NAT em VoIP

Contents

Introduction

Este documento descreve o comportamento do NAT (Network Address Translation) em

roteadores que funcionam como CUBE (Cisco Unified Border Element), CME ou CUCME (Cisco Unified Cummunication Manager Express), Gateways e CUSP (Cisco Unified SIP Proxy).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SIP (Session Initiation Protocol, Protocolo de Iniciação de Sessão)
- Voz sobre IP (Internet Protocol)
- Protocolos de Roteamento

Componentes Utilizados

As informações neste documento são baseadas em

- Qualquer IOS versão 12.4T e superior.
- Qualquer versão do 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.

Informações de Apoio

A Tradução de Endereço de Rede é uma técnica comumente usada para traduzir endereços IP em pacotes que fluem entre redes usando diferentes espaços de endereço. A finalidade deste documento não é revisar o NAT. Em vez disso, este documento tem como objetivo fornecer uma revisão abrangente do NAT como ele é usado nas redes VoIP da Cisco. Além disso, o escopo é limitado aos componentes que compõem a tecnologia MS-Voice.

- O NAT basicamente substitui o endereço IP dentro dos pacotes por um endereço IP diferente
- Permite que vários hosts em uma sub-rede privada *compartilhem* (ou seja, pareçam) um único endereço IP público para acessar a Internet.
- Geralmente, as configurações de NAT alteram apenas o endereço IP dos hosts internos
- O NAT é bidirecional - Se A for convertido em B na interface interna, B chegando à interface externa será convertido em A!
- RFC1631

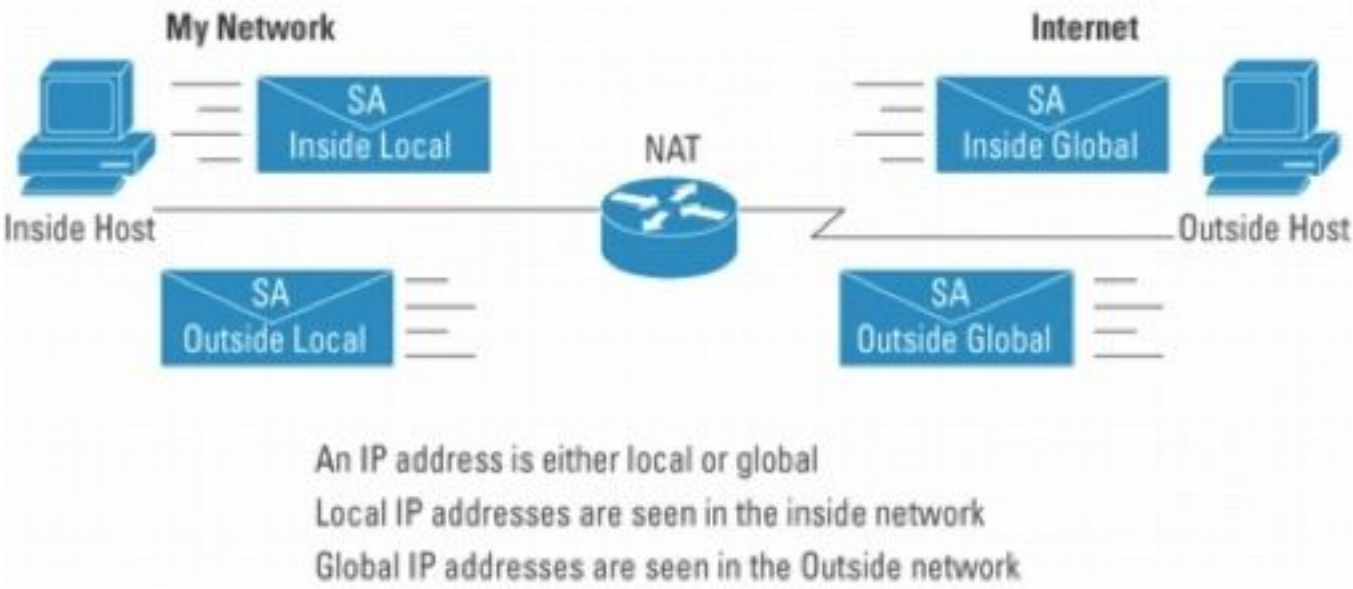


Figure 1

> **Observação**: pode ser útil pensar no NAT como um auxílio para rotear pacotes IP para dentro e fora das redes usando o espaço de endereço privado. Em outras palavras, o NAT torna os endereços não roteáveis roteáveis

A Figura 2 mostra a topologia referenciada nas ilustrações a seguir.

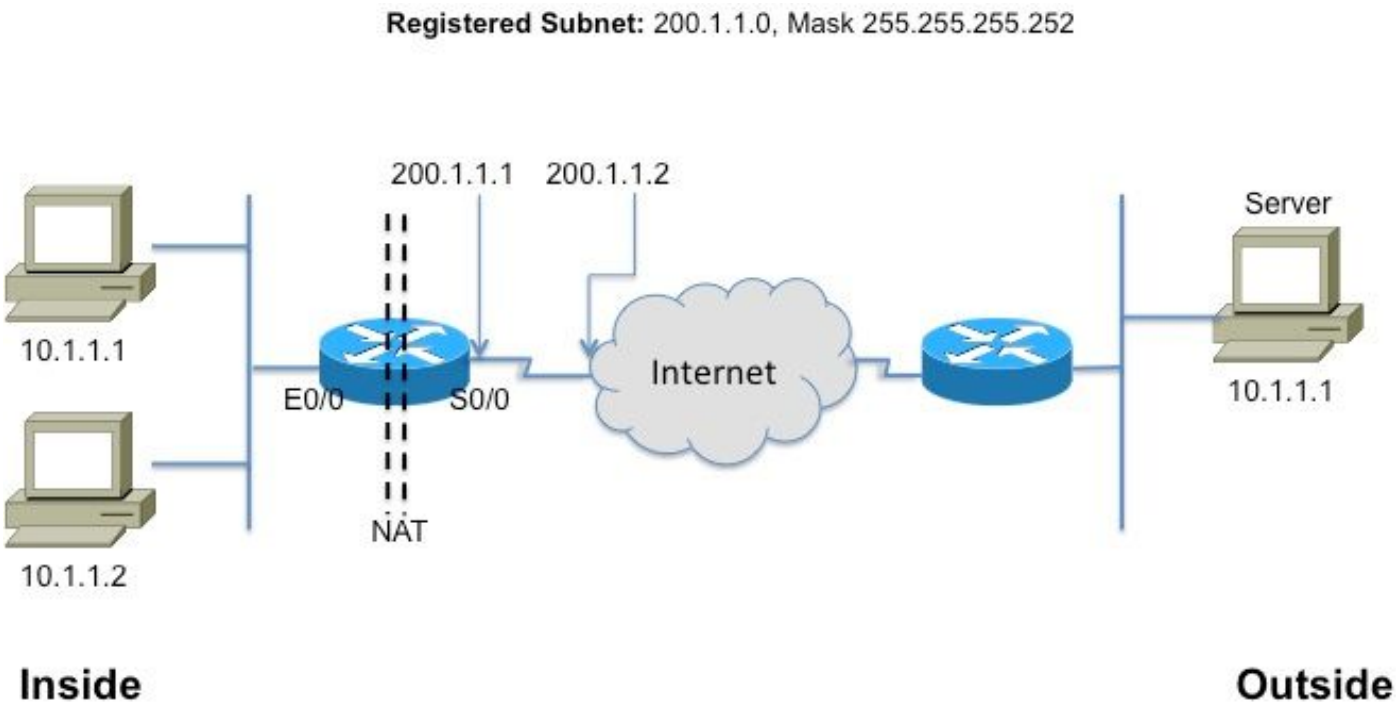


Figure 2

Este glossário é fundamental para entender e descrever o NAT

- **Endereço local interno** — O endereço IP atribuído a um host na *rede interna*. Normalmente, o endereço é de um espaço de endereço privado.
- **Endereço global interno** — Um endereço IP roteável atribuído pela placa de rede ou pelo provedor de serviços que representa um ou mais endereços IP locais internos para o mundo

externo.

- **Endereço local externo** — O endereço IP de um host externo como ele aparece para a rede interna. Não é necessariamente um endereço legítimo, ele é alocado a partir de um espaço para endereço roteável na parte interna.
- **Endereço global externo** — O endereço IP atribuído a um host na rede externa pelo proprietário do host. O endereço é alocado a partir de um endereço ou espaço de rede globalmente roteável.

Observação: fique à vontade com esses termos. Qualquer nota ou documento no NAT certamente fará referência a eles

NAT Estático

Essa é a forma mais simples de NAT, em que em cada endereço interno é convertido estaticamente em um endereço externo (e vice-versa).

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Figure 3

A CLI para configuração da conversão acima é a seguinte

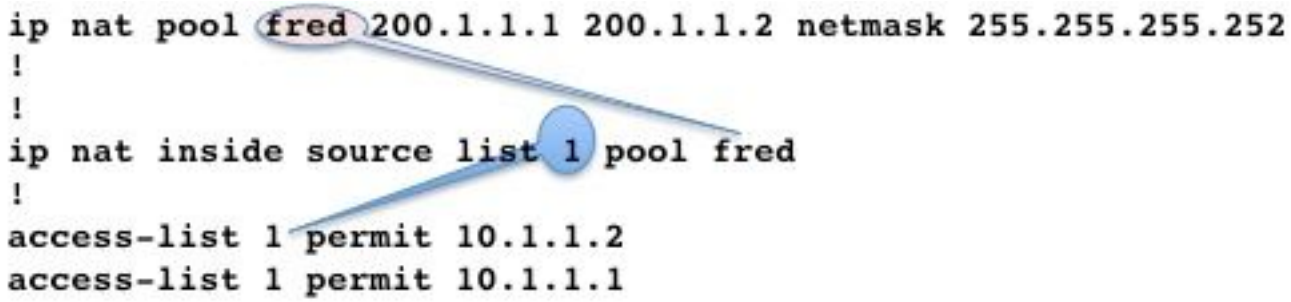
```
interface Ethernet0/0
 endereço ip 10.1.1.3 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 200.1.1.251 255.255.255.252
 ip nat outside <— Obrigatório![2]
ip nat inside source static 10.1.1.2 200.1.1.2
ip nat inside source static 10.1.1.1 200.1.1.1
```

NAT dinâmica

No NAT dinâmico, cada host interno é mapeado para um endereço de um pool de endereços.

- Aloca um endereço IP de um pool de endereços globais internos.
- Se um novo pacote chega de outro host interno e precisa de uma entrada NAT, mas todos os endereços IP agrupados estão em uso, o roteador simplesmente descarta o pacote.
- Essencialmente, o pool de endereços globais internos precisa ser tão grande quanto o número máximo de hosts simultâneos que precisam usar a Internet ao mesmo tempo

A CLI a seguir ilustra a configuração do NAT dinâmico



Sobrecarga de NAT (PAT)

Quando o pool (de endereços IP) é menor que o conjunto de endereços que precisam ser convertidos, esse recurso é útil.

- Vários endereços internos NATed para apenas um ou alguns endereços externos
- O PAT (Port Address Translation) usa números de porta de origem exclusivos no endereço **IP global interno** para distinguir as conversões. Como o número da porta é codificado em 16 bits, o número total poderia teoricamente ser tão alto quanto 65.536 por endereço IP. O PAT tentará preservar a porta de origem original, se essa porta de origem já estiver alocada. O PAT tentará localizar o primeiro número de porta disponível
- A sobrecarga de NAT pode usar mais de 65.000 portas, permitindo que ele escale bem sem precisar de muitos endereços IP registrados — em muitos casos, precisando apenas de um endereço IP global externo.

A Figura 4 ilustra o PAT.

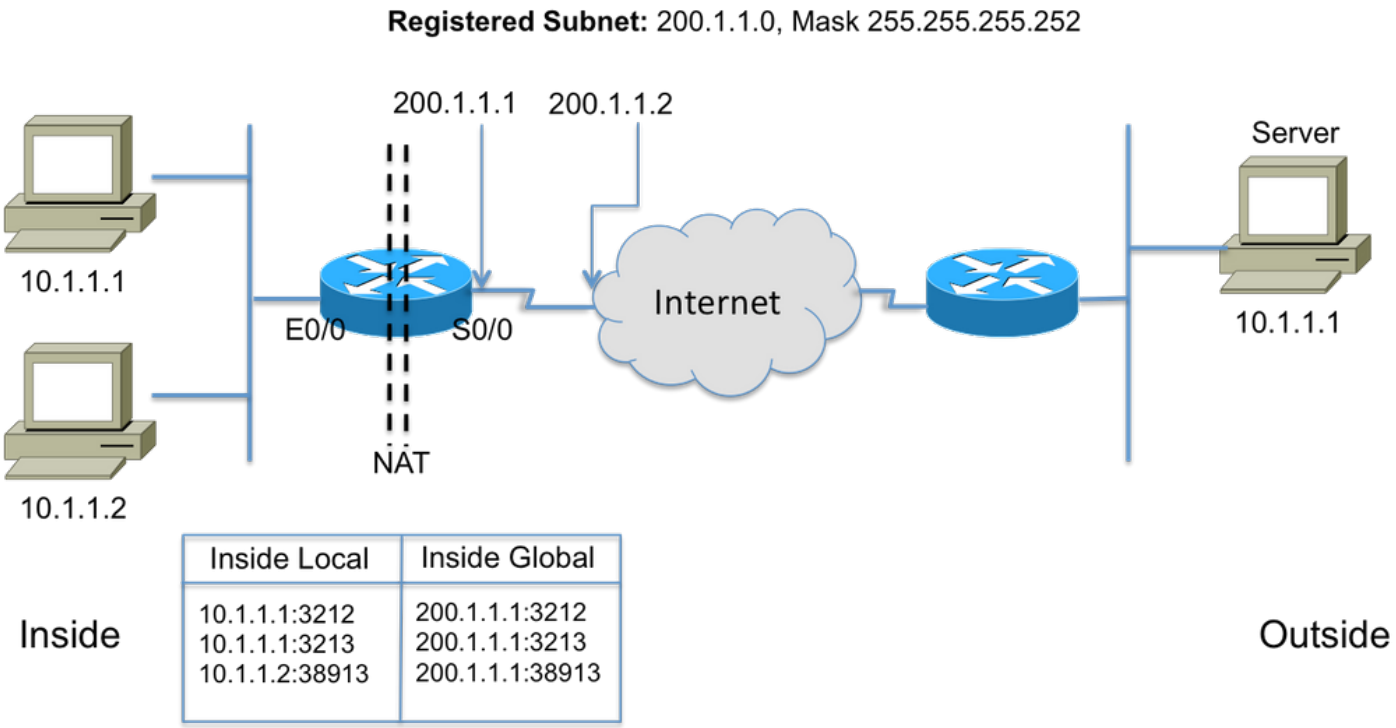


Figure 4

Opções do comando NAT

A implementação do NAT da Cisco é muito versátil com uma série de opções. Alguns estão listados abaixo, mas consulte http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html para obter detalhes sobre a lista completa de aprimoramentos.

- Traduções estáticas com portas - Pacotes de entrada endereçados a uma porta específica (por exemplo, porta 25, para servidor SMTP) enviada a um servidor específico.
- Suporte para mapas de rotas - Flexibilidade na configuração de filtros/ACLs
- Configurações de pool mais flexíveis- para permitir intervalos descontínuos de endereços.
- Preservação do número de host: converta a parte da "rede" e mantenha a parte do "host".

pinhole NAT

Um pinhole na linguagem NAT se refere ao mapeamento entre as tuplas <host IP, porta> e <endereço global, *porta* global>. Ele permite que o dispositivo NAT use o número da porta de destino (que seria a porta *global*) das mensagens recebidas para mapear o destino de volta para o IP do host e a porta que originou a sessão. É importante observar que os pinholes expiram após um período de não utilização e o endereço público é retornado ao pool de NAT.

NAT em VoIP

Então, quais são os problemas e preocupações com NAT em redes VoIP? Bem, lembre-se de que o NAT que discutimos até agora (também conhecido como NAT básico) apenas converte o endereço IP no *cabeçalho do* pacote IP e recalcula a soma de verificação, é claro, mas a

sinalização VoIP carrega endereços incorporados no *corpo* das mensagens de sinalização. Em outras palavras, na camada 5

A Figura 5 ilustra o efeito de deixar os endereços IP incorporados sem tradução. A sinalização da chamada é concluída com êxito, mas o proxy SIP no provedor de serviços falha ao tentar rotear pacotes de mídia (RTP) para o endereço de mídia enviado pelo agente de chamadas!

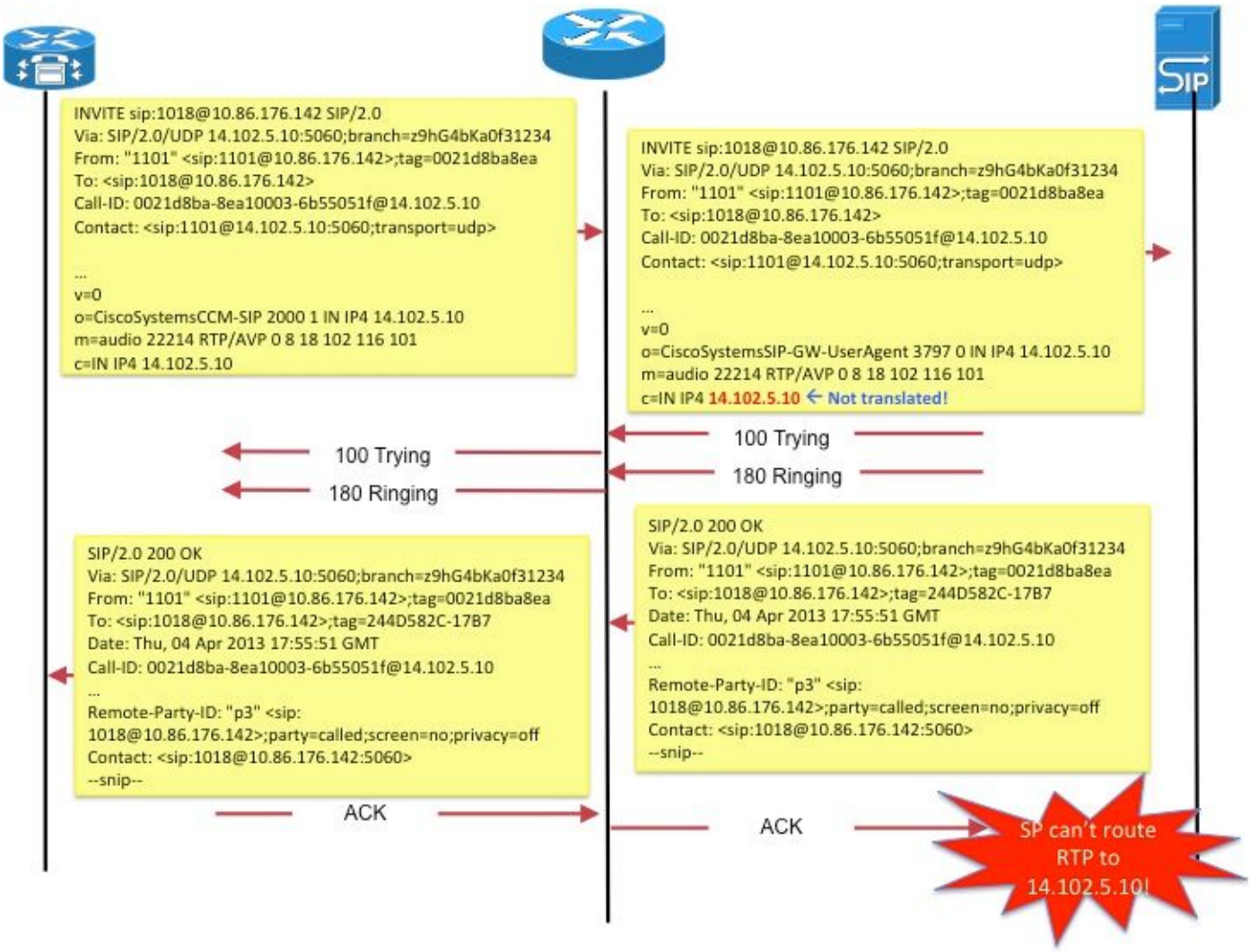


Figure 5

Outro exemplo seria o uso de ***Contato*** pelo endpoint SIP*:* no SDP para comunicar o endereço no qual o ponto final gostaria de receber mensagens de sinalização para novas solicitações.

Esses problemas são tratados por um recurso chamado Gateway de Camada de Aplicativo (ALG).

ALG

Um ALG entende o protocolo usado pelas aplicações específicas que suporta (por exemplo, SIP) e faz a inspeção de pacotes de protocolo e a "correção" de tráfego através dele. Para obter uma boa descrição de como os vários campos são fixos para sinalização de chamada SIP, consulte http://www.voip-info.org/wiki/view/Routers+SIP+ALG.

Nos roteadores Cisco, o suporte para ALG SIP é ativado, por padrão, na porta TCP 5060 padrão.

É possível configurar o ALG para suportar portas fora do padrão para sinalização SIP. Consulte http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.

> **Cuidado**: Cuidado! Não há RFC ou outro padrão que especifique quais campos incorporados devem ser convertidos para os vários protocolos VoIP. Como resultado, as implementações variam entre os fornecedores de equipamentos, resultando em problemas de interoperabilidade (e casos de TAC).

Gateways

Como os gateways, por definição, não são dispositivos ip para ip, o NAT não é aplicável.

CME

Esta seção do documento analisa os cenários de chamada com o CME para entender por que o NAT deve ser usado.

Cenário 1. Telefones locais

Cenário 2. Telefones remotos (com endereços IP públicos)

Cenário 3. Trabalhador remoto

> **Observação**: em todos os casos, para que o áudio flua, o endereço IP do CME precisa ser roteável

Local

Neste cenário (Figura 6), os dois telefones envolvidos na chamada são telefones finos com endereços IP privados.

Figura 6

> **Observação**: Lembre-se de que o telefone mirrado que está conectado em uma chamada com outro telefone mirrado no mesmo sistema CME envia seus pacotes de mídia diretamente para o outro telefone; ou seja, o RTP de telefone local para telefone local NÃO

flui pelo CME.

Portanto, o NAT não é aplicável ou necessário neste caso.

> **Observação**: o CME determina se a mídia (RTP) deve ou não se basear diretamente no fato de os dois telefones envolvidos em uma chamada serem skinny *e* **no mesmo segmento de rede.** Caso contrário, o CME se insere no caminho RTP.

Local para remoto

Neste cenário (Figura 7), o CME se insere no fluxo de RTP de forma que o RTP dos telefones será terminado no CME. O CME recriará os fluxos em direção ao outro telefone. Como o CME fica na rede interna (privada) e na rede externa e envia seu endereço interno para o telefone interno e o endereço externo (público) para o telefone externo, o NAT também não é necessário aqui.

Observe, no entanto, que as portas UDP/TCP (sinalização e RTP) devem ser abertas entre o telefone IP remoto e o endereço IP origem CME. Isso significa que os firewalls ou outros dispositivos de filtragem são configurados para permitir as portas em questão.

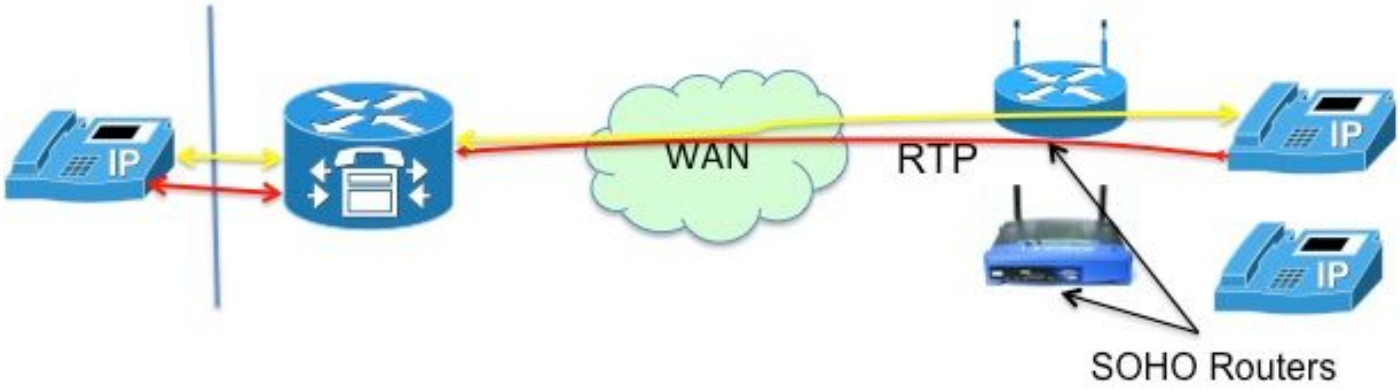


Figura 7

> **Observação**: Observe que a sinalização [mensagens] é sempre terminada no CM

Funcionário remoto

Isso se refere aos telefones IP que se conectam ao CME por uma WAN para oferecer suporte a funcionários remotos que tenham escritórios remotos a partir do roteador CME. Os projetos mais comuns são aqueles que envolvem telefones com endereços IP roteáveis e telefones com endereços IP privados.

Telefones remotos com acesso público (leia: roteáveis) endereços IP

Se ambos os telefones envolvidos na chamada estiverem configurados com endereços IP públicos e roteáveis, a mídia pode fluir entre os telefones diretamente (Figura 8). Portanto, mais uma vez, não há necessidade de NAT!

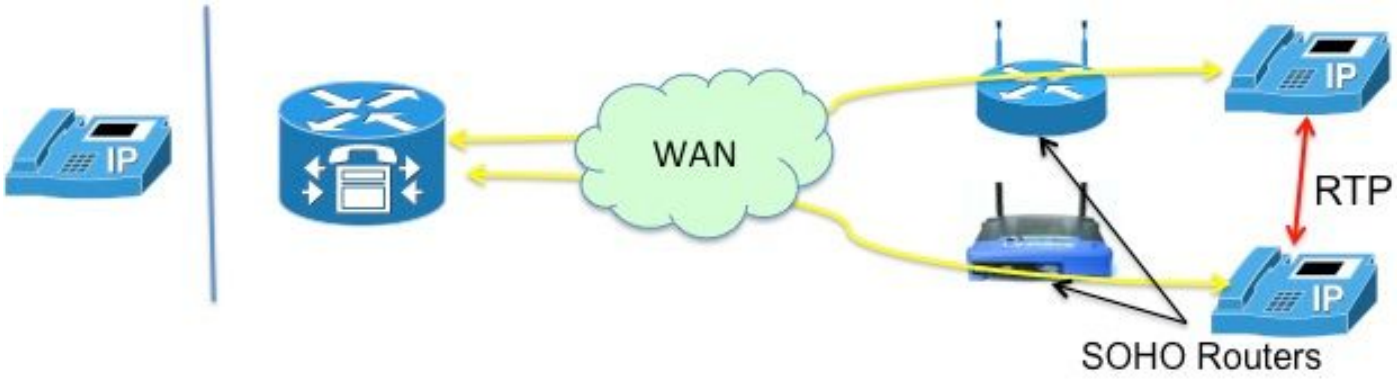


Figura 8

Telefones remotos com endereço IP privado

Neste cenário, a chamada é sinalizada entre telefones finos configurados com endereços IP privados. Os roteadores do escritório doméstico (SOHO), em geral, tendem a não ser "sensíveis ao SCCP". ou seja, incapaz de converter os endereços IP incorporados nas mensagens SCCP. Isso significa que, na conclusão da configuração da chamada, os telefones terminam com o endereço IP privado um do outro. Como ambos os telefones são privados, o CME sinalizará a chamada entre eles de forma que o áudio flua diretamente entre os telefones. No entanto, isso resultará em áudio unidirecional ou não (já que os endereços IP privados, por definição, não podem ser roteados na Internet!), a menos que uma das seguintes soluções seja implementada-

·Configurar rotas estáticas nos roteadores SOHO

·estabelecer uma conexão VPN IPsec com os telefones

Uma maneira melhor de resolver isso seria configurar "mtp". O comando mtp garante que os pacotes de mídia (RTP) de telefones remotos transitem pelo roteador CME (Figura 9).

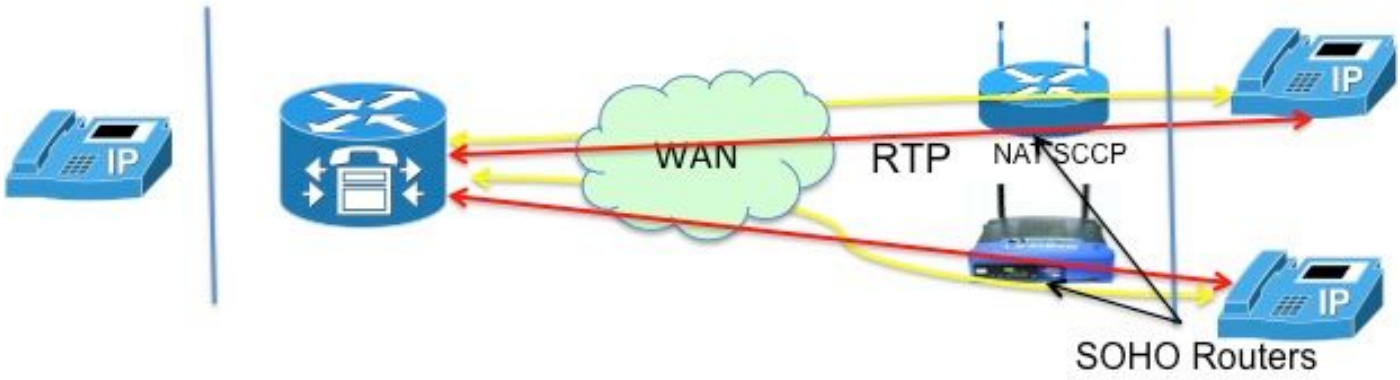


Figura 9

A solução "mtp" é melhor devido a complicações com a abertura de portas de firewall. Os pacotes de mídia que fluem por uma WAN podem ser obstruídos por um firewall. Isso significa que você precisa abrir portas no firewall, mas quais? Com o CME retransmitindo o áudio, os firewalls podem ser facilmente configurados para passar os pacotes RTP. O roteador CME usa uma porta UDP ***específica*** (2000!) para pacotes de mídia. Assim, permitindo apenas pacotes de e para a porta 2000, TODO o tráfego RTP pode ser passado.

A Figura 10 ilustra como configurar o mtp.

```
ephone 1
  mac 1111.2222.3333
  tipo 7965
  mtp
  botão 1:1
```

Figura 10

Nem tudo é maravilhoso com o MTP. Há situações em que o mtp pode não ser desejável

- O MTP não é suave na utilização da CPU
- O MOH multicast geralmente não pode ser encaminhado através de uma WAN- O recurso MOH multicast verifica se o MTP está ativado para um telefone e, se estiver, não envia o MOH para esse phoneL.

Assim, se você tiver uma configuração de WAN que possa encaminhar pacotes multicast e puder permitir pacotes RTP através do firewall, poderá decidir não usar o MTP.

Telefones SIP remotos

Observe que os telefones SIP não foram mencionados nos cenários acima. Isso ocorre porque, se um dos telefones for um telefone SIP, o CME se insere no caminho de áudio. Este se torna o cenário local para remoto descrito anteriormente, no qual o NAT não é necessário.

CUBO

O CUBE executa inerentemente as funções NAT e PAT à medida que termina e origina novamente todas as sessões. O CUBE substitui seu próprio endereço pelo endereço de qualquer endpoint com o qual se comunica, ocultando (convertendo) efetivamente o endereço desse endpoint.

Portanto, o NAT não é necessário com a função CUBE. Há um cenário de serviço de VoIP no qual o NAT é necessário no CUBE, conforme descrito na próxima seção.

NAT transversal hospedado

Um breve histórico sobre o serviço de telefonia hospedada ajudará a entender os fundamentos para esse recurso.

O serviço de telefonia hospedada é uma nova forma de serviço VoIP em que a maioria dos equipamentos reside no local do provedor de serviços. Eles trabalham com os gateways residenciais (HGW), que implementam apenas o NAT básico (ou seja, o NAT em L3/L4). Por exemplo, a Verizon instala o Optical Network Terminal (ONT), que fornece serviços FiOS em casa; a chamada de voz é sinalizada por meio de um processo SIP integrado ao ONT. A sinalização SIP é feita através da rede IP privada da Verizon para novos switches de software, que fornecem o serviço e o controle para estabelecer comunicações de voz para outros clientes de voz digital do FiOS ou para clientes de telefone tradicionais.

Entre os principais requisitos do provedor de serviços de telefonia hospedada estão:

- NAT transversal remoto: a capacidade de fornecer serviços de classe 5 a endpoints que utilizam NAT (que só pode fazer NAT camada 3!) e dispositivos de firewall (fazendo "ALG" remotamente!)
- Suporte a multimídia: a capacidade de enviar mídia entre dispositivos co-localizados onde não faz sentido rotear a mídia de volta para a rede IP
- Nenhum equipamento adicionado, eliminando a necessidade de adicionar qualquer CPE.

Tendo em conta o que precede, que opções existem para implementar tal serviço?

- Substituir o HGW por um ALG caro,
- Use um controlador de borda de sessão (SBC) para modificar os cabeçalhos SIP incorporados para pacotes. Isso envolve um produto hospedado na rede, de classe de operadora, que suporta SIP em uma configuração muito segura e tolerante a falhas. Essa solução é chamada de NAT SBC.

A opção NAT SBC atende aos requisitos do provedor listados acima.

NAT SBC

O SBC do NAT funciona da seguinte maneira (Figura 11)

1. O roteador de acesso converte apenas o endereço IP de L3/L4
2. Endereço IP na mensagem SIP não convertido
3. O NAT SBC intercepta e converte o endereço IP incorporado. No momento em que o SBC vê pacotes SIP destinados a **200.200.200.10**, ele inicia o código nat-sbc.
4. A mídia não é traduzida e vai diretamente entre os telefones[5]

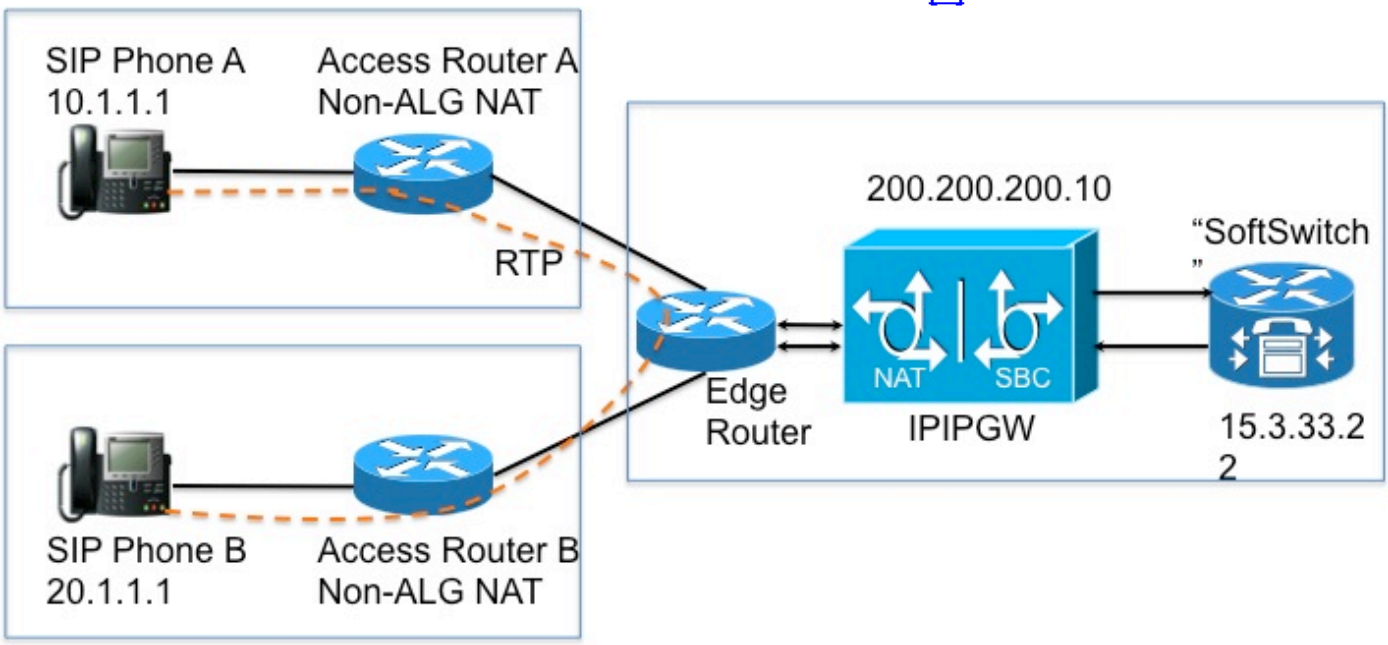


Figura 11

Notas do projeto

- O endereço IP **200.200.200.10** (Figura 12) não está atribuído a nenhuma interface no NAT

SBC. Ele é configurado como o endereço do "proxy" para o qual o Telefone SIP A e o Telefone SIP B enviam mensagens de sinalização.
- Os dispositivos domésticos não traduzem determinados campos *somente de endereço* SIP/SDP (por exemplo, ID de chamada: ,O= , Aviso: cabeçalhos & branch= parâmetro. os parâmetros maddr= e received= foram tratados somente em determinados cenários.). Esses campos são manipulados pelo SBC do NAT, exceto para a autorização de proxy e a tradução de autorização, porque eles interromperão a autenticação.
- Se os dispositivos domésticos estiverem configurados para fazer PAT, os agentes do usuário (telefones e proxy) devem suportar sinalização simétrica[6] e mídia simétrica e inicial. Você deve configurar a porta de substituição no roteador NAT SBC.
- Na ausência de suporte para sinalização simétrica e mídia simétrica e inicial, os roteadores intermediários devem ser configurados sem PAT e o endereço de substituição deve ser configurado no NAT SBC.

Configuração

Segue um exemplo de configuração para um NAT SBC típico.

```
ip nat sip-sbc

  proxy 200.200.200.10 5060 protocolo udp 15.3.33.22 5060

  call-id-pool call-id-pool

  session-timeout 300

  mode allow-flow-around

  porta de substituição

!

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 máscara de rede 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
```

Fluxo de chamada com SBC NAT

As Figuras 13 e 14 ilustram o fluxo de chamadas em termos de conversões. Os seguintes pontos devem ser observados-

- Após o registro, o soft switch anota os dois telefones como
  — Telefone SIP A - 15.3.33.62 2001

  — Telefone SIP B - 15.3.33.62 2002

- Nesse fluxo de chamadas, o NAT do SBC efetivamente deixa o endereço IP da mídia sem tradução.

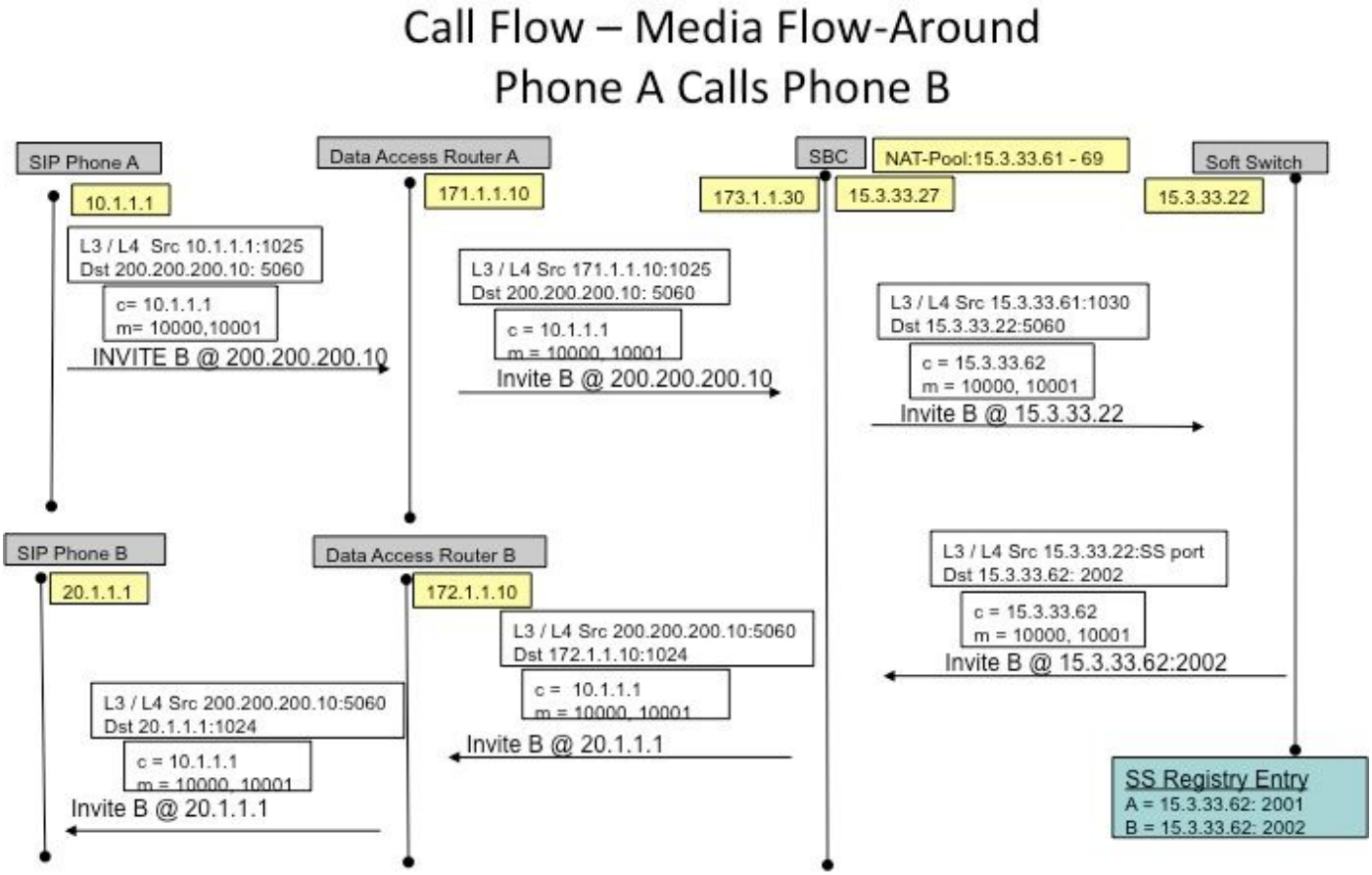


Figura 13

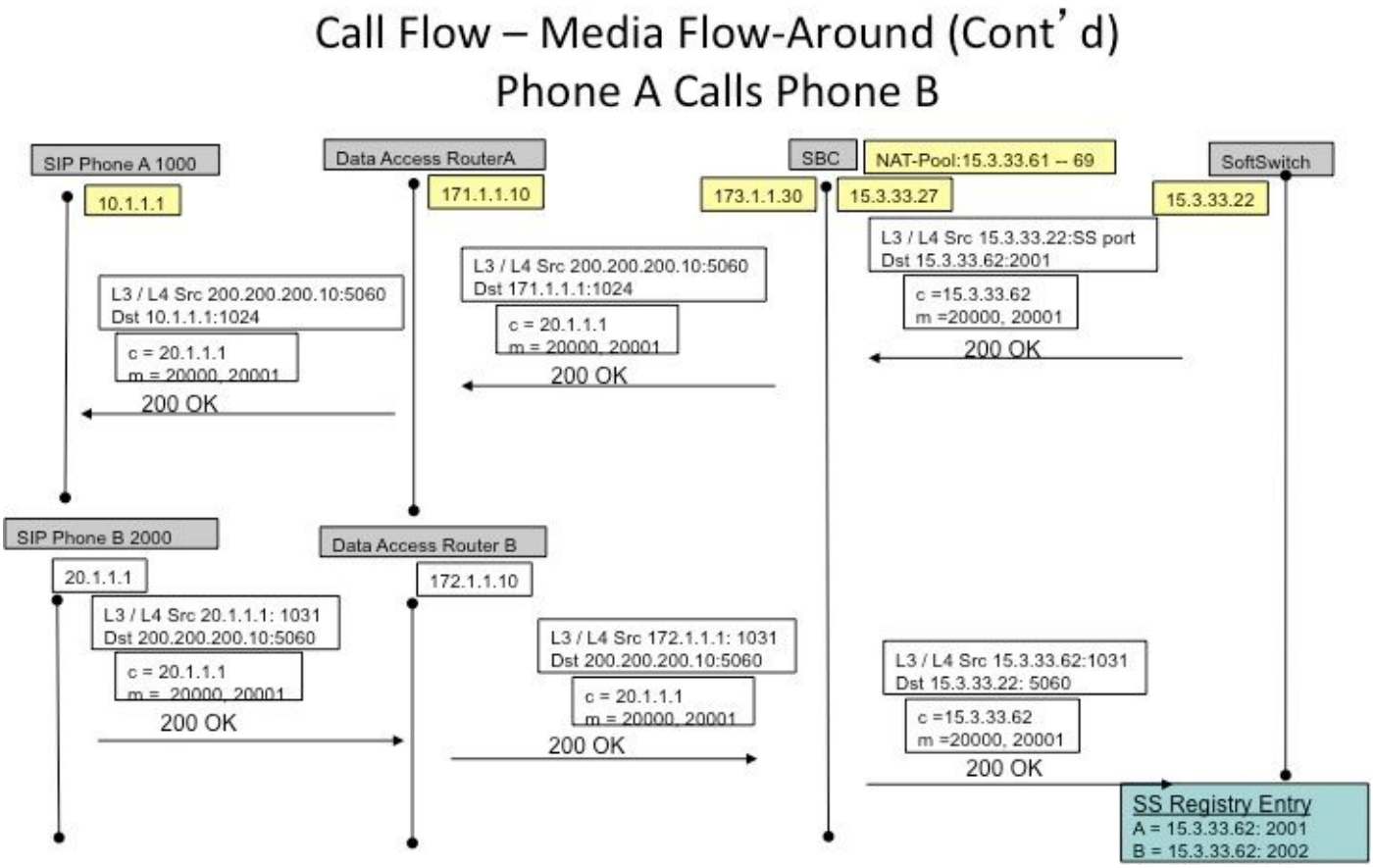


Figura 14

Registro SIP

Em versões anteriores (do NAT SBC), os pontos de extremidade SIP tinham que enviar pacotes *keep-alive* para manter o pinhole de Registro SIP aberto (para permitir que o tráfego out->in flua, por exemplo, chamadas de entrada). Os pacotes *keep-alive* poderiam ser qualquer pacote SIP enviado pelo ponto de extremidade ou pelo registrador (comutador soft). Versões recentes evitam a necessidade disso, com o próprio NAT-SBC (em oposição aos comutadores por software) forçando os endpoints a se registrarem novamente com frequência para manter os pinholes abertos.

> **Note**: Os sintomas de um pinhole de registro expirado podem ser obscuros, com falhas aleatórias de sinalização de chamada.

CUSP

O CUSP tem a noção de uma rede lógica, que se refere a um conjunto de interfaces locais que são tratadas de forma semelhante para (por exemplo, interface, porta, transporte para escuta). Ao configurar uma rede lógica no CUSP, você pode configurá-la para usar NAT. Uma vez configurado, o SIP ALG é automaticamente habilitado. Isso é útil quando determinadas redes lógicas.

Troubleshooting

Sintomas

Um sintoma óbvio pode ser uma chamada falhar em uma ou ambas as direções. Os sintomas menos óbvios podem incluir,

- Áudio de sentido único
- Transferência de áudio unidirecional
- Áudio sem sentido
- Perdendo o registro SIP

Comandos show e debug

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

Itens a serem verificados

- Certifique-se de que a configuração inclua o subcomando de interface **ip nat inside** ou **ip nat outside** . Esses comandos ativam o NAT nas interfaces, e a designação interna/externa é importante.
- Para o NAT estático, certifique-se de que o comando **ip nat source static** liste o endereço local interno primeiro e o endereço IP global interno depois.
- Para o NAT dinâmico, assegure-se de que a ACL configurada para corresponder aos pacotes enviados pelo host interno corresponda aos pacotes desse host, antes de qualquer conversão de NAT ter ocorrido. Por exemplo, se um endereço local interno de 10.1.1.1 deve ser convertido em 200.1.1.1, certifique-se de que a ACL corresponda ao endereço origem 10.1.1.1, não 200.1.1.1.
- Para NAT dinâmico sem PAT, certifique-se de que o pool tenha endereços IP suficientes. Os sintomas de não ter endereços suficientes incluem um valor crescente no segundo contador de erros na saída do comando **show ip nat statistics**, bem como ver todos os endereços no intervalo definido no pool de NAT na lista de conversões dinâmicas.
- Para o PAT, é fácil esquecer de adicionar a opção **overload** no comando **ip nat inside source list**. Sem ele, o NAT funciona, mas o PAT não, geralmente resultando na não conversão dos pacotes dos usuários e na impossibilidade de os hosts chegarem à Internet.
- Talvez o NAT tenha sido configurado corretamente, mas existe uma ACL em uma das interfaces, descartando os pacotes. Observe que o IOS processa ACLs antes do NAT para pacotes que entram em uma interface e depois de converter os endereços para pacotes que saem de uma interface.
- Não se esqueça de configurar "ip nat outside" na interface que faz a interface com a WAN (mesmo que não traduza o endereço externo)!
- Assim que o NAT é configurado, show ip nat translations não mostra nada. Faça ping uma vez e verifique novamente.
- Capture **rastreamentos do Wireshark** em interfaces internas e externas do NAT-SBC

Cenários

A saída de depuração para alguns cenários é mostrada abaixo. São quase sempre

autoexplicativos!

NAT básico

As linhas de configuração e depuração do NAT básico são mostradas abaixo.

```
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

ALG SIP

As linhas de saída de **debug ip nat sip** são mostradas. Nesse caso, o endereço IP incorporado em um pacote de saída é convertido.

```
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:
```

Referências

Overview:

- http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9html
- 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

Matriz de recursos 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_paper09186a00801af2b9html
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919.sht

ml

NAT transversal hospedado:

- 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.