NAT en el VoIP

Contenido

Introducción

Este documento describe el comportamiento del NAT (Network Address Translation) en el Routers que trabaja como CUBO (Cisco Unified Border Element), CME o CUCME (administrador unificado Cisco de Cummunication expreso), los gatewayes y CAMBIO DE SIGNO (Cisco unificó el proxy del SORBO).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- SORBO (Session Initiation Protocol)
- Voz sobre IP (protocolo de Internet)
- Protocolos de ruteo

Componentes Utilizados

La información en este documento se basa encendido

- Cualquier versión de IOS 12.4T y arriba.
- Cualquier versión CME

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

La traducción de dirección de red es una técnica de uso general para traducir los IP Addresses en los paquetes que fluyen entre las redes usando diversos espacios de la dirección. El propósito de este documento no es revisar el NAT. Bastante, este documento apunta proporcionar un estudio completo del NAT como se utiliza en las redes VoIP de Cisco. Además, el alcance se limita a los componentes que componen la tecnología de la MS-Voz.

- El NAT substituye básicamente la dirección IP dentro de los paquetes por una diversa dirección IP
- Host múltiples de los permisos en una subred privada *para compartir* (es decir aparezca como) a un solo IP Address público, para acceder Internet.
- Típicamente, cambio de configuraciones del NAT solamente la dirección IP de los host interiores
- ¡El NAT es bidireccional si A consigue traducida a B en la interfaz interior, B que llega la interfaz exterior conseguirá traducido a A!
- RFC1631

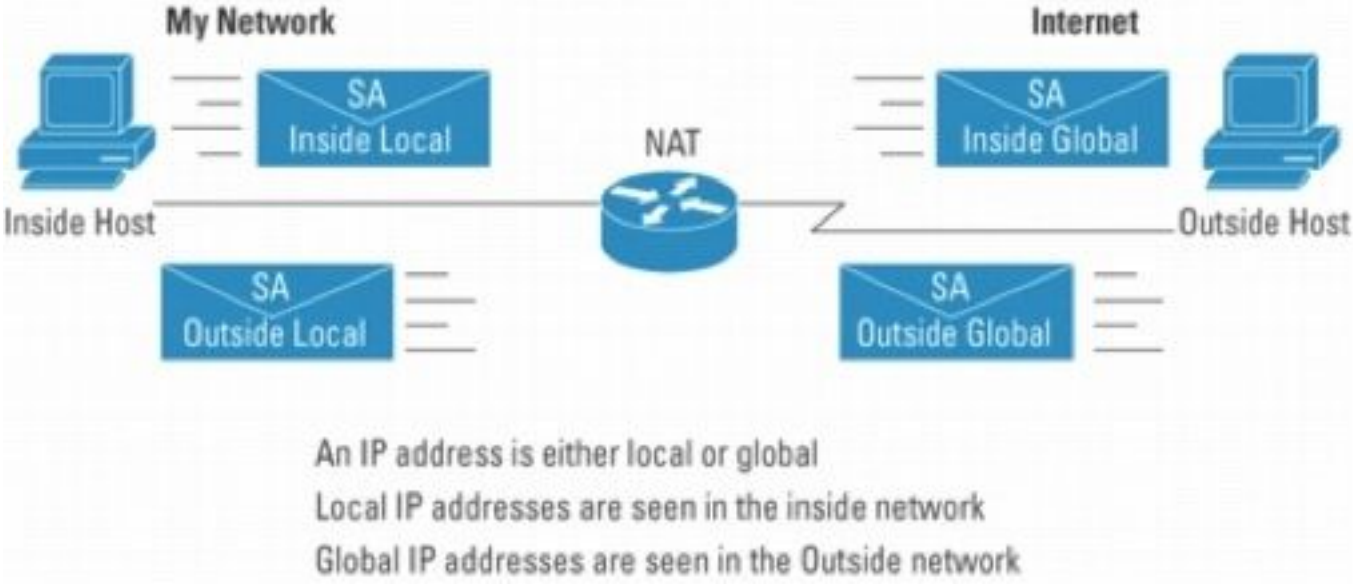


Figura 1

> Nota: Puede ayudar a pensar en el NAT como ayuda para rutear los paquetes del IP en y fuera de las redes usando el espacio de dirección privada. Es decir el NAT hace el routable no routable de los direccionamientos

El cuadro 2 muestra la topología referida a los ejemplos que siguen.

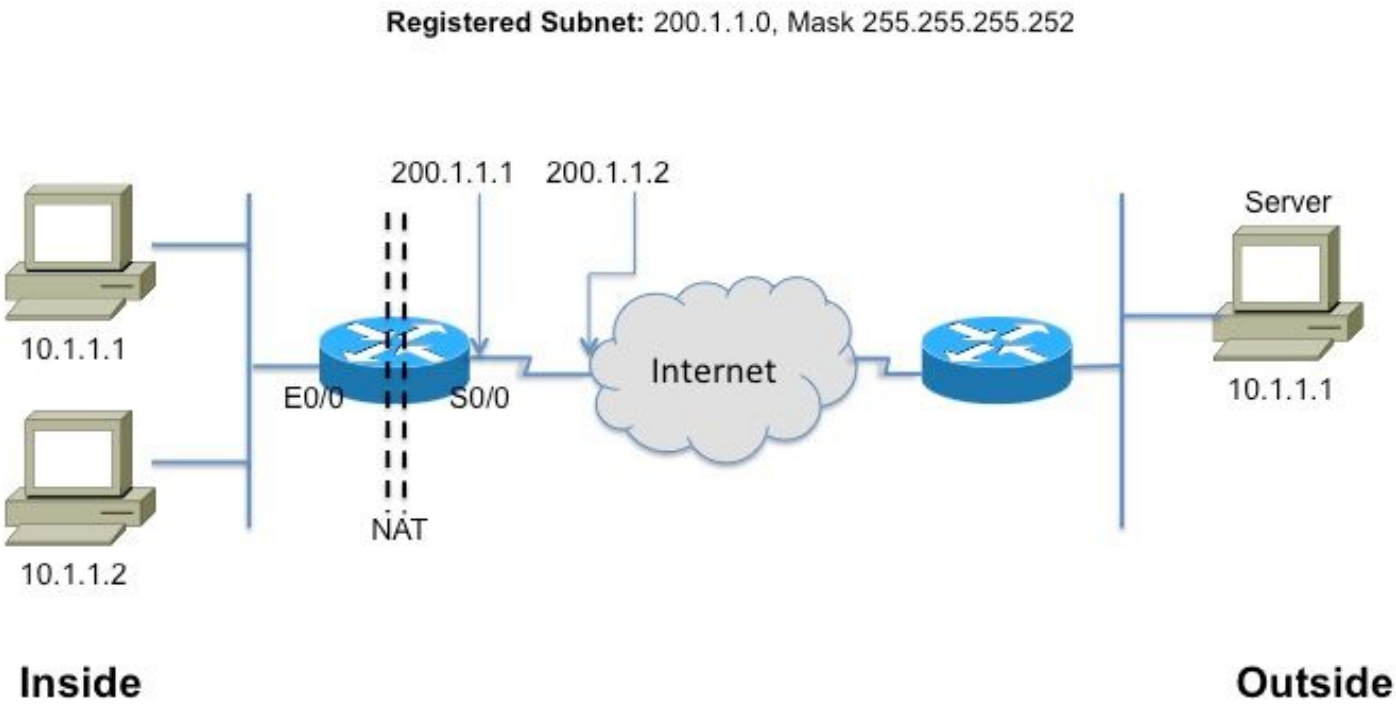


Figura 2

Este glosario es fundamental entender y describir el NAT

- Dirección local interna - La dirección IP asignada a un host en la red interna. Típicamente, el direccionamiento es de un espacio de dirección privada.
- **Dirección global interna** — Un IP Address ruteable asignado por el NIC o el proveedor de servicio que representa uno o más IP Addresses del Inside Local al mundo exterior.
- **Dirección local externa** — La dirección IP de un host exterior como aparece a la red interna. No necesariamente una dirección legítima, está asignada desde un espacio de dirección enrutable en el interior.
- **Dirección global externa** — La dirección IP asignada a un host en la red externa por el propietario del host. El direccionamiento se afecta un aparato global de una dirección enrutable o de un espacio de red.

> Nota: Consiga cómodo con estos términos. Cualquier nota o doc. en el NAT está seguro de referirles

NAT estática

Está la forma ésta más simple de NAT, donde en cada dirección interna se traduce estáticamente a una dirección externa (y vice versa).

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Figura 3

El CLI a la configuración para la traducción antedicha está como sigue

Ethernet0/0 de la interfaz

dirección IP 10.1.1.3 255.255.255.0

interior nacional del IP

¡!

Serial0/0 de la interfaz

dirección IP 200.1.1.251 255.255.255.252

exterior nacional del IP <-- ¡Requerido! [2]

source static interior nacional 10.1.1.2 200.1.1.2 del IP

source static interior nacional 10.1.1.1 200.1.1.1 del IP

NAT dinámica

En el NAT dinámico, cada host interior se asocia a un direccionamiento de una agrupación de direcciones.

- Afecta un aparato una dirección IP de un pool de las direcciones globales internas.
- Si un nuevo paquete llega de otro host interior, y necesita una entrada de NAT, pero todos los IP Addresses reunidos son funcionando, el router desecha simplemente el paquete.
- Esencialmente, el pool de las direcciones globales internas necesita ser tan grande como el número máximo de host simultáneos que necesiten utilizar Internet al mismo tiempo

El CLI siguiente ilustra configurar el NAT dinámico

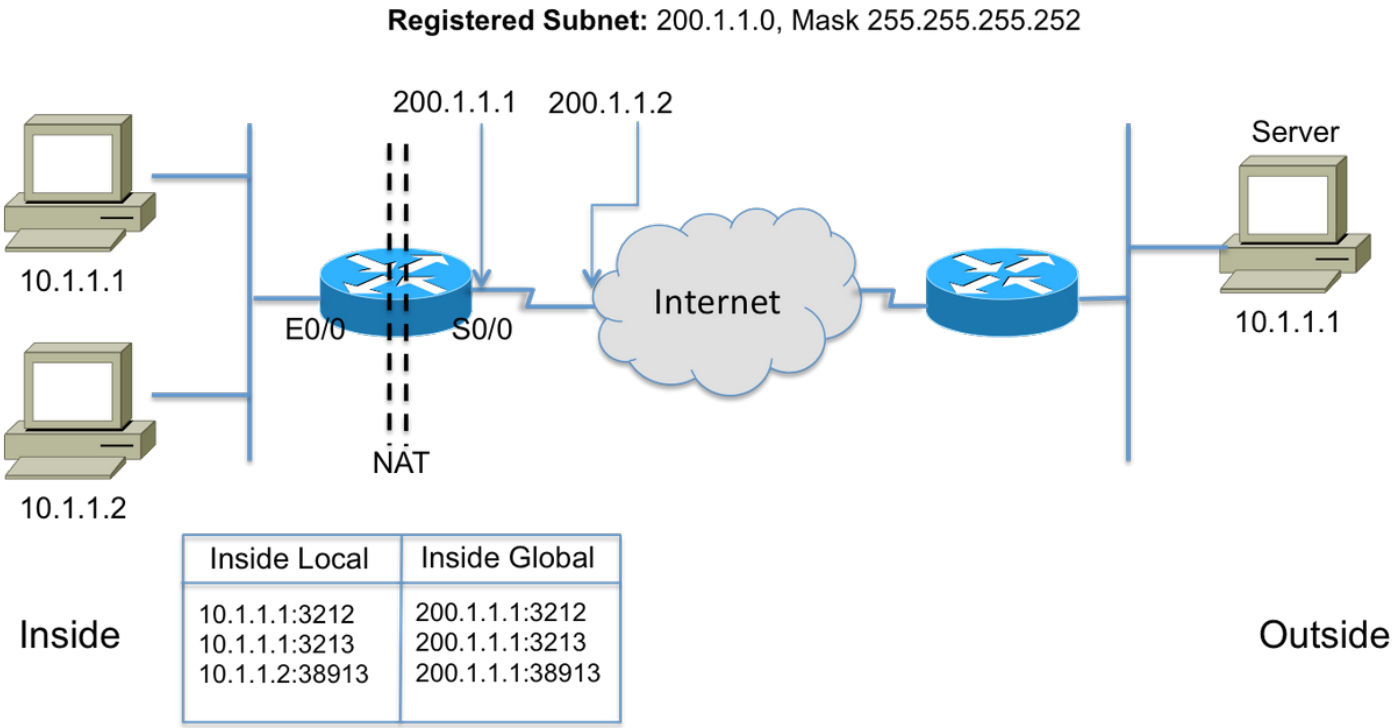
```
ip nat pool fred 200.1.1.1 200.1.1.2 netmask 255.255.255.252
!
!
ip nat inside source list 1 pool fred
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
```

Sobrecarga NAT (PALMADITA)

Cuando el pool (de los IP Addresses) es más pequeño que el conjunto de los direccionamientos que necesitan ser traducidos, esta característica viene en práctico.

- Vario NATed de las direcciones internas a las solamente una o alguna direcciones externas
- La PALMADITA (traducción de dirección de puerto) utiliza los números de puerto de fuente única en la dirección IP del Inside Global para distinguir entre las traducciones. Porque el número del puerto se codifica en 16 bits, el número total podría teóricamente ser tan alto como 65,536 por la dirección IP. La PALMADITA intentará preservar el puerto de fuente original, si este puerto de origen es ya PALMADITA afectada un aparato intenta encontrar el primer número del puerto disponible
- La sobrecarga NAT puede utilizar más de 65,000 puertos, permitiendo que escale bien sin la necesidad de muchos IP Address registrado — en muchos casos, necesitando solamente una dirección IP del Outside Global.

El cuadro 4 ilustra el patente.



'Figura 4'

Opciones del comando nat

La implementación NAT de Cisco es muy versátil con un host de las opciones. Algunos son mencionados abajo, pero refieren por favor a http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html para los detalles en la lista completa de mejoras.

- Traducciones estáticas con los puertos – Paquetes entrantes dirigidos a un puerto específico (e.g puerto 25, porque al servidor SMTP) enviados a un servidor específico.
- Soporte para los mapa del ruta - Flexibilidad en configurar los filtros/ACL
- Configuraciones más flexibles del pool para permitir los rangos de direcciones discontinuos.

- Preservación del host number - Traduzca la pieza de la “red”, conserve la partición del “host”.

Agujerito NAT

Un agujerito en el lenguaje NAT refiere a la asignación entre el IP del <host, el port> y el direccionamiento <global, los tuples *globales del* port>. Permite que el dispositivo NAT utilice el número de puerto de destino (que sería el puerto *global*) de mensajes entrantes para asociar el destino de nuevo al IP del host y para virar hacia el lado de babor que originado la sesión. Es importante observar que los agujeritos miden el tiempo hacia fuera después de un período de no utilización y vuelven a la dirección pública al agrupamiento NAT.

NAT en el VoIP

¿Así pues, cuáles son los problemas y las preocupaciones con el NAT en las redes VoIP? Bien, recuerde ese NAT que hemos discutido hasta ahora (losely referredto como NAT básico) traduzcamos solamente la dirección IP en encabezado del paquete IP *y recalcula la suma de comprobación, por supuesto, solamente la señalización VoIP lleva los direccionamientos integrados en el cuerpo de los* mensajes de señalización. Es decir en la capa 5

El cuadro 5 ilustra el efecto de dejar los IP Address incluidos sin traducir. ¡La señalización de llamada completa acertado, pero el proxy del SORBO en el proveedor de servicio falla intentar rutear los paquetes del (RTP) de los media al direccionamiento de los media enviado por el agente de la llamada!

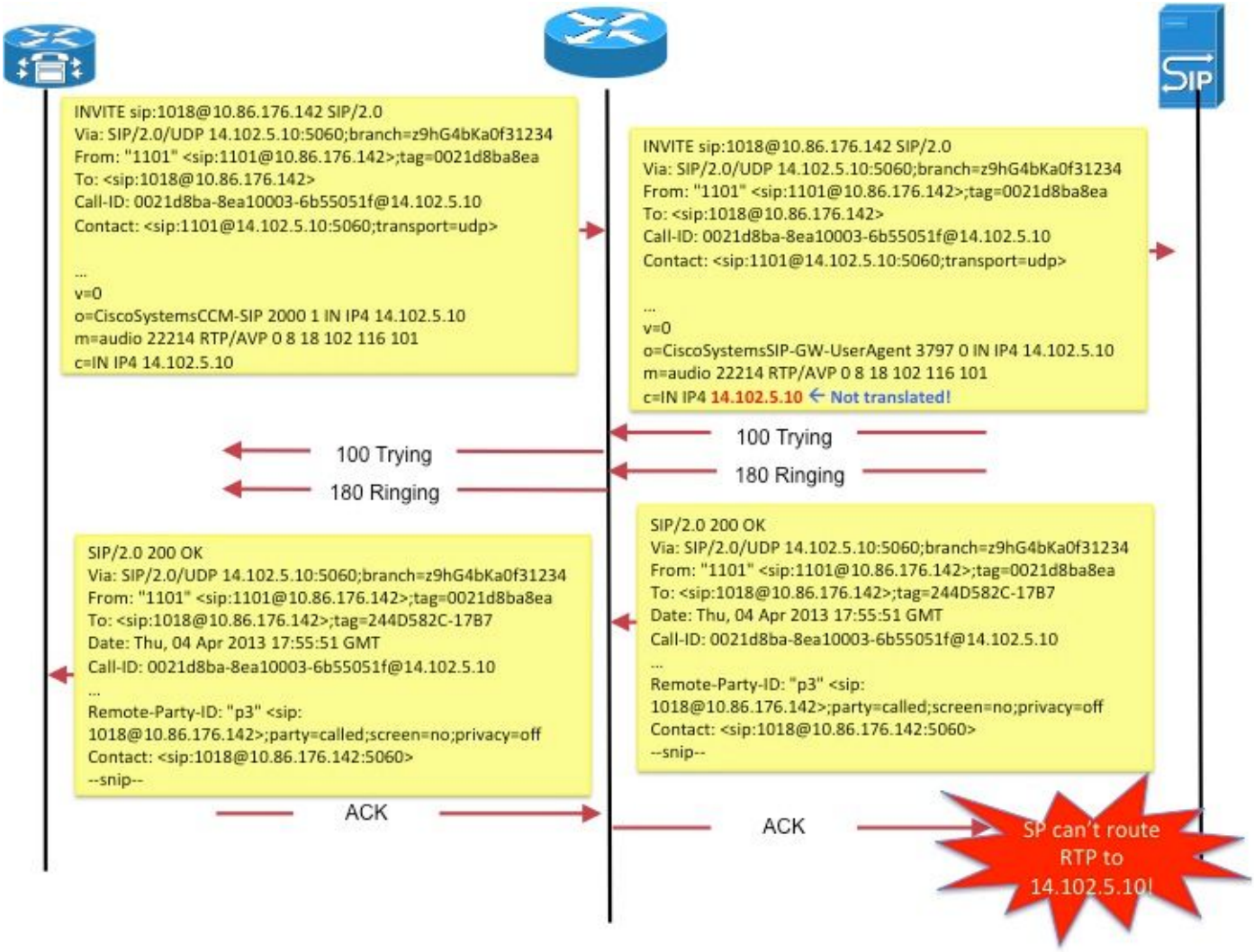


Figura 5

Otro ejemplo sería el uso del punto final del SORBO del ***contacto:*** coloque en el SDP para comunicar el direccionamiento en el cual el punto final quisiera recibir los mensajes de señalización para las nuevas peticiones.

Estos problemas son abordados por una característica llamada el gateway de capa de aplicación (ALG).

ALG

Un ALG entiende el protocolo usado por las aplicaciones específicas que soporta (e.g. SORBO) y hace la inspección de paquetes y el "fixup" del protocolo del tráfico a través de él. Para una buena descripción de cómo los diversos campos se reparan-para arriba para la señalización de llamada del SORBO, refiera a http://www.voip-info.org/wiki/view/Routers+SIP+ALG.

En los routeres Cisco, el soporte para el SORBO ALG se habilita, por abandono, en el puerto TCP estándar 5060. Es posible configurar ALG para soportar los puertos no estándar para la señalización del SORBO. Refiera a http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.

> Precaución: ¡Guárdese! No hay el RFC o el otro estándar que de los encantos los campos hacia fuera que integró se deben traducir para los diversos protocolos VoIP. Como

consecuencia, las implementaciones varían, entre los vendedores del equipo, dando por resultado los problemas del interop (y los casos TAC).

Gateways

Desde los gatewayes, por definición, no están los dispositivos IP-a-IP, NAT son no corresponde.

CME

Esta sección de los escenarios de llamada del documento revisa con el CME para entender porqué el NAT debe ser utilizado.

Teléfonos locales del escenario 1.

Teléfonos remotos del escenario 2. (con los IP Address públicos)

Teletrabajador del telecontrol del escenario 3.

> Nota: En todas las cajas, para que el audio fluya, la dirección IP CME necesita ser routable

Local

En este escenario (el cuadro 6), los dos teléfonos implicados en la llamada es teléfonos básicos con los IP Address privados.

'Figura 6'

> Nota: Recuerde que ese teléfono básico que esté conectado en una llamada con otro teléfono básico 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 atraviesa el CME.

Por lo tanto, el NAT es no corresponde o requerido en este caso.

> Nota: El CME determina si (RTP) de los media directamente o no basado encendido si los dos teléfonos implicados en una llamada son flacos *y* en el mismo segmento de red. Si no,

el CME se inserta en la trayectoria RTP.

Local al telecontrol

En este escenario (el cuadro 7), CME se inserta en la secuencia RTP tales que el RTP de los teléfonos será terminado en el CME. El CME re-originará las secuencias hacia el otro teléfono. Puesto que el CME se sienta en la red (privada) interior y la red externa y envía a su dirección interna al direccionamiento interior del teléfono y del exterior (público) al teléfono exterior, el NAT no se requiere aquí tampoco.

Observe sin embargo, eso los puertos UDP/TCP (señalización así como RTP) debe estar abierto entre el teléfono del IP remoto y la dirección IP de origen CME. Esto significa que los Firewall u otros dispositivos de filtrado están configurados para permitir los puertos en la pregunta.

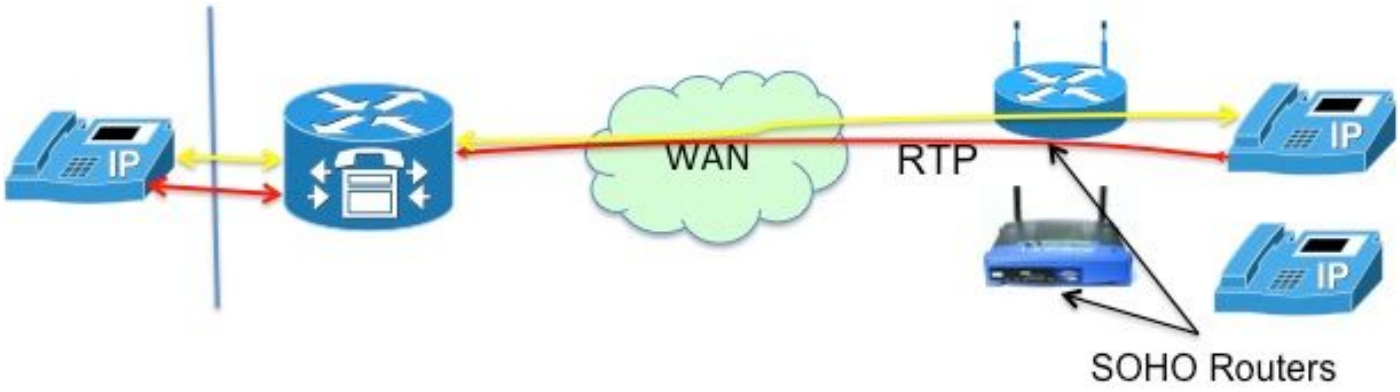


Figura 7

Nota: Observe que señalando el [messages] están terminados siempre en el CM

Teletrabajador remoto

Esto refiere a los Teléfonos IP que conectan con el CME sobre WAN para apoyar a los teletrabajadores que tienen oficinas que sean remotas del CME Router. Los diseños mas comunes son ésos que implican los teléfonos con los IP Address ruteables y los teléfonos con los IP Address privados.

Teléfonos remotos con el público (leído: IP Addresses del routable)

Si ambos los teléfonos implicados en la llamada se configuran con el público, los IP Address ruteables, los media pueden fluir entre el cuadro de los teléfonos directamente 8). ¡Por lo tanto, de nuevo, ninguna necesidad del NAT!

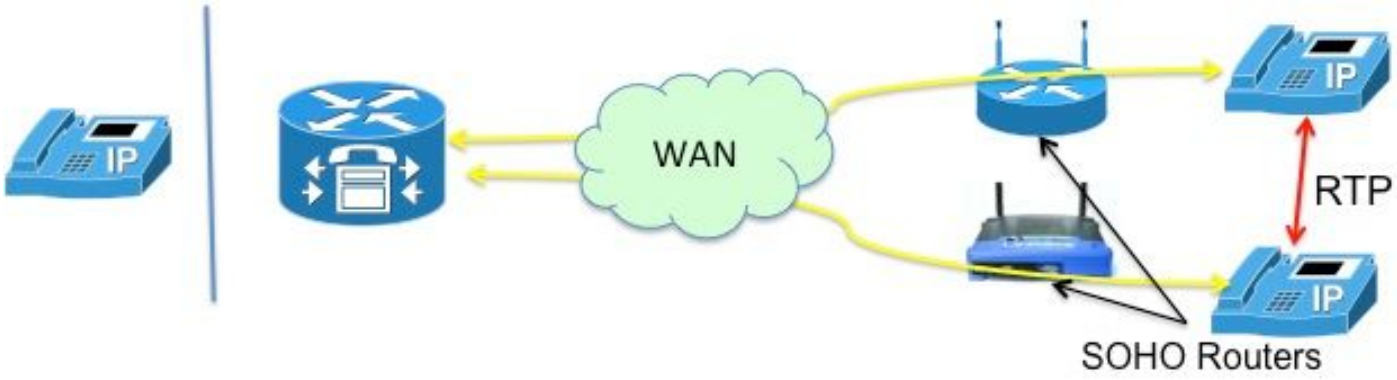


Figura 8

Teléfonos remotos con el IP Address privado

En este escenario, la llamada se señala entre los teléfonos básicos configurados con los IP Address privados. El Routers de la oficina en el hogar (SOHO), tiende generalmente a no ser "SCCP enterado". es decir incapaz de traducir los IP Addresses integrados en los mensajes SCCP. Esto significa que, sobre la realización de la configuración de la llamada, los teléfonos terminan para arriba con el IP Address privado de cada uno. Puesto que ambos los teléfonos son privados, el CME señalará la llamada entre ellos tales que el audio fluye directamente entre los teléfonos. Esto sin embargo, dará lugar al audio de una forma o de la ninguna manera (desde los IP Address privados, por definición, no puede ser ruteado en al Internet!), a menos que uno de los workarounds siguientes se implemente -

· Configure las Static rutas en los routeres sohos

· establezca una conexión del IPSec VPN a los teléfonos

Una mejor manera de resolver esto sería configurar el "mtp". El comando del mtp se asegura de que los paquetes del (RTP) de los media de los teléfonos remotos transiten a través del CME Router (cuadro 9).

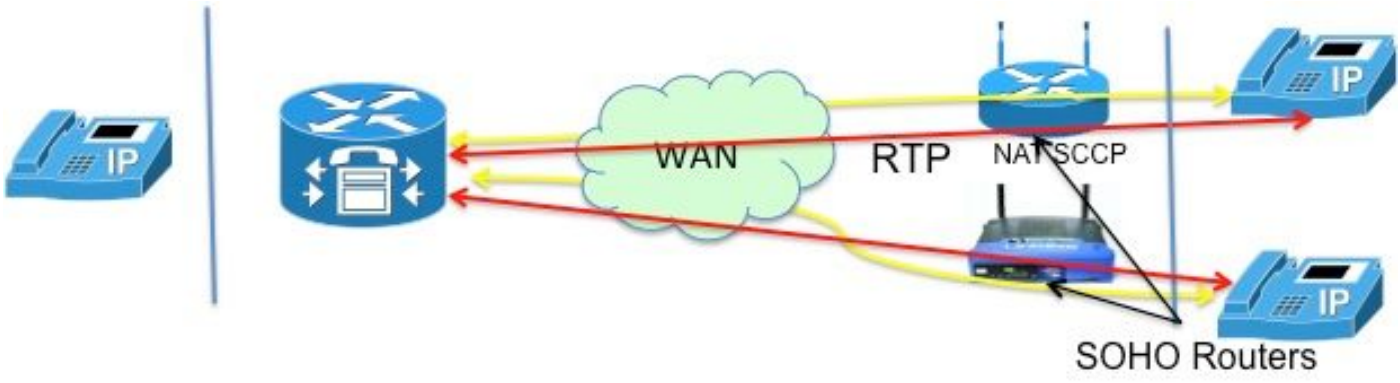


Figura 9

La solución del "mtp" es mejor debido a las complicaciones con la apertura de los puertos de firewall. Los paquetes de medios que fluyen sobre WAN se pueden obstruir por un Firewall. ¿Esto significa que usted necesita los puertos abiertos en el Firewall, pero cuáles? Con el CME retransmitiendo el audio, los Firewall se pueden configurar fácilmente para pasar los paquetes RTP. El CME Router utiliza un UDP ***específico*** port(2000!) para los paquetes de medios. Así pues, apenas permitiendo los paquetes a y desde el puerto 2000, TODO EL tráfico RTP puede

ser pasado.

El cuadro 10 ilustra cómo configurar el mtp.

```
ephone 1

 mac 1111.2222.3333

 tipo 7965

 mtp

 botón 1:1
```

Figura 10

Todo no es maravilloso con el mtp. Hay las situaciones donde el mtp puede no ser deseable

- El MTP no es apacible en la utilización de la CPU
- El Multicast MOH no se puede remitir generalmente sobre WAN los controles de la característica del Multicast MOH para considerar si el MTP se habilita para un teléfono y si es, no envía el MOH a ese phoneL.

Así, si usted tiene una configuración WAN que pueda remitir los paquetes de multidifusión y usted puede permitir los paquetes RTP con su Firewall, usted puede decidir no utilizar el MTP.

Teléfonos remotos del SORBO

Observe que los teléfonos del SORBO no fueron mencionados en los escenarios antedichos. Éste es debido al hecho de que si uno de los teléfonos es un teléfono del SORBO, el CME se inserta en el trayecto de audio. Éste entonces se convierte en el escenario del local-a-telecontrol descrito anterior, en donde el NAT no se requiere.

CUBO

El CUBO intrínsecamente realiza las funciones NAT y de la PALMADITA mientras que termina y re-origina todas las sesiones. El CUBO substituye su propio direccionamiento para el direccionamiento de cualquier punto final que comunique con, así con eficacia ocultando (el traducir) el direccionamiento de ese punto final.

Así, el NAT no se requiere con la función del CUBO. Hay un escenario del servicio de VoIP en el cual el NAT se requiere en el CUBO, según lo descrito en la siguiente sección.

Traversal recibido NAT

Un fondo abreviado en el servicio de telefonía recibido ayudará a entender el fundamento para esta característica.

El servicio de telefonía recibido es una nueva forma de servicio de VoIP en la cual la mayor parte

del engranaje reside en la ubicación del proveedor de servicio. Trabajan con los gatewayes de inicio (HGW), que implementan solamente NAT básico (es decir NAT en L3/L4). E.g. Verizon instala la terminal de red óptica (Ontario), que proporciona los servicios de FiOS en el hogar; la llamada de voz se señala usando un proceso del SORBO incorporado al Ontario. La señalización del SORBO se hace sobre la red del IP privada de Verizon al nuevo Switches suave, que proporcionan el servicio y el control para establecer las comunicaciones por voz a otros clientes de la voz digital de FiOS, o a los clientes del teléfono tradicional.

Entre los requisitos dominantes del proveedor para el servicio de telefonía recibido incluya,

- Traversal remoto NAT: la capacidad de entregar los servicios de la clase 5 a los puntos finales que utilizan el NAT (que puede hacer solamente la capa 3 NAT!) y los dispositivos del Firewall (haciendo “ALG” remotamente!)
- soporte de los Co-media: la capacidad de enviar los media entre los dispositivos colocalizados donde no tiene sentido de rutear los media de nuevo a la red del IP
- Ningún equipo agregado, eliminando la necesidad de agregar cualquier CPE.

¿Dado el antedicho, qué opciones existen para implementar tal servicio?

- Substituya el HGW por un ALG costoso,
- Utilice un regulador de la frontera de la sesión (SBC) para modificar las encabezados integradas del SORBO para los paquetes. Esto implica red-haber recibido, producto del portador-grado que soporta el SORBO en una configuración muy segura, incidente-tolerante. Esta solución es SBC referido NAT.

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

SBC NAT

Los trabajos SBC NAT como sigue (cuadro 11)

1. El router de acceso traduce solamente la dirección IP L3/L4
2. Dirección IP en el mensaje del SORBO no traducido
3. El SBC NAT intercepta y traduce el IP Address incluido. El momento que el SBC ve los paquetes del SORBO destinados a **200.200.200.10**, él golpea adentro el código con el pie NAT-sbc.
4. El media no se traduce y va directamente entre el phones[5]

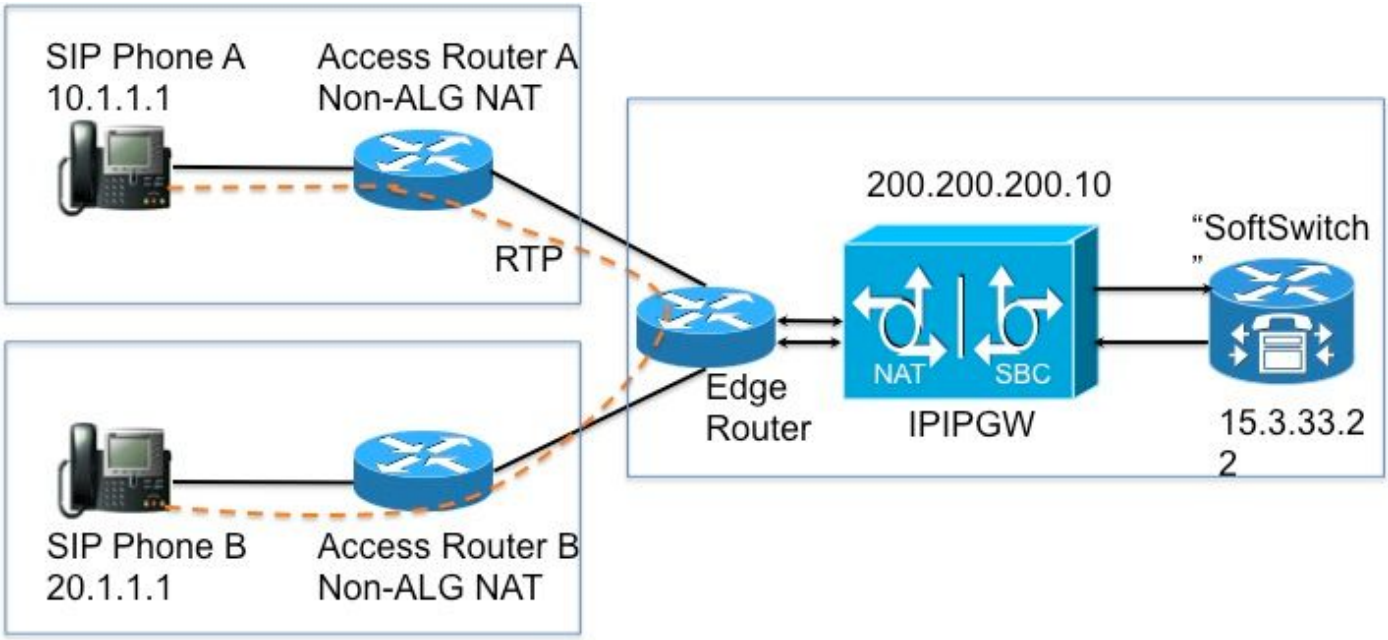


Figura 11

Notas del diseño

- No asignan la dirección IP 200.200.200.10 (cuadro 12) a ninguna interfaz en el SBC NAT. Se configura mientras que el direccionamiento del “proxy” a cuál envían el teléfono A del SORBO y el teléfono B del SORBO los mensajes de señalización.
- Los dispositivos caseros no traducen ciertos campos del *direccionamiento-solamente* SIP/SDP (e.g. ID de llamada: , O=, advirtiendo: encabezados y parámetro del branch=. los parámetros del maddr= y del received= fueron manejados en ciertos escenarios solamente.). Estos campos son manejados por el SBC NAT, a excepción de la traducción de la proxy-autorización y de la autorización, porque éstos romperán la autenticación.
- Si los dispositivos caseros se configuran para hacer la PALMADITA, los agentes de usuario (los teléfonos y proxy) deben soportar signaling[6] simétrico y los media simétricos y tempranos. Usted debe configurar el puerto de la invalidación en el router SBC NAT.
- En ausencia del soporte para la señalización simétrica y los media simétricos y tempranos, los routeres intermedios deben ser configurados sin la PALMADITA y el direccionamiento de la invalidación se debe configurar en el SBC NAT.

Configuración

La configuración de muestra para un SBC típico NAT sigue.

```
sorbo-sbc nacional del IP

 UDP del protocolo de 200.200.200.10 5060 15.3.33.22 5060 del proxy

 llamada-identificación-pool del llamada-identificación-pool

 sesión-descanso 300

 modo permitir-flujo-alrededor de
```

```
 puerto de la invalidación

¡!

netmask 255.255.0.0 del ip nat pool sbc1 15.3.33.61 15.3.33.69

netmask 255.255.0.0 del ip nat pool sbc2 15.3.33.91 15.3.33.99

netmask 255.255.0.0 de 1.1.1.1 1.1.255.254 del llamada-identificación-pool del ip nat pool

netmask 255.255.255.0 de 200.200.200.100 200.200.200.200 del exterior-pool del ip nat pool

sobrecarga interior nacional del pool sbc1 de la lista de origen 1 del IP

pool interior nacional sbc2 de la lista de origen 2 del IP

agregar-ruta nacional del exterior-pool del pool de la lista de fuente externa del IP 3

llamada-identificación-pool interior nacional del pool de la lista de origen 4 del IP

¡!

permiso 10.1.1.0 0.0.0.255 de la lista de acceso 1

permiso 171.1.1.0 0.0.0.255 de la lista de acceso 1

permiso 20.1.1.0 0.0.0.255 del access-list 2

permiso 172.1.1.0 0.0.0.255 del access-list 2

permiso 15.4.0.0 0.0.255.255 de la lista de acceso 3

permiso 15.5.0.0 0.0.255.255 de la lista de acceso 3

permiso 10.1.0.0 0.0.255.255 de la lista de acceso 4

permiso 20.1.0.0 0.0.255.255 de la lista de acceso 4
```

Flujo de llamada con SBC NAT

El cuadro 13 y el cuadro 14 ilustran el flujo de llamada en términos de traducciones. Las puntas siguientes deben ser observadas

- Sobre el registro, el Switch suave observa abajo de los dos teléfonos como
  -- Teléfono A del SORBO – 15.3.33.62 2001

  -- Teléfono B del SORBO – 15.3.33.62 2002

- En este flujo de llamada, el SBC NAT con eficacia sale de la dirección IP de los media sin traducir.

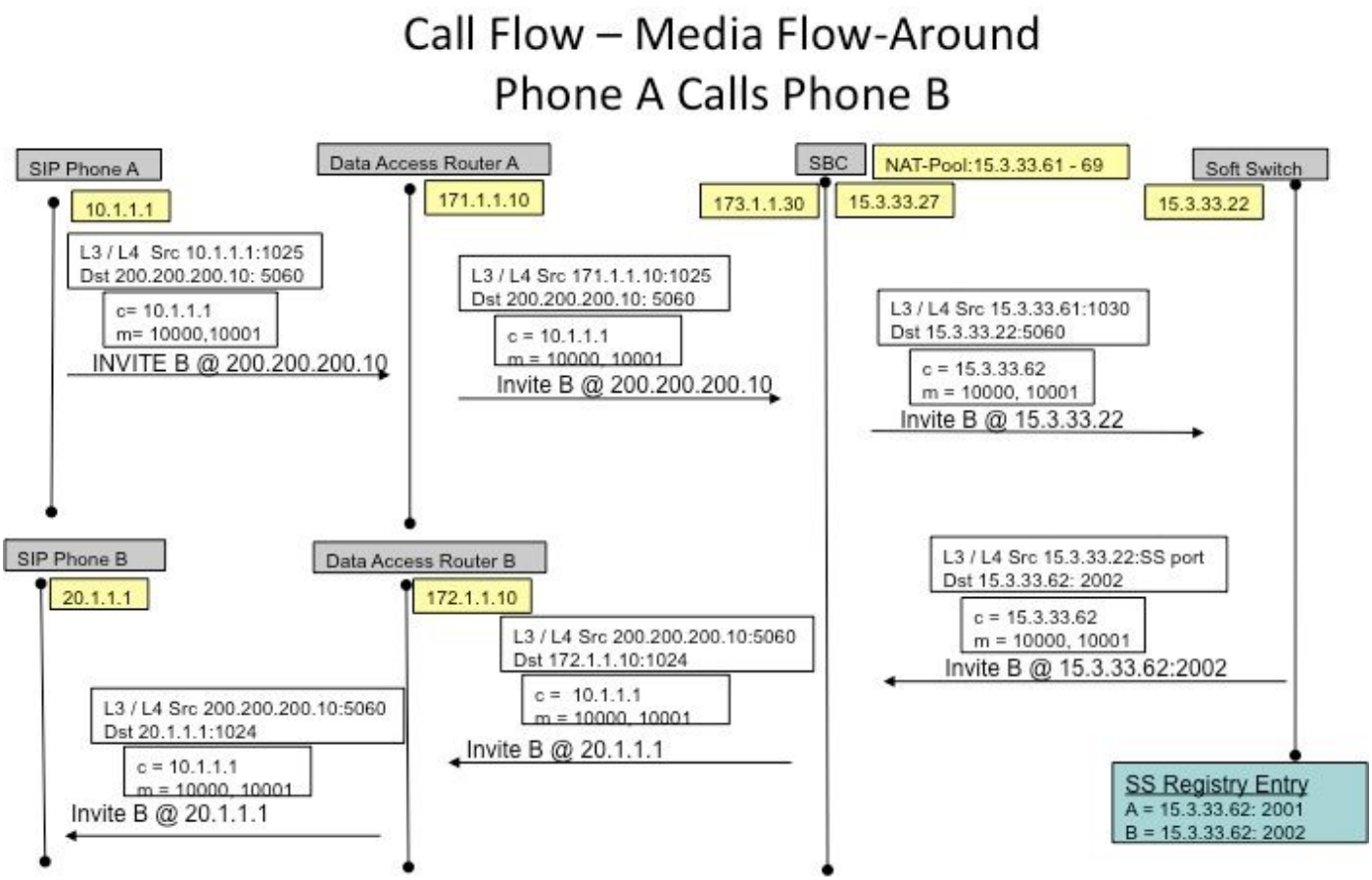


Figura 13

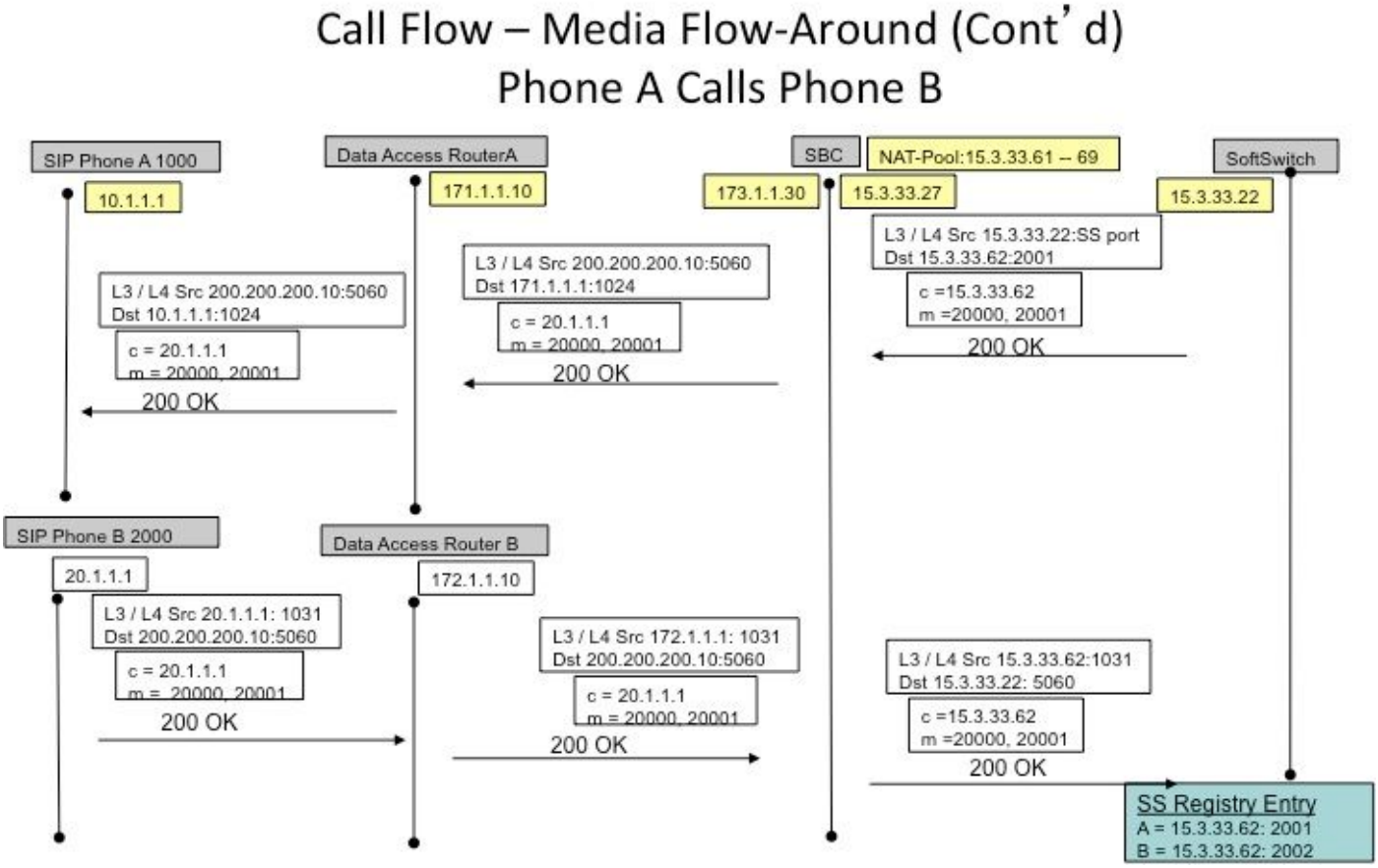


Figura 14

Registro del SORBO

En las versiones anteriores (de SBC NAT), los puntos finales del SORBO tuvieron que enviar los *paquetes de señal de mantenimiento* para mantener el agujerito del registro del SORBO abierto (permitir que el tráfico del out->in fluya, e.g las llamadas entrantes). los paquetes de señal de mantenimiento podrían ser cualquier paquete del SORBO enviado por el punto final o el secretario (Switch suave). Las versiones recientes evitan la necesidad de esto, con el NAT-SBC sí mismo (en comparación con el Switches suave) forzando los puntos finales para reregistrar con frecuencia para guardar los agujeritos se abren.

> Nota: Los síntomas de un agujerito expirado del registro pueden ser indeterminados, con los errores al azar de la señalización de llamada.

CAMBIO DE SIGNO

El CAMBIO DE SIGNO tiene la noción de una red lógica, que refiere a una colección de interfaces locales que se traten semejantemente para (e.g interfaz, puerto, transporte para escuchar) los propósitos de ruteo. Al configurar una red lógica en el CAMBIO DE SIGNO, usted puede configurarlo para utilizar el NAT. Una vez que está configurado, el SORBO ALG se habilita automáticamente. Esto es útil cuando ciertas redes lógicas.

Resolución de problemas

Síntomas

Un síntoma evidente pudo ser que una llamada falla en una o las ambas direcciones. Menos síntomas evidentes pudieron incluir,

- Audio unidireccional
- Audio unidireccional en la transferencia
- Audio de la ninguna manera
- Registro perdidoso del SORBO

Comandos show y debug

- `IP DEB nacional [sorbo | flaco]`
- `show ip nat statistics`
- `show ip nat translations`

Cosas a marcar

- Asegúrese de que la configuración incluya el **interior nacional del IP** o el submandato **nacional de la interfaz exterior del IP**. Estos comandos enable NAT en las interfaces, y la designación del interior/del exterior es importantes.

- Para el NAT estático, asegúrese de que el **IP las** listas de **comando source static nacionales la** dirección local interna primero y el IP Address global interior en segundo lugar.
- Para el NAT dinámico, asegúrese de que el ACL configurado para hacer juego los paquetes enviados por el host interior haga juego que han ocurrido los paquetes del host, antes de cualquier traducción de NAT. Por ejemplo, si traducen a una dirección local interna de 10.1.1.1 a 200.1.1.1, asegúrese de que el ACL haga juego a la dirección de origen 10.1.1.1, no 200.1.1.1.
- Para el NAT dinámico sin la PALMADITA, asegúrese de que el pool tenga bastantes IP Addresses. Los síntomas del no tener las suficientes direcciones incluyen un valor cada vez mayor en las segundas faltas al revés en la salida del **comando show ip nat statistics**, así como consideran todos los direccionamientos en el rango definido en el agrupamiento NAT en la lista de traducciones dinámicas.
- Para la PALMADITA, es fácil olvidar agregar la opción de la **sobrecarga** en el **comando ip nat inside source list**. Sin él, los trabajos NAT, sino la PALMADITA no hace, a menudo dando por resultado los paquetes de los usuarios no siendo traducido y los host el no poder llegar a Internet.
- Quizás el NAT se ha configurado correctamente, pero un ACL existe en una de las interfaces, desechando los paquetes. Observe que los procesos IOS ACL antes de que NAT para los paquetes que ingresan una interfaz, y después de traducir los direccionamientos para los paquetes que salen una interfaz.
- ¡No olvide configurar el “exterior nacional del IP” en la interconexión haciendo frente a WAN (incluso si no traduce a la dirección externa)!
- Tan pronto como se configure el NAT, las traducciones nacionales del IP de la demostración no muestran cualquier cosa. Haga ping una vez y después marque otra vez.
- Asga las **trazas del wireshark** en las interfaces interior y exterior del NAT-SBC

Escenarios

Muestran la salida de los debugs para un par de escenarios abajo. ¡Son sobre todo que se explica por sí mismo!

NAT básico

Las líneas de la configuración y del debug para el NAT básico se muestran abajo.

```
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

SORBO ALG

Las líneas de salida del **sorbo nacional del IP del debug** se muestran. En este caso, el IP Address incluido en un paquete de salida se traduce.

```
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

Descripción:

- 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

- DOC-5406
- http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-security/id-60290.html

Matriz de la función 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.shtml

Traversal recibido NAT:

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

SBC NAT

- 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