NAT in VoIP

Sommario

Introduzione

Questo documento descrive il comportamento NAT (Network Address Translation) nei router che

operano come CUBE (Cisco Unified Border Element), CME o CUCME (Cisco Unified Communications Manager Express), Gateways e CUSP (Cisco Unified SIP Proxy).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SIP (Session Initiation Protocol)
- Voice over IP (protocollo Internet)
- Protocolli di routing

Componenti usati

Le informazioni di questo documento si basano

- Qualsiasi IOS versione 12.4T e successive.
- Qualsiasi versione CME

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Network Address Translation è una tecnica comunemente utilizzata per tradurre gli indirizzi IP in pacchetti che passano tra reti utilizzando spazi di indirizzi diversi. Lo scopo di questo documento non è rivedere il NAT. Piuttosto, questo documento ha lo scopo di fornire una revisione completa di NAT come viene usato nelle reti VoIP di Cisco. Inoltre, l'ambito di applicazione è limitato ai componenti che costituiscono la tecnologia MS-Voice.

- In pratica, NAT sostituisce l'indirizzo IP all'interno dei pacchetti con un indirizzo IP diverso
- Consente a più host in una subnet privata di *condividere* (ovvero apparire come) un singolo indirizzo IP pubblico per accedere a Internet.
- In genere, le configurazioni NAT modificano solo l'indirizzo IP degli host interni
- NAT è bidirezionale: se A viene tradotto in B sull'interfaccia interna, B in arrivo all'interfaccia esterna verrà tradotto in A!
- RFC 1631

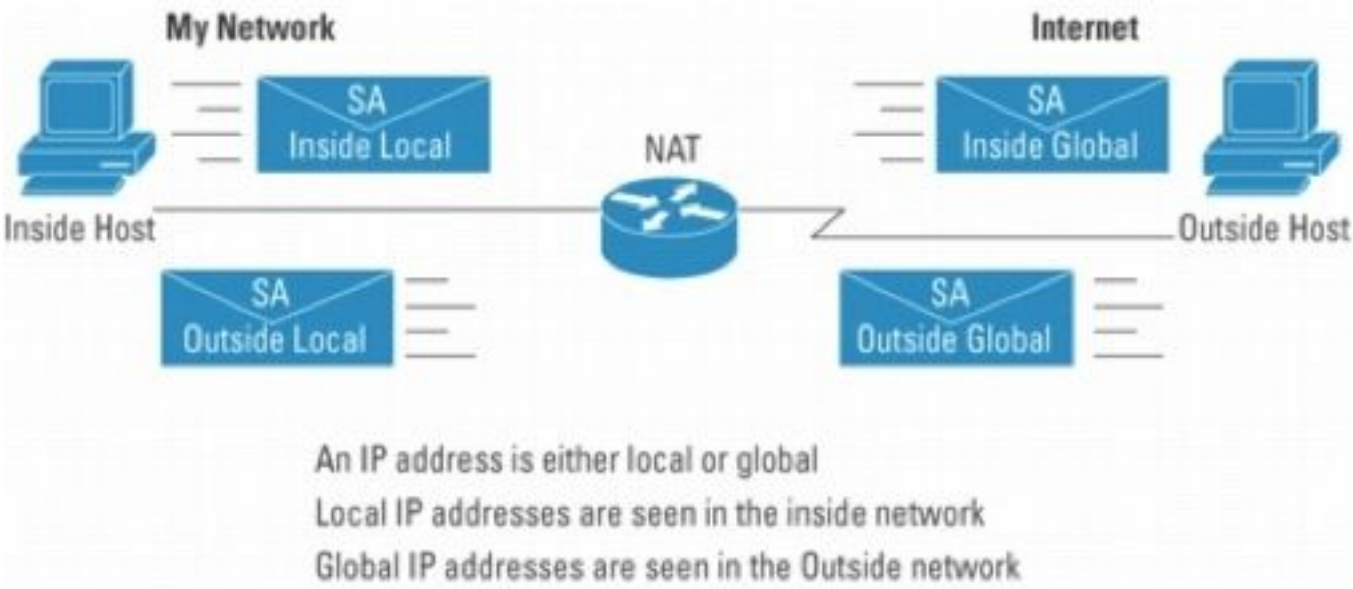

Figura 1

> **Nota**: potrebbe essere utile pensare al NAT come un aiuto per instradare i pacchetti IP in entrata e in uscita dalle reti utilizzando lo spazio degli indirizzi privato. In altre parole, NAT rende instradabili gli indirizzi non instradabili

La Figura 2 mostra la topologia a cui si fa riferimento nelle illustrazioni che seguono.

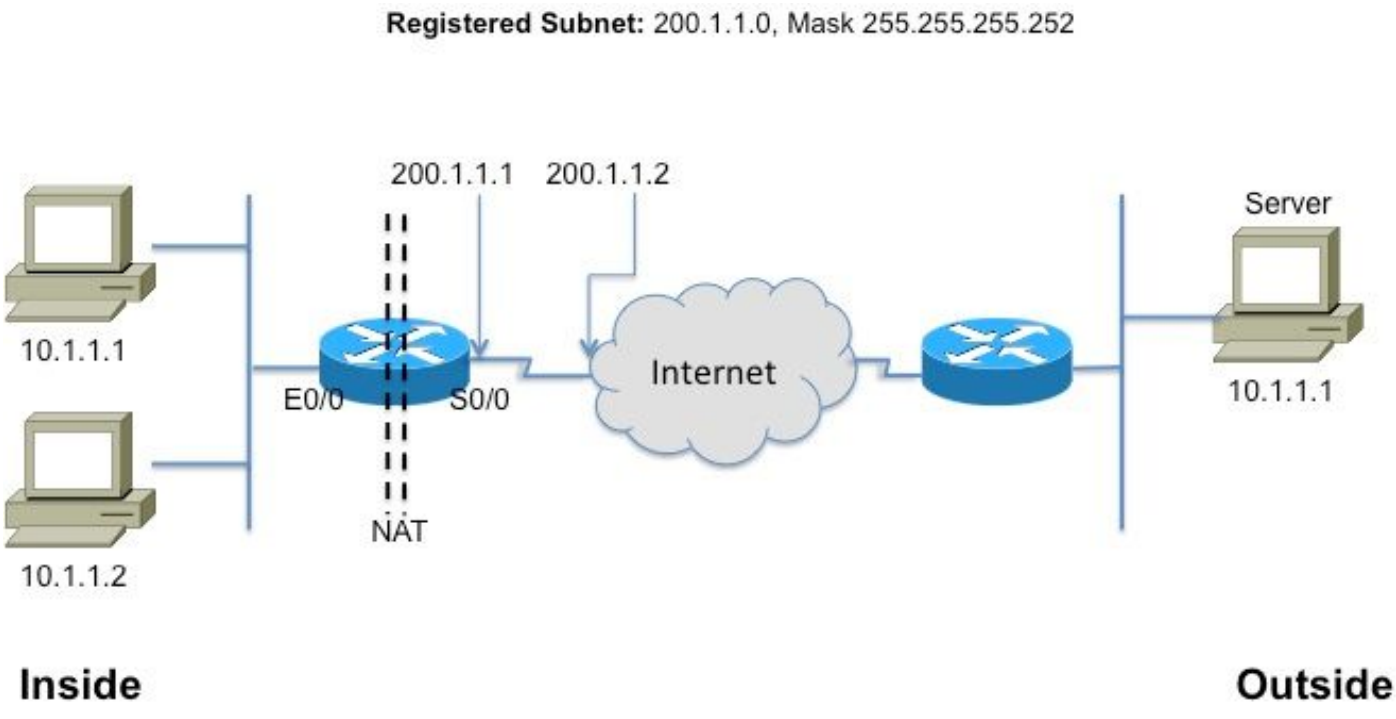

Figura 2

Questo glossario è fondamentale per comprendere e descrivere NAT

- **Indirizzo locale interno**: l'indirizzo IP assegnato a un host nella rete *interna*. In genere, l'indirizzo proviene da uno spazio degli indirizzi privato.
- **Indirizzo globale interno**: un indirizzo IP instradabile assegnato dalla scheda NIC o dal provider di servizi che rappresenta uno o più indirizzi IP locali interni al mondo esterno.

- **Indirizzo locale esterno**: l'indirizzo IP di un host esterno così come viene visualizzato alla rete interna. Non è necessariamente un indirizzo legittimo, è allocato da uno spazio di indirizzi instradabile all'interno.
- **Indirizzo globale esterno**: l'indirizzo IP assegnato a un host sulla rete esterna dal proprietario dell'host. L'indirizzo viene allocato da un indirizzo o da uno spazio di rete instradabile globalmente.

  Nota: questi termini possono essere facilmente accettati. Qualsiasi nota o documento su NAT farà sicuramente riferimento a tali informazioni

NAT statico

Questa è la forma più semplice di NAT, dove in ogni indirizzo interno viene convertito staticamente in un indirizzo esterno (e viceversa).

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Figura 3

La CLI per la configurazione per la traduzione di cui sopra è la seguente

interface Ethernet0/0

indirizzo ip 10.1.1.3 255.255.255.0

ip nat inside

!

interfaccia Serial0/0

indirizzo ip 200.1.1.251.255.255.255.252

ip nat esterno <— Obbligatorio![2]

origine interna ip nat statica 10.1.1.2 200.1.1.2

origine interna ip nat statica 10.1.1.1 200.1.1.1

NAT dinamico

Nel NAT dinamico, ogni host interno è mappato a un indirizzo da un pool di indirizzi.

- Alloca un indirizzo IP da un pool di indirizzi globali interni.

- Se un nuovo pacchetto arriva da un altro host interno e ha bisogno di una voce NAT, ma tutti gli indirizzi IP del pool sono in uso, il router scarta il pacchetto.
- In sostanza, il pool di indirizzi globali interni deve essere grande quanto il numero massimo di host simultanei che devono utilizzare Internet contemporaneamente

La seguente CLI illustra la configurazione di NAT dinamico

```
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
```

Sovraccarico NAT (PAT)

Quando il pool (di indirizzi IP) è più piccolo del set di indirizzi da tradurre, questa funzione si rivela utile.

- Numerosi indirizzi interni NAT vengono associati solo a uno o a pochi indirizzi esterni
- PAT (Port Address Translation) utilizza numeri di porta di origine univoci sull'indirizzo IP **globale** interno per distinguere le traduzioni. Poiché il numero di porta è codificato in 16 bit, il numero totale potrebbe teoricamente essere pari a 65.536 per indirizzo IP. PAT tenterà di mantenere la porta di origine originale, se questa porta di origine è già allocata. PAT tenterà di trovare il primo numero di porta disponibile
- Il sovraccarico NAT può utilizzare più di 65.000 porte, consentendo una buona scalabilità senza la necessità di molti indirizzi IP registrati, in molti casi con la necessità di un solo indirizzo IP globale esterno.

La figura 4 illustra PAT.

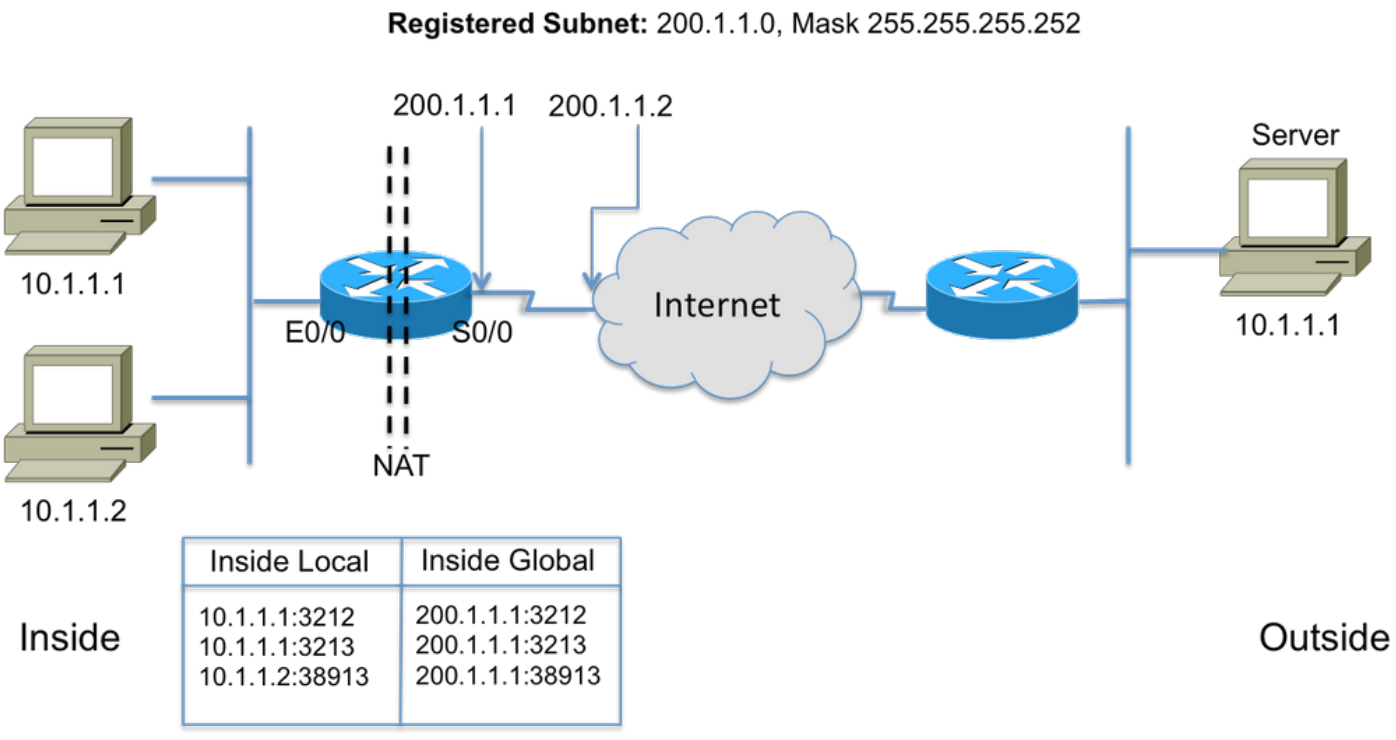

Figura 4

Opzioni del comando NAT

L'implementazione di Cisco NAT è molto versatile con una vasta gamma di opzioni. Di seguito sono elencati alcuni miglioramenti, ma per ulteriori informazioni sull'elenco completo, visitare il sito Web all'indirizzo http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html.

- Traduzioni statiche con porte - Pacchetti in arrivo indirizzati a una porta specifica (ad es. 25, per il server SMTP) inviate a un server specifico.
- Supporto delle route map - Flessibilità nella configurazione di filtri/ACL
- Configurazioni pool più flessibili per consentire intervalli di indirizzi discontinui.
- Conservazione dei numeri host: traduce la parte "rete" e mantiene la parte "host".

Pozzetto NAT

Un foro nel linguaggio NAT si riferisce al mapping tra le tuple <indirizzo IP host, porta> e <indirizzo globale, porta *globale*>. Consente al dispositivo NAT di utilizzare il numero della porta di destinazione (che sarebbe la porta *globale*) dei messaggi in arrivo per mappare nuovamente la destinazione all'IP host e alla porta da cui ha avuto origine la sessione. È importante notare che dopo un periodo di non utilizzo si verifica il timeout dei fori e l'indirizzo pubblico viene restituito al pool NAT.

NAT in VoIP

Quindi, quali sono i problemi e le preoccupazioni con NAT nelle reti VoIP? Bene, ricordate che il NAT di cui abbiamo parlato fino ad ora (lossemente chiamato NAT di base) traduce solo l'indirizzo IP nell'*intestazione* del pacchetto IP e ricalcola il checksum, ovviamente, ma la segnalazione VoIP porta gli indirizzi integrati nel *corpo* dei messaggi di segnalazione. In altre parole, al livello 5

Nella Figura 5 è illustrato l'effetto della mancata conversione degli indirizzi IP incorporati. La segnalazione della chiamata è stata completata, ma il proxy SIP presso il provider di servizi non è riuscito a instradare i pacchetti multimediali (RTP) all'indirizzo multimediale inviato dall'agente di chiamata.

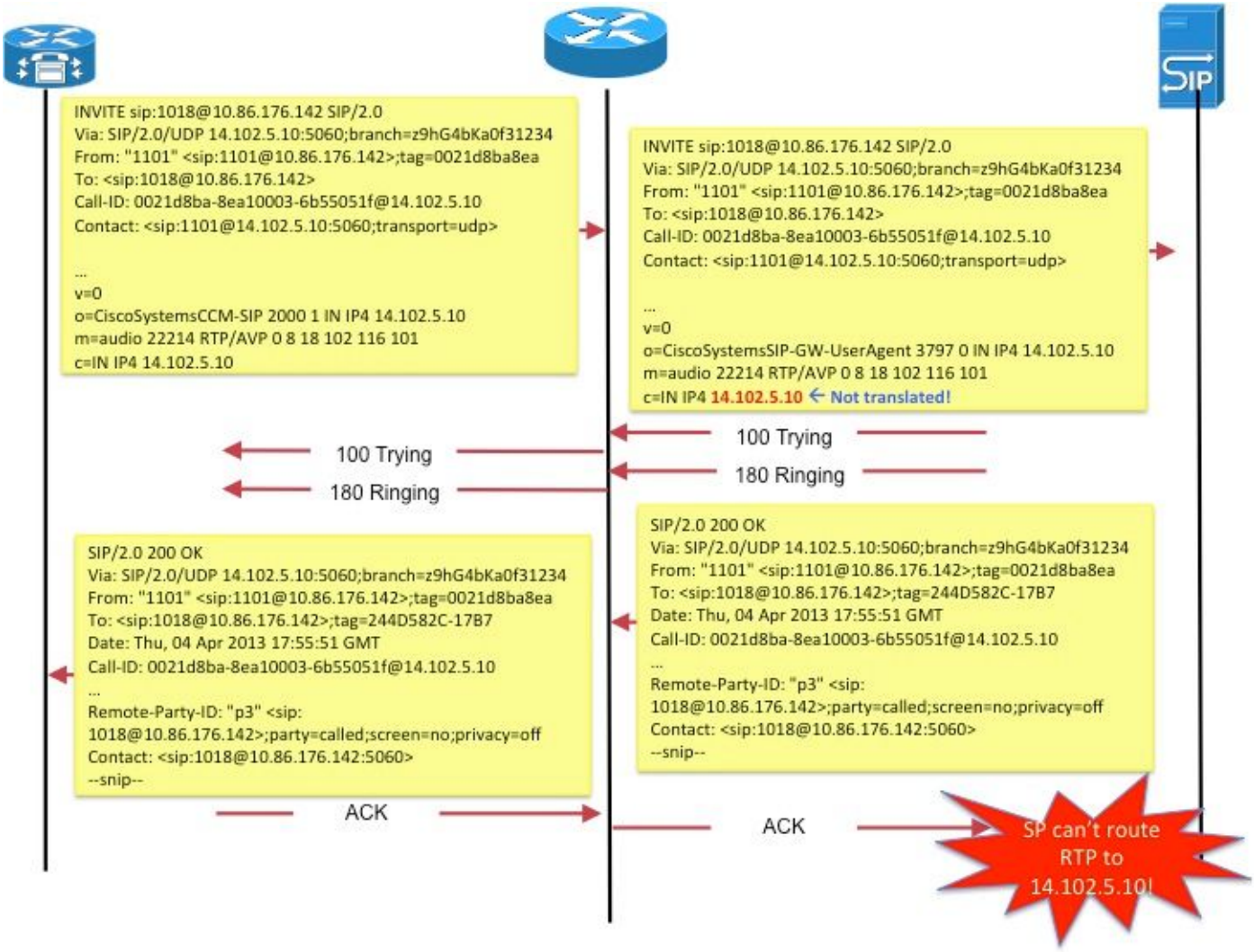

Figura 5

Un altro esempio è l'uso del ***contatto*** da parte dell'endpoint SIP*:* in SDP per comunicare l'indirizzo a cui l'endpoint desidera ricevere i messaggi di segnalazione per le nuove richieste.

Per risolvere questi problemi, è disponibile una funzionalità denominata ALG (Application Layer Gateway).

ALGA

Un GAL conosce il protocollo utilizzato dalle applicazioni specifiche che supporta (ad esempio SIP) e controlla i pacchetti del protocollo e "corregge" il traffico che attraversano. Per una buona descrizione di come i vari campi sono corretti per la segnalazione delle chiamate SIP, fare riferimento a http://www.voip-info.org/wiki/view/Routers+SIP+ALG.

Sui router Cisco, il supporto per ALG SIP è abilitato, per impostazione predefinita, sulla porta TCP standard 5060. È possibile configurare ALG per supportare porte non standard per la segnalazione SIP. Fare riferimento a http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.

> **Attenzione**: Attenzione! Non esiste un RFC o un altro standard che specifichi quali campi incorporati devono essere tradotti per i vari protocolli VoIP. Di conseguenza, le implementazioni variano, a seconda dei fornitori di apparecchiature, determinando problemi

di interoperabilità (e casi TAC).

Gateway

Poiché i gateway, per definizione, non sono dispositivi ip-to-ip, NAT non è applicabile.

CME

Questa sezione del documento esamina gli scenari di chiamata con CME per capire perché NAT deve essere utilizzato.

Scenario 1. Telefoni locali

Scenario 2. Telefoni (con indirizzi IP pubblici)

Scenario 3. Teleworker remoto

> **Nota**: in tutti i casi, affinché l'audio fluisca, l'indirizzo IP del CME deve essere instradabile

Locale

In questo scenario (Figura 6), i due telefoni coinvolti nella chiamata sono telefoni magri con indirizzi IP privati.

Figura 6

> **Nota**: ricordare che il telefono skinny collegato in una chiamata con un altro telefono skinny nello stesso sistema CME invia i pacchetti multimediali direttamente all'altro telefono; ad esempio, l'RTP da telefono locale a telefono locale NON passa attraverso CME.

Pertanto, NAT non è applicabile o richiesto in questo caso.

> **Nota**: CME determina se i media (RTP) devono essere direttamente o meno basati sul fatto che i due telefoni coinvolti in una chiamata siano entrambi sottili *e* nello stesso segmento di rete. In caso contrario, CME si inserisce nel percorso RTP.

Da locale a remoto

In questo scenario (Figura 7), la CME si inserisce nel flusso RTP in modo che il RTP dai telefoni venga terminato sulla CME. CME riprodurrà i flussi verso l'altro telefono. Dal momento che CME si trova sia sulla rete interna (privata) che su quella esterna e invia il suo indirizzo interno al telefono interno e l'indirizzo esterno (pubblico) al telefono esterno, NAT non è richiesto nemmeno in questo caso.

Tuttavia, le porte UDP/TCP (segnalazione e RTP) devono essere aperte tra il telefono IP remoto e l'indirizzo IP di origine CME. Ciò significa che i firewall o altri dispositivi di filtraggio sono configurati in modo da consentire le porte in questione.

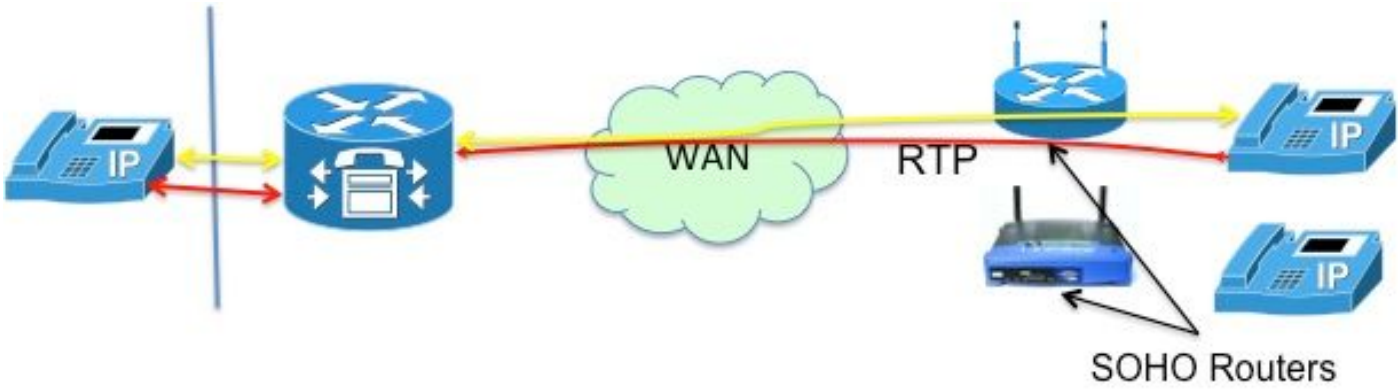

Figura 7

Nota: si noti che i [messaggi] di segnalazione sono sempre terminati in CM

Teleworker remoto

Questo si riferisce ai telefoni IP che si connettono a CME su una WAN per supportare i telelavoratori che hanno uffici remoti dal router CME. I progetti più comuni sono quelli che prevedono l'utilizzo di telefoni con indirizzi IP instradabili e telefoni con indirizzi IP privati.

Telefoni pubblici (leggere: instradabile) indirizzi IP

Se entrambi i telefoni coinvolti nella chiamata sono configurati con indirizzi IP pubblici e instradabili, i supporti possono passare direttamente tra i telefoni (Figura 8). Pertanto, ancora una volta, non c'è bisogno di NAT!

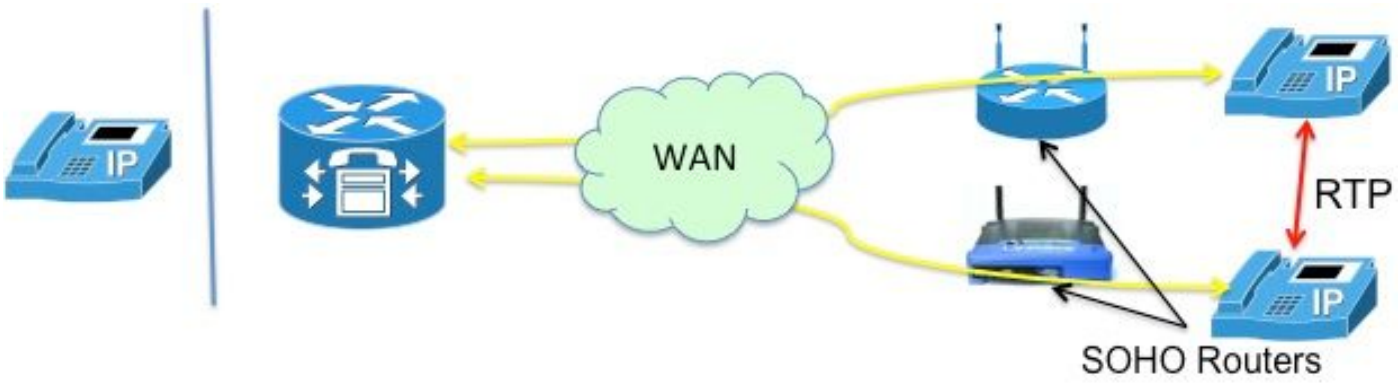

Figura 8

Telefoni con indirizzo IP privato

In questo scenario, la chiamata viene segnalata tra telefoni skinny configurati con indirizzi IP privati. In generale, i router degli uffici domestici (SOHO) tendono a non essere "compatibili con SCCP". ossia incapace di tradurre gli indirizzi IP incorporati nei messaggi SCCP. Ciò significa che, al completamento della configurazione delle chiamate, i telefoni terminano con l'indirizzo IP privato dell'altro. Poiché entrambi i telefoni sono privati, CME segnalerà la chiamata tra di loro in modo che l'audio fluisca direttamente tra i telefoni. Ciò, tuttavia, determinerà un audio unidirezionale o non direzionale (poiché gli indirizzi IP privati, per definizione, non possono essere indirizzati a su Internet!), a meno che non venga implementata una delle seguenti soluzioni alternative:

·Configurazione di route statiche sui router SOHO

·stabilire una connessione VPN IPsec ai telefoni

Un modo migliore per risolvere questo problema sarebbe configurare "mtp". Il comando mtp garantisce che i pacchetti multimediali (RTP) provenienti dai telefoni remoti transitino attraverso il router CME (Figura 9).

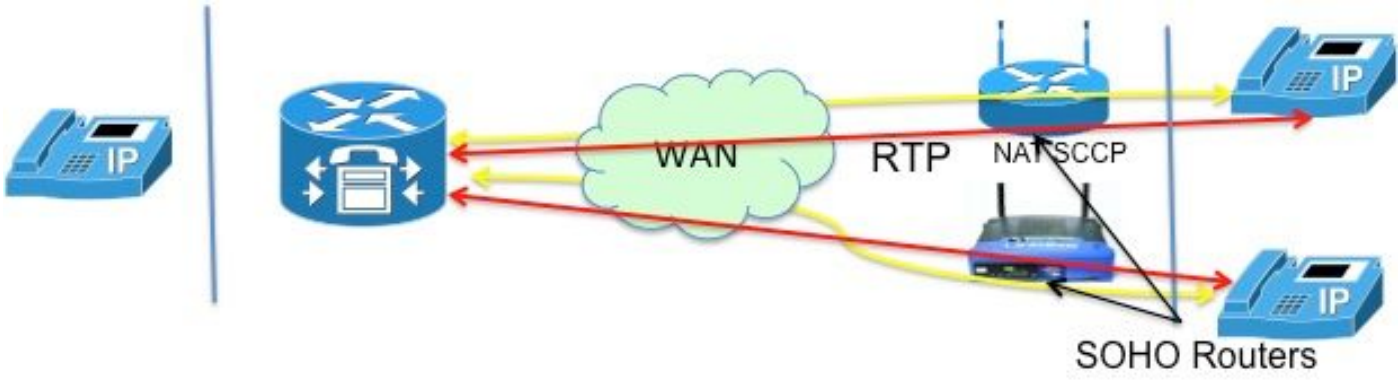

Figura 9

La soluzione "mtp" è migliore a causa delle complicazioni legate all'apertura delle porte del firewall. I pacchetti multimediali che passano su una WAN possono essere ostruiti da un firewall. Ciò significa che è necessario aprire le porte del firewall, ma quali? Con il CME che trasmette l'audio, i firewall possono essere facilmente configurati per passare i pacchetti RTP. Il router CME utilizza una porta UDP ***specifica*** (2000!) per i pacchetti multimediali. Pertanto, permettendo solo i pacchetti da e verso la porta 2000, TUTTO il traffico RTP può essere passato.

La Figura 10 mostra come configurare il protocollo mtp.

```
Telefono 1
  mac 1111.222.3333
  tipo 7965
  mtp
  tasto 1:1
```

Figura 10

Non è tutto meraviglioso con mtp. In alcune situazioni il protocollo mtp potrebbe non essere opportuno

- L'MTP non è delicato sull'utilizzo della CPU
- Il multicast MOH generalmente non può essere inoltrato su una WAN: la funzione Multicast MOH controlla se il MTP è abilitato per un telefono e, in caso affermativo, non invia il MOH a quel telefono.

Pertanto, se si dispone di una configurazione WAN in grado di inoltrare pacchetti multicast e si possono consentire pacchetti RTP attraverso il firewall, è possibile decidere di non utilizzare il protocollo MTP.

Telefoni SIP remoti

Si noti che i telefoni SIP non sono stati menzionati negli scenari sopra riportati. Ciò è dovuto al fatto che se uno dei telefoni è un telefono SIP, CME si inserisce nel percorso audio. Questo diventa quindi lo scenario da locale a remoto descritto in precedenza, in cui NAT non è richiesto.

CUBO

Il CUBE esegue intrinsecamente le funzioni NAT e PAT man mano che termina e rigenera tutte le sessioni. Il CUBE sostituisce il proprio indirizzo con l'indirizzo di qualsiasi endpoint con cui comunica, nascondendo (traducendo) in modo efficace l'indirizzo di tale endpoint.

Pertanto, NAT non è richiesto con la funzione CUBE. In uno scenario di servizio VoIP in cui è richiesto NAT sul CUBE, come descritto nella sezione successiva.

Hosted NAT Traversal

Una breve panoramica sul servizio di telefonia ospitata consentirà di comprendere le ragioni alla base di questa funzionalità.

Il servizio di telefonia ospitata è una nuova forma di servizio VoIP in cui la maggior parte degli attrezzi risiede nella sede del fornitore di servizi. Lavorano con i gateway domestici (HGW), che implementano solo NAT di base (ad esempio NAT a L3/L4). Ad esempio, Verizon installa il terminale di rete ottica (ONT), che fornisce i servizi FiOS a casa; la chiamata vocale viene segnalata utilizzando un processo SIP incorporato nel ONT. La segnalazione SIP viene effettuata attraverso la rete IP privata di Verizon ai nuovi soft switch, che forniscono il servizio e il controllo per stabilire comunicazioni vocali con altri clienti FiOS Digital Voice, o ai clienti telefonici tradizionali.

Tra i principali requisiti del provider per il servizio di telefonia ospitata vi sono:

- Attraversamento NAT remoto: la capacità di fornire servizi di Classe 5 agli endpoint utilizzando NAT (che può solo fare NAT layer 3!) e dispositivi firewall (facendo "ALG" in remoto!)
- Supporto co-media: la capacità di inviare supporti tra dispositivi situati nello stesso luogo dove non ha senso indirizzarli nuovamente alla rete IP
- Nessuna apparecchiatura aggiuntiva, eliminando la necessità di aggiungere CPE.

Alla luce di quanto sopra, quali opzioni esistono per l'implementazione di tale servizio?

- Sostituire l'HGW con un costoso ALG,
- Usare un SBC (Session Border Controller) per modificare le intestazioni SIP incorporate per i pacchetti. Questo implica un prodotto di livello carrier ospitato in rete che supporta il SIP in una configurazione molto sicura e a tolleranza di errore. Questa soluzione è indicata come NAT SBC.

L'opzione NAT SBC soddisfa i requisiti del provider elencati sopra.

NAT SBC

L'SBC NAT funziona come segue (Figura 11)

1. Il router di accesso converte solo l'indirizzo IP L3/L4
2. Indirizzo IP nel messaggio SIP non convertito
3. SBC NAT intercetta e converte l'indirizzo IP incorporato. Nel momento in cui la SBC vede i pacchetti SIP destinati a **200.200.200.10**, immette il codice nat-sbc.
4. I file multimediali non vengono tradotti e si spostano direttamente tra i telefoni[5]

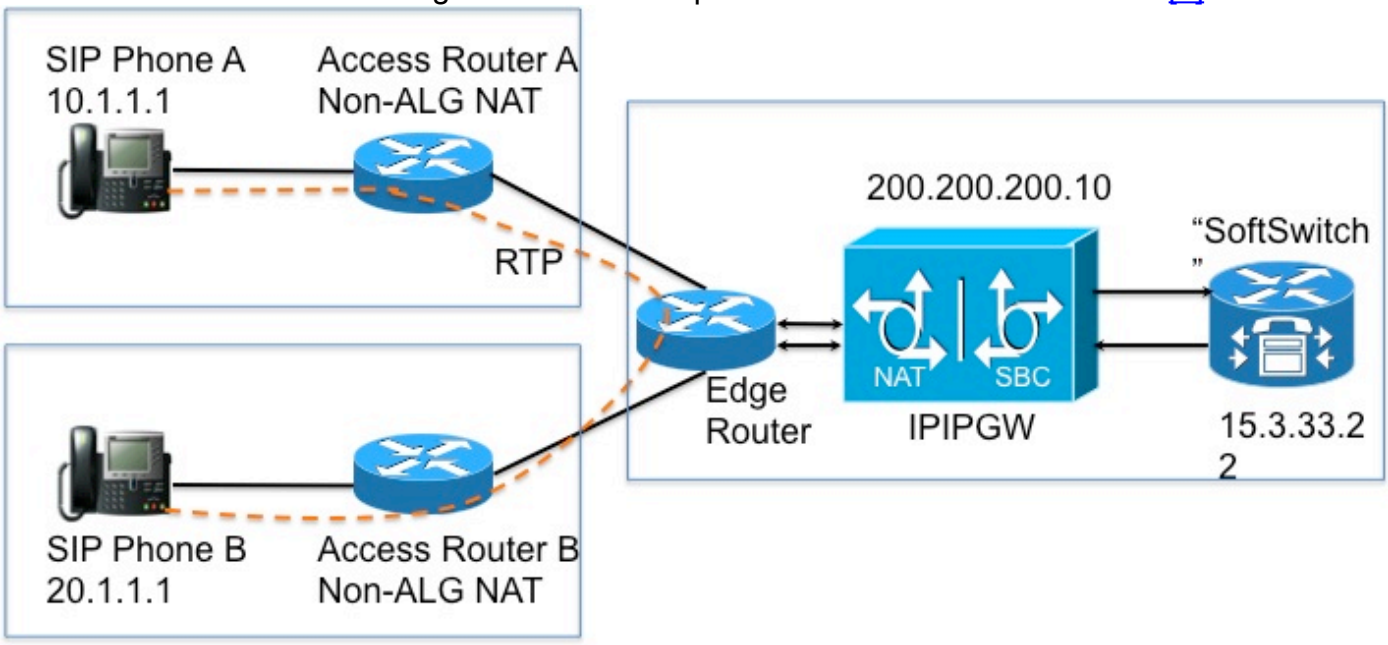

Figura 11

Note per la progettazione

- L'indirizzo IP **200.200.200.10** (Figura 12) non è assegnato ad alcuna interfaccia sull'SBC NAT. È configurato come l'indirizzo del "proxy" a cui il telefono SIP A e il telefono SIP B inviano messaggi di segnalazione.
- I dispositivi di casa non traducono alcuni campi di *solo indirizzo* SIP/SDP (ad esempio Call-Id: ,O= , Avviso: headers & branch=. i parametri maddr= e received= sono stati gestiti solo in alcuni scenari.) Questi campi vengono gestiti da NAT SBC, ad eccezione della traduzione autorizzazione proxy e dell'autorizzazione, in quanto possono interrompere l'autenticazione.
- Se i dispositivi di casa sono configurati per eseguire il PAT, gli agenti utente (telefoni e proxy) devono supportare la segnalazione simmetrica[6] e supporti simmetrici e recenti. È necessario

configurare la porta sostitutiva sul router NAT SBC.
- In assenza di supporto per la segnalazione simmetrica e i supporti simmetrici e recenti, i router intermedi devono essere configurati senza PAT e l'indirizzo di override deve essere configurato nel Cisco NAT.

Configurazione

Di seguito è riportata la configurazione di esempio per un NAT SBC tipico.

```
ip nat sip-sbc

  proxy 200.200.200.10 5060 15.3.33.22 5060 protocollo udp

  call-id-pool call-id-pool

  session-timeout 300

  modalità allow-flow-around

  porta di sostituzione

!

pool ip nat sbc1 15.3.33.61 15.3.33.69 netmask 255.255.0.0

pool ip nat 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 interno elenco origini 1 pool sbc1 overload

ip nat interno elenco fonti 2 pool sbc2

ip nat lista origini esterne 3 pool esterno add-route

ip nat nell'elenco delle origini 4 pool call-id-pool

!

access-list 1 permesso 10.1.1.0 0.0.0.255

access-list 1 permesso 171.1.1.0 0.0.0.255

access-list 2 permesso 20.1.1.0 0.0.0.255

access-list 2 allow 172.1.1.0 0.0.0.255

access-list 3 allow 15.4.0.0 0.0.255.255

access-list 3 allow 15.5.0.0 0.0.255.255

access-list 4 allow 10.1.0.0 0.0.255.255

access-list 4 allow 20.1.0.0 0.0.255.255
```

Flusso di chiamata con SBC NAT

La Figura 13 e la Figura 14 illustrano il flusso di chiamate in termini di traduzioni. Si rilevano i seguenti punti:

- Una volta effettuata la registrazione, l'interruttore software rileva i due telefoni come
  — SIP Phone A - 15.3.33.62.2001

  — SIP Phone B - 15.3.33.62.2002

- In questo flusso di chiamate, SBC NAT lascia effettivamente l'indirizzo IP del supporto non tradotto.

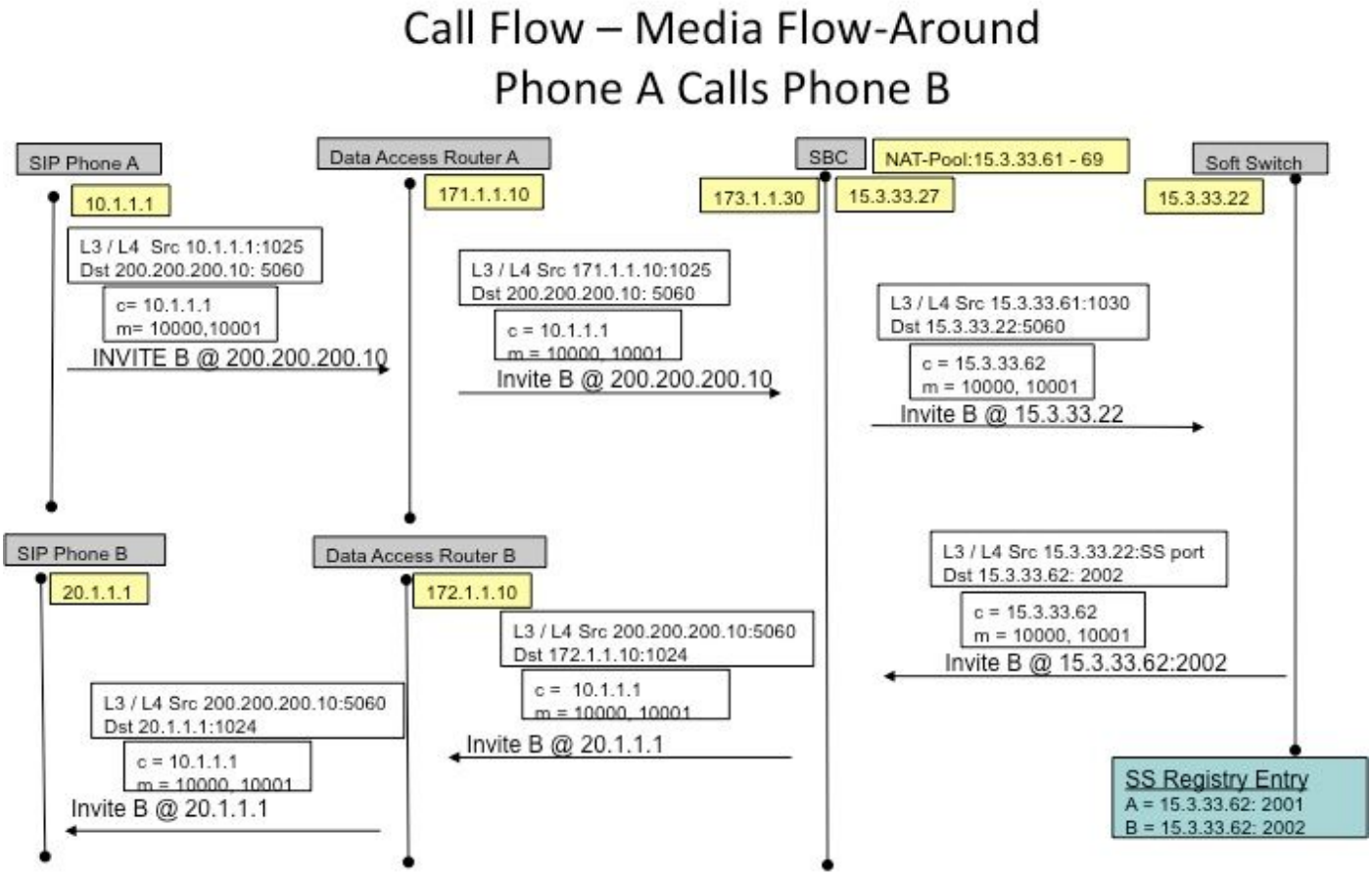

Figura 13

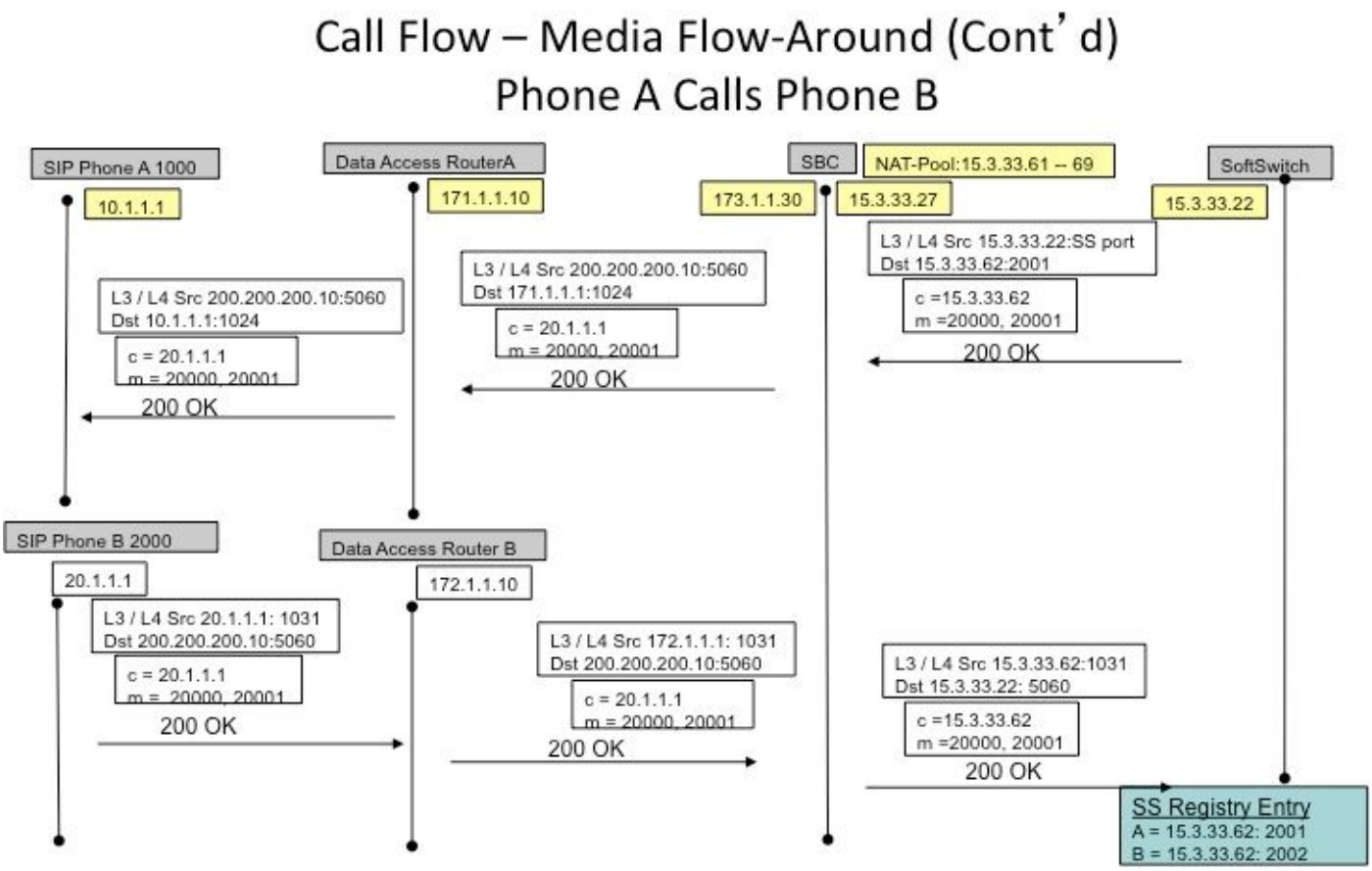

Figura 14

Registrazione SIP

Nelle versioni precedenti (di SBC NAT), gli endpoint SIP dovevano inviare pacchetti *keep-alive* per tenere aperto il foro di registrazione SIP (per consentire il flusso out-in>nel traffico, ad esempio le chiamate in entrata). I pacchetti *keep-alive* potevano essere qualsiasi pacchetto SIP inviato dall'endpoint o dal registrar (soft switch). Le versioni più recenti eliminano questa necessità, in quanto la stessa NAT-SBC (a differenza dei soft switch) costringe gli endpoint a registrarsi di nuovo frequentemente per tenere i fori aperti.

> **Nota:** I sintomi di un foro di registrazione scaduto possono essere oscuri, con errori casuali di segnalazione delle chiamate.

CUSPIDE

CUSP ha il concetto di rete logica, che si riferisce a una raccolta di interfacce locali per le quali vengono trattati in modo simile (ad esempio interfaccia, porta, trasporto per l'ascolto). Quando si configura una rete logica in CUSP, è possibile configurarla per l'utilizzo di NAT. Dopo la configurazione, SIP ALG viene abilitato automaticamente. Ciò è utile quando si utilizzano determinate reti logiche.

Risoluzione dei problemi

Sintomi

Un sintomo ovvio potrebbe essere che una chiamata non riesce in una o in entrambe le direzioni. I sintomi meno evidenti possono includere:

- Audio unidirezionale
- Audio unidirezionale durante il trasferimento
- Audio indipendente
- Perdita della registrazione SIP

Comandi Show ed debug

- `deb ip nat [sip | magro]`
- `mostra statistiche ip nat`
- `mostra traduzioni ip nat`

Elementi da controllare

- verificare che la configurazione includa il sottocomando **ip nat inside** o **ip nat outside** interface. Questi comandi abilitano NAT sulle interfacce e la designazione interna/esterna è importante.
- Per il protocollo NAT statico, verificare che il comando **ip nat source static** elenchi prima l'indirizzo locale interno e quindi l'indirizzo IP globale interno.
- Per il protocollo NAT dinamico, verificare che l'ACL configurato per la corrispondenza dei pacchetti inviati dall'host interno corrisponda ai pacchetti di tale host, prima di qualsiasi conversione NAT. Ad esempio, se un indirizzo locale interno di 10.1.1.1 deve essere convertito in 200.1.1.1, verificare che l'ACL corrisponda all'indirizzo di origine 10.1.1.1 e non a 200.1.1.1.
- Per un NAT dinamico senza PAT, verificare che il pool disponga di indirizzi IP sufficienti. I sintomi di indirizzi insufficienti includono un valore crescente nel secondo contatore degli accessi non riusciti nell'output del comando **show ip nat statistics**, nonché la visualizzazione di tutti gli indirizzi nell'intervallo definito nel pool NAT nell'elenco delle traduzioni dinamiche.
- Per PAT, è facile dimenticare di aggiungere l'opzione **overload** sul comando **ip nat inside source list**. Senza di esso, NAT funziona, ma PAT no, spesso determinando la mancata traduzione dei pacchetti degli utenti e l'impossibilità per gli host di accedere a Internet.
- Forse il NAT è stato configurato correttamente, ma su una delle interfacce esiste un ACL che scarta i pacchetti. Notare che IOS elabora gli ACL prima del NAT per i pacchetti che entrano in un'interfaccia e dopo aver tradotto gli indirizzi per i pacchetti che escono da un'interfaccia.
- Non dimenticate di configurare "ip nat outside" sull'interfaccia verso la WAN (anche se non traduce l'indirizzo esterno)!
- Non appena NAT viene configurato, le traduzioni con ip nat non mostrano nulla. Eseguire il ping una volta e quindi controllare nuovamente.
- Tracce di **wireshark** sulle interfacce interna ed esterna della NAT-SBC

Scenari

Di seguito sono riportati i risultati del debug per un paio di scenari. Per la maggior parte sono auto-esplicativi!

NAT di base

Di seguito sono riportate le righe di configurazione e debug per NAT di base.

```
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

Vengono mostrate le linee di output del comando **debug ip nat sip**. In questo caso, l'indirizzo IP incorporato in un pacchetto in uscita viene convertito.

```
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:
```

Riferimenti

Panoramica:

- http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html
- Anatomia: 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 e 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 funzionalità 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_paper09186a00801af2b9.html
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919.sht

ml

Attraversamento NAT ospitato:

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

NAT SBC

- EDCS-61162
- 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).