NAT in VoIP

Inhoud

Inleiding

Dit document beschrijft NAT-gedrag (netwerkadresomzetting) in routers die werken als CUBE

(Cisco Unified border-element), CME of CUCME (Cisco Unified Communications Manager Express), gateways en CUSP (Cisco Unified SIP proxy).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SIP (Session Initiation Protocol)
- Voice-over-IP (Internet-protocol)
- Routing-protocollen

Gebruikte componenten

De informatie in dit document is gebaseerd op

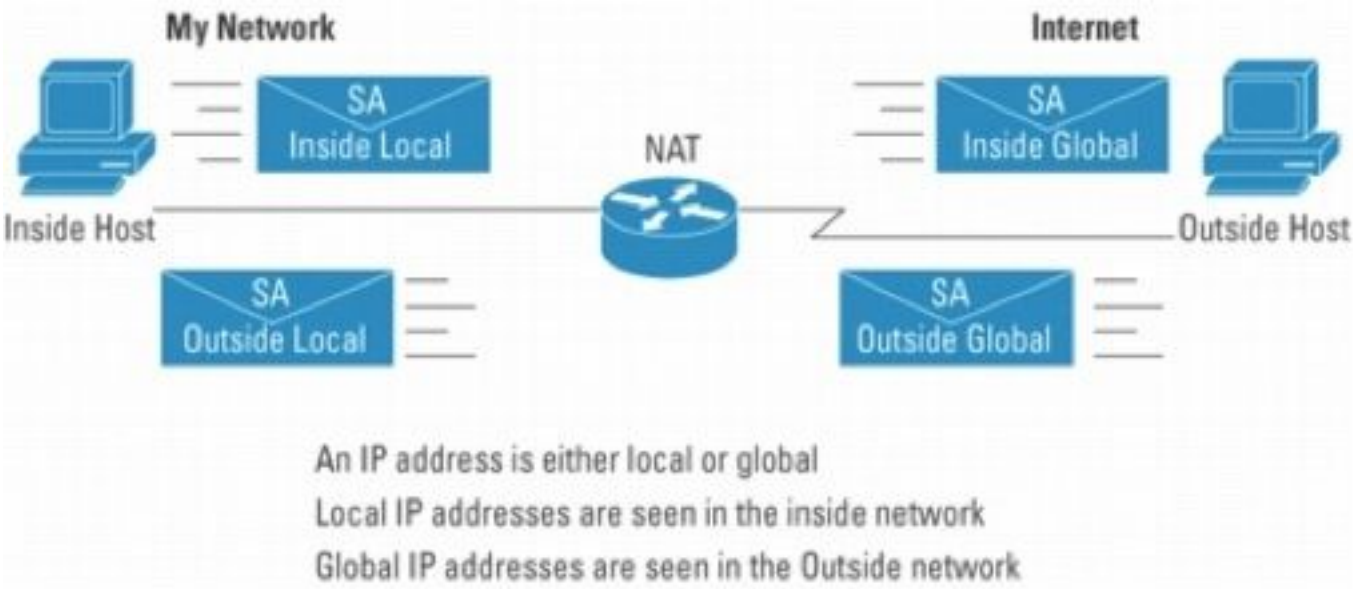
- Elke IOS-versie 12.4T en hoger.
- Elke CME-versie

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Netwerkadresomzetting is een veelgebruikte techniek voor het vertalen van IP-adressen op pakketten die tussen netwerken stromen door gebruik te maken van verschillende adresruimtes. Het doel van dit document is niet om NAT te herzien. Dit document is eerder bedoeld om een uitgebreid overzicht van NAT te bieden zoals het wordt gebruikt in Cisco VoIP-netwerken. Bovendien is de reikwijdte beperkt tot componenten die deel uitmaken van de MS-Voice-technologie.

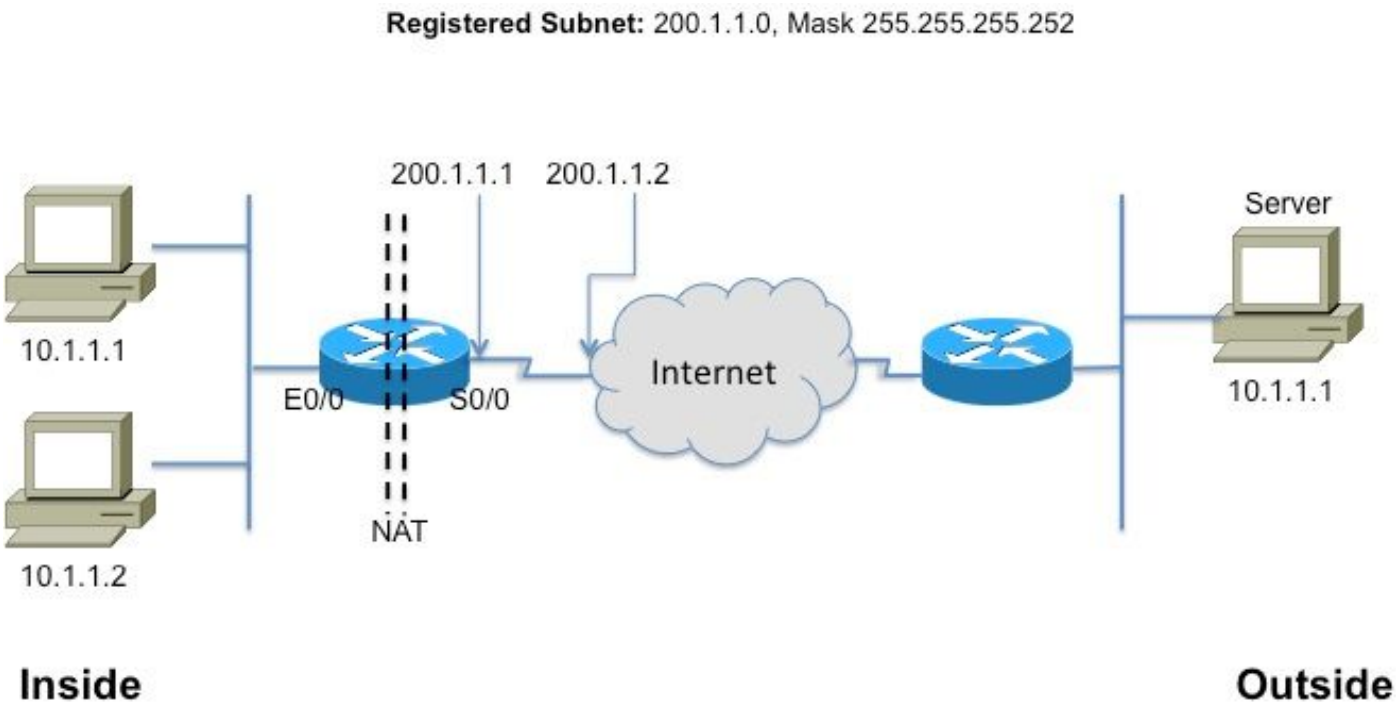
- NAT vervangt in principe het IP-adres in pakketten met een ander IP-adres
- Maakt het mogelijk dat meerdere hosts in een privé-subnetverbinding één openbaar IP-adres *delen* (dat wil zeggen er zo uitzien), om toegang tot het internet te krijgen.
- Normaal gesproken wijzigen NAT-configuraties alleen het IP-adres van interne hosts
- NAT is bidirectioneel - Als A vertaald wordt naar B op de binneninterface, zal B die bij buiteninterface aankomt vertaald worden naar A!
- RFC 1631



Afbeelding 1

> **Opmerking**: het kan helpen om aan NAT te denken als een ondersteuning om IP-pakketten naar en uit netwerken te leiden met behulp van privé-adresruimte. Met andere woorden, NAT maakt niet-routable adressen routable

Figuur 2 toont de topologie die in de illustraties van verwijzingen wordt voorzien die volgen.



Afbeelding 2

Deze verklarende woordenlijst is fundamenteel om NAT te begrijpen en te beschrijven

- **Binnen lokaal adres**—Het IP-adres dat is toegewezen aan een host *binnen* het netwerk. Het adres komt meestal uit een privé-adresruimte.
- **Binnen globaal adres**-een routeerbaar IP adres dat door de NIC of de dienstverlener wordt toegewezen die één of meerdere binnen lokale IP adressen aan de buitenwereld

vertegenwoordigen.

- **Buiten het lokale adres**: het IP-adres van een externe host zoals dit wordt weergegeven in het interne netwerk. Niet noodzakelijk een legitiem adres, het wordt toegewezen van een adresruimte routable aan de binnenkant.
- **Buiten globaal adres**-het IP adres dat aan een gastheer op het buitennetwerk door de gastheereigenaar wordt toegewezen. Het adres wordt toegewezen van een globaal routable adres of netwerkruimte.

Opmerking: Maak u op uw gemak met deze bepalingen. Alle notities of documenten op NAT kunnen hier zeker naar verwijzen

Statische NAT

Dit is de eenvoudigste vorm van NAT, waar in elk binnenadres statisch wordt vertaald naar een buitenadres (en vice versa).

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Afbeelding 3

De CLI naar configuratie voor de bovenstaande vertaling is als volgt

interface Ethernet0/0

IP-adres 10.1.1.3 255.255.255.0

IP NAT binnen

!

interface Serial0/0

IP-adres 200.1.1.251 255.255.255.252

ip Nat buiten <— Vereist![2]

ip Nat binnenbron statisch 10.1.1.2 200.1.1.2

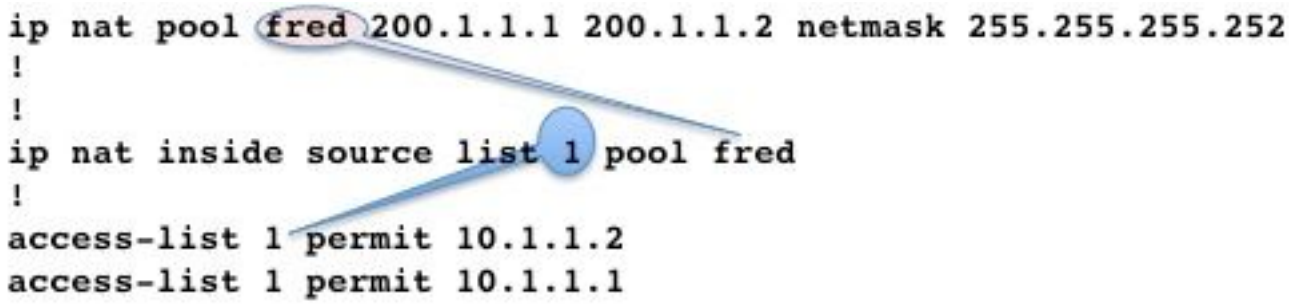
ip Nat binnenbron statisch 10.1.1.1 200.1.1.1

Dynamische NAT

In dynamische NAT, wordt elke binnengastheer in kaart gebracht aan een adres van een pool van adressen.

- Wijst een IP-adres toe uit een pool van globale adressen binnen.
- Als een nieuw pakket van nog een andere binnengastheer aankomt, en het een NAT ingang nodig heeft, maar alle gepoolde IP adressen zijn in gebruik, verwerpt de router eenvoudig het pakket.
- In wezen, de pool van binnen globale adressen moet zo groot zijn als het maximumaantal gelijktijdige hosts die nodig zijn om het internet op hetzelfde moment te gebruiken

De volgende CLI illustreert het configureren van dynamische NAT

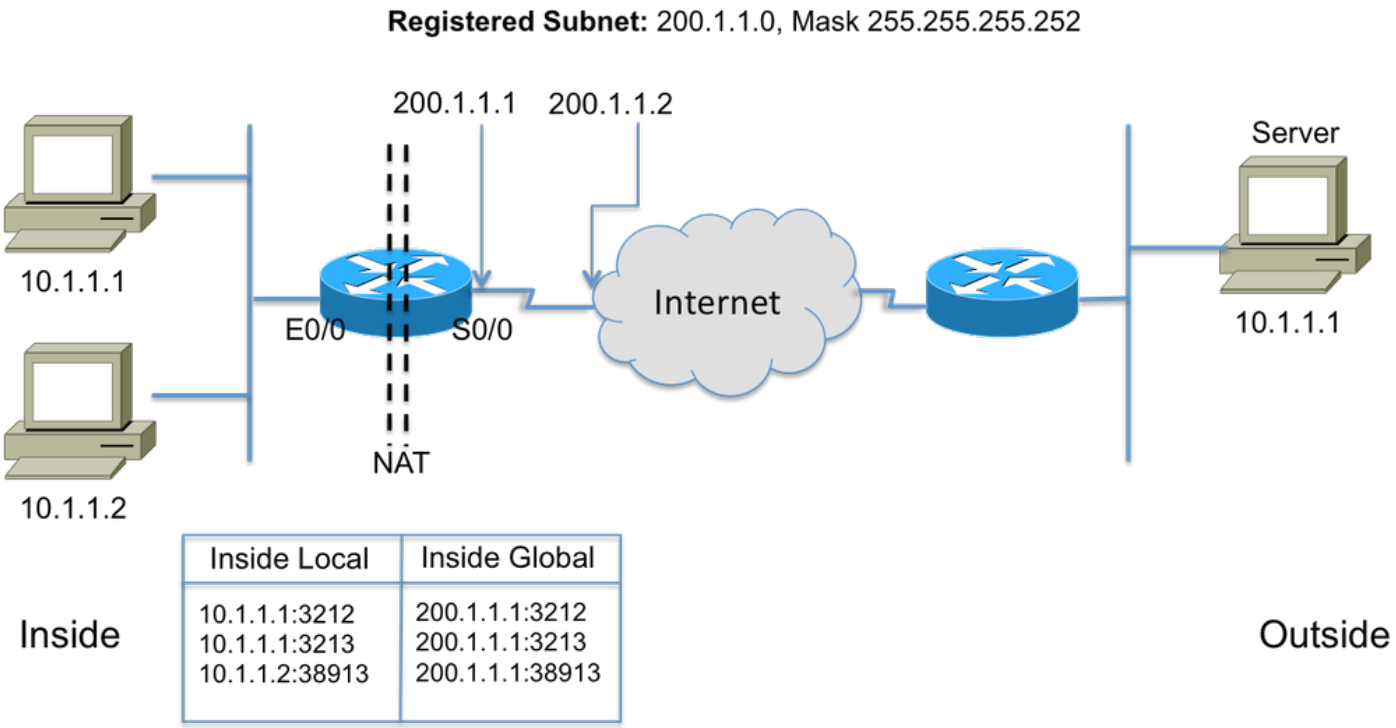


NAT-overbelasting (PAT)

Wanneer de pool (van IP-adressen) kleiner is dan de set adressen die moeten worden vertaald, komt deze functie van pas.

- Verschillende interne adressen NATed aan slechts één of enkele externe adressen
- PAT (Port Address Translation) gebruikt unieke bronpoortnummers op het **wereldwijde** IP-adres Inside om onderscheid te maken tussen vertalingen. Omdat het poortnummer in 16 bits is gecodeerd, kan het totale aantal theoretisch oplopen tot 65.536 per IP-adres. PAT zal proberen de oorspronkelijke bronpoort te behouden als deze bronpoort al is toegewezen. PAT zal proberen het eerste beschikbare poortnummer te vinden.
- NAT-overbelasting kan meer dan 65.000 poorten gebruiken, waardoor het goed kan worden geschaald zonder dat er veel geregistreerde IP-adressen nodig zijn. In veel gevallen is er slechts één extern IP-adres nodig.

Afbeelding 4 illustreert PAT.



Afbeelding 4

NAT-opdrachtopties

Cisco NAT-implementatie is zeer veelzijdig met een groot aantal opties. Een paar worden hieronder vermeld, maar gelieve te verwijzen naar http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html voor details op de volledige lijst van verbeteringen.

- Statische vertalingen met poorten - Inkomende pakketten gericht op een specifieke poort (bijv. poort 25, voor SMTP-server) verzonden naar een specifieke server.
- Ondersteuning voor routekaarten - Flexibiliteit bij het configureren van filters/ACL's
- Flexibelere poolconfiguraties - om discontinue reeksen van adressen toe te staan.
- Het behoud van het gastheeraantal - Vertaal het "netwerk"deel, behoud het "gastheer"deel.

NAT-speldenprik

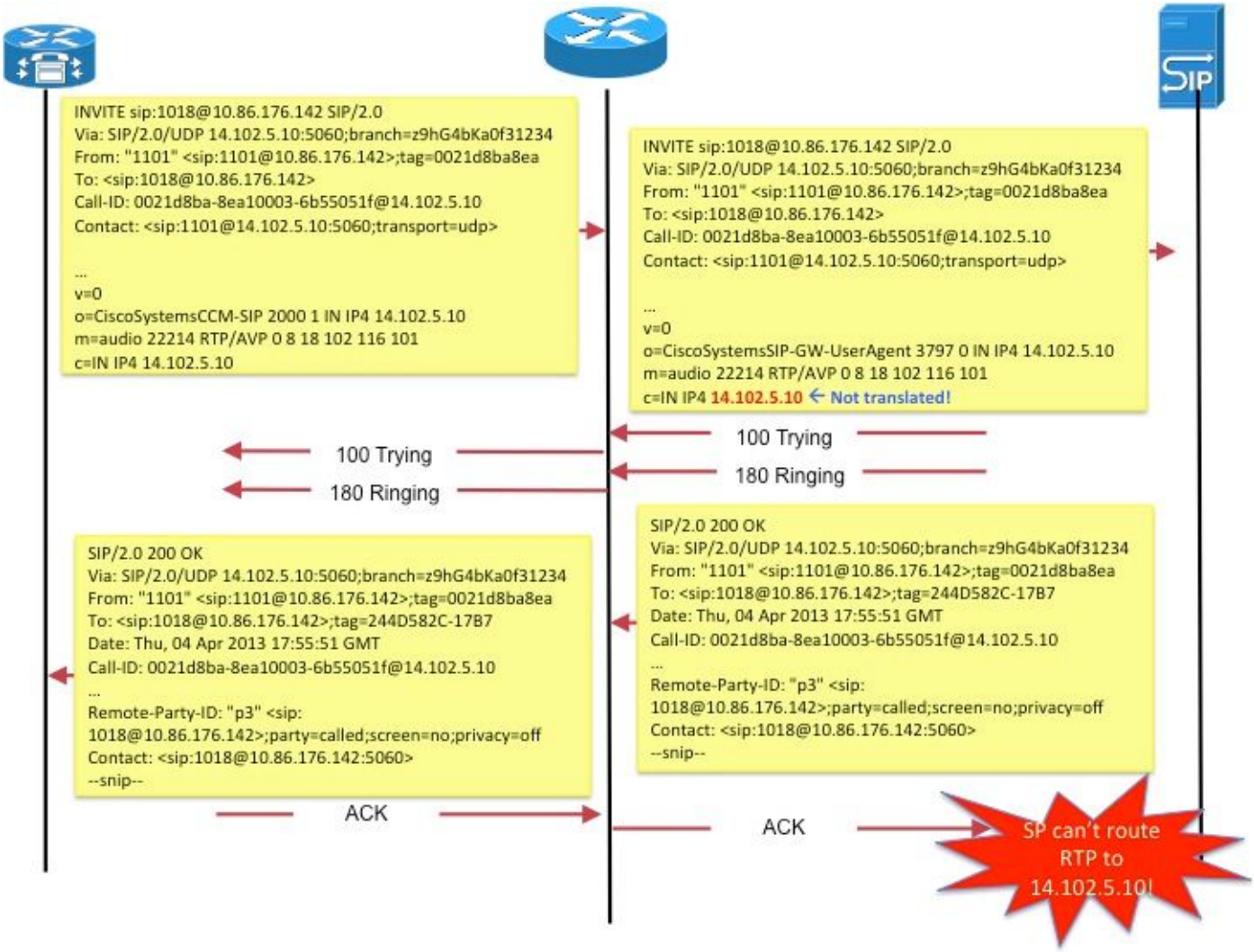
Een spelletje in NAT-taal verwijst naar de koppeling tussen de <host IP, port> en <global address, *global* port> tuples. Het staat het NAT apparaat toe om het aantal van de bestemmingshaven (dat de *globale* haven zou zijn) van inkomende berichten te gebruiken om de bestemming terug naar de gastheer IP en de haven in kaart te brengen die de zitting voortkwamen. Het is belangrijk om op te merken dat pinholes time-out na een periode van niet-gebruik en het publieke adres wordt teruggegeven aan de NAT pool.

NAT in VoIP

Zo, wat zijn de kwesties en de zorgen met NAT in de netwerken van VoIP? Denk eraan dat NAT die we tot nu toe hebben besproken (losjes aangeduid als basis-NAT) alleen het IP-adres vertaalt

in de IP-*pakketheader* en de controlesom herberekent, natuurlijk, maar VoIP-signalering bevat adressen die zijn ingebed in de *kern* van de signaleringsberichten. Met andere woorden, op Layer 5

Afbeelding 5 illustreert het effect van het niet-vertaald laten van de ingesloten IP-adressen. De vraag die signaleert voltooit succesvol, maar de proxy van SIP bij de dienstverlener ontbreekt het proberen om media (RTP) pakketten aan media adres te leiden dat door de call agent wordt verzonden!



Afbeelding 5

Een ander voorbeeld is het gebruik van ***Contact*** door SIP-endpoints*:* veld in SDP om het adres door te geven waar het eindpunt signaleringsberichten voor nieuwe verzoeken wil ontvangen.

Deze kwesties worden behandeld door een eigenschap genoemd Application Layer Gateway (ALG).

ALG

Een ALG begrijpt het protocol dat wordt gebruikt door de specifieke toepassingen die hij ondersteunt (bijv. SIP) en voert protocolpakketinspectie en "fixup" van verkeer door. Zie http://www.voip-info.org/wiki/view/Routers+SIP+ALG voor een goede beschrijving van de manier waarop de verschillende velden zijn ingesteld voor SIP-gesprekssignalering.

Op Cisco-routers is ondersteuning voor ALG SIP standaard ingeschakeld op de standaard TCP-poort 5060. Het is mogelijk om ALG te configureren om niet-standaard poorten voor SIP-signalering te ondersteunen. Raadpleeg http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.

> **Waarschuwing**: Pas op! Er is geen RFC of andere standaard die aangeeft welke ingesloten velden vertaald moeten worden voor de verschillende VoIP protocollen. Als gevolg daarvan verschillen de implementaties van leverancier van apparatuur, wat leidt tot problemen met de interfaces (en TAC-cases).

Gateways

Aangezien gateways per definitie geen ip-to-ip apparaten zijn, is NAT niet van toepassing.

CME

Deze sectie van de de vraagscenario's van het documentoverzicht met CME om te begrijpen waarom NAT moet worden gebruikt.

Scenario 1. Lokale telefoons

Scenario 2. Externe telefoons (met openbare IP-adressen)

Scenario 3. telewerker op afstand

> **Opmerking**: in alle gevallen moet het CME IP-adres routeerbaar zijn om audio te laten stromen

Lokaal

In dit scenario (Afbeelding 6) zijn de twee telefoons die bij de oproep betrokken zijn mager telefoons met privé IP-adressen.

Afbeelding 6

> **Opmerking**: Onthoud dat mager telefoon die is aangesloten in een gesprek met een andere

mager telefoon in hetzelfde CME-systeem zijn mediapakketten rechtstreeks naar de andere telefoon stuurt; D.w.z. RTP voor lokale telefoons naar lokale telefoons stroomt NIET door CME.

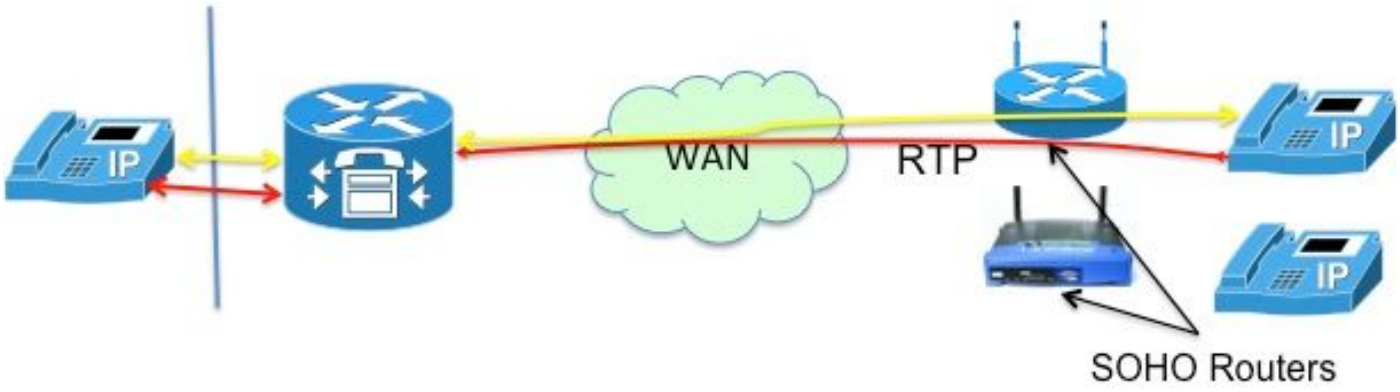
Daarom is NAT in dit geval niet van toepassing of vereist.

Opmerking: CME bepaalt of media (RTP) direct of niet gebaseerd moeten zijn op de vraag of de twee telefoons betrokken bij een oproep zowel mager zijn *als* in hetzelfde netwerksegment. Anders voegt CME zichzelf in het RTP-pad in.

Lokaal naar extern

In dit scenario (afbeelding 7) plaatst CME zichzelf in de RTP-stream zodat RTP van de telefoons op de CME wordt beëindigd. CME zal de stromen naar de andere telefoon opnieuw genereren. Aangezien CME zowel op het binnen (privé) netwerk als het buitennetwerk zit en zijn binnenadres naar de binnentelefoon en buiten (openbaar) adres naar de buitentelefoon verzendt, is NAT ook hier niet vereist.

Houd er echter rekening mee dat de UDP/TCP-poorten (zowel signalering als RTP) moeten zijn geopend tussen externe IP-telefoon en CME-bronIP-adres. Dit betekent dat de firewalls of andere filterapparaten zodanig zijn geconfigureerd dat de poorten in kwestie zijn toegestaan.



Afbeelding 7

Opmerking: Let op dat signalering [berichten] altijd worden beëindigd op CM

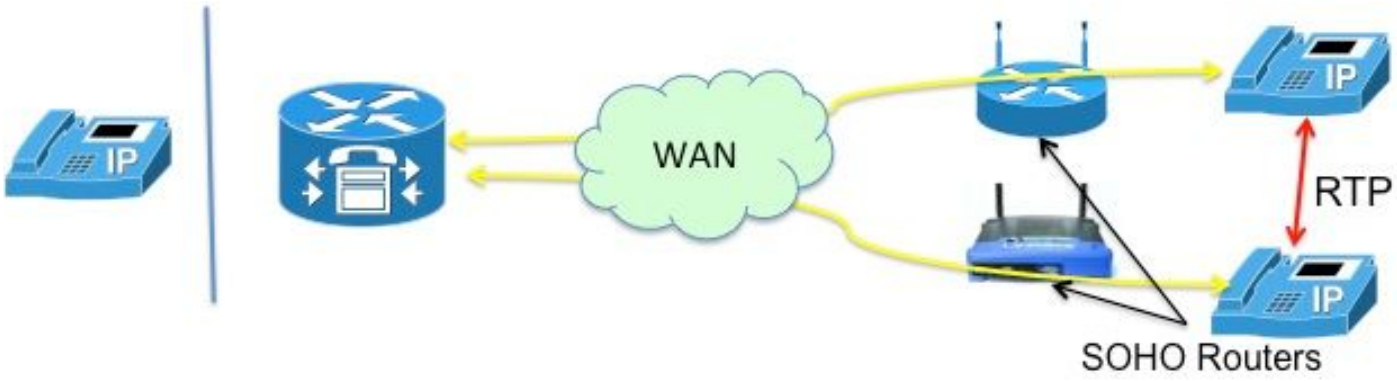
Afstandsbediening

Dit verwijst naar IP-telefoons die via een WAN verbinding maken met CME ter ondersteuning van telewerkers met vestigingen die ver van de CME-router staan. De meest voorkomende ontwerpen zijn die waarbij telefoons met routeerbare IP-adressen en telefoons met privé IP-adressen betrokken zijn.

Verre telefoons met openbaar (lees: routable) IP-adressen

Als beide telefoons betrokken bij de vraag met openbare, routable IP adressen worden gevormd, kunnen de media rechtstreeks tussen de telefoons (figuur 8) stromen. Daarom opnieuw, geen

behoefte aan NAT!



Afbeelding 8

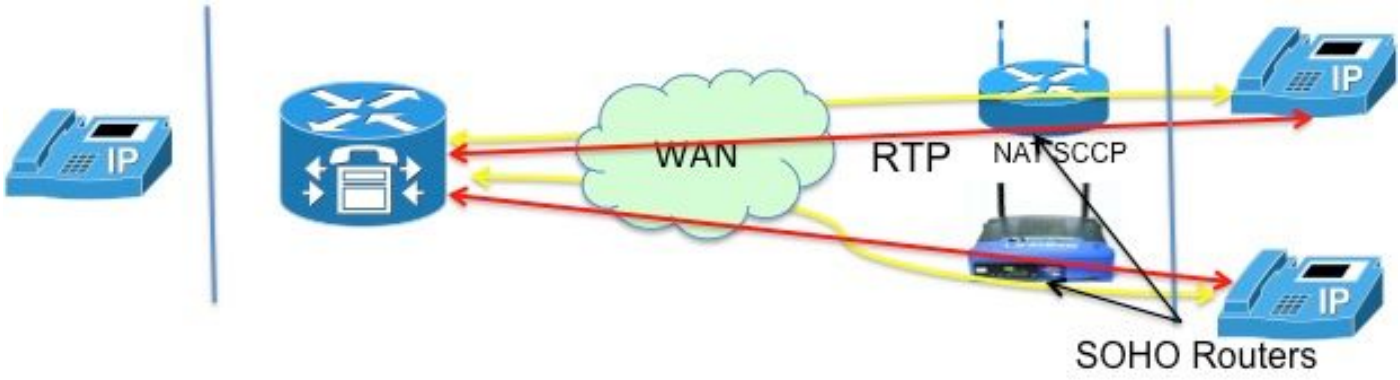
Remote-telefoons met privaat IP-adres

In dit scenario wordt de oproep gesignaleerd tussen skinny telefoons geconfigureerd met privé IP-adressen. De routers van het huisbureau (SOHO), over het algemeen, neigen "SCCP bewust"te zijn. d.w.z. niet in staat om de in de SCCP-berichten ingesloten IP-adressen te vertalen. Dit betekent dat de telefoons op het moment dat de installatie is voltooid, eindigen met elkaars privé IP-adres. Aangezien beide telefoons privé zijn, zal CME de vraag tussen hen zo signaleren dat de audio direct tussen de telefoons stroomt. Dit zal echter resulteren in eenrichtings- of eenrichtingsaudio (aangezien privé IP-adressen per definitie niet op het internet kunnen worden gerouteerd!), tenzij een van de volgende tijdelijke oplossingen wordt geïmplementeerd-

·Statische routes op de SOHO-routers configureren

·een IPsec VPN-verbinding met de telefoons tot stand brengen

Een betere manier om dit op te lossen is het configureren van "mtp". Het mtp-bevel zorgt ervoor dat media (RTP)-pakketten van externe telefoons door de CME-router worden verzonden (afbeelding 9).



Afbeelding 9

De "mtp"oplossing is beter wegens complicaties met het openen van firewallhavens. De mediapakketten die via een WAN worden verzonden, kunnen door een firewall worden geblokkeerd. Dit betekent dat u poorten op de firewall moet openen, maar welke? Met CME die de audio aflost, kunnen de firewalls gemakkelijk worden gevormd om de pakketten over te gaan RTP. CME router gebruikt een ***specifieke*** UDP-poort (2000!) voor mediapakketten. Dus door pakketten toe te staan van en naar poort 2000 kan AL het RTP-verkeer worden doorgegeven.

Afbeelding 10 illustreert hoe u mtp kunt configureren.

```
Telefoon 1

  mac 111.222.333

  type 7965

  mtp

  knop 1:1
```

Afbeelding 10

Alles is niet geweldig met mtp. Er zijn situaties waarbij mtp niet gewenst is

- MTP is niet zacht voor CPU-gebruik
- Multicast MOH kan over het algemeen niet over WAN door:sturen - de Multicast MOH-eigenschap controleert om te zien of MTP voor een telefoon wordt toegelaten en als het is, verzendt geen MOH naar die telefoonL.

Als u dus een WAN-configuratie hebt die multicast-pakketten kan doorsturen en u kunt RTP-pakketten via uw firewall toestaan, kunt u beslissen om MTP niet te gebruiken.

Remote SIP-telefoons

Merk op dat SIP telefoons niet werden genoemd in de bovenstaande scenario's. Dit komt door het feit dat als een van de telefoons een SIP-telefoon is, CME zichzelf invoegt in het audiopad. Dit wordt dan het lokaal-naar-externe scenario dat eerder wordt beschreven, waarbij NAT niet nodig is.

KUBUS

De CUBE voert inherent NAT- en PAT-functies uit aangezien alle sessies worden beëindigd en opnieuw gestart. De CUBE vervangt zijn eigen adres door het adres van elk eindpunt waarmee het communiceert, en verbergt (vertaalt) zo effectief het adres van dat eindpunt.

Zodoende is NAT niet vereist voor de CUBE-functie. Er is een VoIP-servicescenario waarin NAT op de CUBE is vereist, zoals in de volgende sectie wordt beschreven.

Hosted NAT-traject

Een korte achtergrond bij Hosted Telephony Service helpt de beweegredenen voor deze functie te begrijpen.

Hosted telefhony Service is een nieuwe vorm van VoIP-service waarin het grootste deel van het tandwiel zich op de locatie van de dienstverlener bevindt. Ze werken met de thuisgateways (HGW), die alleen basis-NAT implementeren (bijv. NAT op L3/L4). Bijvoorbeeld Verizon installeert de Optical Network Terminal (ONT), die FiOS-diensten in huis verleent; spraakoproep wordt gesignaleerd met behulp van een SIP-proces dat in het ONT is ingebouwd. De SIP-signalering wordt via het private IP-netwerk van Verizon gemaakt voor nieuwe soft switches, die de service en

controle leveren om spraakcommunicatie tot stand te brengen met andere klanten van de FiOS Digital Voice, of met traditionele telefoonklanten.

Tot de belangrijkste vereisten voor de gehoste telefoniedienst behoren onder meer:

- Afstandsbediening NAT-omzetting: de capaciteit om de diensten van Klasse 5 aan eindpunten te leveren die NAT (die NAT laag 3 slechts kunnen doen!) gebruiken en firewallapparaten (door "ALG"ver te doen!)
- Mediaondersteuning: de mogelijkheid om media te verzenden tussen apparaten die zich op dezelfde locatie bevinden, waar het geen zin heeft om de media terug te sturen naar het IP-netwerk
- Geen extra apparatuur, waardoor het niet nodig is om CPE toe te voegen.

Welke mogelijkheden zijn er, gezien het bovenstaande, om een dergelijke dienst te realiseren?

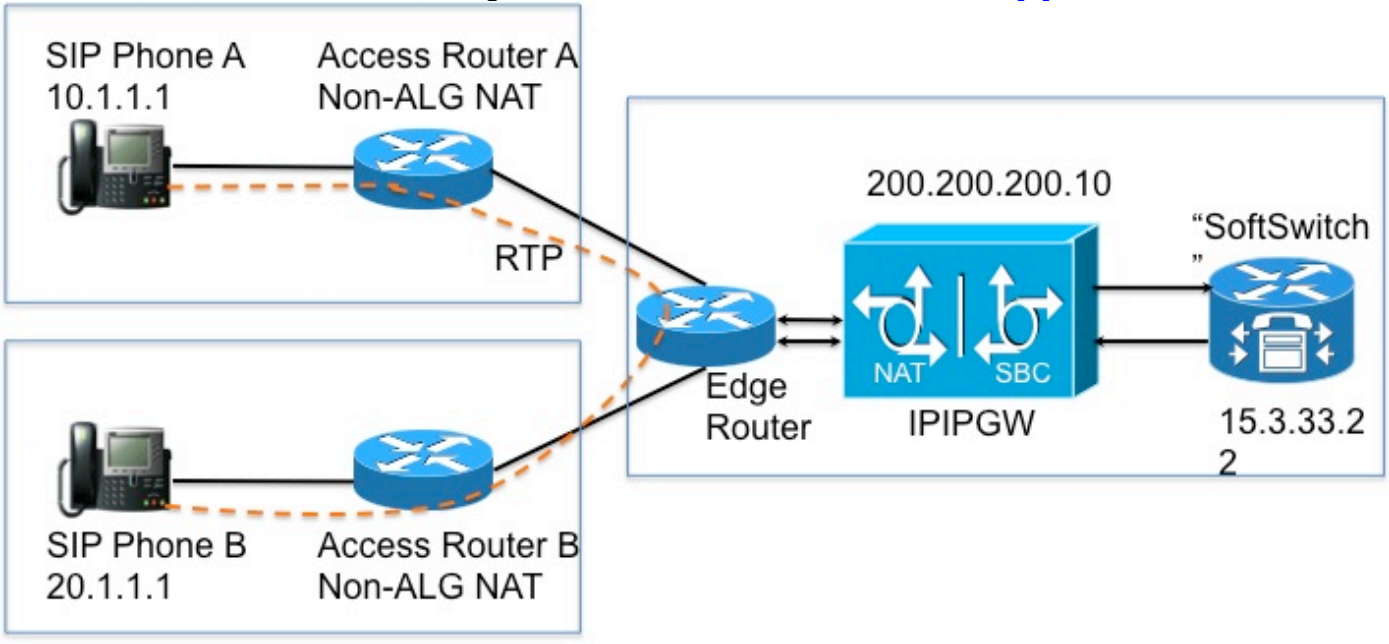
- Vervang de HGW door een dure ALG,
- Gebruik een Session border-controller (SBC) om de ingesloten SIP-kopregels voor pakketten aan te passen. Dit impliceert een netwerk-ontvangen, drager-rang product ondersteunend SIP in een zeer veilige, fout-verdraagzame configuratie. Deze oplossing wordt NAT SBC genoemd.

De NAT SBC-optie voldoet aan de bovenvermelde providervereisten.

NAT SBC

De NAT SBC werkt als volgt (afbeelding 11)

1. Access router vertaalt alleen het L3/L4 IP-adres
2. IP-adres in het SIP-bericht niet vertaald
3. SBC NAT onderschept en vertaalt het ingesloten IP-adres. Op het moment dat de SBC SIP-pakketten ziet bestemd voor **200.200.200.10**, wordt de Nat-sbc-code ingevoerd.
4. Media wordt niet vertaald en gaat rechtstreeks tussen de telefoons[5]



Afbeelding 11

Ontwerpopmerkingen

- Het IP-adres **200.200.200.10** (afbeelding 12) wordt niet toegewezen aan enige interface op de NAT SBC. Het wordt geconfigureerd als het adres van de "proxy" waarnaar SIP-telefoon A en SIP-telefoon B signaleringsberichten verzenden.
- Thuisapparaten vertalen bepaalde velden *waarop* SIP/SDP-*adressen* zijn *alleen* (bijv. Call-ID: ,O= , Waarschuwing: headers & branch= parameter. maddr= and Receive= parameters werden alleen in bepaalde scenario's verwerkt.) Deze velden worden behandeld door de NAT SBC, behalve voor de proxy-autorisatie en autorisatie vertaling, omdat deze de authenticatie zullen breken.
- Als de thuisapparaten zijn geconfigureerd voor PAT, moeten de gebruikersagents (telefoons en proxy's) symmetrische signalering[6] en symmetrische en vroege media ondersteunen. U moet de override poort configureren op de NAT SBC router.
- Bij gebrek aan ondersteuning voor symmetrische signalering en symmetrische en vroege media, moeten de tussenliggende routers zonder PAT worden geconfigureerd en moet het override-adres in NAT SBC worden geconfigureerd.

Configuratie

De voorbeeldconfiguratie voor een typische NAT SBC volgt.

```
IP NAT SIP-sbc

  proxy 200.200.200.10 5060 15.3.33.22 5060 protocol udp

  call-id-pool

  sessie-time-out 300

  modus toegestaan doorstroming

  poort negeren

!

ip NAT-pool sbc1 15.3.33.61 15.3.33.69 netmasker 255.255.0.0

ip nat pool sbc2 15.3.33.91 15.3.33.99 netmasker 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 buitenzwembad 200.200.200.100 200.200.200.200 netmask 255.255.255.0

IP NAT binnen bronlijst 1 pool sbc1 overload

IP NAT binnen bronlijst 2 pool sbc2

IP Nat buiten bronlijst 3 pool buiten-pool add-route

IP NAT binnen bronlijst 4 pool call-id-pool

!

toegangslijst 1 vergunning 10.1.1.0 0.0.0.255

toegangslijst 1 vergunning 171.1.1.0 0.0.0.255

toegangslijst 2 vergunning 20.1.1.0 0.0.0.255
```

```
toegangslijst 2-vergunning 172.1.1.0 0.0.0.255

toegangslijst 3-vergunning 15.4.0.0 0.0.255.255

toegangslijst 3-vergunning 15.5.0.0 0.0.255.255

toegangslijst 4 vergunning 10.1.0.0 0.0.255.255

toegangslijst 4 vergunning 20.1.0.0 0.0.255.255
```

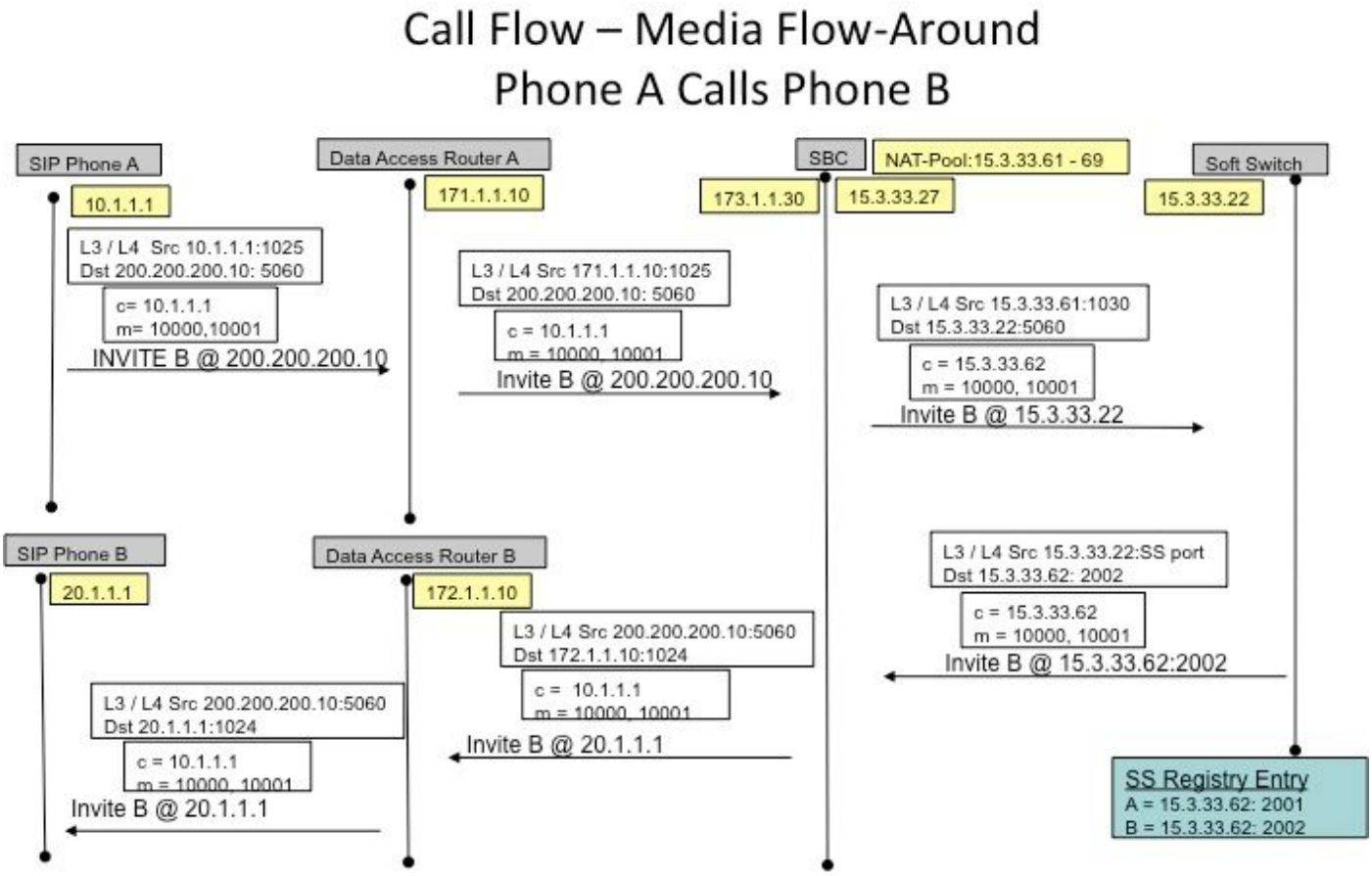
Call Flow met SBC NAT

Afbeelding 13 en afbeelding 14 illustreren de gespreksstroom in termen van de vertalingen. De volgende punten moeten worden opgemerkt:

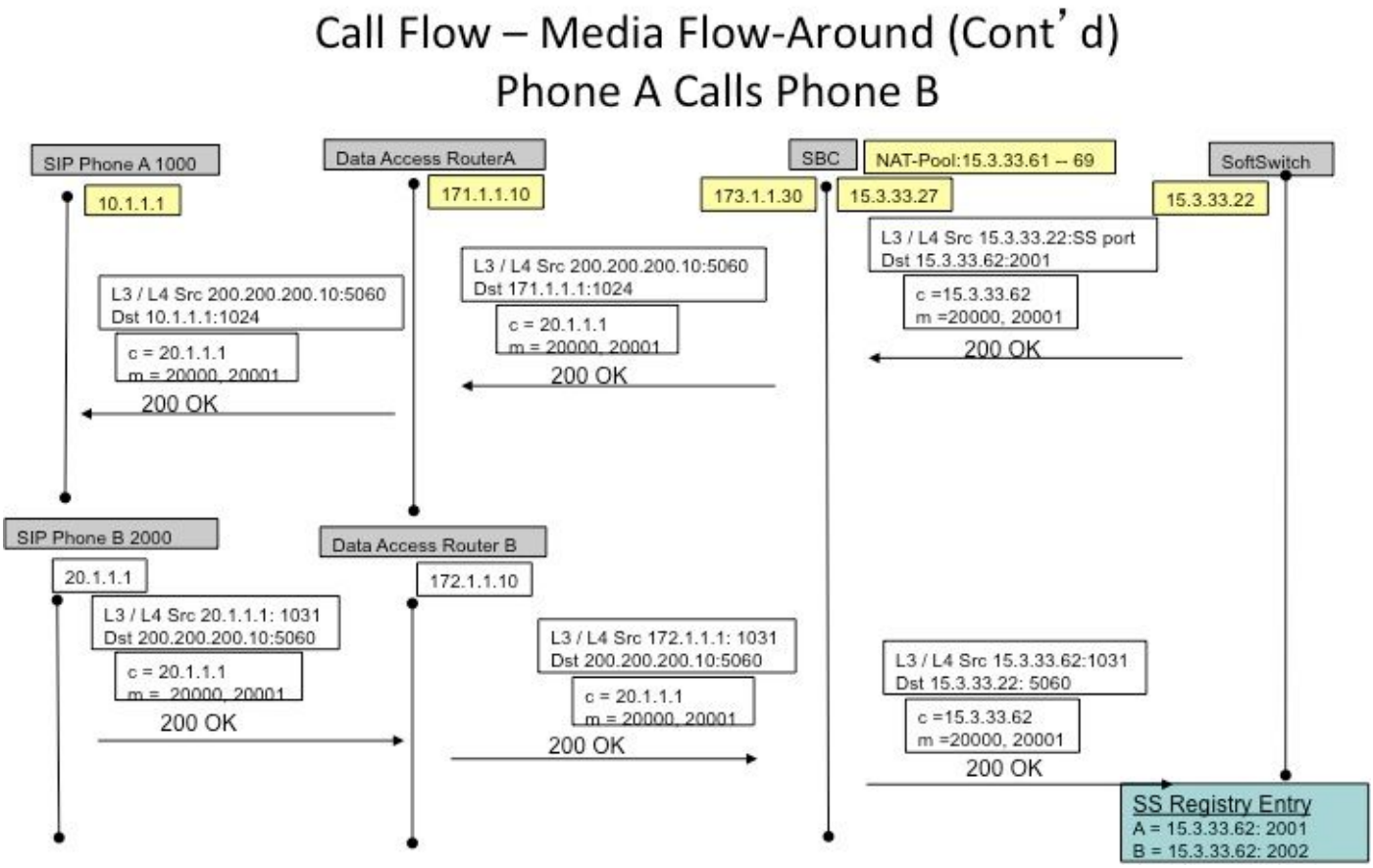
- Bij registratie merkt de zachte switch de twee telefoons op als
  — SIP-telefoon A - 15.3.3.62 2001

  — SIP-telefoon B - 15.3.33.62 2002

- In deze call flow laat SBC NAT het IP-adres van de media onvertaald.



Afbeelding 13



Afbeelding 14

SIP-registratie

In eerdere versies (van SBC NAT) moesten SIP-endpoints *levensechte* pakketten verzenden om de SIP-registratiepijp open te houden (zodat out->in het verkeer kan stromen, bijvoorbeeld inkomende gesprekken). *bewaar-levendige* pakketten konden elk SIP-pakket zijn dat door het eindpunt of de registratieserver (zachte switch) werd verzonden. Recente versies voorkomen dat dit nodig is, waarbij de NAT-SBC zelf (in tegenstelling tot zachte switches) de eindpunten dwingt om regelmatig opnieuw te registreren om de speldengaten open te houden.

> **Opmerking:** Symptomen van een verlopen registratiepunt kunnen obscuur zijn, met willekeurige vraag signalering mislukkingen.

KUSSEN

CUSP heeft de notie van een logisch netwerk, dat verwijst naar een verzameling van lokale interfaces die op dezelfde manier worden behandeld voor (bijv. interface, poort, transport voor het luisteren) routering doeleinden. Wanneer u een logisch netwerk configureert op CUSP, kunt u dit configureren om NAT te gebruiken. Na configuratie wordt SIP ALG automatisch ingeschakeld. Dit is nuttig bij bepaalde logische netwerken.

Probleemoplossing

Symptomen

Een duidelijk symptoom zou kunnen zijn dat een vraag in één of beide richtingen ontbreekt. Minder duidelijke symptomen kunnen zijn:

- Eenvoudige audio
- Enkele-weg audio bij overdracht
- Geen geluid
- SIP-registratie verliezen

Opdrachten tonen en debuggen

- `deb ip nat [slokje | mager]`
- `IP NAT-statistieken tonen`
- `ip nat-vertalingen tonen`

Dingen om te controleren

- Zorg ervoor dat de configuratie de **ip Nat binnen** of **ip Nat buiten** interfacesubopdracht omvat. Deze opdrachten maken NAT op de interfaces mogelijk en de binnen-/buitenkant-aanduiding is belangrijk.
- Zorg er voor statische NAT voor dat de **statische** opdracht **IP-bron** eerst het lokale adres en vervolgens het wereldwijde IP-adres aangeeft.
- Voor dynamische NAT, zorg ervoor dat ACL die wordt gevormd om pakketten aan te passen die door de binnengastheer worden verzonden dat de pakketten van de gastheer aanpassen, alvorens om het even welke NAT vertaling is voorgekomen. Als bijvoorbeeld een binnen lokaal adres van 10.1.1.1 vertaald zou moeten worden naar 200.1.1.1, zorg er dan voor dat de ACL overeenkomt met het bronadres 10.1.1.1, niet 200.1.1.1.
- Voor dynamische NAT zonder PAT, zorg ervoor dat de pool genoeg IP adressen heeft. De symptomen van het niet hebben van genoeg adressen omvatten een groeiende waarde in de tweede missenteller in de output van de **show ip nationaal statistieken**, evenals het zien van alle adressen in de waaier die in de NAT pool in de lijst van dynamische vertalingen wordt bepaald.
- Voor PAT, is het gemakkelijk om te vergeten om de **overbelastingsoptie** op de **ip nationaal binnen** bevel **van de bronlijst** toe te voegen. Zonder dit systeem werkt NAT, maar PAT niet, wat er vaak toe leidt dat pakketten van gebruikers niet worden vertaald en dat hosts niet naar het internet kunnen komen.
- Misschien is NAT correct gevormd, maar er bestaat ACL op één van de interfaces, verwerpend de pakketten. Merk op dat IOS ACL's verwerkt vóór NAT voor pakketten die een interface invoeren en na het vertalen van de adressen voor pakketten die een interface verlaten.
- Vergeet niet om "ip Nat buiten" op de interface met het WAN te configureren (zelfs als u geen extern adres vertaalt)!
- Zodra NAT is geconfigureerd, laat ip Nat-vertalingen niets zien. Ping eenmaal en controleer dit nogmaals.
- Grab **wireshark Traces** op binnen- en buiteninterfaces van de NAT-SBC

Scenario's

Debug uitvoer voor een paar scenario's worden hieronder getoond. Ze zijn meestal voor zichzelf!

Basis NAT

De configuratie en debug lijnen voor basisNAT worden hieronder getoond.

```
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

De uitvoerlijnen van **debug ip Nat SIP** worden weergegeven. In dit geval wordt het ingesloten IP-adres op een uitgaand pakket vertaald.

```
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:
```

Referenties

Overzicht:

- 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 en 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

NAT-functiematrix

- 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.sht

ml

Hosted NAT-traject:

- 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/configuratie/guide/sbcu/sbc_cucm.html

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.