NAT dans VoIP

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- NAT statique
- NAT dynamique
- Surcharge NAT (PAT)
- Options de commande NAT
- trou d'épingle NAT
- NAT dans VoIP
- ALGUES
- Passerelles
- CME
- Municipal
- Local à distant
- Télétravailleur distant
  - Téléphones distants avec accès public (lecture : routable) adresses IP
  - Téléphones distants avec adresse IP privée
- Téléphones SIP distants
- CUBE
- Traversée NAT hébergée
- NAT SBC
  - Notes de conception
  - Configuration
  - Flux d'appels avec NAT SBC
  - Enregistrement SIP
- CUSPIDE
- Dépannage
  - Symptômes
  - Commandes show et debug
  - Choses à vérifier
  - Scénarios
    - NAT de base
    - SIP ALG
- Références

Introduction

Ce document décrit le comportement NAT (Network Address Translation) dans les routeurs fonctionnant sous CUBE (Cisco Unified Border Element), CME ou CUCME (Cisco Unified Communications Manager Express), les passerelles et CUSP (Cisco Unified SIP Proxy).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SIP (Session Initiation Protocol)
- Voix sur IP (Internet Protocol)
- Protocoles de routage

Composants utilisés

Les informations contenues dans ce document sont basées sur

- Toute version 12.4T et ultérieure de la plate-forme logicielle Cisco IOS
- Toute version de CME

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

La traduction d’adresses réseau est une technique couramment utilisée pour traduire des adresses IP sur des paquets qui circulent entre des réseaux en utilisant des espaces d’adressage différents. L'objectif de ce document n'est pas de réviser la NAT. Ce document vise plutôt à fournir une analyse complète de la NAT telle qu'elle est utilisée dans les réseaux VoIP de Cisco. En outre, le champ d'application est limité aux composants qui constituent la technologie MS-Voice.

- La fonction NAT remplace essentiellement l'adresse IP des paquets par une adresse IP différente
- Permet à plusieurs hôtes d’un sous-réseau privé de partager (c’est-à-dire d’apparaître comme) une adresse IP publique unique pour accéder à Internet.
- En général, les configurations NAT modifient uniquement l’adresse IP des hôtes internes
- NAT est bidirectionnel : si A est traduit en B sur l'interface interne, B arrivant sur l'interface externe sera traduit en A !
- RFC1631

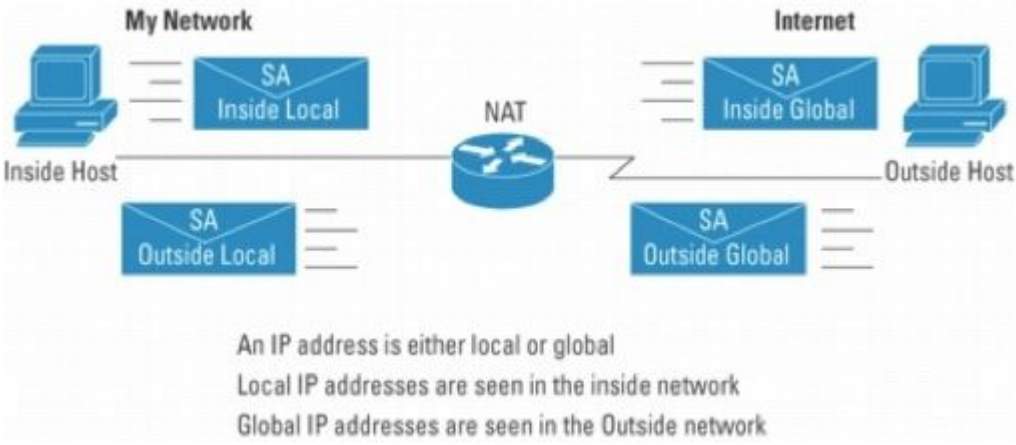


Figure 1

Remarque : il peut être utile de considérer la NAT comme une aide pour acheminer des paquets IP vers et depuis des réseaux utilisant un espace d'adressage privé. En d'autres termes, la fonction NAT rend routables les adresses non routables

---

La Figure 2 illustre la topologie référencée dans les illustrations suivantes.

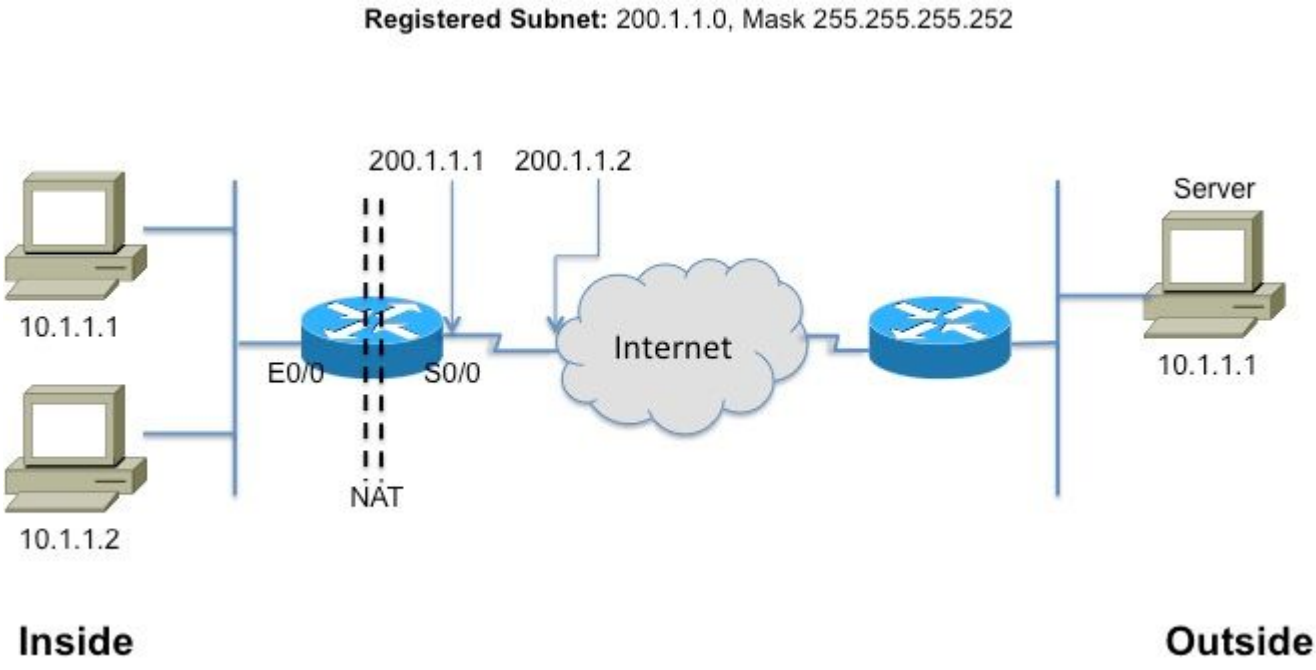


Figure 2

Ce glossaire est essentiel pour comprendre et décrire la fonction NAT

- Adresse locale interne : adresse IP attribuée à un hôte sur le réseau interne. En général, l'adresse provient d'un espace d'adressage privé.
- Adresse globale interne : adresse IP routable attribuée par la carte réseau ou le fournisseur d'accès qui représente une ou plusieurs adresses IP locales internes au monde extérieur.
- Outside local address : adresse IP d'un hôte externe telle qu'elle apparaît au réseau interne. Pas nécessairement une adresse légitime, elle est allouée à partir d'un espace d'adressage

routable à l'intérieur.
- Outside global address : adresse IP attribuée à un hôte sur le réseau externe par le propriétaire de l'hôte. L'adresse est attribuée à partir d'une adresse routable globalement ou d'un espace réseau.

Remarque : soyez à l'aise avec ces termes. Toute note ou document sur NAT est sûr de s'y référer

---

NAT statique

Il s'agit de la forme la plus simple de la NAT, dans laquelle chaque adresse interne est traduite statiquement en une adresse externe (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

La CLI de configuration pour la traduction ci-dessus est la suivante

interface Ethernet0/0

adresse ip 10.1.1.3 255.255.255.0

ip nat inside

!

interface Serial0/0

adresse ip 200.1.1.251 255.255.255.252

ip nat outside <— Obligatoire ![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

NAT dynamique

Dans la NAT dynamique, chaque hôte interne est mappé à une adresse d'un pool d'adresses.

- Alloue une adresse IP à partir d'un pool d'adresses globales internes.
- Si un nouveau paquet arrive d'un autre hôte interne et qu'il a besoin d'une entrée NAT, mais que toutes les adresses IP regroupées sont utilisées, le routeur rejette simplement le paquet.

- En fait, le pool d'adresses globales internes doit être aussi grand que le nombre maximal d'hôtes simultanés devant utiliser Internet en même temps

L'ILC suivante illustre la configuration de la 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)

Lorsque le pool (d'adresses IP) est plus petit que l'ensemble d'adresses à traduire, cette fonctionnalité est pratique.

- Plusieurs adresses internes sont associées à une seule adresse ou à quelques adresses externes
- La fonction PAT (Port Address Translation) utilise des numéros de port source uniques sur l'adresse IP globale interne pour distinguer les traductions. Comme le numéro de port est codé sur 16 bits, le nombre total peut théoriquement atteindre 65 536 par adresse IP. PAT tentera de conserver le port source d'origine, si ce port source est déjà attribué, PAT tentera de trouver le premier numéro de port disponible
- La surcharge NAT peut utiliser plus de 65 000 ports, ce qui lui permet de s'adapter facilement sans avoir besoin de nombreuses adresses IP enregistrées (dans de nombreux cas, une seule adresse IP globale externe est nécessaire).

La Figure 4 illustre la PAT.

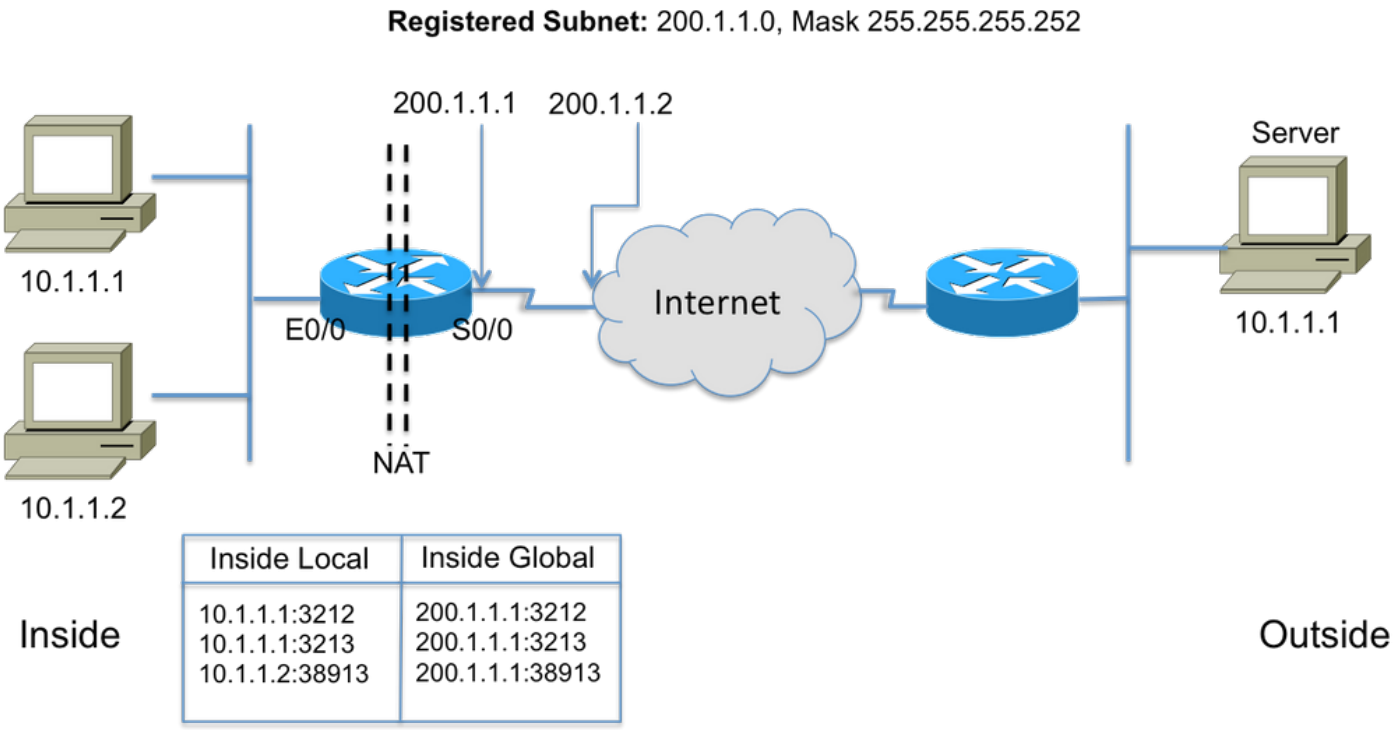


Figure 4

Options de commande NAT

La mise en oeuvre de la fonction NAT de Cisco est très polyvalente avec de nombreuses options. Quelques-unes sont répertoriées ci-dessous, mais veuillez vous reporter à http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a008 pour obtenir des détails sur la liste complète des améliorations.

- Traductions statiques avec ports : paquets entrants adressés à un port spécifique (par ex. port 25, pour le serveur SMTP) envoyé à un serveur spécifique.
- Prise en charge des cartes de routage - Flexibilité dans la configuration des filtres/ACL
- Configurations de pool plus flexibles : pour permettre des plages d'adresses discontinues.
- Conservation du numéro d'hôte - Traduisez la partie « réseau » et conservez la partie « hôte ».

trou d'épingle NAT

Un trou d'épingle dans le langage NAT fait référence au mappage entre les tuples <adresse IP hôte, port> et <adresse globale, port global>. Il permet au périphérique NAT d'utiliser le numéro de port de destination (qui serait le port global) des messages entrants pour mapper la destination vers l'IP hôte et le port qui a lancé la session. Il est important de noter que les trous d'épingle expirent après une période de non-utilisation et que l'adresse publique est renvoyée au pool NAT.

NAT dans VoIP

Quels sont donc les problèmes et les préoccupations liés à la fonction NAT dans les réseaux VoIP ? Rappelez-vous que la NAT dont nous avons parlé jusqu'à présent (appelée NAT de base) traduit uniquement l'adresse IP dans l'en-tête de paquet IP et recalcule la somme de contrôle, bien sûr, mais la signalisation VoIP transporte les adresses intégrées dans le corps des messages de signalisation. En d'autres termes, au niveau de la couche 5

La Figure 5 illustre l'effet de laisser les adresses IP intégrées non traduites. La signalisation d'appel a réussi, mais le proxy SIP du fournisseur de services ne parvient pas à acheminer les paquets de support (RTP) vers l'adresse de support envoyée par l'agent d'appel !

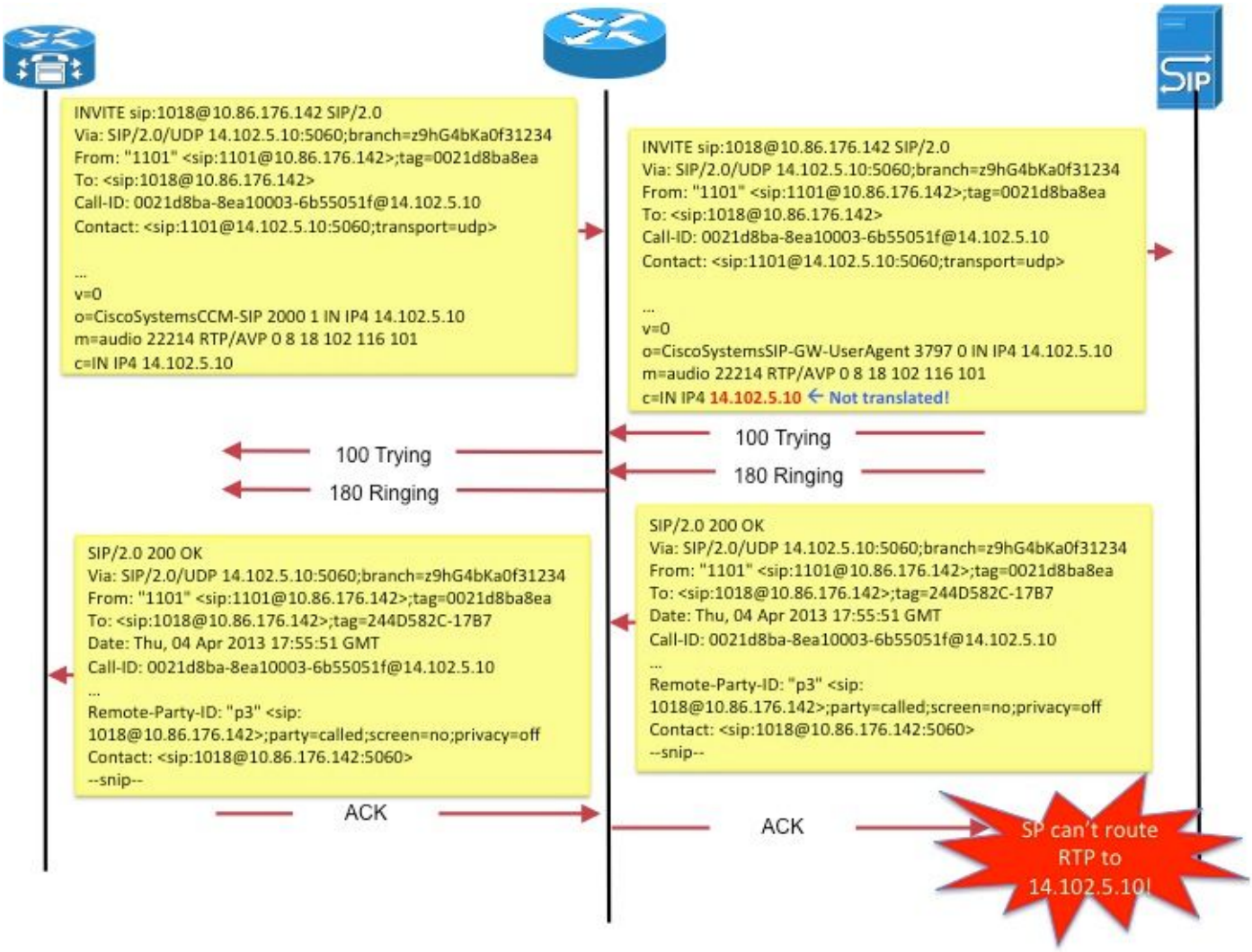


Figure 5

L'utilisation de Contact par le terminal SIP est un autre exemple : dans SDP pour communiquer l'adresse à laquelle le terminal souhaite recevoir des messages de signalisation pour les nouvelles requêtes.

Ces problèmes sont résolus par une fonctionnalité appelée passerelle de couche application (ALG).

ALGUES

Un ALG comprend le protocole utilisé par les applications spécifiques qu'il prend en charge (par exemple, SIP) et procède à l'inspection des paquets de protocole et à la « correction » du trafic qui le traverse. Pour une description correcte de la façon dont les différents champs sont corrigés pour la signalisation d'appel SIP, référez-vous à http://www.voip-info.org/wiki/view/Routers+SIP+ALG.

Sur les routeurs Cisco, la prise en charge du protocole SIP ALG est activée par défaut sur le port TCP 5060 standard. Il est possible de configurer ALG pour prendre en charge des ports non standard pour la signalisation SIP. Reportez-vous à la [page http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.](http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.)

⚠ Attention : Attention ! Il n'existe aucune RFC ou autre norme qui précise quels champs incorporés doivent être traduits pour les différents protocoles VoIP. Par conséquent, les mises en oeuvre varient d'un fournisseur d'équipement à l'autre, ce qui entraîne des problèmes d'interopérabilité (et des cas TAC).

Passerelles

Étant donné que les passerelles ne sont pas, par définition, des périphériques ip à ip, la fonction NAT n'est pas applicable.

CME

Cette section du document passe en revue les scénarios d'appel avec CME pour comprendre pourquoi la NAT doit être utilisée.

Scénario 1. Téléphones locaux

Scénario 2. Téléphones distants (avec adresses IP publiques)

Scénario 3. Télétravailleur distant

Remarque : dans tous les cas, pour que le flux audio puisse s'effectuer, l'adresse IP CME doit être routable

Municipal

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



Figure 6

Remarque : n'oubliez pas que le téléphone maigre connecté lors d'un appel à un autre téléphone maigre du même système CME envoie ses paquets multimédias directement à l'autre téléphone. C'est-à-dire que le protocole RTP entre les téléphones locaux ne passe PAS par CME.

Par conséquent, la fonction NAT n'est pas applicable ou requise dans ce cas.

Remarque : CME détermine si le support (RTP) doit être directement ou non basé sur le fait que les deux téléphones impliqués dans un appel sont minces et dans le même segment de réseau. Sinon, CME s'insère dans le chemin RTP.

Local à distant

Dans ce scénario (Figure 7), CME s'insère dans le flux RTP de sorte que le RTP des téléphones se termine sur le CME. CME va réacheminer les flux vers l'autre téléphone. Comme CME est installé à la fois sur le réseau interne (privé) et sur le réseau externe et envoie son adresse interne au téléphone interne et son adresse externe (publique) au téléphone externe, la fonction NAT n'est pas requise ici non plus.

Notez cependant que les ports UDP/TCP (signalisation et RTP) doivent être ouverts entre le téléphone IP distant et l'adresse IP source CME. Cela signifie que les pare-feu ou autres périphériques de filtrage sont configurés pour autoriser les ports en question.

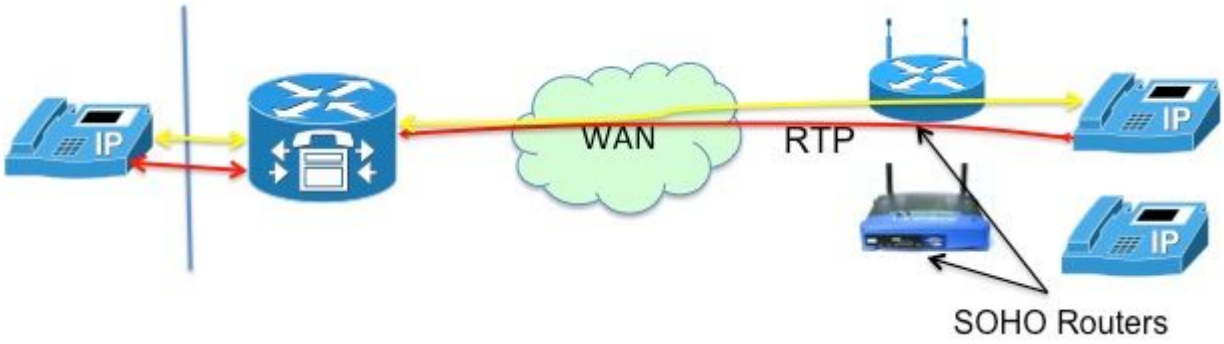


Figure 7

Remarque : notez que la signalisation [messages] se termine toujours sur CM

Télétravailleur distant

Il s'agit des téléphones IP qui se connectent à CME sur un réseau étendu pour prendre en charge les télétravailleurs dont les bureaux sont distants du routeur CME. Les conceptions les plus courantes sont celles impliquant des téléphones avec des adresses IP routables et des téléphones avec des adresses IP privées.

Téléphones distants avec accès public (lecture : routable) adresses IP

Si les deux téléphones impliqués dans l'appel sont configurés avec des adresses IP routables publiques, le média peut circuler entre les téléphones directement (Figure 8). Par conséquent, une fois de plus, la fonction NAT n'est pas nécessaire !

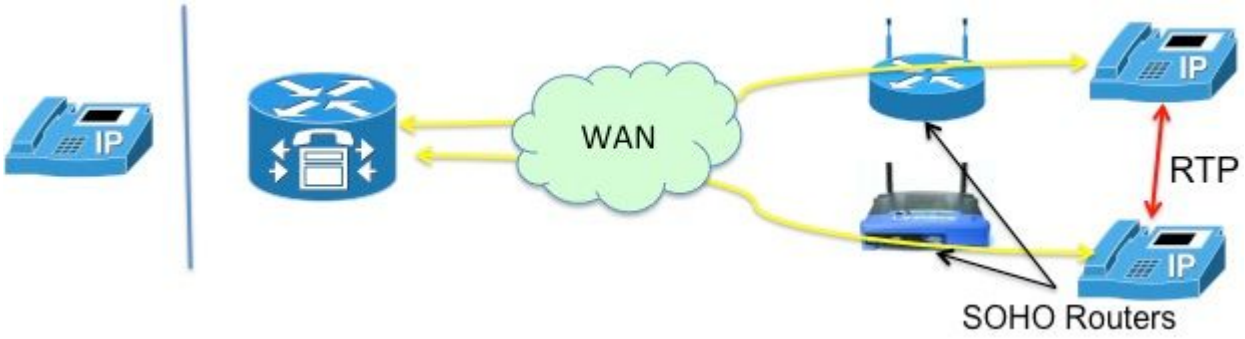


Figure 8

Téléphones distants avec adresse IP privée

Dans ce scénario, l'appel est signalé entre des téléphones maigres configurés avec des adresses IP privées. En général, les routeurs de bureau à domicile (SOHO) ne sont pas compatibles avec le protocole SCCP. c'est-à-dire incapable de traduire les adresses IP intégrées dans les messages SCCP. Cela signifie qu'à la fin de l'établissement de l'appel, les téléphones se terminent par l'adresse IP privée de l'autre. Comme les deux téléphones sont privés, CME signale l'appel entre eux de sorte que le flux audio circule directement entre les téléphones. Cependant, cela aboutira à un son unidirectionnel ou non (puisque les adresses IP privées, par définition, ne peuvent pas être routées vers sur Internet !), à moins que l'une des solutions de contournement suivantes ne soit implémentée-

· Configurer des routes statiques sur les routeurs SOHO

· Établir une connexion VPN IPsec aux téléphones

Une meilleure façon de résoudre ce problème serait de configurer « mtp ». La commande mtp garantit que les paquets de support (RTP) des téléphones distants transitent par le routeur CME (Figure 9).

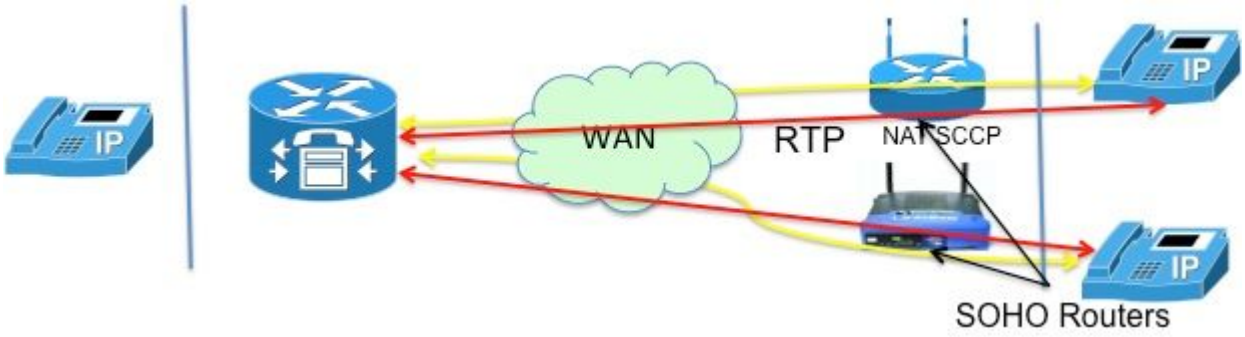


Figure 9

La solution « mtp » est plus adaptée en raison des complications liées à l'ouverture des ports de pare-feu. Les paquets multimédias circulant sur un réseau étendu peuvent être bloqués par un pare-feu. Cela signifie que vous devez ouvrir des ports sur le pare-feu, mais lesquels ? Avec CME relayant l'audio, les pare-feu peuvent être facilement configurés pour transmettre les paquets RTP. Le routeur CME utilise un port UDP spécifique (2000 !) pour les paquets multimédias. Ainsi,

en autorisant simplement les paquets à destination et en provenance du port 2000, TOUT le trafic RTP peut être transmis.

La Figure 10 illustre la configuration de mtp.

```
Ephone 1
  mac 111.222.3333
  type 7965
  mtp
  bouton 1:1
```

Figure 10

Tout n'est pas merveilleux avec mtp. Il existe des situations où mtp peut ne pas être souhaitable

- MTP n'est pas doux sur l'utilisation du CPU
- L'attente musicale multidiffusion ne peut généralement pas être transférée sur un réseau étendu : la fonctionnalité d'attente musicale multidiffusion vérifie si le protocole MTP est activé pour un téléphone et, si tel est le cas, n'envoie pas d'attente musicale à ce téléphoneL.

Ainsi, si vous avez une configuration WAN qui peut transférer des paquets multicast et que vous pouvez autoriser des paquets RTP à travers votre pare-feu, vous pouvez décider de ne pas utiliser MTP.

Téléphones SIP distants

Notez que les téléphones SIP n'ont pas été mentionnés dans les scénarios ci-dessus. En effet, si l'un des téléphones est un téléphone SIP, CME s'insère dans le chemin audio. Cela devient alors le scénario local-à-distant décrit précédemment, dans lequel la NAT n'est pas requise.

CUBE

Le CUBE exécute de manière inhérente les fonctions NAT et PAT lorsqu'il termine et réinitialise toutes les sessions. Le CUBE substitue sa propre adresse à l'adresse de tout terminal avec lequel il communique, masquant ainsi (traduisant) efficacement l'adresse de ce terminal.

Par conséquent, la fonction NAT n'est pas requise avec la fonction CUBE. Il existe un scénario de service VoIP dans lequel la NAT est requise sur le CUBE, comme décrit dans la section suivante.

Traversée NAT hébergée

Un bref aperçu du service de téléphonie hébergée vous aidera à comprendre la raison d'être de cette fonctionnalité.

Le service de téléphonie hébergée est une nouvelle forme de service VoIP dans laquelle la plupart des équipements se trouvent sur le site du fournisseur de services. Ils fonctionnent avec les passerelles domestiques (HGW), qui implémentent uniquement la NAT de base (c'est-à-dire la NAT au niveau des couches 3 et 4). Par exemple, Verizon installe le terminal de réseau optique (ONT), qui fournit des services FiOS dans la maison ; l'appel vocal est signalé à l'aide d'un processus SIP intégré à l'ONT. La signalisation SIP est effectuée sur le réseau IP privé de Verizon vers de nouveaux commutateurs logiciels, qui fournissent le service et le contrôle pour établir des communications vocales à d'autres clients de voix numérique FiOS, ou à des clients de téléphone traditionnels.

Parmi les principales exigences du fournisseur pour le service de téléphonie hébergé figurent :

- Traversée NAT distante : la possibilité de fournir des services de classe 5 aux terminaux utilisant la NAT (qui ne peut faire que la couche 3 de la NAT !) et les périphériques pare-feu (en faisant « ALG » à distance !)
- Prise en charge du co-média : La possibilité d'envoyer des supports entre des périphériques colocalisés lorsqu'il n'est pas logique de les router vers le réseau IP
- Aucun équipement supplémentaire, ce qui élimine la nécessité d'ajouter des CPE.

Compte tenu de ce qui précède, quelles options existe-t-il pour mettre en oeuvre un tel service ?

- Remplacer le matériel par un équipement ALG onéreux,
- Utilisez un SBC (Session Border Controller) pour modifier les en-têtes SIP intégrés des paquets. Il s'agit d'un produit hébergé sur le réseau, de qualité opérateur, prenant en charge le protocole SIP dans une configuration très sécurisée et à tolérance de panne. Cette solution est appelée NAT SBC.

L'option NAT SBC répond aux exigences du fournisseur énumérées ci-dessus.

NAT SBC

Le SBC NAT fonctionne comme suit (Figure 11)

1. Le routeur d'accès traduit uniquement l'adresse IP L3/L4
2. Adresse IP du message SIP non traduite
3. La fonction NAT SBC intercepte et traduit l'adresse IP intégrée. Dès que le SBC voit des paquets SIP destinés à 200.200.200.10, il lance le code nat-sbc.
4. Le support n'est pas traduit et passe directement d'un téléphone à l'autre[5]

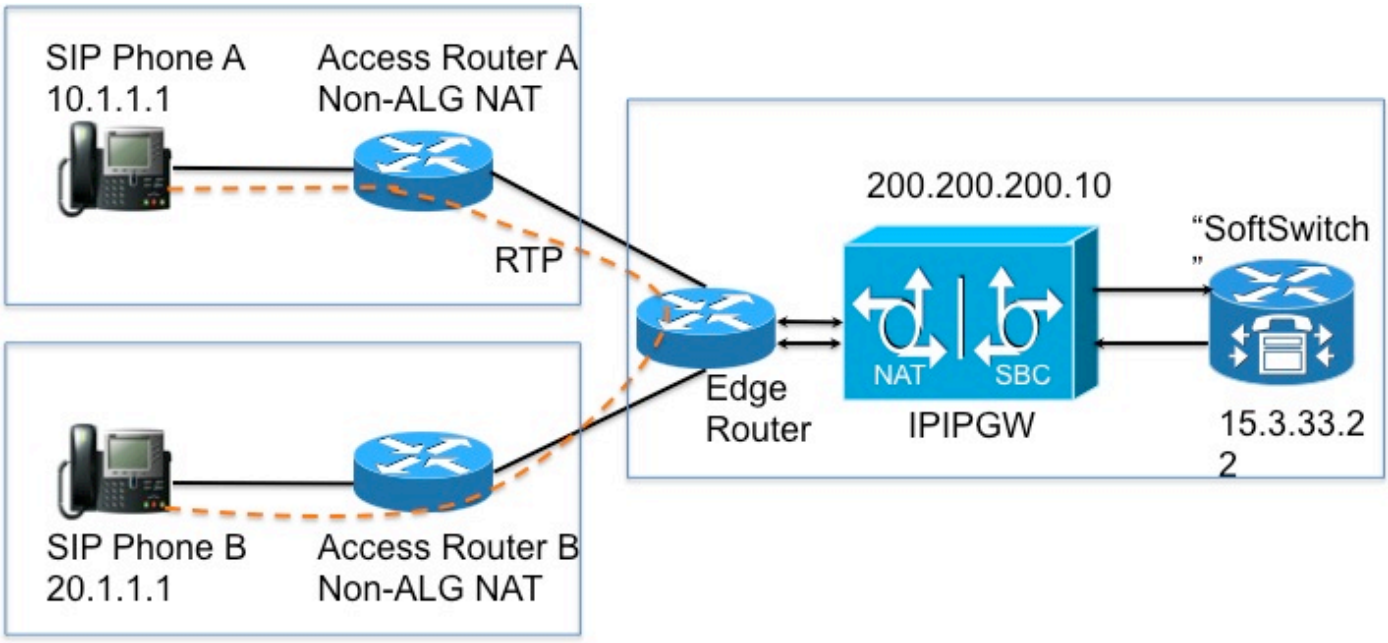


Figure 11

Notes de conception

- L'adresse IP 200.200.200.10 (Figure 12) n'est attribuée à aucune interface sur le SBC NAT. Il est configuré comme l'adresse du « proxy » auquel les téléphones SIP A et B envoient des messages de signalisation.
- Les périphériques domestiques ne traduisent pas certains champs d'adresse SIP/SDP uniquement (par exemple Call-Id: , O= , Avertissement : headers & branch= paramètre. les paramètres maddr= et received= ont été traités dans certains scénarios uniquement.) Ces champs sont gérés par le SBC NAT, à l'exception de l'autorisation proxy et de la traduction d'autorisation, car ils interrompent l'authentification.
- Si les périphériques domestiques sont configurés pour effectuer la PAT, les agents utilisateurs (téléphones et proxy) doivent prendre en charge la signalisation symétrique[6] et les supports symétriques et précoces. Vous devez configurer le port de remplacement sur le routeur NAT SBC.
- En l'absence de prise en charge de la signalisation symétrique et des supports symétriques et précoces, les routeurs intermédiaires doivent être configurés sans PAT et l'adresse de remplacement doit être configurée dans le SBC NAT.

Configuration

Voici un exemple de configuration pour un SBC NAT typique.

```
ip nat sip-sbc

  proxy 200.200.200.10 5060 15.3.33.22 5060 protocole udp

  call-id-pool call-id-pool

  session-timeout 300
```

```
  mode allow-flow-around
  port de priorité
!
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 0.0.0.25
access-list 1 permit 171.1.1.0 0.0.0.25
access-list 2 permit 20.1.1.0 0.0.0.25
access-list 2 permit 172.1.1.0 0.0.0.25
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
```

Flux d'appels avec NAT SBC

Les figures 13 et 14 illustrent le flux d'appels en termes de traductions. Il convient de noter les points suivants :

- Lors de l'enregistrement, le commutateur logiciel note les deux téléphones comme
  - — Téléphone SIP A - 15.3.3.62 2001
  - — Téléphone SIP B - 15.3.3.62 2002
- Dans ce flux d'appels, la fonction NAT SBC laisse effectivement l'adresse IP du support non

traduite.

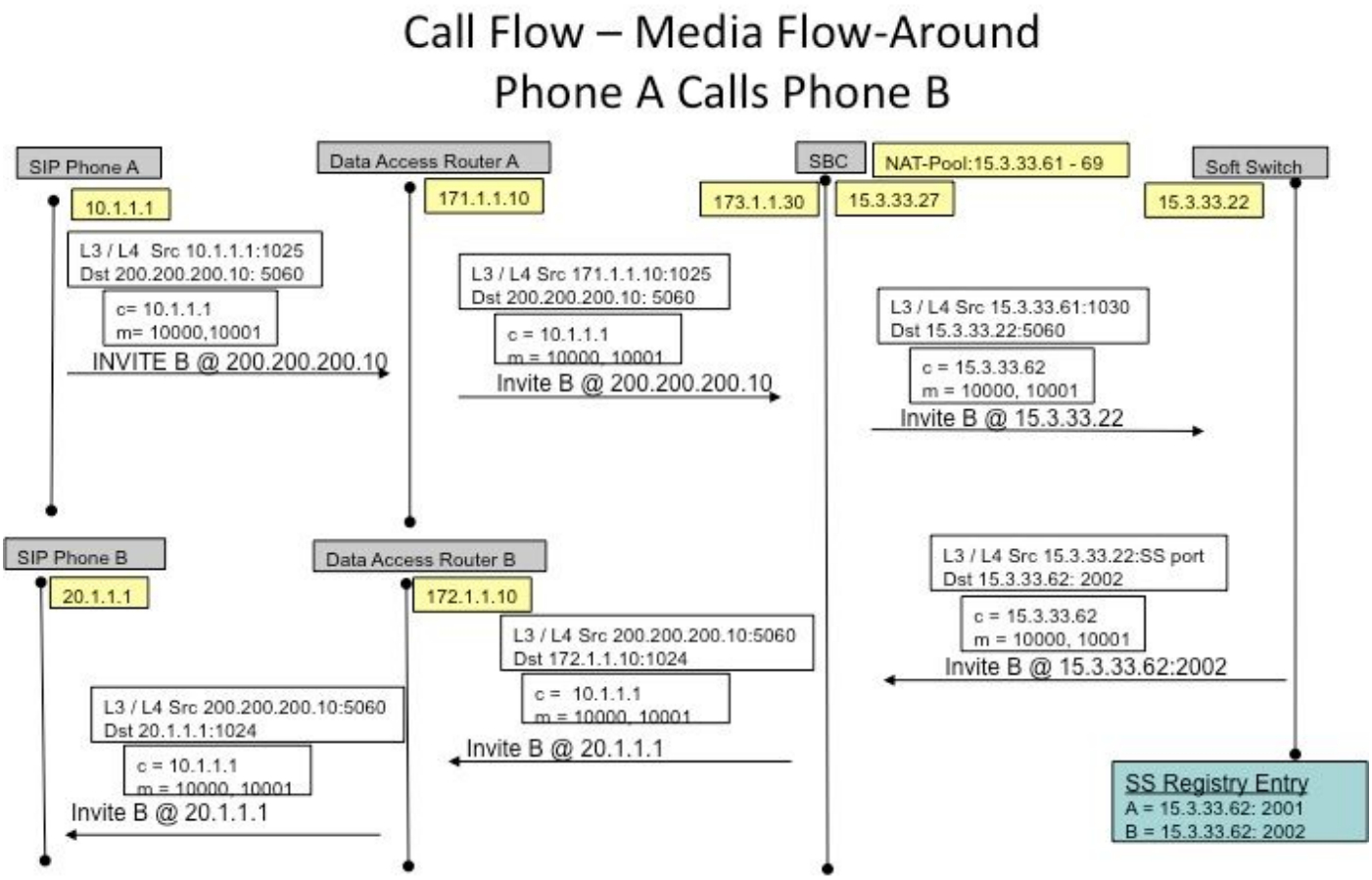


Figure 13

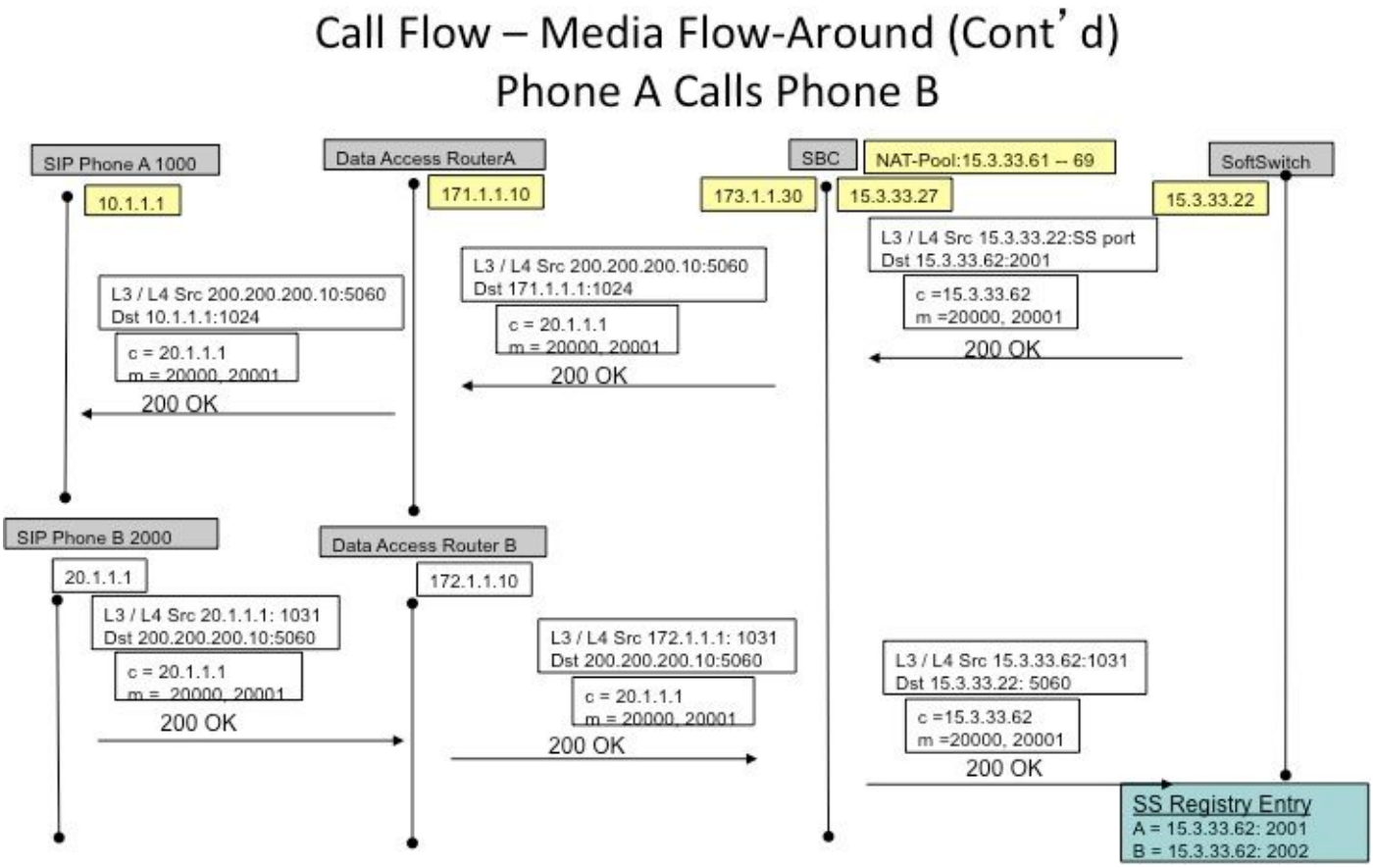


Figure 14

Enregistrement SIP

Dans les versions précédentes (de la NAT SBC), les terminaux SIP devaient envoyer des paquets keep-alive pour maintenir le trou d'épingle SIP Registration ouvert (pour permettre au trafic sortant->entrant de circuler, par exemple des appels entrants). Les paquets keep-alive pouvaient être n'importe quel paquet SIP envoyé par le terminal ou le registrar (commutateur logiciel). Les versions récentes n'en ont pas besoin, le NAT-SBC lui-même (par opposition aux commutateurs logiciels) obligeant les terminaux à se réenregistrer fréquemment pour garder les trous d'épingle ouverts.

Remarque : Les symptômes d'un sténopé d'enregistrement expiré peuvent être obscurs, avec des échecs de signalisation d'appel aléatoires.

CUSPIDE

CUSP a la notion d'un réseau logique, qui se réfère à un ensemble d'interfaces locales qui sont traitées de la même manière pour (par ex. interface, port, transport pour l'écoute). Lorsque vous configurez un réseau logique sur CUSP, vous pouvez le configurer pour utiliser la NAT. Une fois configuré, SIP ALG est automatiquement activé. Cela est utile lorsque certains réseaux logiques.

Dépannage

Symptômes

Un symptôme évident peut être qu'un appel échoue dans une direction ou dans les deux. Les symptômes moins évidents peuvent inclure :

- Son unidirectionnel
- Audio unidirectionnel lors du transfert
- Audio sans issue
- Perte de l'enregistrement SIP

Commandes show et debug

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

Choses à vérifier

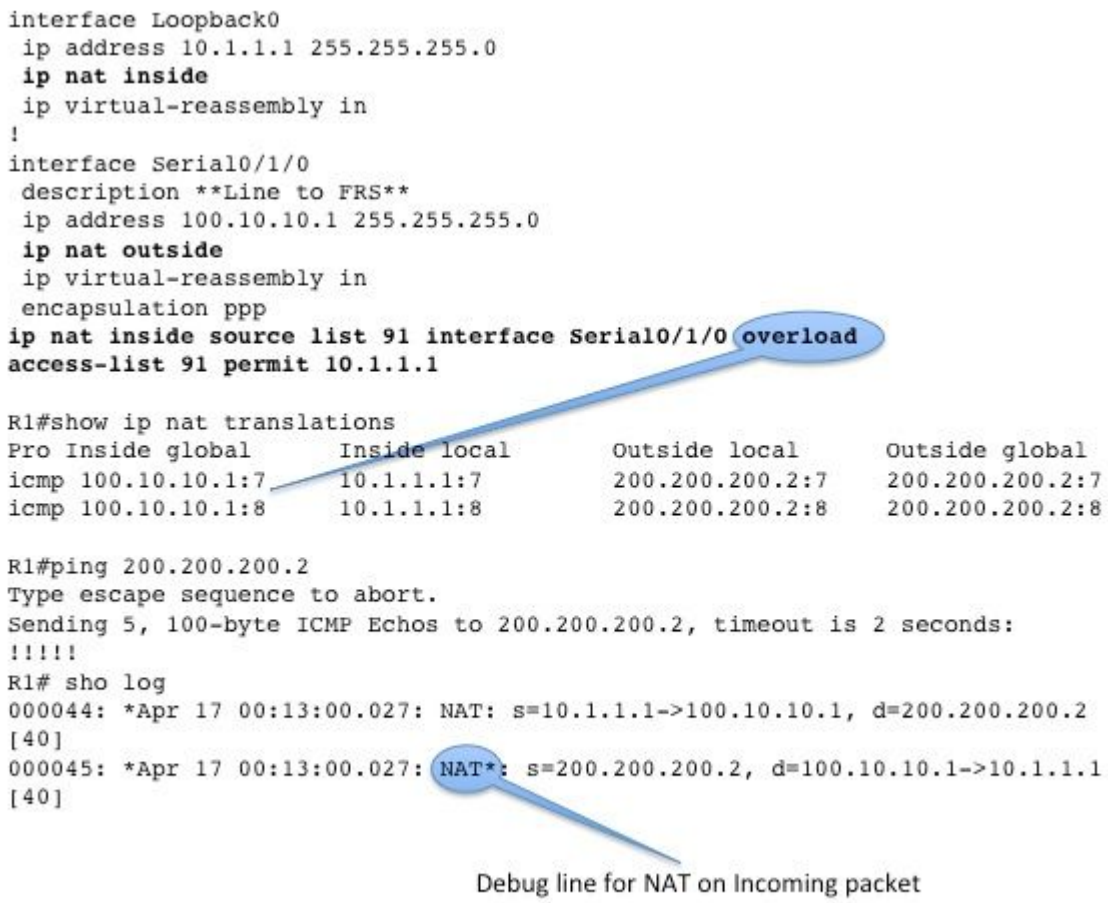
- Assurez-vous que la configuration inclut la sous-commande ip nat inside ou ip nat outside interface. Ces commandes activent NAT sur les interfaces, et la désignation interne/externe est importante.
- Pour la NAT statique, assurez-vous que la commande ip nat source static liste d'abord l'adresse locale interne et ensuite l'adresse IP globale interne.
- Pour la NAT dynamique, assurez-vous que la liste de contrôle d’accès configurée pour correspondre aux paquets envoyés par l’hôte interne correspond aux paquets de cet hôte, avant toute traduction NAT. Par exemple, si une adresse locale interne de 10.1.1.1 doit être traduite en 200.1.1.1, assurez-vous que la liste de contrôle d’accès correspond à l’adresse source 10.1.1.1 et non à 200.1.1.1.
- Pour la NAT dynamique sans PAT, assurez-vous que le pool a suffisamment d'adresses IP. Les symptômes d'un manque d'adresses incluent une valeur croissante dans le deuxième compteur d'échecs dans la sortie de commande show ip nat statistics, ainsi que l'affichage de toutes les adresses dans la plage définie dans le pool NAT dans la liste des traductions dynamiques.
- Pour PAT, il est facile d'oublier d'ajouter l'option overload sur la commande ip nat inside source list. Sans cela, la fonction NAT fonctionne, mais pas la fonction PAT, ce qui entraîne souvent une non-traduction des paquets des utilisateurs et une impossibilité pour les hôtes d'accéder à Internet.
- La fonction NAT a peut-être été configurée correctement, mais une liste de contrôle d’accès existe sur l’une des interfaces, rejetant les paquets. Notez que l’IOS traite les listes de contrôle d’accès avant NAT pour les paquets entrant dans une interface et après avoir traduit les adresses pour les paquets sortant d’une interface.
- N'oubliez pas de configurer « ip nat outside » sur l'interface faisant face au WAN (même si vous ne traduisez pas l'adresse externe) !
- Dès que NAT est configuré, show ip nat translations n'affiche rien. Envoyez une requête ping, puis vérifiez à nouveau.
- Accédez à wireshark Traces sur les interfaces internes et externes de NAT-SBC

Scénarios

Les résultats du débogage pour quelques scénarios sont présentés ci-dessous. Elles sont pour la plupart explicites !

NAT de base

Les lignes de configuration et de débogage pour la NAT de base sont présentées ci-dessous.



SIP ALG

Les lignes de sortie de debug ip nat sip sont affichées. Dans ce cas, l'adresse IP intégrée 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_paper0918
- 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

Voix sur IP 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 de fonctionnalités NAT

- 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_paper09186a0080
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919.shtml

Traversée NAT hébergée :

- 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#wp107737
- http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc_cucm.html

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.