NAT en VoIP

Contenido

Introducción

Este documento describe el comportamiento de NAT (traducción de direcciones de red) en

routers que funcionan como CUBE (Cisco Unified Border Element), CME o CUCME (Cisco Unified Communication Manager Express), gateways y CUSP (Cisco Unified SIP Proxy).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- SIP (protocolo de inicio de sesión)
- Voz sobre IP (protocolo de Internet)
- Protocolos de ruteo

Componentes Utilizados

La información de este documento se basa en

- Cualquier versión de IOS 12.4T o superior.
- Cualquier versión 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.

Antecedentes

La traducción de direcciones de red es una técnica utilizada comúnmente para traducir direcciones IP en paquetes que fluyen entre redes utilizando diferentes espacios de direcciones. El propósito de este documento no es revisar NAT. Más bien, este documento pretende proporcionar una revisión completa de NAT tal como se utiliza en las redes VoIP de Cisco. Además, el alcance se limita a los componentes que conforman la tecnología MS-Voice.

- La NAT básicamente reemplaza la dirección IP dentro de los paquetes con una dirección IP diferente
- Habilita varios hosts en una subred privada para *compartir* (es decir, aparecer como) una única dirección IP pública, para acceder a Internet.
- Normalmente, las configuraciones NAT cambian sólo la dirección IP de los hosts internos
- NAT es bidireccional: si A se traduce a B en la interfaz interna, B que llegue a la interfaz externa se traducirá a A!
- RFC1631

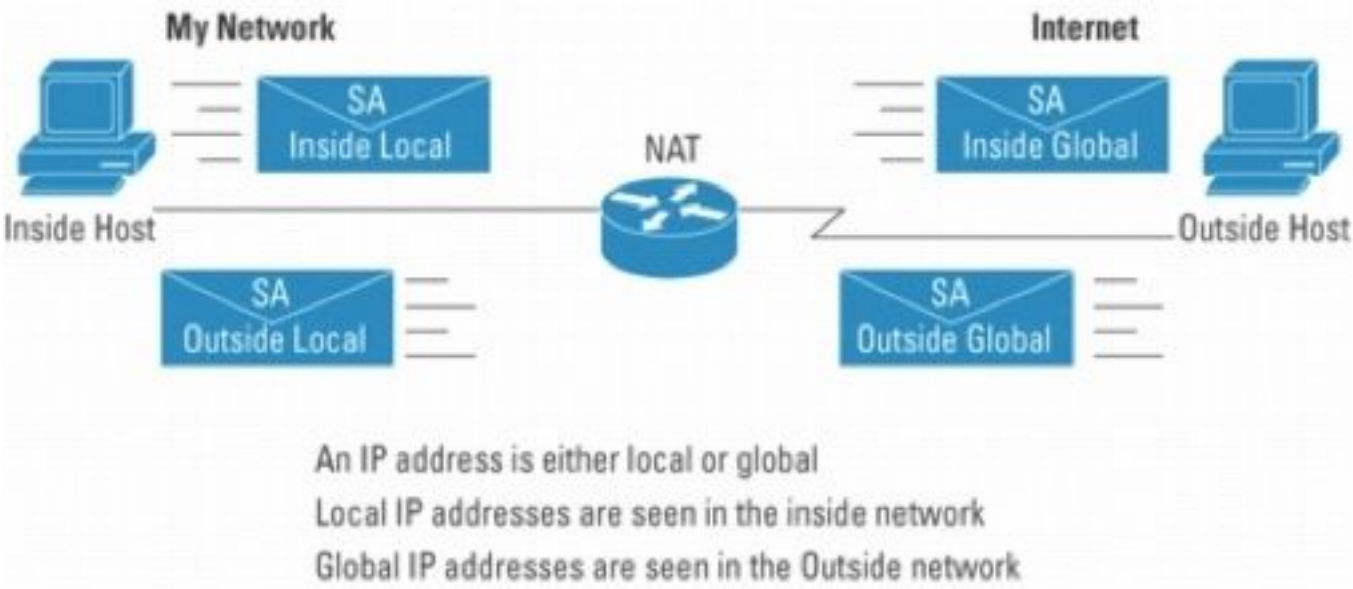

Figure 1

> **Nota**: Puede ayudar pensar en NAT como una ayuda para rutear paquetes IP dentro y fuera de las redes usando espacio de direcciones privadas. En otras palabras, NAT hace que las direcciones no enrutables sean enrutables

En la figura 2 se muestra la topología a la que se hace referencia en las ilustraciones siguientes.

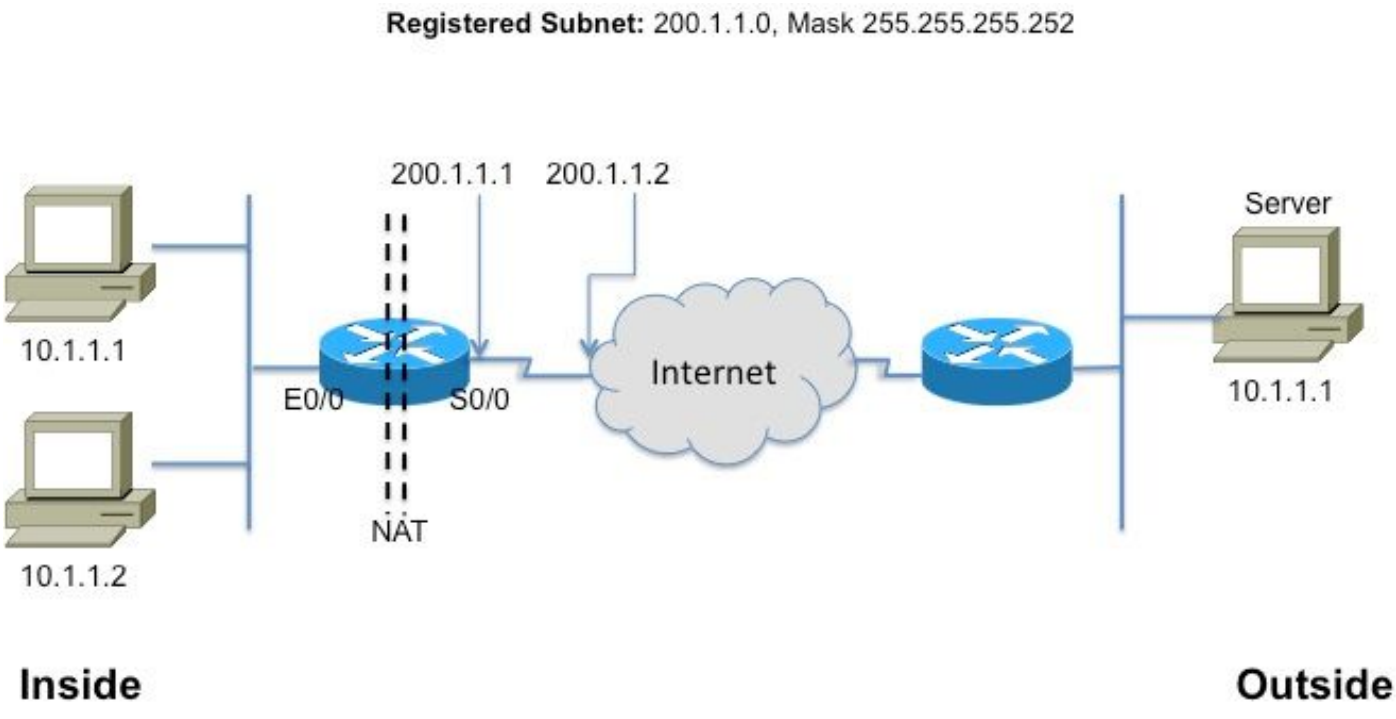

Figure 2

Este glosario es fundamental para comprender y describir la NAT

- **Dirección local interna**: dirección IP asignada a un host de la red *interna*. Normalmente, la dirección proviene de un espacio de direcciones privado.
- **Dirección global interna**: dirección IP enrutable asignada al mundo exterior por la NIC o el proveedor de servicios que representa una o más direcciones IP locales internas.

- **Dirección local externa**: la dirección IP de un host externo tal como aparece en la red interna. No necesariamente una dirección legítima, está asignada desde un espacio de dirección enrutable en el interior.
- **Dirección global externa**: dirección IP asignada a un host de la red externa por el propietario del host. La dirección se asigna desde una dirección o espacio de red enrutable globalmente.

  Nota: Ponte cómodo con estos términos. Cualquier nota o documento de NAT debe hacer referencia a ellos

NAT estática

Esta es la forma más simple de NAT, donde en cada dirección interna se traduce estáticamente a una dirección externa (y viceversa).

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Figure 3

La CLI para la configuración de la traducción anterior es la siguiente

interface Ethernet0/0

IP address 10.1.1.3 255.255.255.0

ip nat inside

!

Interfaz serial0/0

ip address 200.1.1.251 255.255.255.252

ip nat outside <—¡Obligatorio![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 dinámica

En NAT dinámica, cada host interno se asigna a una dirección de un conjunto de direcciones.

- Asigna una dirección IP desde un conjunto de direcciones globales internas.
- Si llega un nuevo paquete desde otro host interno y necesita una entrada NAT, pero todas las

direcciones IP agrupadas están en uso, el router simplemente descarta el paquete.
- Básicamente, el conjunto de direcciones globales internas debe ser tan grande como el número máximo de hosts simultáneos que necesitan utilizar Internet al mismo tiempo

La siguiente CLI ilustra la configuración de NAT dinámica

```
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
```

Sobrecarga NAT (PAT)

Cuando el conjunto (de direcciones IP) es más pequeño que el conjunto de direcciones que se deben traducir, esta función es muy útil.

- Varias direcciones internas NATed a una o varias direcciones externas
- PAT (traducción de direcciones de puerto) utiliza números de puerto de origen únicos en la dirección IP **global interna** para distinguir entre traducciones. Debido a que el número de puerto está codificado en 16 bits, el número total teóricamente podría ser tan alto como 65.536 por dirección IP. PAT intentará conservar el puerto de origen original; si este puerto de origen ya está asignado, PAT intentará encontrar el primer número de puerto disponible
- La sobrecarga de NAT puede utilizar más de 65 000 puertos, lo que le permite ampliarse sin necesidad de muchas direcciones IP registradas; en muchos casos, solo necesita una dirección IP global externa.

La figura 4 ilustra PAT.

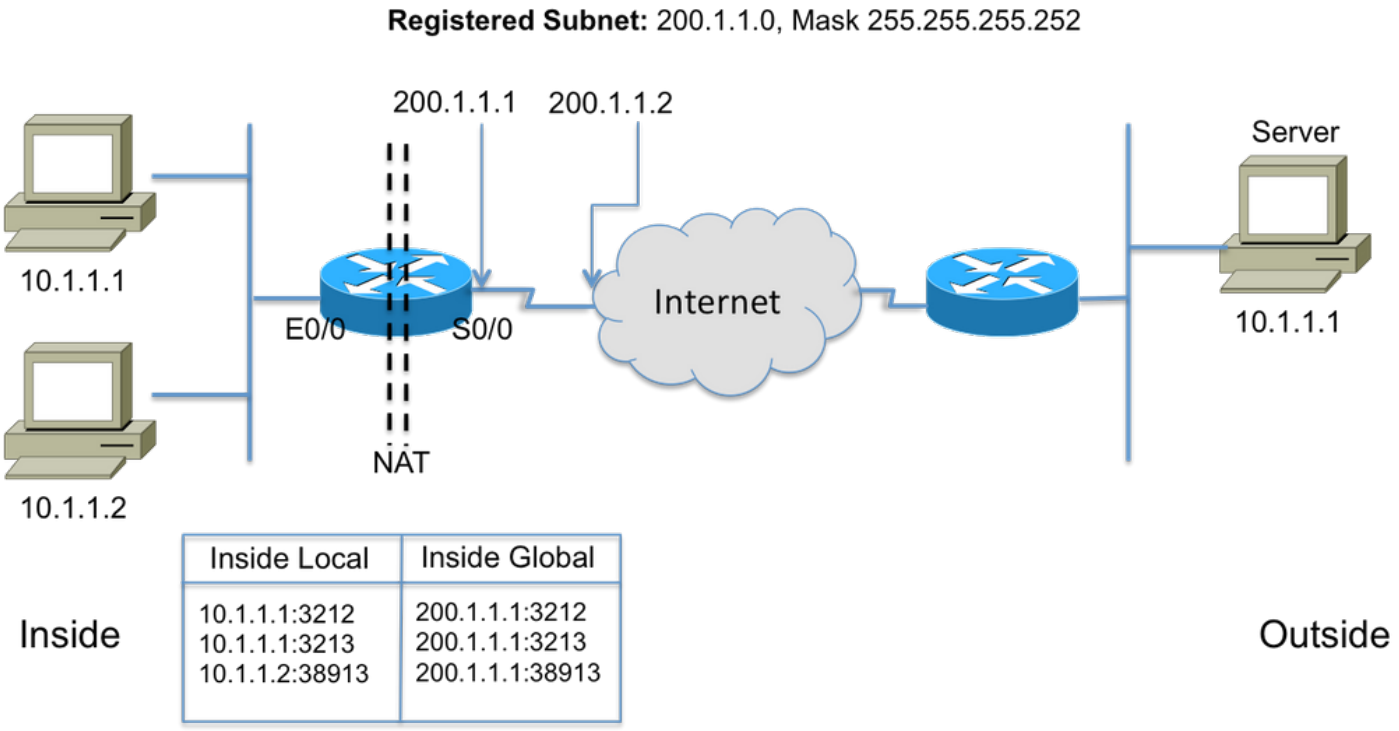

Figure 4

Opciones del comando NAT

La implementación de NAT de Cisco es muy versátil con una gran variedad de opciones. A continuación se enumeran algunas, pero consulte http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html para obtener detalles sobre la lista completa de mejoras.

- Traducciones estáticas con puertos: paquetes entrantes dirigidos a un puerto específico (p. ej. puerto 25, para servidor SMTP) enviado a un servidor específico.
- Compatibilidad con mapas de ruta: flexibilidad a la hora de configurar filtros/ACL
- Configuraciones de grupos más flexibles para permitir intervalos discontinuos de direcciones.
- Conservación de números de host: traduzca la parte "red" y conserve la parte "host".

agujerito NAT

Un agujero en el lenguaje NAT hace referencia a la correspondencia entre las tuplas <host IP, port> y <global address, *global* port>. Permite que el dispositivo NAT utilice el número de puerto de destino (que sería el puerto *global*) de los mensajes entrantes para mapear el destino nuevamente a la IP de host y al puerto que originó la sesión. Es importante tener en cuenta que los agujeros de seguridad se agotan después de un período de no uso y la dirección pública se devuelve al conjunto NAT.

NAT en VoIP

Entonces, ¿cuáles son los problemas y preocupaciones con NAT en las redes VoIP? Bueno, recuerde que la NAT que hemos discutido hasta ahora (conocida como NAT básica) solo traduce la dirección IP en el *encabezado* del paquete IP y vuelve a calcular la suma de comprobación, por supuesto, pero la señalización VoIP lleva direcciones integradas en el *cuerpo* de los mensajes de señalización. En otras palabras, en la capa 5

La figura 5 ilustra el efecto de dejar las direcciones IP integradas sin traducir. La señalización de llamada se completa correctamente, pero el proxy SIP del proveedor de servicios no puede enrutar los paquetes de medios (RTP) a la dirección de medios enviada por el agente de llamada.

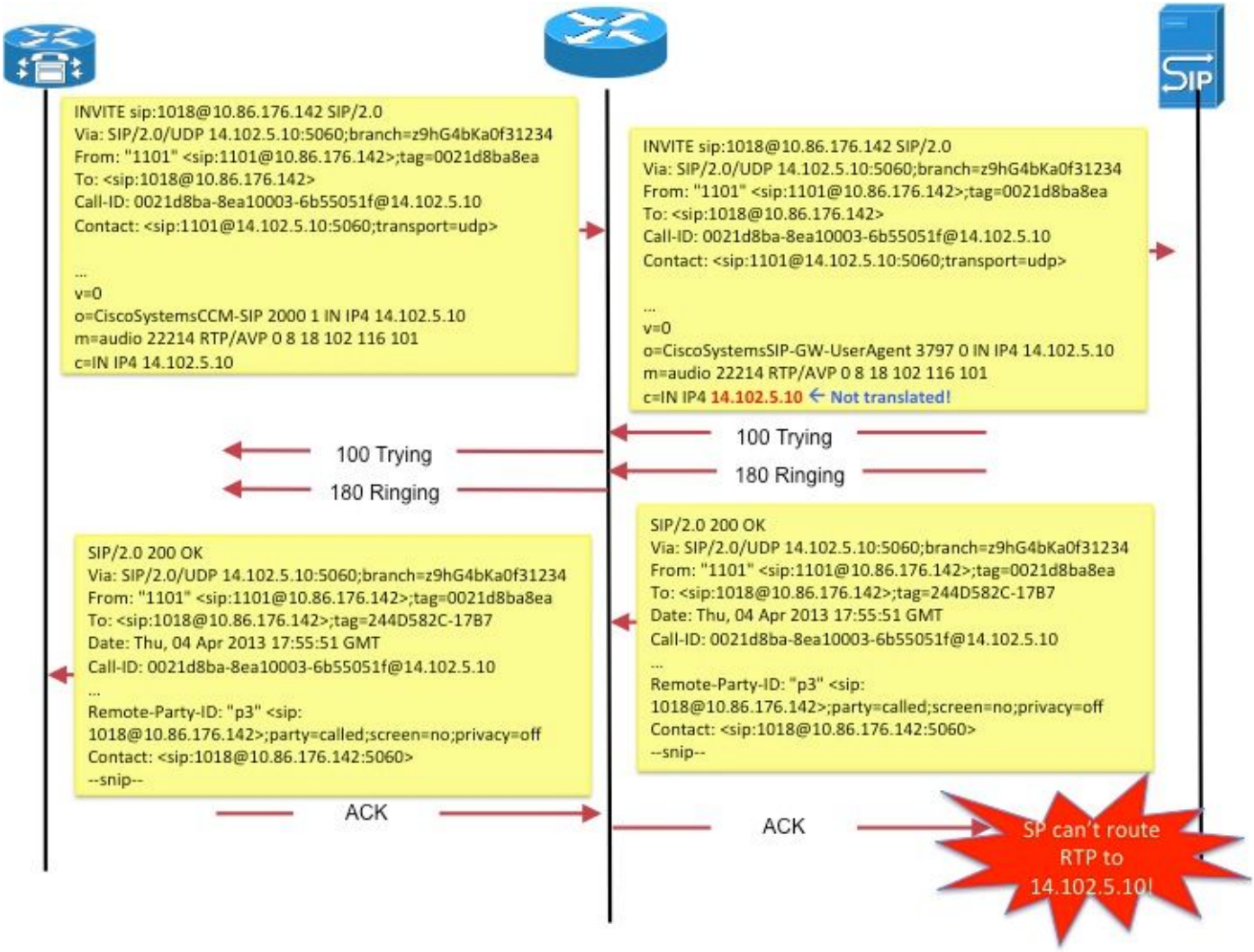

Figure 5

Otro ejemplo sería el uso de ***Contact*** por parte del terminal SIP*:* en SDP para comunicar la dirección en la que el terminal desea recibir mensajes de señalización para nuevas solicitudes.

Estos problemas se solucionan mediante una función denominada Application Layer Gateway (ALG).

ALG

Un ALG entiende el protocolo utilizado por las aplicaciones específicas que admite (por ejemplo, SIP) y realiza la inspección de paquetes de protocolo y la "reparación" del tráfico que lo atraviesa. Para obtener una buena descripción de cómo se arreglan los diversos campos para la señalización de llamadas SIP, consulte http://www.voip-info.org/wiki/view/Routers+SIP+ALG.

En los routers Cisco, el soporte para ALG SIP está habilitado, de forma predeterminada, en el puerto TCP estándar 5060. Es posible configurar ALG para admitir puertos no estándar para la señalización SIP. Consulte http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.

> **Precaución**: ¡Cuidado! No existe ningún RFC u otro estándar que especifique qué campos incrustados deben traducirse para los diversos protocolos VoIP. Como resultado, las implementaciones varían entre los proveedores de equipos, lo que da lugar a problemas de

interoperabilidad (y casos de TAC).

Gateways

Dado que las gateways, por definición, no son dispositivos de IP a IP, NAT no es aplicable.

CME

Esta sección del documento revisa los escenarios de llamadas con CME para entender por qué debe usarse NAT.

Situación 1. Teléfonos locales

Situación 2. Teléfonos remotos (con direcciones IP públicas)

Situación 3. Teletrabajador remoto

> **Nota**: En todos los casos, para que el audio fluya, la dirección IP de CME debe ser enrutable

Local

En esta situación (Figura 6), los dos teléfonos implicados en la llamada son teléfonos skinny con direcciones IP privadas.

'Figura 6'

> **Nota**: Recuerde que el teléfono ligero que está conectado en una llamada con otro teléfono ligero en el mismo sistema CME envía sus paquetes de medios directamente al otro teléfono; Es decir, el RTP para el teléfono local al teléfono local NO fluye a través del CME.

Por lo tanto, NAT no es aplicable ni obligatoria en este caso.

> **Nota**: CME determina si los medios (RTP) deben basarse directamente o no en si los dos teléfonos implicados en una llamada están delgados *y* en el mismo segmento de red. De lo contrario, CME se inserta en la trayectoria RTP.

Local a remoto

En este escenario (Figura 7), CME se inserta en el flujo RTP de modo que el RTP de los teléfonos se terminará en el CME. CME volverá a originar los flujos hacia el otro teléfono. Dado que CME se encuentra tanto en la red interna (privada) como en la red externa y envía su dirección interna al teléfono interno y su dirección externa (pública) al teléfono externo, tampoco se requiere NAT en este caso.

Sin embargo, tenga en cuenta que los puertos UDP/TCP (señalización y RTP) deben estar abiertos entre el teléfono IP remoto y la dirección IP de origen de CME. Esto significa que los firewalls u otros dispositivos de filtrado están configurados para permitir los puertos en cuestión.

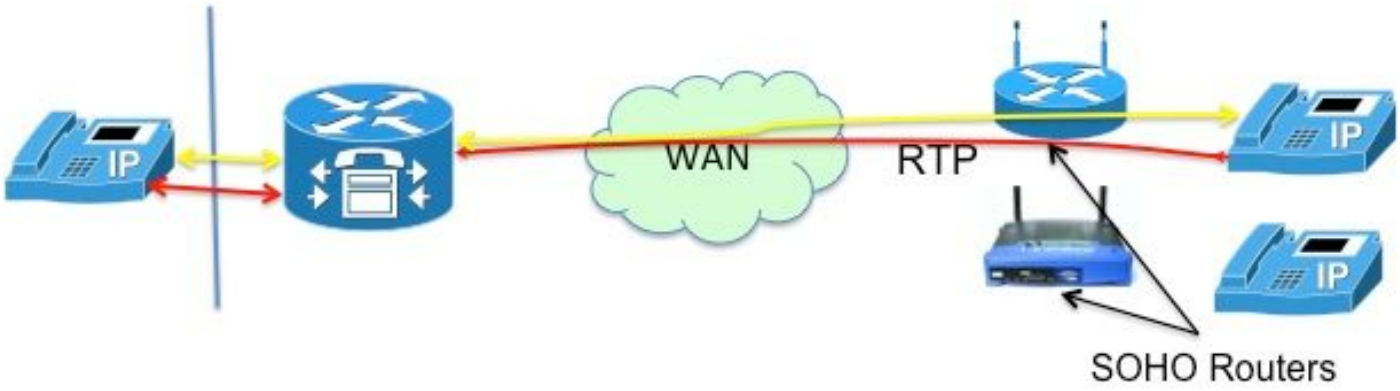

Figura 7

Nota: Tenga en cuenta que la señalización [mensajes] siempre termina en CM

Teletrabajador remoto

Esto se refiere a teléfonos IP que se conectan a CME a través de una WAN para admitir teletrabajadores que tienen oficinas remotas desde el router CME. Los diseños más comunes son aquellos que incluyen teléfonos con direcciones IP enrutables y teléfonos con direcciones IP privadas.

Teléfonos remotos con acceso público (lea: enrutable)

Si ambos teléfonos implicados en la llamada están configurados con direcciones IP enrutables públicas, los medios pueden fluir entre los teléfonos directamente (Figura 8). Por lo tanto, una vez más, no hay necesidad de NAT!

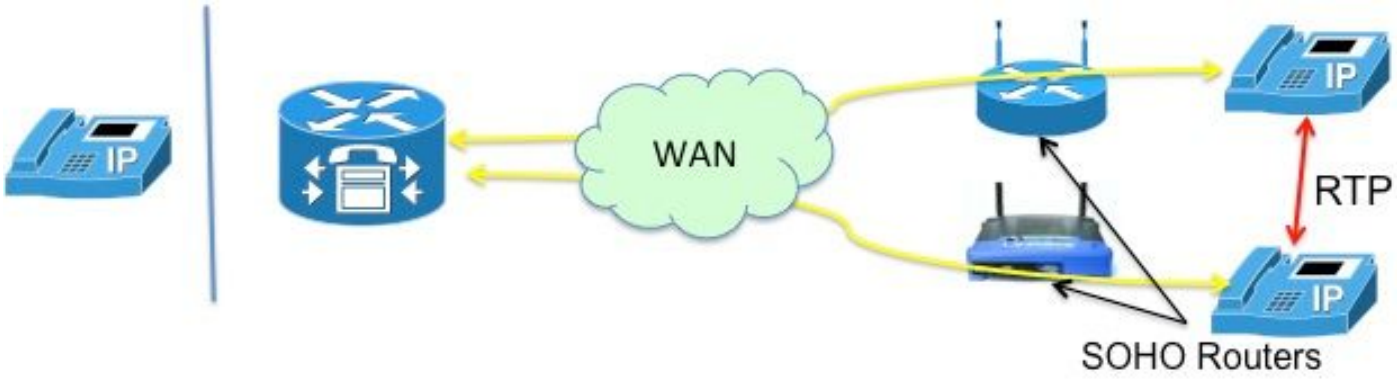

Figura 8

Teléfonos remotos con dirección IP privada

En este escenario, la llamada se señala entre teléfonos skinny configurados con direcciones IP privadas. Los routers de oficinas domésticas (SOHO), en general, tienden a no ser compatibles con SCCP. es decir, incapaz de traducir las direcciones IP integradas en los mensajes SCCP. Esto significa que, una vez finalizada la configuración de la llamada, los teléfonos acaban con la dirección IP privada de cada uno. Dado que ambos teléfonos son privados, CME indicará la llamada entre ellos de manera que el audio fluya directamente entre los teléfonos. Sin embargo, esto dará como resultado un audio unidireccional o no unidireccional (ya que las direcciones IP privadas, por definición, no se pueden enrutar a Internet), a menos que se implemente una de las siguientes soluciones:

·Configurar rutas estáticas en los routers SOHO

·establecer una conexión VPN IPsec con los teléfonos

Una mejor manera de resolver esto sería configurar "mtp". El comando mtp garantiza que los paquetes de medios (RTP) de los teléfonos remotos transiten a través del router CME (Figura 9).

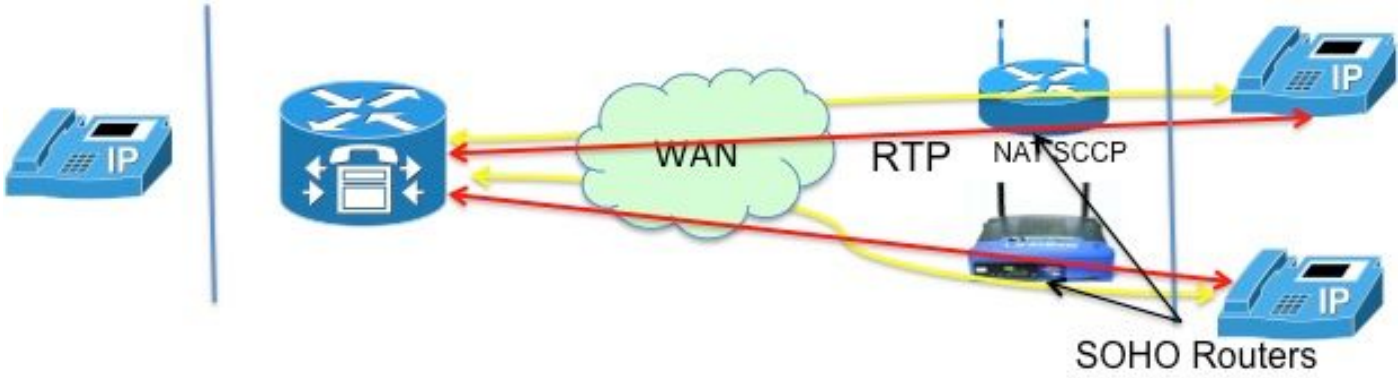

Figura 9

La solución "mtp" es mejor debido a las complicaciones con la apertura de los puertos de firewall. Un firewall puede obstruir los paquetes de medios que fluyen por una WAN. Esto significa que debe abrir puertos en el firewall, pero ¿cuáles? Con la retransmisión de audio CME, los firewalls se pueden configurar fácilmente para pasar los paquetes RTP. El router CME utiliza un puerto UDP ***específico*** (2000!) para los paquetes de medios. Por lo tanto, con solo permitir paquetes hacia y desde el puerto 2000, se puede pasar TODO el tráfico RTP.

La figura 10 ilustra cómo configurar mtp.

```
ephone 1
  mac 1111.222.3333
  tipo 7965
  mtp
  botón 1:1
```

Figura 10

No todo es maravilloso con mtp. Hay situaciones donde mtp puede no ser deseable

- MTP no es suave en la utilización de la CPU
- La MOH de multidifusión generalmente no se puede reenviar a través de una WAN- La función MOH de multidifusión verifica si MTP está habilitado para un teléfono y, si lo está, no envía MOH a ese teléfonoL.

Por lo tanto, si tiene una configuración de WAN que **puede** reenviar paquetes multicast y puede permitir paquetes RTP a través de su firewall, puede decidir no utilizar MTP.

Teléfonos SIP remotos

Tenga en cuenta que los teléfonos SIP no se mencionaron en las situaciones anteriores. Esto se debe al hecho de que si uno de los teléfonos es un teléfono SIP, CME se inserta en la ruta de audio. Esto luego se convierte en el escenario local a remoto descrito anteriormente, donde no se requiere NAT.

CUBO

El CUBE realiza de forma inherente las funciones NAT y PAT a medida que termina y vuelve a originar todas las sesiones. El CUBE sustituye su propia dirección por la dirección de cualquier punto final con el que se comunique, ocultando (traduciendo) de manera efectiva la dirección de ese punto final.

Por lo tanto, no se requiere NAT con la función CUBE. Existe un escenario de servicio VoIP en el que se requiere NAT en el CUBE, como se describe en la siguiente sección.

NAT transversal alojada

Una breve información sobre el servicio de telefonía alojado ayudará a comprender la justificación de esta función.

El servicio de telefonía alojado es una nueva forma de servicio VoIP en la que la mayor parte del equipo reside en la ubicación del proveedor de servicios. Funcionan con los gateways domésticos (HGW), que implementan solo NAT básica (es decir, NAT en L3/L4). Por ejemplo, Verizon instala la Terminal de Red Óptica (ONT), que proporciona servicios FiOS en el hogar; la llamada de voz se señala mediante un proceso SIP integrado en la ONT. La señalización SIP se realiza a través de la red IP privada de Verizon a los nuevos switches de software, que proporcionan el servicio y el control para establecer comunicaciones de voz a otros clientes de voz digital de FiOS, o a

clientes de teléfono tradicionales.

Entre los requisitos clave del proveedor para el servicio de telefonía alojado se incluyen los siguientes:

- NAT transversal remota: la capacidad de ofrecer servicios de clase 5 a los terminales mediante NAT (que solo puede realizar NAT de capa 3) y dispositivos de firewall (mediante "ALG" de forma remota).
- Compatibilidad con medios compartidos: la capacidad de enviar medios entre dispositivos ubicados en el mismo sitio donde no tiene sentido volver a enrutar los medios a la red IP
- Sin necesidad de agregar equipos adicionales, lo que elimina la necesidad de agregar CPE.

Teniendo en cuenta lo anterior, ¿qué opciones existen para implementar dicho servicio?

- Sustituir el HGW por un ALG caro,
- Utilice un controlador de borde de sesión (SBC) para modificar los encabezados SIP integrados para paquetes. Esto implica un producto alojado en red de clase operador que admite SIP en una configuración muy segura y tolerante a fallos. Esta solución se refiere a NAT SBC.

La opción NAT SBC satisface los requisitos del proveedor enumerados anteriormente.

NAT SBC

El SBC NAT funciona de la siguiente manera (Figura 11)

1. El router de acceso traduce solamente la dirección IP L3/L4
2. Dirección IP del mensaje SIP no traducida
3. SBC NAT intercepta y traduce la dirección IP integrada. En el momento en que el SBC ve los paquetes SIP destinados a **200.200.200.10**, activa el código nat-sbc.
4. Los medios no se traducen y van directamente entre los teléfonos[5]

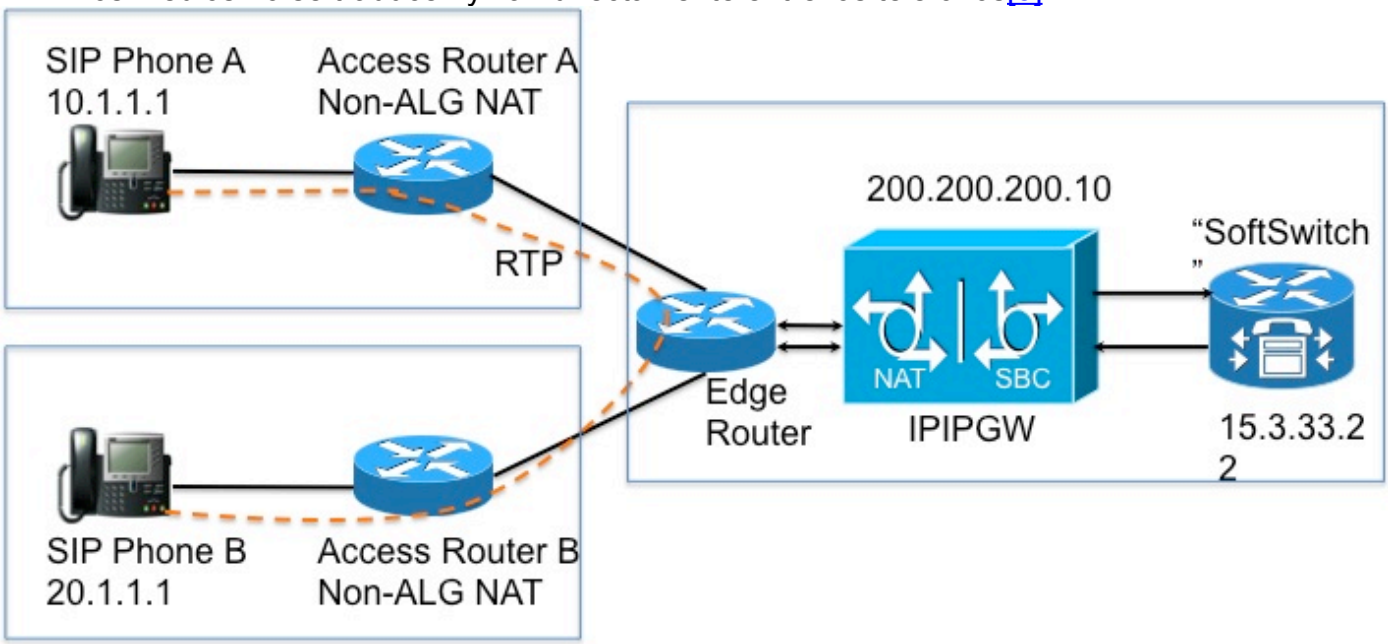

Figura 11

Notas de diseño

- La dirección IP **200.200.200.10** (Figura 12) no está asignada a ninguna interfaz en el SBC NAT. Se configura como la dirección del "proxy" al que los teléfonos SIP A y B envían mensajes de señalización.
- Los dispositivos domésticos no traducen determinados campos *de dirección* SIP/SDP (por ejemplo, ID de llamada: ,O= , Advertencia: Headers & Branch= parámetro. los parámetros maddr= y received= sólo se gestionaron en algunos escenarios.) Estos campos son manejados por el SBC NAT, excepto para la autorización de proxy y la traducción de autorización, porque esto interrumpirá la autenticación.
- Si los dispositivos domésticos están configurados para realizar PAT, los agentes de usuario (teléfonos y proxy) deben admitir la señalización simétrica[6] y medios simétricos y tempranos. Debe configurar el puerto de reemplazo en el router SBC NAT.
- En ausencia de soporte para señalización simétrica y medios simétricos y tempranos, los routers intermedios deben configurarse sin PAT y la dirección de reemplazo debe configurarse en el SBC NAT.

Configuración

A continuación se muestra un ejemplo de configuración para un SBC NAT típico.

```
ip nat sip-sbc

  proxy 200.200.200.10 5060 15.3.33.22 protocolo 5060 udp

  call-id-pool call-id-pool

  session-timeout 300

  mode allow-flow-around

  puerto de anulación

!

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 0.0.0.255

access-list 1 permit 171.1.1.0 0.0.0.255

access-list 2 permit 20.1.1.0 0.0.0.255

access-list 2 permit 172.1.1.0 0.0.0.255

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
```

Flujo de llamada con NAT SBC

Las figuras 13 y 14 ilustran el flujo de llamadas en términos de traducciones. Cabe señalar los siguientes aspectos:

- Tras el registro, el switch de software anota los dos teléfonos como
  — Teléfono SIP A: 15.3.33.62.2001

  — Teléfono SIP B - 15.3.33.62 2002

- En este flujo de llamadas, la NAT de SBC deja la dirección IP de medios sin traducir.

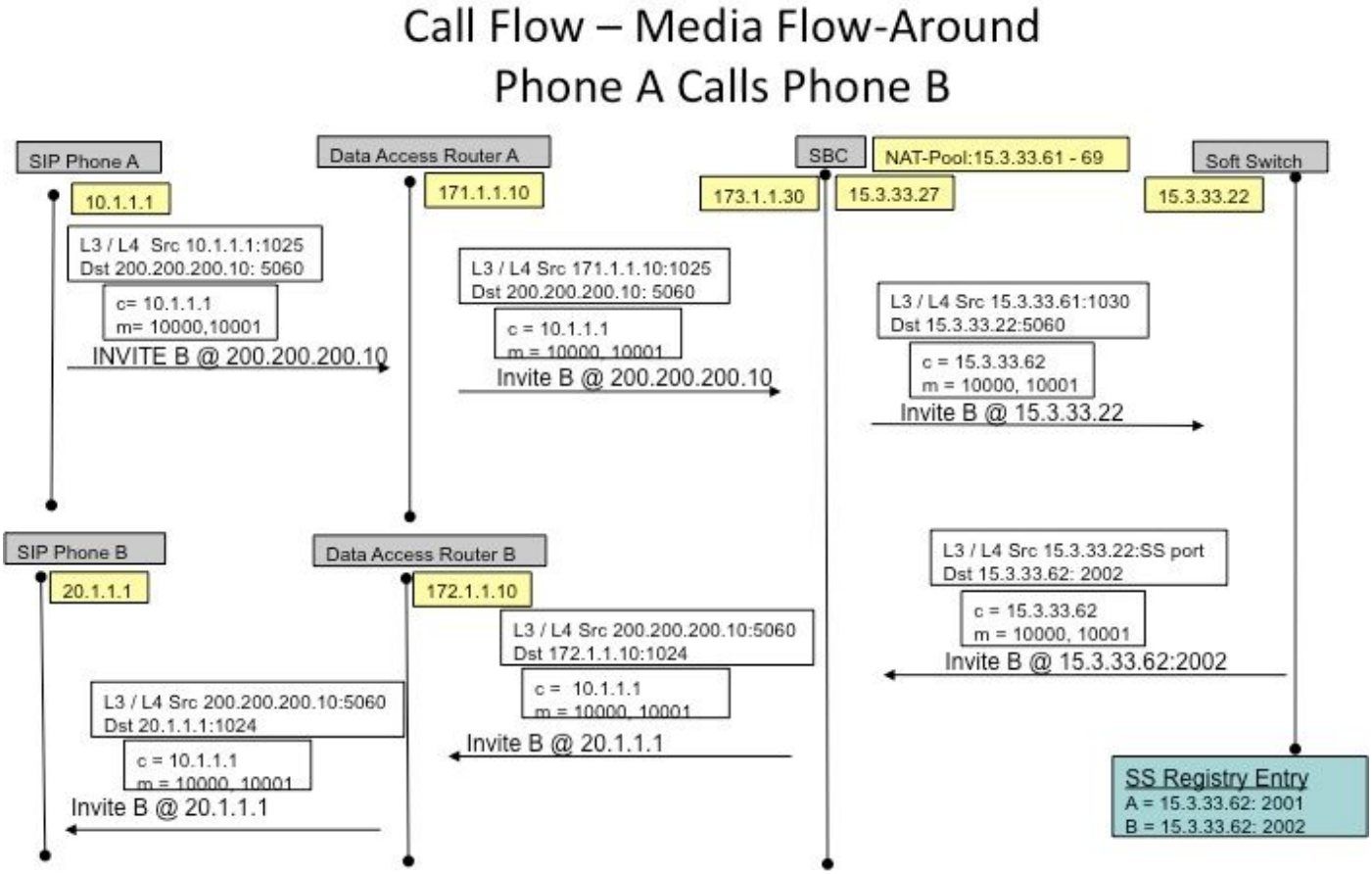

Figura 13

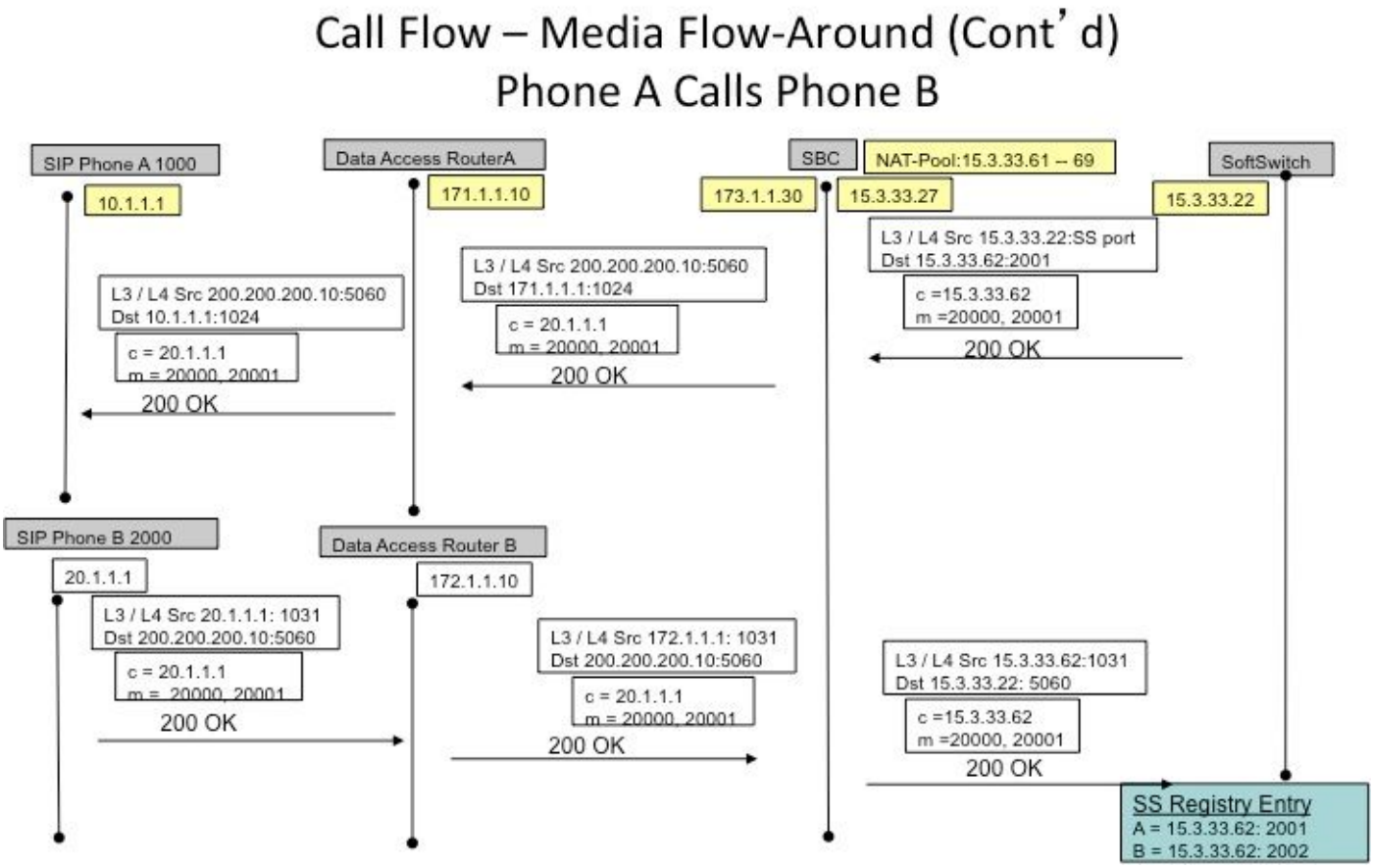

Figura 14

Registro SIP

En versiones anteriores (de SBC NAT), los terminales SIP tenían que enviar paquetes *keepalive* para mantener abierto el agujero de alfiler de registro SIP (para permitir el flujo de tráfico saliente->entrante, por ejemplo, llamadas entrantes). Los paquetes *keepalive* podían ser cualquier paquete SIP enviado por el terminal o el registrador (switch de software). Las versiones recientes obvian la necesidad de esto, ya que el propio NAT-SBC (a diferencia de los switches de software) obliga a los terminales a volver a registrarse con frecuencia para mantener los agujeros de alfiler abiertos.

> **Nota:** Los síntomas de un agujero de alfiler de registro caducado pueden ser oscuros, con fallas de señalización de llamadas aleatorias.

CÚSPIDE

CUSP tiene la noción de una red lógica, que se refiere a una colección de interfaces locales que son tratadas de manera similar para (e.g. interfaz, puerto, transporte para escucha) con fines de ruteo. Al configurar una red lógica en CUSP, puede configurarla para utilizar NAT. Una vez configurado, SIP ALG se activa automáticamente. Esto es útil cuando ciertas redes lógicas.

Resolución de problemas

Síntomas

Un síntoma obvio podría ser que una llamada falla en una o ambas direcciones. Los síntomas menos obvios pueden incluir,

- Audio unidireccional
- Audio unidireccional en transferencia
- Audio sin interferencias
- Pérdida del registro SIP

Comandos show y debug

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

Cosas que comprobar

- Asegúrese de que la configuración incluya el subcomando de interfaz **ip nat inside** o **ip nat outside**. Estos comandos habilitan NAT en las interfaces, y la designación interna/externa es importante.
- Para NAT estática, asegúrese de que el comando **ip nat source static** enumera la dirección local interna primero y la dirección IP global interna en segundo lugar.
- Para NAT dinámica, asegúrese de que la ACL configurada para hacer coincidir los paquetes enviados por el host interno coincidan con los paquetes de ese host, antes de que se haya producido cualquier traducción NAT. Por ejemplo, si una dirección local interna de 10.1.1.1 se debe traducir a 200.1.1.1, asegúrese de que la ACL coincida con la dirección de origen 10.1.1.1, no 200.1.1.1.
- Para NAT dinámica sin PAT, asegúrese de que el conjunto tenga suficientes direcciones IP. Los síntomas de no tener suficientes direcciones incluyen un valor creciente en el segundo contador misses en el resultado del comando **show ip nat statistics**, así como ver todas las direcciones en el rango definido en el conjunto NAT en la lista de traducciones dinámicas.
- Para PAT, es fácil olvidarse de agregar la opción **overload** en el comando **ip nat inside source list**. Sin ella, NAT funciona, pero PAT no, lo que a menudo provoca que los paquetes de los usuarios no se traduzcan y que los hosts no puedan acceder a Internet.
- Quizás NAT se ha configurado correctamente, pero existe una ACL en una de las interfaces, descartando los paquetes. Observe que el IOS procesa las ACL antes de la NAT para los paquetes que ingresan a una interfaz y después de traducir las direcciones para los paquetes que salen de una interfaz.
- No olvide configurar "ip nat outside" en la interfaz de cara a la WAN (incluso si no traduce la dirección externa).
- Tan pronto como se configura NAT, show ip nat translations no muestra nada. Haga ping una vez y vuelva a comprobarlo.
- Agarre **Wireshark Traces** en las interfaces internas y externas de NAT-SBC

Escenarios

A continuación se muestra el resultado de la depuración para un par de escenarios. ¡Se explican por sí mismos!

NAT básico

A continuación se muestran las líneas de configuración y depuración para NAT básica.

```
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

Se muestran las líneas de salida de **debug ip nat sip**. En este caso, se traduce la dirección IP integrada en un paquete saliente.

```
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:
```

Referencias

Información general:

- http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html
- Anatomía: 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 y 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

Matriz de funciones 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

NAT transversal alojada:

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

NAT SBC

- EDCS-611622
- EDCS-526070

ALG:

- http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-0s/iadnat-applvlgw.html
- http://www.voip-info.org/wiki/view/Routers+SIP+ALG
- http://www.commpartners.us/knowledge/attachments/voip-nat.pdf
- http://www.cisco.com/en/US/partner/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html

CME

- http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/srnd/design/guide/security.html#wp1077376
- http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc_cucm.html

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).