcharge NAT peut utiliser plus de 65,000 ports, lui permettant pour mesurer bien sans avoir besoin de beaucoup d'adresses IP enregistrées — dans de nombreux cas, ayant besoin de seulement une adresse IP globale d'extérieur.

La figure 4 montre le brevet.

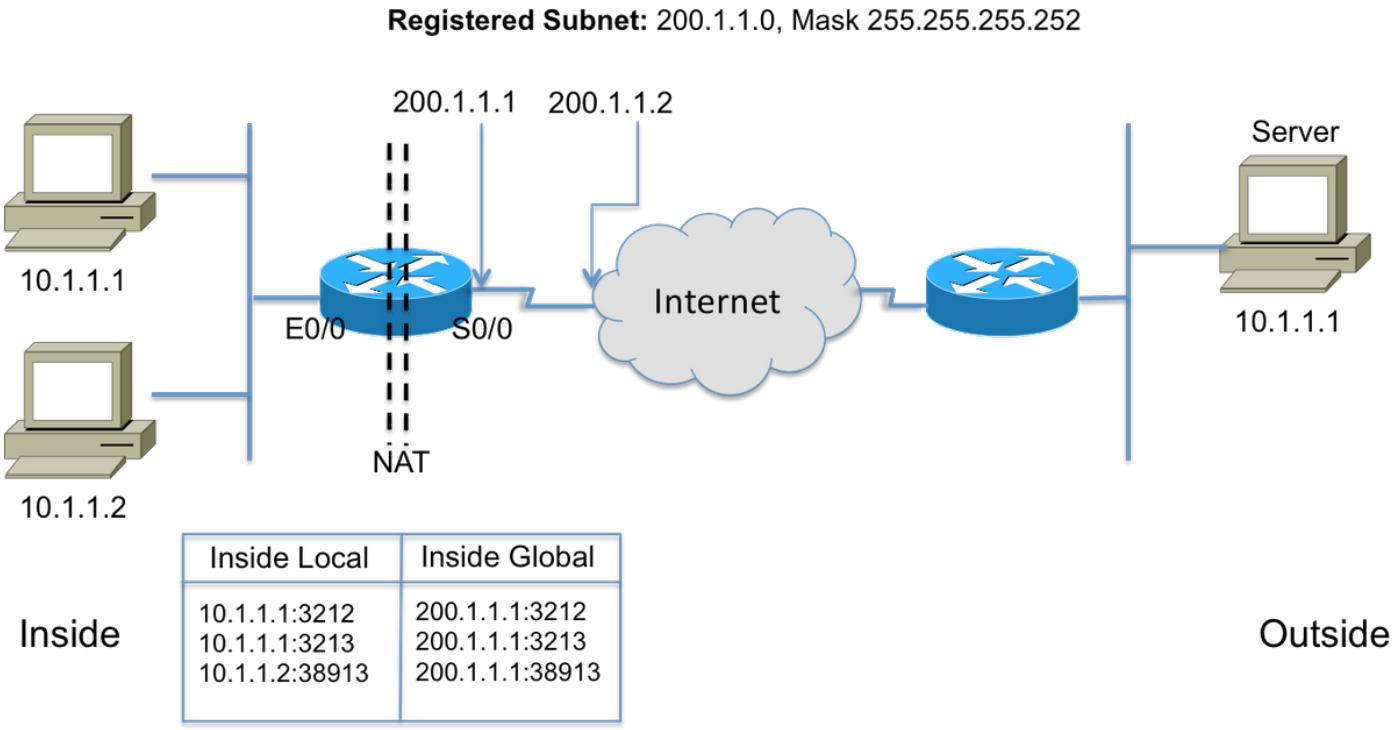

Figure 4

Options NAT de commande

L'implémentation NAT de Cisco est très souple avec une foule d'options. Quelques uns sont répertoriés ci-dessous, mais se rapportent s'il vous plaît à http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html pour des détails sur la liste complète d'améliorations.

- Traductions statiques avec des ports – Paquets entrant adressés à un port spécifique (par exemple port 25, parce que au serveur SMTP) envoyés à un serveur spécifique.
- Soutien des mappages de route - Flexibilité en configurant des filtres/ACLs
- Des configurations plus flexibles de groupe pour permettre les plages d'adresses discontinues.

- Conservation de host number - Traduisez la pièce de « réseau », retenez la cloison de « hôte ».

Trou d'épingle NAT

Un trou d'épingle dans le langage NAT se rapporte au mappage entre l'IP de <host, le port> et l'adresse <global, des tuples *globaux de* port>. Il permet au périphérique NAT pour employer le nombre de destination port (qui serait le port *global*) de messages entrant pour tracer la destination de nouveau à l'IP d'hôte et pour mettre en communication que d'origine la session. Il est important de noter que les trous d'épingle chronomètrent après une période de non-utilisation et l'annonce publique est retournée au groupe NAT.

NAT dans le VoIP

Ainsi, quels sont les questions et les soucis avec NAT dans les réseaux VoIP ? Bien, rappelez cela NAT que nous avons discuté jusqu'ici (losely referredto comme NAT de base) traduit seulement l'adresse IP dans l'*en-tête de* paquet IP et recalculez la somme de contrôle, naturellement, mais signalisation VoIP portez les adresses incluses dans le *corps des* messages de signalisation. En d'autres termes, à la couche 5

La figure 5 montre l'effet de laisser les IP address inclus non traduits. La signalisation d'appel se termine réussi, mais le proxy SIP au fournisseur de services échoue essayant de conduire des paquets de medias (RTP) à l'adresse de medias envoyée par l'agent d'appel !

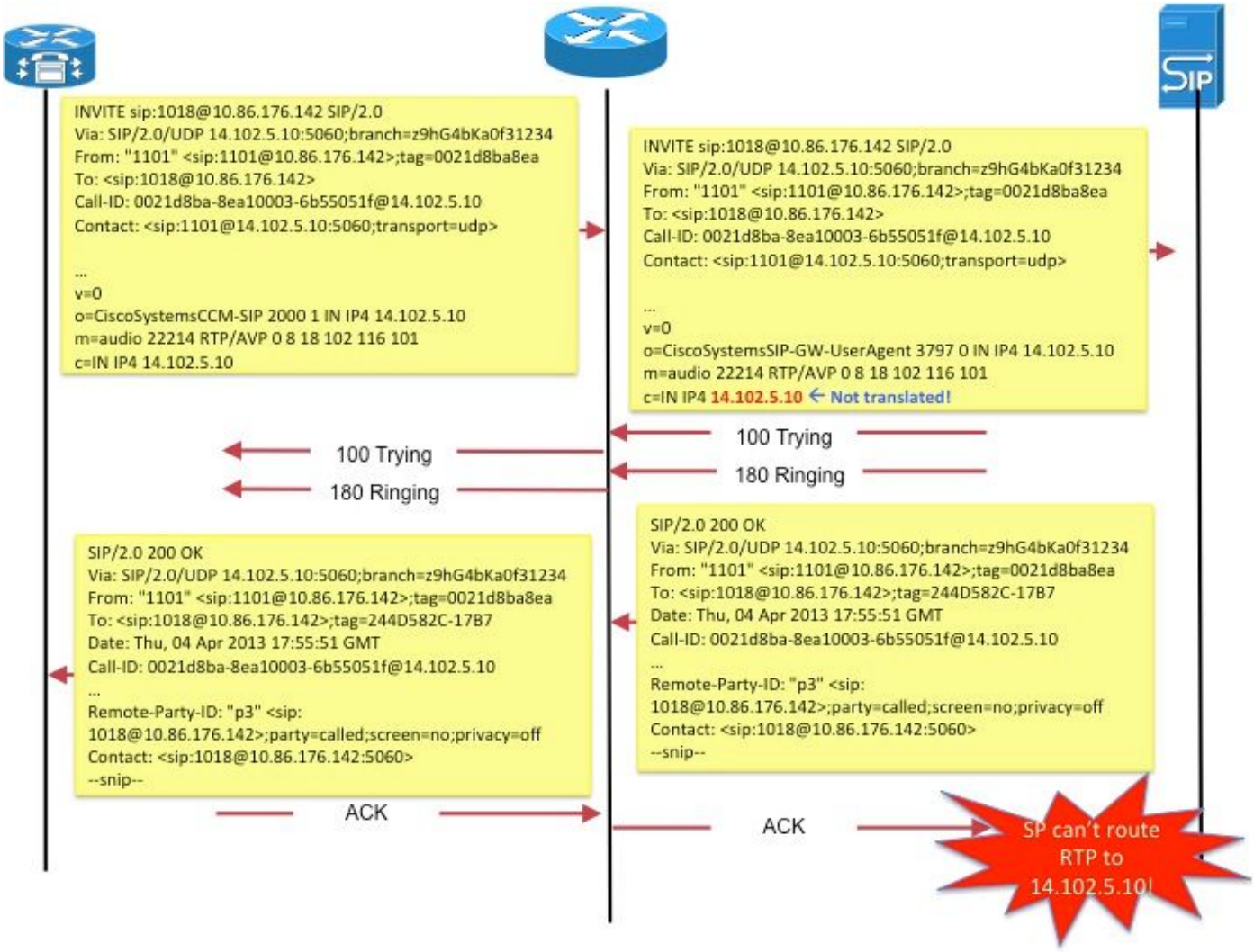

Figure 5

Un autre exemple serait l'utilisation du point final de SIP du ***contact :*** mettez en place dans le SDP pour communiquer l'adresse à laquelle le point final voudrait recevoir des messages de signalisation pour de nouvelles demandes.

Ces questions sont abordées par une caractéristique appelée la passerelle de couche application (ALG).

ALG

Un ALG comprend le protocole utilisé par les applications spécifiques qu'il prend en charge (par exemple SIP) et fait la paquet-inspection et le « fixup » de protocole du trafic par lui. Pour une bonne description de la façon dont les divers champs sont réparés- pour la signalisation d'appel de SIP, référez-vous à http://www.voip-info.org/wiki/view/Routers+SIP+ALG.

Sur des Routeurs de Cisco, le soutien du SIP ALG est activé, par défaut, sur le port TCP standard 5060. Il est possible de configurer ALG pour prendre en charge les ports non standard pour la signalisation de SIP. Référez-vous à http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.

> **Attention** : Prenez garde ! Il y a aucun RFC ou toute autre norme que de définitions des champs qui a encastré ne devraient être traduit pour les divers protocoles VoIP. En

conséquence, les réalisations varient, parmi des constructeurs de matériel, ayant pour résultat des questions d'interop (et des cas TAC).

Passerelles

Depuis des passerelles, par définition, ne sont pas les périphériques IP-à-IP, NAT s'applique pas applicable.

CME

Cette section des scénarios d'appel d'examen de document avec CME pour comprendre pourquoi NAT doit être utilisé.

Téléphones de gens du pays du scénario 1.

Téléphones distants du scénario 2. (avec des adresses IP publique)

Télétravailleur de distant du scénario 3.

> Remarque: Dans des toutes les caisses, pour que l'audio circule, l'adresse IP de CME doit être routable

Gens du pays

Dans ce scénario (le schéma 6), les deux téléphones impliqués dans l'appel sont les téléphones maigres avec des adresses IP privées.

Figure 6

> Remarque: Souvenez-vous que maigre téléphonez qui est connecté dans un appel à un autre téléphone maigre dans le même système de CME envoie ses paquets de medias directement à l'autre téléphone ; c.-à-d. le RTP pour le gens du pays-téléphone de gens du pays-téléphone ne traverse pas CME.

Par conséquent, NAT est le pas applicable ou requis dans ce cas.

Remarque: CME détermine si des medias (RTP) si directement ou non basé en fonction si les deux téléphones impliqués dans un appel sont maigres *et* dans le même segment de réseau. Autrement, CME s'insère dans le chemin de RTP.

Gens du pays au distant

Dans ce scénario (le schéma 7), CME s'insère dans le flot de RTP tels que le RTP des téléphones sera terminé sur CME. CME re-commencera les flots vers l'autre téléphone. Puisque CME se repose sur le réseau (privé) intérieur et le réseau extérieur et envoie son adresse intérieure au téléphone d'intérieur et adresse d'extérieur (public) au téléphone d'extérieur, NAT n'est pas exigé ici non plus.

Notez cependant, ce les ports UDP/TCP (signalisation aussi bien que RTP) doit être ouvert entre le téléphone IP distant et l'adresse IP source de CME. Ceci signifie que les Pare-feu ou d'autres périphériques de filtrage sont configurés pour permettre les ports en question.

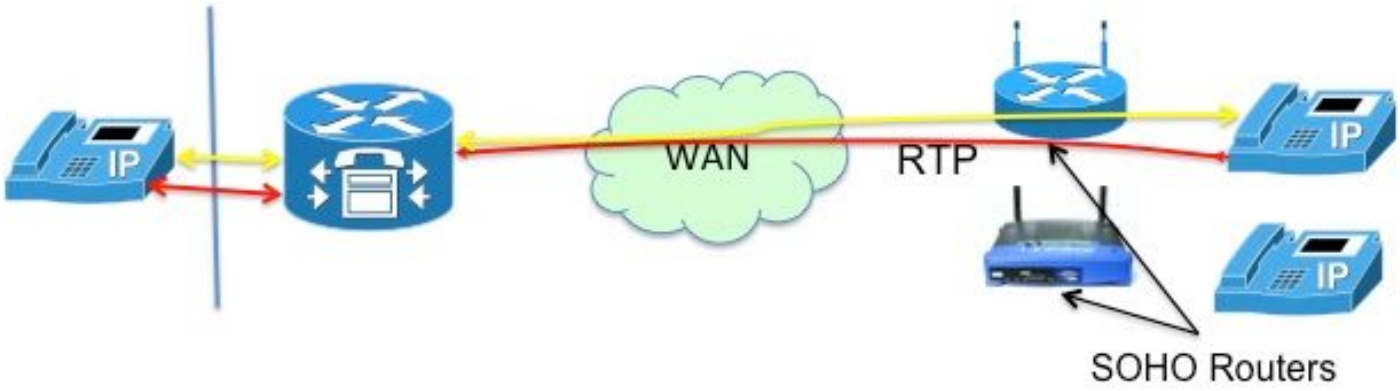

Figure 7

Remarque: Notez que signalant [des messages] sont toujours terminés sur le cm

Télétravailleur distant

Ceci se rapporte à des Téléphones IP se connectant à CME au-dessus d'un WAN pour prendre en charge les télétravailleurs qui ont des bureaux qui sont éloignés du routeur de CME. Les conceptions les plus communes sont ceux qui impliquent des téléphones des adresses IP routable et des téléphones des adresses IP privées.

Téléphones distants avec le public (lu :) adresses IP routable

Si les les deux les téléphones impliqués dans l'appel sont configurés avec les adresses IP publiques et routable, les medias peuvent circuler entre le schéma de téléphones directement 8). Par conséquent, de nouveau, aucun besoin de NAT !

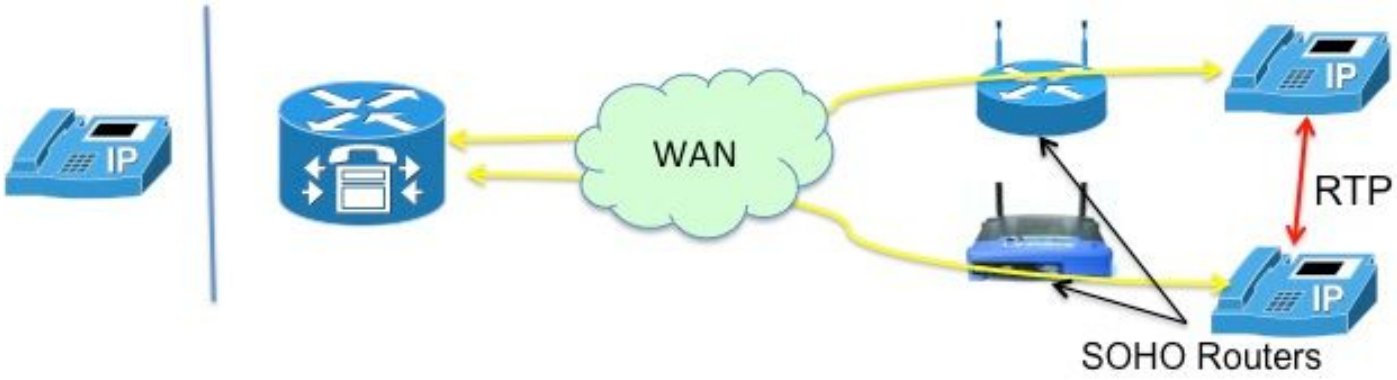

Figure 8

Téléphones distants avec l'adresse IP privée

Dans ce scénario, l'appel est signalé entre les téléphones maigres configurés avec des adresses IP privées. Les Routeurs du bureau à domicile (SOHO), tendent généralement à ne pas être « SCCP averti ». c.-à-d. incapable de traduire les adresses IP incluses dans les messages de SCCP. Ceci signifie que, sur la fin d'établissement d'appel, les téléphones finissent par avec l'adresse IP privée de chacun. Puisque les les deux les téléphones sont privés, CME signalera l'appel entre eux tels que l'audio circule directement entre les téléphones. Ceci cependant, aura comme conséquence l'audio d'one-way ou de NO--manière (depuis des adresses IP privées, par définition, ne peut pas être conduit à sur l'Internet !), à moins qu'un des contournements suivants soit mis en application -

· Configurez les artères statiques sur les Routeurs SOHO

· établissez une connexion VPN d'IPsec aux téléphones

Une meilleure manière de résoudre ceci serait de configurer le « mtp ». La commande de mtp s'assure que les paquets de medias (RTP) des téléphones distants transitent par le routeur de CME (le schéma 9).

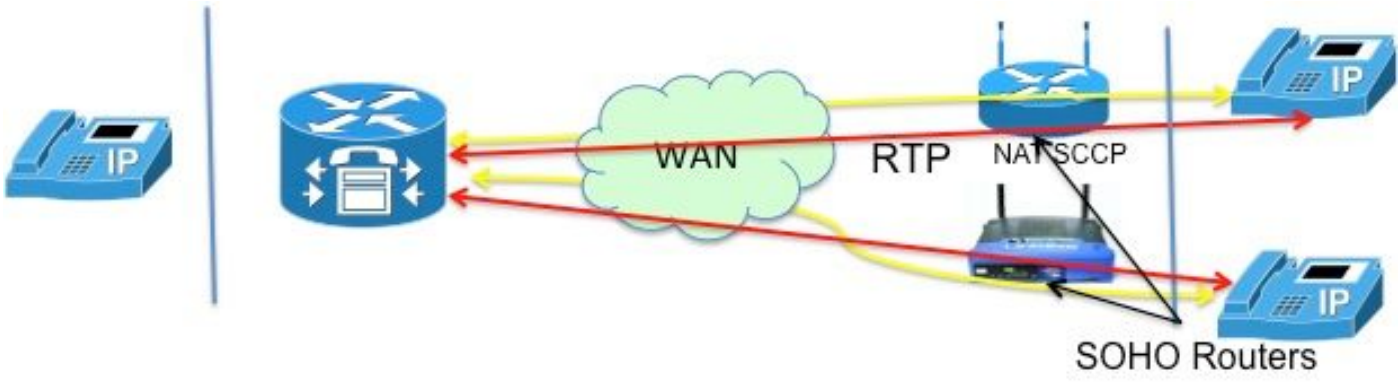

Figure 9

La solution de « mtp » est meilleure en raison des complications avec ouvrir des ports de Pare-feu. Les paquets de medias circulant au-dessus d'un WAN peuvent être obstrués par un Pare-feu. Ceci signifie que vous avez besoin des ports ouverts sur le Pare-feu, mais lesquels ? Avec CME transmettant par relais l'audio, des Pare-feu peuvent être facilement configurés pour passer les paquets de RTP. Le routeur de CME utilise un UDP ***spécifique*** port(2000!) pour des paquets de medias. Ainsi, en permettant juste des paquets à et du port 2000, TOUT LE trafic de RTP peut

être passé.

La figure 10 montre comment configurer le mtp.

```
ephone 1

 MAC 1111.2222.3333

 type 7965

 mtp

 bouton 1:1
```

Figure 10

Tout n'est pas merveilleux avec le mtp. Il y a des situations où le mtp peut ne pas être desirable

- MTP n'est pas doux sur l'utilisation du processeur
- La Multidiffusion MOH généralement ne peut pas être expédiée au-dessus d'un WAN les contrôles de caractéristique de la Multidiffusion MOH pour voir si MTP est activé pour un téléphone et s'il est, n'envoie pas MOH à ce phoneL.

Ainsi, si vous avez une configuration BLÊME qui **peut** expédier des paquets de multidiffusion et vous pouvez permettre des paquets de RTP par votre Pare-feu, vous pouvez décider de ne pas utiliser MTP.

Téléphones SIP distants

Notez que des téléphones SIP n'ont pas été mentionnés dans les scénarios ci-dessus. C'est en raison du fait que si un des téléphones est un téléphone SIP, CME s'insère dans le chemin audio. Ceci devient alors le scénario de gens du pays-à-distant décrit plus tôt, où NAT n'est pas exigé.

CUBE

Le CUBE en soi exécute NAT et TAPOTE des fonctions pendant qu'il termine et re-commence toutes les sessions. Le CUBE substitue sa propre adresse à l'adresse de n'importe quel point final qu'elle communique avec, de ce fait efficacement masquant (se traduire) l'adresse de ce point final.

Ainsi, NAT n'est pas exigé avec la fonction de CUBE. Il y a un scénario de service VoIP dans lequel NAT est exigé sur le CUBE, comme décrit dans la section suivante.

Hosted NAT Traversal

Un bref fond sur le service téléphonique hébergé aidera à comprendre le raisonnement pour cette caractéristique.

Le service téléphonique hébergé est une nouvelle forme de service VoIP dans laquelle la majeure

partie de l'équipement réside à l'emplacement du fournisseur de services. Ils fonctionnent avec les passerelles domestiques (HGW), qui implémentent seulement NAT fondamental (c.-à-d. NAT à L3/L4). Par exemple Verizon installe le terminal de réseau optique (Ontario), qui fournit des services de FiOS dans la maison ; la communication voix est signalée utilisant un processus de SIP établi dans l'Ontario. La signalisation de SIP est faite au-dessus du réseau IP privé de Verizon aux nouveaux Commutateurs mous, qui fournissent le service et le contrôle pour établir des communications vocales à d'autres clients de voix numérique de FiOS, ou aux clients traditionnels de téléphone.

Parmi le fournisseur principal les conditions requises pour le service téléphonique hébergé incluent,

- NAT Traversal distant : la capacité de fournir des services de la classe 5 à l'utilisation de points finaux NAT (qui peut seulement faire la couche NAT 3 !) et périphériques de Pare-feu (en faisant « ALG » à distance !)
- support de Co-supports : la capacité d'envoyer des medias entre les périphériques coïmplantés où elle ne semble pas raisonnable de conduire les medias de nouveau au réseau IP
- Aucun matériel ajouté, éliminant la nécessité d'ajouter tout CPE.

Etant donné ce qui précède, quelles options existent pour implémenter un tel service ?

- Remplacez le HGW par un ALG cher,
- Utilisez un contrôleur de cadre de session (SBC) pour modifier les en-têtes encastrées de SIP pour des paquets. Ceci implique réseau-hébergé, produit de transporteur-niveau prenant en charge le SIP dans une configuration très sécurisée et insensible aux défaillances. Cette solution est NAT visé SBC.

SBC l'option NAT répond aux exigences de fournisseur répertoriées ci-dessus.

NAT SBC

Le NAT fonctionne SBC comme suit (la figure 11)

1. Le routeur d'Access traduit seulement l'adresse IP L3/L4
2. Adresse IP dans le message SIP non traduit
3. Les interceptions SBC NAT et traduit l'adresse IP incluse. Le moment voit SBC des paquets de SIP destinés à **200.200.200.10**, il donne un coup de pied dedans le code nat-sbc.
4. Le support n'est pas traduit et va directement entre le phones[5]

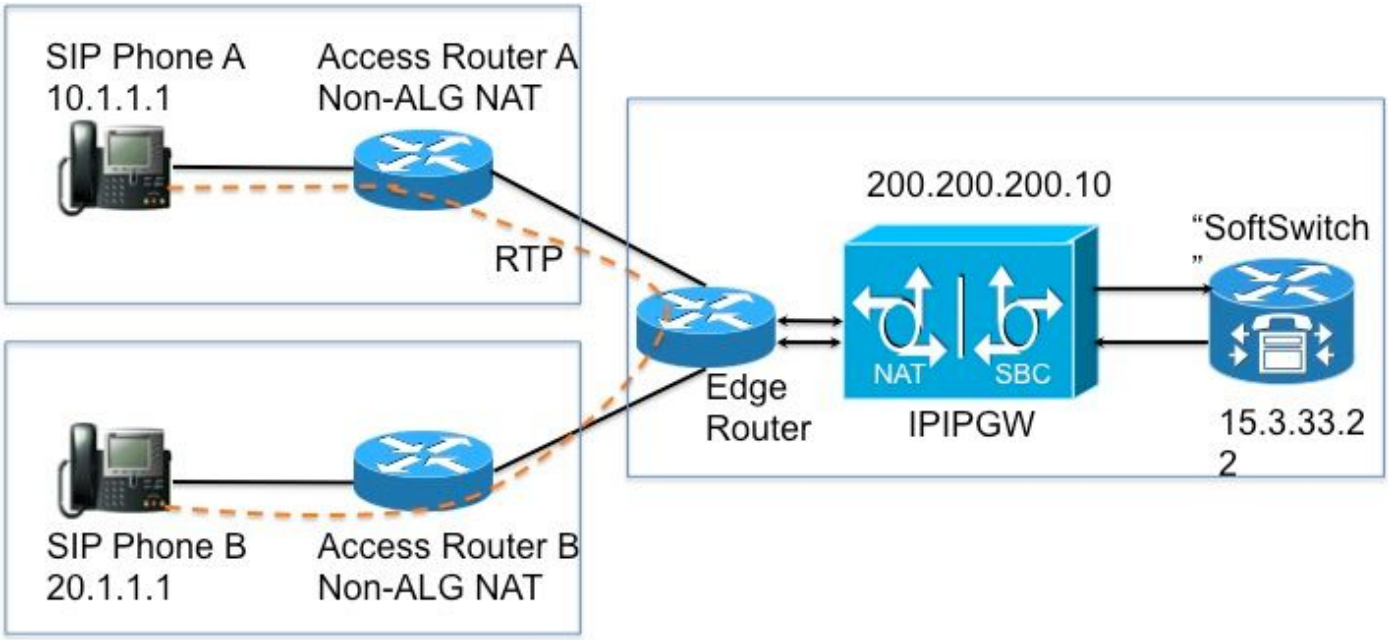

Figure 11

Notes sur la conception

- L'IP address **200.200.200.10** (figure 12) n'est assigné à aucune interface sur le NAT SBC. Il est configuré comme l'adresse du « proxy » à quel téléphone SIP A et le téléphone SIP B envoyez à des messages de signalisation.
- Les appareils domestiques ne traduisent pas certains champs *réservés à l'adresse* SIP/SDP (par exemple Appel-id : , O=, avertissant : en-têtes et paramètre de branch=. des paramètres de maddr= et de received= ont été manipulés dans certains scénarios seulement.). Ces champs sont manipulés par le NAT SBC, excepté la traduction de proxy-autorisation et d'autorisation, parce que ceux-ci casseront l'authentification.
- Si les appareils domestiques sont configurés pour faire PAT, les agents d'utilisateur (des téléphones et proxy) doivent prendre en charge signaling[6] symétrique et medias symétriques et tôt. Vous devez configurer le port de priorité sur SBC le routeur NAT.
- Faute de soutien de la signalisation symétrique et des medias symétriques et tôt, les routeurs intermédiaires doivent être configurés sans PAT et l'adresse de priorité devrait être configurée dans le NAT SBC.

Configuration

La configuration d'échantillon pour un NAT typique suit SBC.

```
ip nat sip-sbc

  UDP de protocole de 200.200.200.10 5060 15.3.33.22 5060 de proxy

  appel-id-groupe d'appel-id-groupe

  session-timeout 300

  mode autoriser-écoulement-autour de
```

```
 port de priorité

!

netmask 255.255.0.0 de l'ip nat pool sbc1 15.3.33.61 15.3.33.69

netmask 255.255.0.0 de l'ip nat pool sbc2 15.3.33.91 15.3.33.99

netmask 255.255.0.0 de 1.1.1.1 1.1.255.254 d'appel-id-groupe d'ip nat pool

netmask 255.255.255.0 de 200.200.200.100 200.200.200.200 d'extérieur-groupe d'ip nat pool

surcharge du groupe sbc1 de la liste 1 d'ip nat inside source

groupe sbc2 de la liste 2 d'ip nat inside source

ajouter-artère d'extérieur-groupe de groupe de la liste 3 d'ip nat outside source

appel-id-groupe de groupe de la liste 4 d'ip nat inside source

!

autorisation 10.1.1.0 0.0.0.255 de la liste d'accès 1

autorisation 171.1.1.0 0.0.0.255 de la liste d'accès 1

autorisation 20.1.1.0 0.0.0.255 de la liste d'accès 2

autorisation 172.1.1.0 0.0.0.255 de la liste d'accès 2

autorisation 15.4.0.0 0.0.255.255 de la liste d'accès 3

autorisation 15.5.0.0 0.0.255.255 de la liste d'accès 3

autorisation 10.1.0.0 0.0.255.255 de la liste d'accès 4

autorisation 20.1.0.0 0.0.255.255 de la liste d'accès 4
```

Écoulement d'appel avec SBC NAT

La figure 13 et la figure 14 montrent l'écoulement d'appel en termes de traductions. Les points suivants devraient être notés

- Lors de l'enregistrement, le commutateur mou note en bas des deux téléphones As
  -- Téléphone SIP A – 15.3.33.62 2001

  -- Téléphone SIP B – 15.3.33.62 2002

- Dans cet écoulement d'appel, SBC NAT laisse efficacement l'adresse IP de medias non traduite.

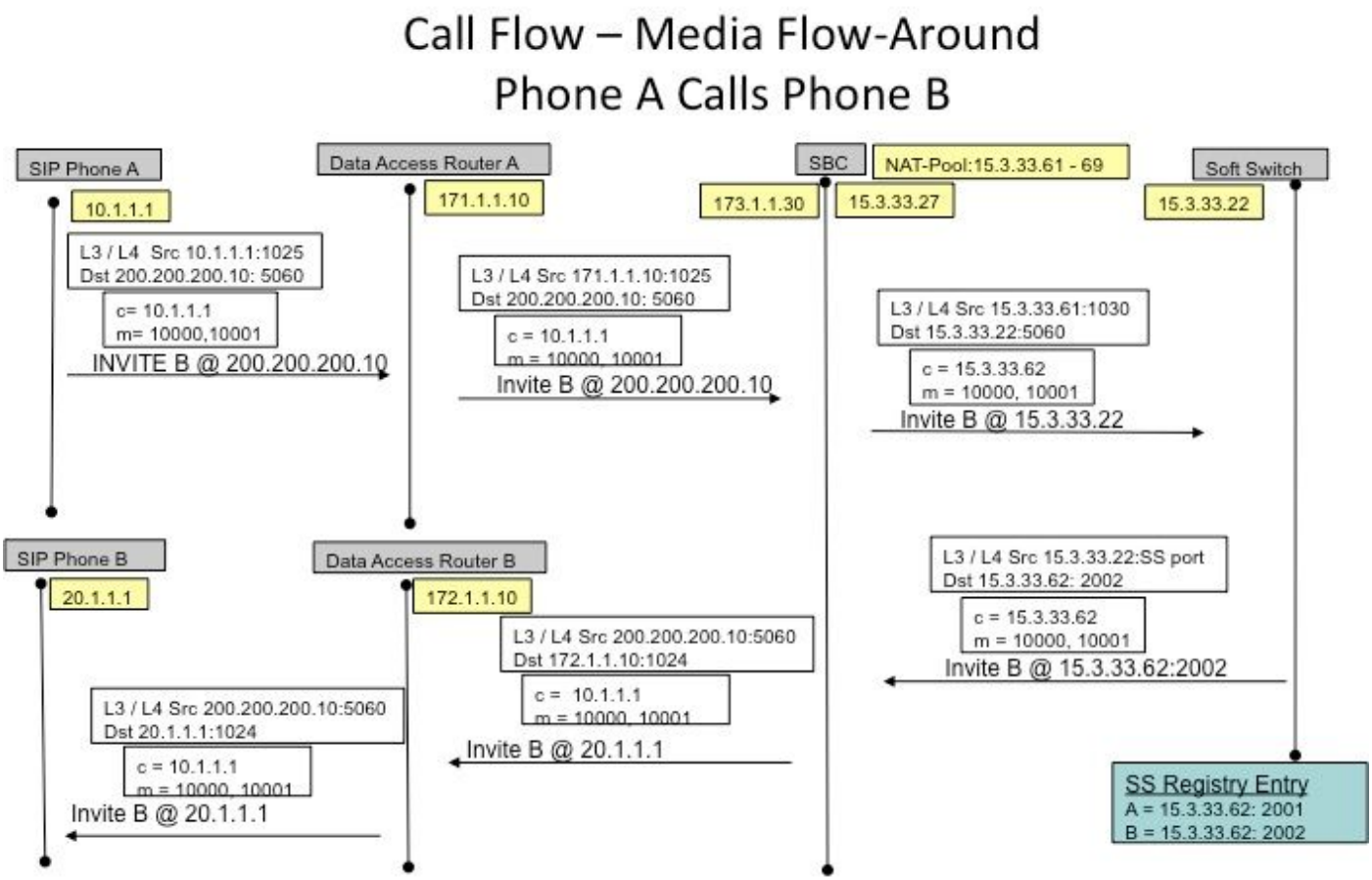

Figure 13

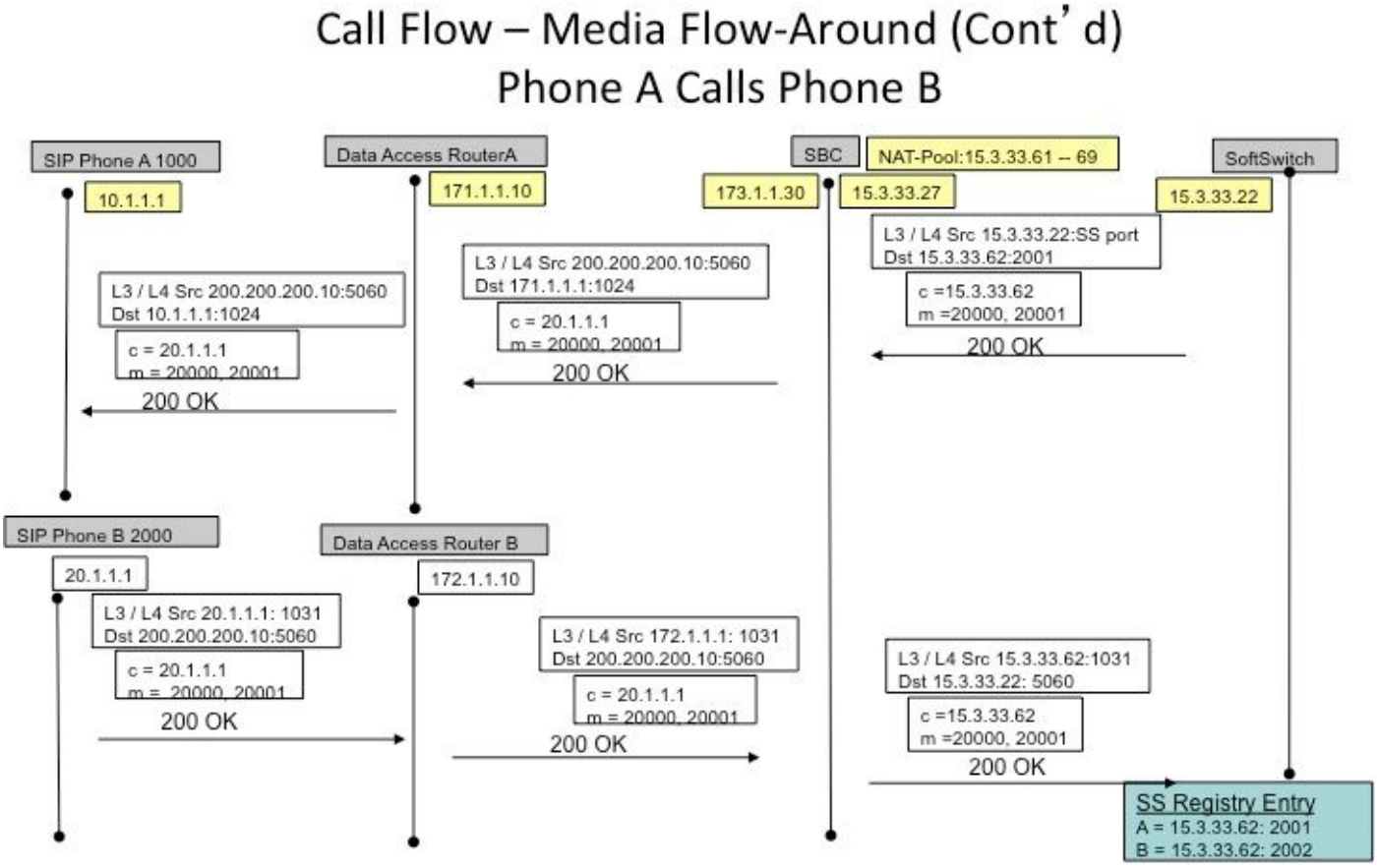

Figure 14

Enregistrement de SIP

Dans les versions antérieures (SBC de NAT), les points finaux de SIP ont dû envoyer des paquets de *keep-alive* pour maintenir le trou d'épingle d'enregistrement de SIP ouvert (pour permettre au trafic d'out->in pour circuler, par exemple des appels d'arrivée). *les paquets de* keep-alive pourraient être n'importe quel paquet de SIP envoyé par le point final ou le registrar (commutateur mou). Les versions récentes obvient au besoin de ceci, avec le NAT-SBC lui-même (par opposition aux Commutateurs mous) forçant le re-registre de points finaux fréquemment pour garder les trous d'épingle s'ouvrent.

> Remarque: Les symptômes d'un trou d'épingle expiré d'enregistrement peuvent être obscurs, avec des pannes aléatoires de signalisation d'appel.

TRANCHANT

Le TRANCHANT a la notion d'un réseau logique, qui se rapporte à une collection d'interfaces locales qui sont traitées pareillement pour (par exemple interface, port, transport pour l'écoute) conduire des buts. En configurant un réseau logique sur le TRANCHANT, vous pouvez le configurer pour utiliser NAT. Une fois que configuré, le SIP ALG est automatiquement activé. C'est utile quand certains réseaux logiques.

Dépannage

Symptômes

Un symptôme évident pourrait être qu'un appel échoue dans une ou les deux directions. Les symptômes moins évidents pourraient inclure,

- Audio à sens unique
- Audio à sens unique sur le transfert
- audio de NO--manière
- Enregistrement perdant de SIP

Commandes d'exposition et de débogage

- `ip nat DEB [sip | maigre]`
- `show ip nat statistics`
- `show ip nat translations`

Choses à vérifier

- Assurez-vous que la configuration inclut l'**ip nat intérieur** ou la commande secondaire d'interface d'**ip nat outside**. Ces commandes activent NAT sur les interfaces, et la désignation d'intérieur/extérieur est importante.

- Pour NAT statique, assurez-vous que l'**ip nat source les** listes de commandes **statiques l'**adresse d'interne local d'abord et l'intérieur adresse IP globale en second lieu.
- Pour NAT dynamique, assurez-vous que l'ACL configuré pour apparier des paquets envoyés par l'hôte interne s'assortissent que les paquets de l'hôte, avant n'importe quelle traduction NAT s'est produits. Par exemple, si une adresse d'interne local de 10.1.1.1 est traduite à 200.1.1.1, assurez ce l'adresse source 10.1.1.1 de correspondances d'ACL, pas 200.1.1.1.
- Pour NAT dynamique sans PAT, assurez-vous que le groupe a assez d'adresses IP. Les symptômes de ne pas avoir des assez d'adresse incluent une valeur croissante dans les deuxièmes coups manqués parent dans la sortie de commande de **show ip nat statistics**, aussi bien que voient toutes les adresses dans la plage définie dans le groupe NAT dans la liste de traductions dynamiques.
- Pour PAT, il est facile d'oublier d'ajouter l'**option'overload'**sur la commande de **liste d'ip nat inside source**. Sans lui, travaux NAT, mais PAT ne fait pas, souvent ayant pour résultat les paquets des utilisateurs n'étant pas traduit et les hôtes ne pas pouvoir arriver à l'Internet.
- Peut-être NAT a été configuré correctement, mais un ACL existe sur une des interfaces, jetant les paquets. Notez que des processus IOS ACLs avant NAT pour des paquets écrivant une interface, et après avoir traduit les adresses pour des paquets quittant une interface.
- N'oubliez pas de configurer le « ip nat outside » sur l'interfaçage faisant face au WAN (même si ne traduisant pas l'adresse extérieure) !
- Dès que NAT sera configuré, show ip nat translations n'affiche rien. Cinglez une fois et vérifiez alors de nouveau.
- Saisissez les **suivis de wireshark** sur des interfaces internes et externes du NAT-SBC

Scénarios

La sortie de débogage pour quelques scénarios sont affichées ci-dessous. Ils sont en grande partie explicites !

NAT de base

La configuration et mettent au point des lignes pour NAT de base sont affichées ci-dessous.

```
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

Des lignes de sortie du **sip de debug ip nat** sont affichées. Dans ce cas, l'adresse IP incluse sur un paquet sortant est traduite.

```
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:
```

Références

Aperçu :

- http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html
- Anatomie : 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 et NAT

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

Matrice NAT de caractéristique

- 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

NAT Traversal hébergé :

- 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