NAT in VoIP

Inhalt

Einleitung

Dieses Dokument beschreibt das NAT-Verhalten (Network Address Translation) bei Routern, die

als CUBE (Cisco Unified Border Element), CME oder CUCME (Cisco Unified Communication Manager Express), Gateways und CUSP (Cisco Unified SIP Proxy) arbeiten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SIP (Session Initiation Protocol)
- Voice over IP (Internetprotokoll)
- Routing-Protokolle

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf

- Alle IOS-Versionen 12.4T und höher.
- Beliebige CME-Version

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Network Address Translation ist eine häufig verwendete Technik zum Übersetzen von IP-Adressen in Paketen, die über unterschiedliche Adressräume zwischen Netzwerken übertragen werden. NAT soll in diesem Dokument nicht behandelt werden. Vielmehr soll das Dokument eine umfassende Überprüfung der NAT ermöglichen, wie sie in Cisco VoIP-Netzwerken verwendet wird. Außerdem ist der Umfang auf Komponenten beschränkt, aus denen die MS-Voice-Technologie besteht.

- NAT ersetzt im Wesentlichen die IP-Adresse in Paketen durch eine andere IP-Adresse
- Ermöglicht mehreren Hosts in einem privaten Subnetz, auf das Internet zuzugreifen und eine einzelne öffentliche IP-Adresse *gemeinsam* zu nutzen (d. h. so zu erscheinen).
- In der Regel ändern NAT-Konfigurationen nur die IP-Adresse interner Hosts.
- NAT ist bidirektional: Wenn A auf der internen Schnittstelle in B übersetzt wird, wird B, das an der externen Schnittstelle eingeht, in A übersetzt!
- RFC 1631

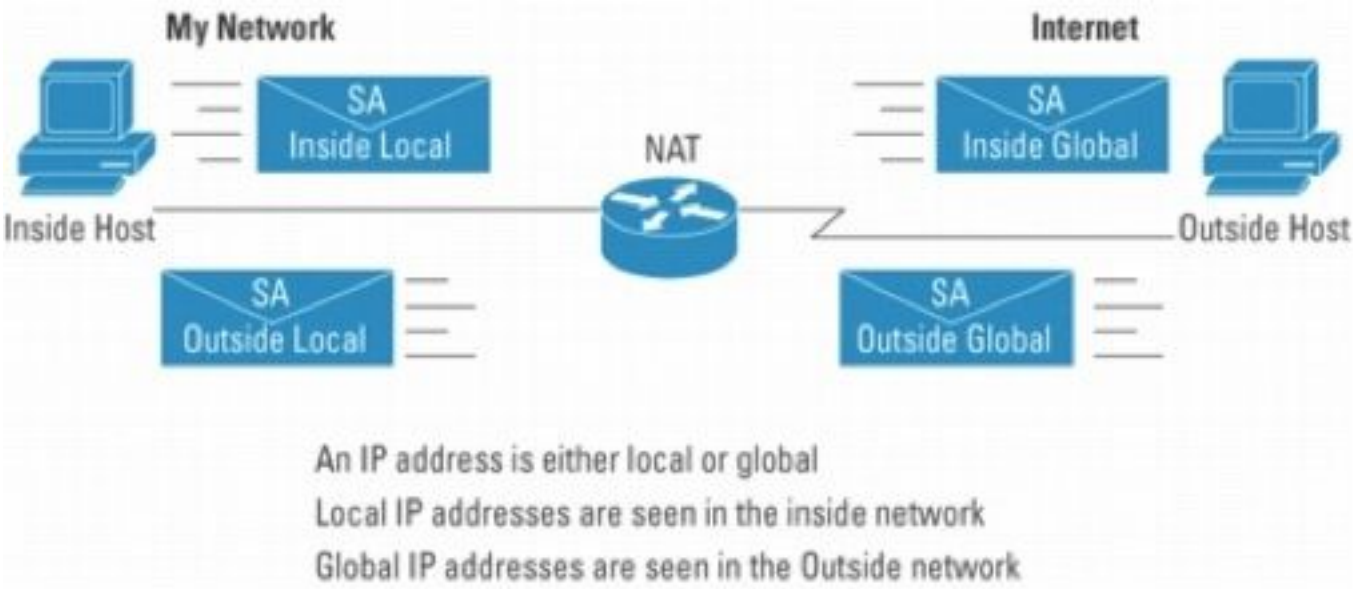

Abbildung 1

> **Hinweis**: NAT kann dabei helfen, IP-Pakete mithilfe von privatem Adressraum zum Netzwerk hin- und herzuleiten. Mit anderen Worten: NAT macht nicht routbare Adressen routbar

Abbildung 2 zeigt die Topologie, auf die in den folgenden Abbildungen verwiesen wird.

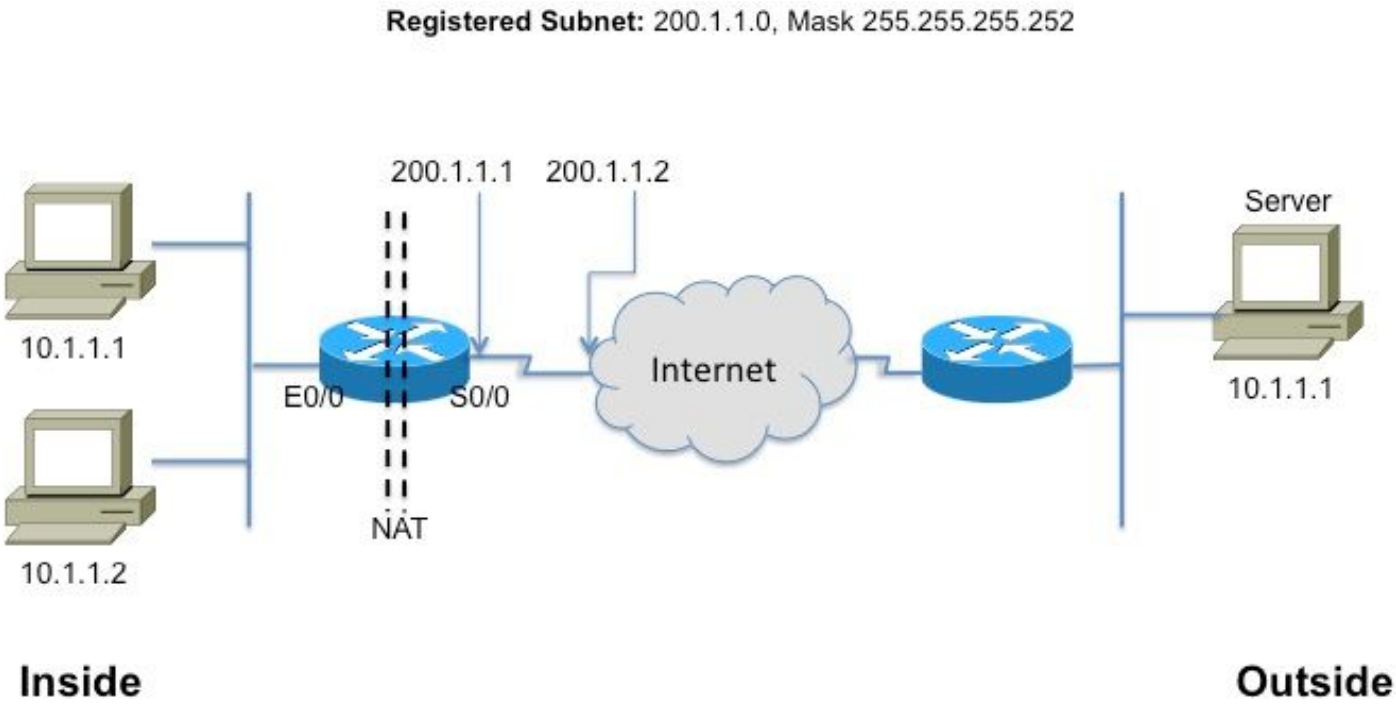

Abbildung 2

Dieses Glossar ist grundlegend für das Verständnis und die Beschreibung von NAT.

- **Interne lokale Adresse** - Die IP-Adresse, die einem Host im *internen* Netzwerk zugewiesen ist. Normalerweise stammt die Adresse aus einem privaten Adressbereich.
- **Interne globale Adresse** - Eine routbare IP-Adresse, die von der Netzwerkkarte oder dem Service Provider zugewiesen wird und eine oder mehrere interne lokale IP-Adressen nach außen repräsentiert.

- **Outside local address (Externe lokale Adresse)**: Die IP-Adresse eines externen Hosts, wie sie dem internen Netzwerk angezeigt wird. Sie ist nicht unbedingt eine legitime Adresse, sondern wird aus einem innenroutbaren Adressraum zugewiesen.
- **Externe globale Adresse** - Die IP-Adresse, die einem Host im externen Netzwerk vom Host-Besitzer zugewiesen wird. Die Adresse wird aus einer global routbaren Adresse oder einem Netzwerkbereich zugewiesen.

  Hinweis: Machen Sie sich mit diesen Bedingungen vertraut. Jede Anmerkung oder jedes Dokument zu NAT bezieht sich auf sie

Statisches NAT

Dies ist die einfachste Form der NAT, bei der jede interne Adresse statisch in eine externe Adresse übersetzt wird (und umgekehrt).

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Abbildung 3

Die CLI für die obige Übersetzung muss wie folgt konfiguriert werden:

Schnittstelle Ethernet0/0

ip address 10.1.1.1.3 255.255.255.0

ip nat innen

!

interface Serial0/0

ip address 200.1.1.1.251 255.255.255.252

ip nat outside <— Erforderlich![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

Dynamisches NAT

Bei der dynamischen NAT wird jeder interne Host einer Adresse aus einem Adresspool zugeordnet.

- Weist eine IP-Adresse aus einem Pool interner globaler Adressen zu.

- Wenn ein neues Paket von einem anderen internen Host eingeht und einen NAT-Eintrag benötigt, aber alle gepoolten IP-Adressen verwendet werden, verwirft der Router das Paket einfach.
- Der Pool interner globaler Adressen muss so groß sein wie die maximale Anzahl gleichzeitiger Hosts, die das Internet gleichzeitig nutzen müssen.

Die folgende CLI veranschaulicht die Konfiguration der dynamischen NAT.

```
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
```

NAT-Überlastung (PAT)

Wenn der Pool (mit IP-Adressen) kleiner ist als der Satz von Adressen, die übersetzt werden müssen, ist diese Funktion praktisch.

- Mehrere interne Adressen, die nur einer oder mehreren externen Adressen zugeordnet sind
- PAT (Port Address Translation) verwendet eindeutige Quellportnummern der **globalen** Inside IP-Adresse, um zwischen Übersetzungen zu unterscheiden. Da die Portnummer in 16 Bit codiert ist, kann die Gesamtzahl theoretisch bis zu 65.536 pro IP-Adresse betragen. PAT versucht, den ursprünglichen Quell-Port beizubehalten, wenn dieser Quell-Port bereits zugewiesen ist. PAT versucht, die erste verfügbare Port-Nummer zu finden.
- NAT-Überlastung kann mehr als 65.000 Ports verwenden und lässt sich somit gut skalieren, ohne viele registrierte IP-Adressen zu benötigen. In vielen Fällen ist nur eine externe globale IP-Adresse erforderlich.

Abbildung 4 zeigt die PAT.

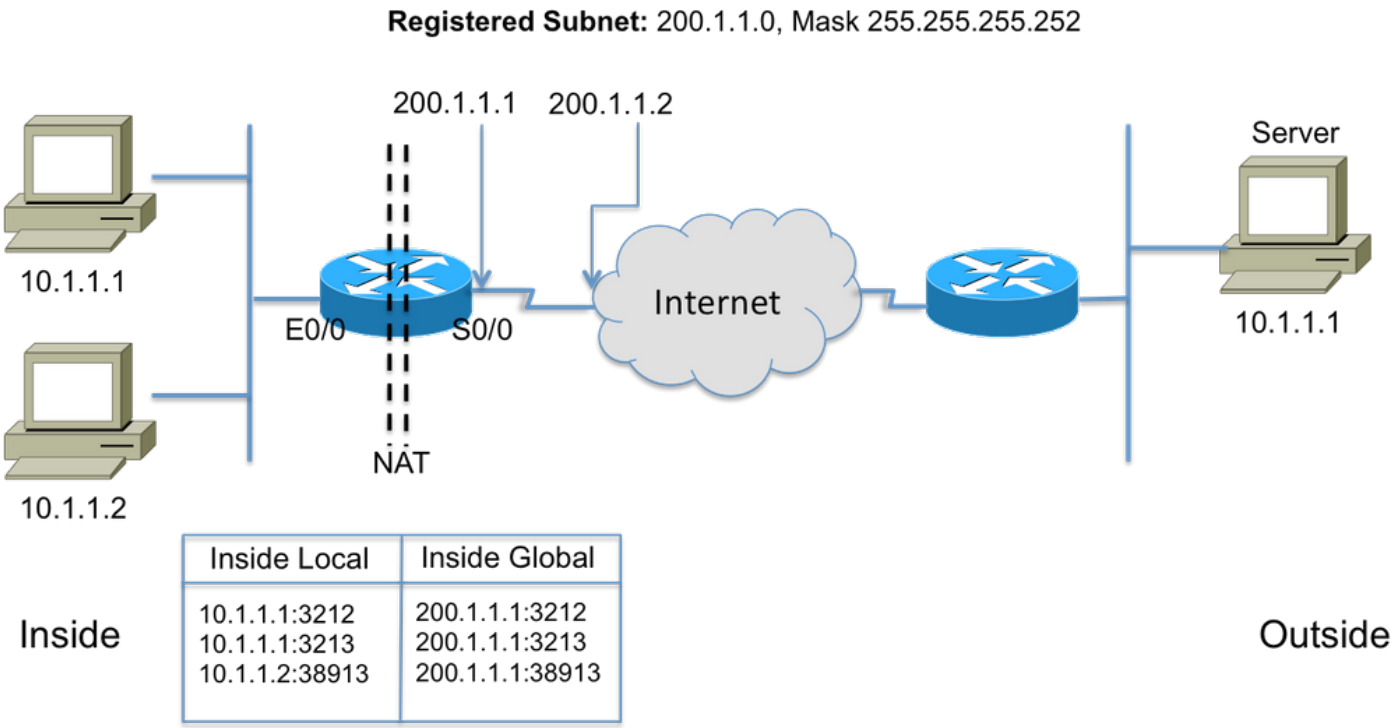

Abbildung 4

NAT-Befehlsoptionen

Die Cisco NAT-Implementierung ist sehr vielseitig und bietet eine Vielzahl von Optionen. Einige der nachfolgend aufgeführten Funktionen sind verfügbar. Eine vollständige Liste der Verbesserungen finden Sie unter http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html.

- Statische Übersetzungen mit Ports - eingehende Pakete, die an einen bestimmten Port adressiert sind (z. Port 25 für SMTP-Server) an einen bestimmten Server gesendet.
- Unterstützung für Routenzuordnungen - Flexible Konfiguration von Filtern/ACLs
- Flexiblere Pool-Konfigurationen zur Ermöglichung diskontinuierlicher Adressbereiche
- Erhalt der Hostnummer - Übersetzen Sie den Teil "Netzwerk", und behalten Sie den Teil "Host" bei.

NAT-Pinhole

Ein Nadelloch in der NAT-Sprache bezieht sich auf die Zuordnung zwischen den <Host-IP, Port> und <globale Adresse, *globaler* Port>-Tupeln. Es ermöglicht dem NAT-Gerät, die Zielportnummer (d. h. den *globalen* Port) eingehender Nachrichten zu verwenden, um das Ziel wieder der Host-IP und dem Port zuzuordnen, von dem die Sitzung gestartet wurde. Beachten Sie, dass die Zeitüberschreitung bei den Pinholes nach einer bestimmten Zeit der Nichtbenutzung auftritt und die öffentliche Adresse an den NAT-Pool zurückgegeben wird.

NAT in VoIP

Worin bestehen also die Probleme und Bedenken bezüglich NAT in VoIP-Netzwerken? Nun, erinnern Sie sich, dass NAT, die wir bisher besprochen haben (lose bezeichnet als grundlegende NAT) nur übersetzt die IP-Adresse im IP-Paket-*Header* und berechnet die Prüfsumme, natürlich, aber VoIP-Signalisierung tragen Adressen in den *Körper* der Signalisierungsnachrichten eingebettet. Mit anderen Worten, auf Layer 5

Abbildung 5 veranschaulicht die Auswirkungen, die auftreten, wenn die eingebetteten IP-Adressen nicht übersetzt werden. Die Anrufsignalisierung wurde erfolgreich abgeschlossen, aber der SIP-Proxy des Service Providers versucht nicht, Medienpakete (RTP) an die vom Anruf-Agenten gesendete Medienadresse weiterzuleiten.

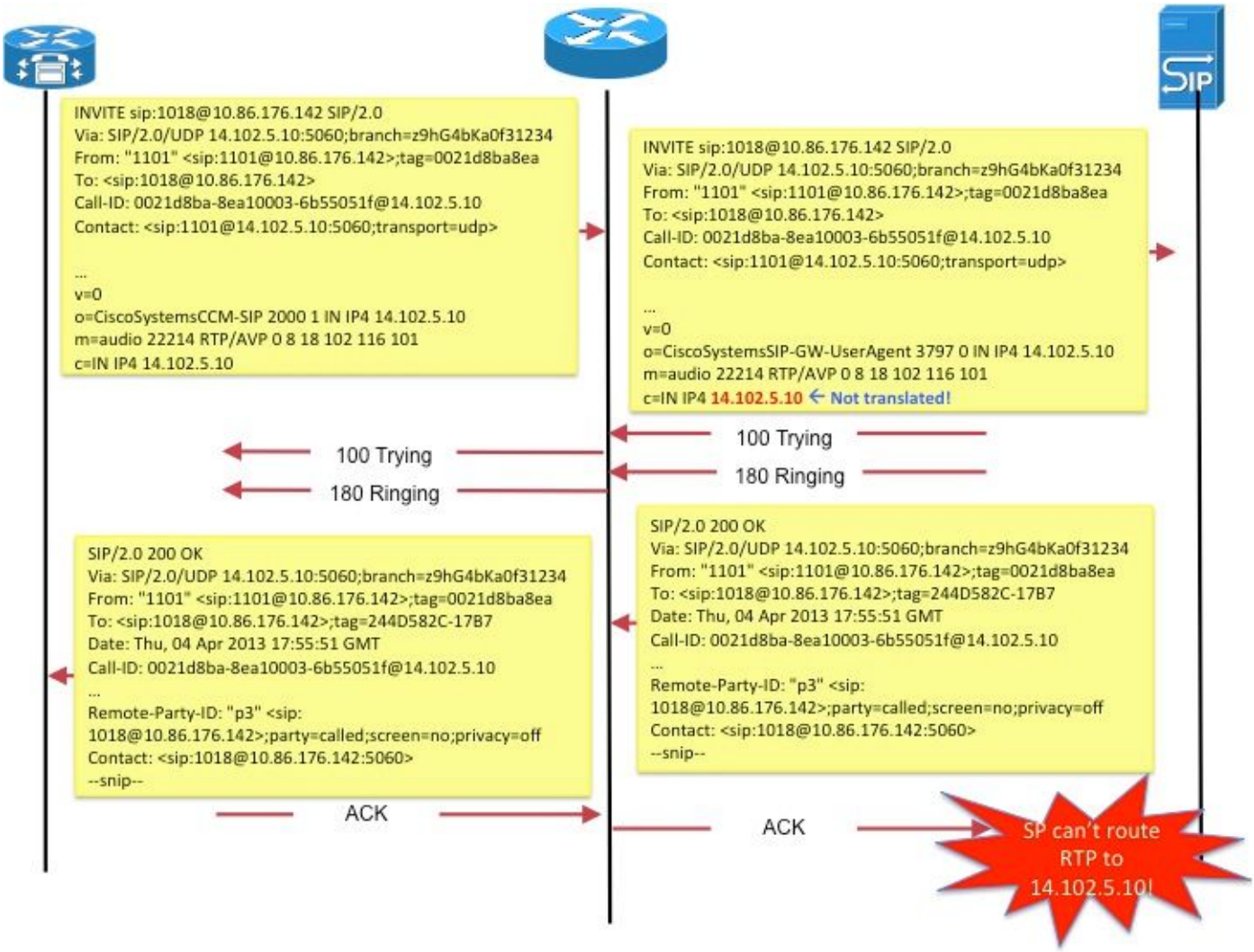

Abbildung 5

Ein weiteres Beispiel wäre die Verwendung des ***Kontakts*** durch das SIP-Endgerät***:*** -Feld in SDP ein, um die Adresse mitzuteilen, an der der Endpunkt Signalisierungsnachrichten für neue Anforderungen empfangen möchte.

Diese Probleme werden durch die Funktion Application Layer Gateway (ALG) behoben.

ALG

Ein ALG versteht das Protokoll, das von den spezifischen Anwendungen verwendet wird, die es unterstützt (z. B. SIP), und führt eine Protokollpaketprüfung und die Korrektur des Datenverkehrs

durch dieses Protokoll durch. Eine gute Beschreibung der verschiedenen Felder für die SIP-Anrufsignalisierung finden Sie unter http://www.voip-info.org/wiki/view/Routers+SIP+ALG.

Auf Cisco Routern ist die Unterstützung für ALG SIP auf dem standardmäßigen TCP-Port 5060 standardmäßig aktiviert. Es ist möglich, das ALG so zu konfigurieren, dass nicht standardmäßige Ports für die SIP-Signalisierung unterstützt werden. Weitere Informationen finden Sie unter http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html.

> **Achtung**: Vorsicht! Es gibt weder RFC noch einen anderen Standard, der genau festlegt, welche eingebetteten Felder für die verschiedenen VoIP-Protokolle übersetzt werden sollen. Daher unterscheiden sich die Implementierungen je nach Gerätehersteller, was zu Interoperabilitätsproblemen (und TAC-Fällen) führt.

Gateways

Da Gateways definitionsgemäß keine IP-to-IP-Geräte sind, kann NAT nicht angewendet werden.

CME

In diesem Abschnitt des Dokuments werden Anrufszenarien mit CME erörtert, um zu verstehen, warum NAT verwendet werden muss.

Szenario 1. Lokale Telefone

Szenario 2. Remote-Telefone (mit öffentlichen IP-Adressen)

Szenario 3. Telearbeiter

> **Hinweis**: In allen Fällen muss die CME-IP-Adresse routingfähig sein, damit Audio übertragen werden kann.

Lokal

In diesem Szenario (Abbildung 6) handelt es sich bei den beiden am Anruf beteiligten Telefonen um Skinny-Telefone mit privaten IP-Adressen.

Abbildung 6

Hinweis: Denken Sie daran, dass das Skinny-Telefon, das in einem Gespräch mit einem anderen Skinny-Telefon im gleichen CME-System verbunden ist, seine Medienpakete direkt an das andere Telefon sendet. d. h. RTP für "local-phone" zu "local-phone" läuft NICHT über CME.

NAT ist daher in diesem Fall nicht anwendbar oder erforderlich.

Hinweis: CME legt fest, ob Medien (RTP) direkt oder indirekt genutzt werden sollen. Dies hängt davon ab, ob die beiden an einem Anruf beteiligten Telefone dünn sind *und* sich im gleichen Netzwerksegment befinden. Andernfalls fügt CME sich selbst in den RTP-Pfad ein.

Lokal zu Remote

In diesem Szenario (Abbildung 7) fügt CME sich selbst in den RTP-Stream ein, sodass RTP von den Telefonen auf dem CME terminiert wird. CME leitet die Streams zum anderen Telefon zurück. Da CME sowohl im internen (privaten) Netzwerk als auch im externen Netzwerk sitzt und seine interne Adresse an das interne Telefon und seine externe (öffentliche) Adresse an das externe Telefon sendet, ist auch hier keine NAT erforderlich.

Beachten Sie jedoch, dass die UDP-/TCP-Ports (Signalisierung sowie RTP) zwischen dem Remote-IP-Telefon und der CME-Quell-IP-Adresse offen sein müssen. Dies bedeutet, dass die Firewalls oder andere Filtergeräte so konfiguriert sind, dass sie die betreffenden Ports zulassen.

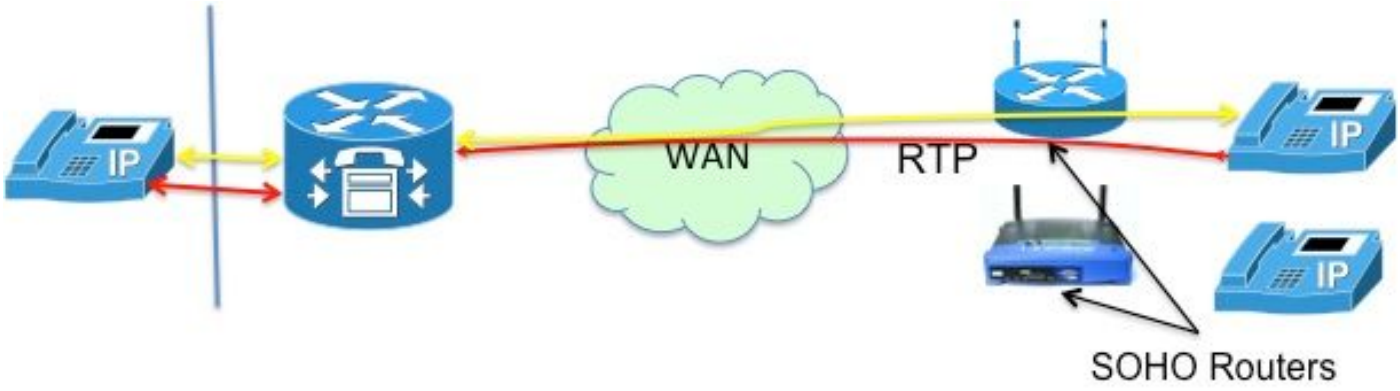

Abbildung 7

Hinweis: Beachten Sie, dass die Signalisierung [Nachrichten] am CM immer beendet wird.

Telearbeiter

Dies bezieht sich auf IP-Telefone, die über ein WAN mit CME verbunden sind, um Telearbeiter mit Zweigstellen am CME-Router zu unterstützen. Die gängigsten Designs sind Telefone mit routbaren IP-Adressen und Telefone mit privaten IP-Adressen.

Remote-Telefone mit öffentlichen (lesen Sie: routable) IP-Adressen

Wenn beide am Anruf beteiligten Telefone mit öffentlichen, routbaren IP-Adressen konfiguriert

sind, können Medien direkt zwischen den Telefonen übertragen werden (Abbildung 8). Daher wieder einmal keine Notwendigkeit für NAT!

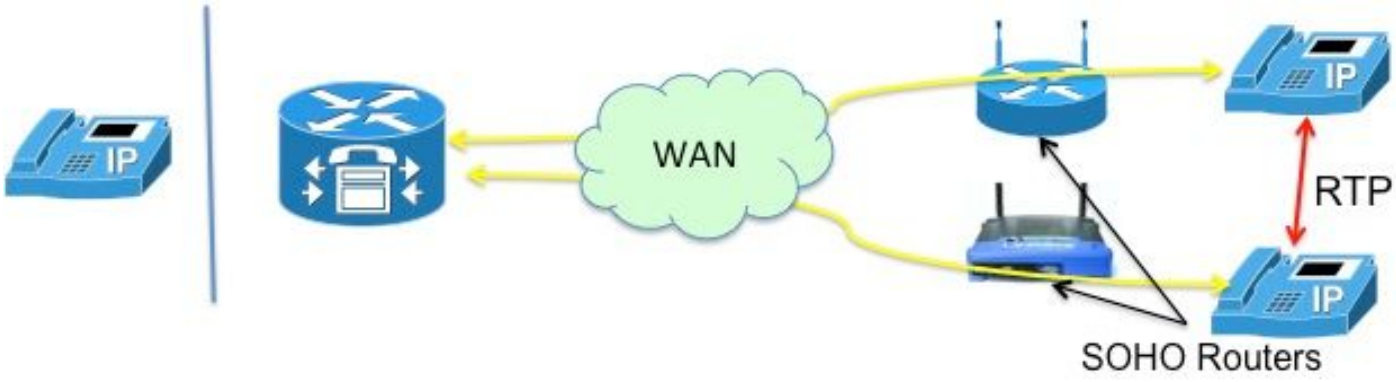

Abbildung 8

Remote-Telefone mit privater IP-Adresse

In diesem Szenario wird der Anruf zwischen Skinny-Telefonen signalisiert, die mit privaten IP-Adressen konfiguriert sind. Die Router im Heimbüro (SOHO) sind im Allgemeinen nicht "SCCP-fähig". d. h. die in den SCCP-Nachrichten eingebetteten IP-Adressen nicht übersetzen können. Das bedeutet, dass die Telefone nach Abschluss der Anrufeinrichtung jeweils die private IP-Adresse des anderen Telefons erhalten. Da beide Telefone privat sind, signalisiert CME den Anruf so, dass die Audioübertragung direkt zwischen den Telefonen stattfindet. Dies führt jedoch zu unidirektionalem oder undirektionalem Audio (da private IP-Adressen per Definition nicht über das Internet angesprochen werden können!), es sei denn, eine der folgenden Abhilfemaßnahmen ist implementiert-

- Konfigurieren statischer Routen auf den SOHO-Routern
- eine IPsec-VPN-Verbindung zu den Telefonen herstellen

Eine bessere Möglichkeit, dies zu beheben, wäre die Konfiguration von "mtp". Der Befehl mtp stellt sicher, dass RTP-Pakete (Media Packets) von Remote-Telefonen den CME-Router passieren (Abbildung 9).

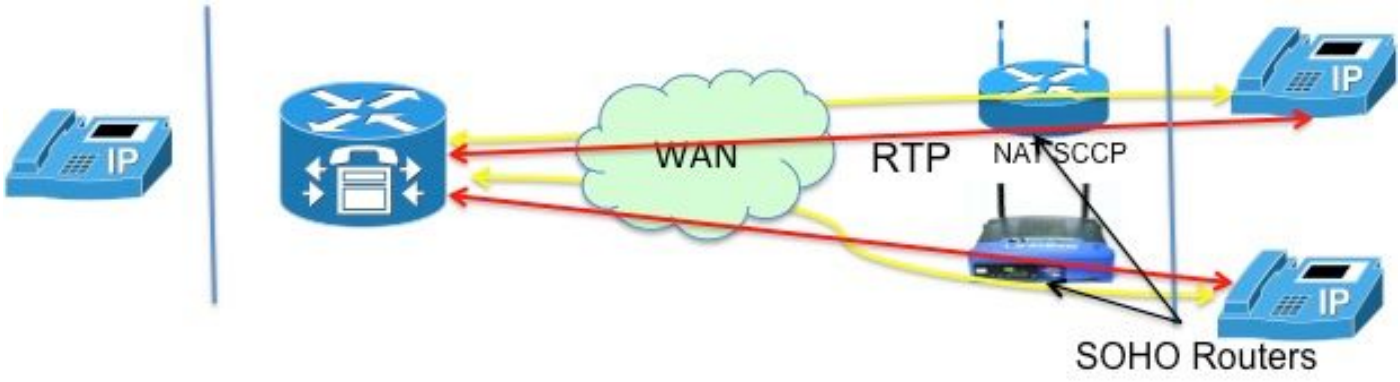

Abbildung 9

Die MTP-Lösung ist besser, da Probleme beim Öffnen von Firewall-Ports auftreten. Die Medienpakete, die über ein WAN übertragen werden, können durch eine Firewall blockiert werden. Das bedeutet, dass Sie Ports auf der Firewall öffnen müssen, aber welche? Wenn CME die Audiodaten weiterleitet, können die Firewalls auf einfache Weise für die Weiterleitung der

RTP-Pakete konfiguriert werden. Der CME-Router verwendet einen ***bestimmten*** UDP-Port (2000!) für Medienpakete. Wenn also nur Pakete von und zu Port 2000 zugelassen werden, kann der GESAMTE RTP-Verkehr weitergeleitet werden.

Abbildung 10 zeigt die Konfiguration von MTP.

```
ePhone 1

  Mac 1111 2222 3333

  Typ 7965

  MTP

  Taste 1:1
```

Abbildung 10

Mit mtp ist nicht alles wunderbar. Es gibt Situationen, in denen MTP nicht wünschenswert ist.

- MTP ist nicht abhängig von der CPU-Auslastung
- Multicast-Warteschleifenmusik kann im Allgemeinen nicht über ein WAN weitergeleitet werden. Die Multicast-Warteschleifenmusik-Funktion überprüft, ob MTP für ein Telefon aktiviert ist, und sendet keine Warteschleifenmusik an dieses Telefon.

Wenn Sie also eine WAN-Konfiguration haben, die Multicast-Pakete weiterleiten **kann,** und Sie RTP-Pakete über Ihre Firewall zulassen können, können Sie sich gegen die Verwendung von MTP entscheiden.

Remote-SIP-Telefone

Beachten Sie, dass SIP-Telefone in den obigen Szenarien nicht erwähnt wurden. Dies liegt daran, dass CME sich in den Audiopfad einfügt, wenn eines der Telefone ein SIP-Telefon ist. Dies wird dann zu dem zuvor beschriebenen Szenario, bei dem eine lokale Anbindung an eine entfernte Verbindung nicht erforderlich ist.

WÜRFEL

Das CUBE führt NAT- und PAT-Funktionen automatisch aus, da es alle Sitzungen beendet und ihren Ursprung erneut festlegt. Das CUBE ersetzt seine eigene Adresse durch die Adresse jedes Endpunkts, mit dem es kommuniziert. Auf diese Weise wird die Adresse dieses Endpunkts effektiv ausgeblendet (übersetzt).

Bei der CUBE-Funktion ist daher keine NAT erforderlich. Es gibt ein VoIP-Service-Szenario, in dem für das CUBE eine NAT erforderlich ist, wie im nächsten Abschnitt beschrieben.

Gehostete NAT-Überbrückung

Ein kurzer Hintergrund zum gehosteten Telefoniedienst hilft Ihnen, die Gründe für diese Funktion zu verstehen.

Ein gehosteter Telefoniedienst ist eine neue Form des VoIP-Dienstes, bei dem sich der Großteil des Geräts am Standort des Service Providers befindet. Sie arbeiten mit den Home-Gateways (HGW) zusammen, die nur eine grundlegende NAT implementieren (d. h. NAT auf L3/L4). Verizon installiert z. B. das Optical Network Terminal (ONT), das Wi-FiOS-Dienste im Haus bereitstellt. Sprachanrufe werden mithilfe eines in die ONT integrierten SIP-Prozesses signalisiert. Die SIP-Signalisierung wird über das private IP-Netzwerk von Verizon an neue Soft-Switches übertragen, die den Service und die Steuerung für die Sprachkommunikation mit anderen FiOS Digital Voice-Kunden oder herkömmlichen Telefonkunden bereitstellen.

Zu den wichtigsten Anforderungen an die Anbieter gehosteter Telefoniedienste gehören:

- Remote-NAT-Traversal: die Möglichkeit, Endgeräten Klasse-5-Services über NAT (dies ist nur auf NAT-Layer-3 möglich) und Firewall-Geräten (über Remote-Zugriff mit "ALG") bereitzustellen.
- Co-Media-Unterstützung: Die Möglichkeit, Medien zwischen Geräten am gleichen Standort zu senden, wenn es nicht sinnvoll ist, die Medien zurück zum IP-Netzwerk zu leiten.
- Keine zusätzliche Ausrüstung, sodass keine CPE hinzugefügt werden müssen.

Welche Möglichkeiten gibt es in Anbetracht der obigen Ausführungen, einen solchen Dienst zu implementieren?

- Ersetzen Sie den HGW durch eine teure ALG.
- Ändern Sie die eingebetteten SIP-Header für Pakete mithilfe eines Session Border Controllers (SBC). Diese umfasst ein im Netzwerk gehostetes Produkt der Carrier-Klasse, das SIP in einer sehr sicheren, fehlertoleranten Konfiguration unterstützt. Diese Lösung wird als NAT-SBC bezeichnet.

Die NAT-SBC-Option erfüllt die oben genannten Anbieteranforderungen.

NAT-SBC

Der NAT-SBC funktioniert wie folgt (Abbildung 11)

1. Access Router übersetzt nur die L3/L4-IP-Adresse
2. IP-Adresse in der SIP-Nachricht nicht umgewandelt
3. SBC NAT fängt die eingebettete IP-Adresse ab und übersetzt sie. Sobald der SBC SIP-Pakete erkennt, die an **200.200.200.10** gerichtet sind, beginnt er mit dem Code nat-sbc.
4. Medien werden nicht übersetzt und können direkt zwischen den Telefonen ausgetauscht werden[5]

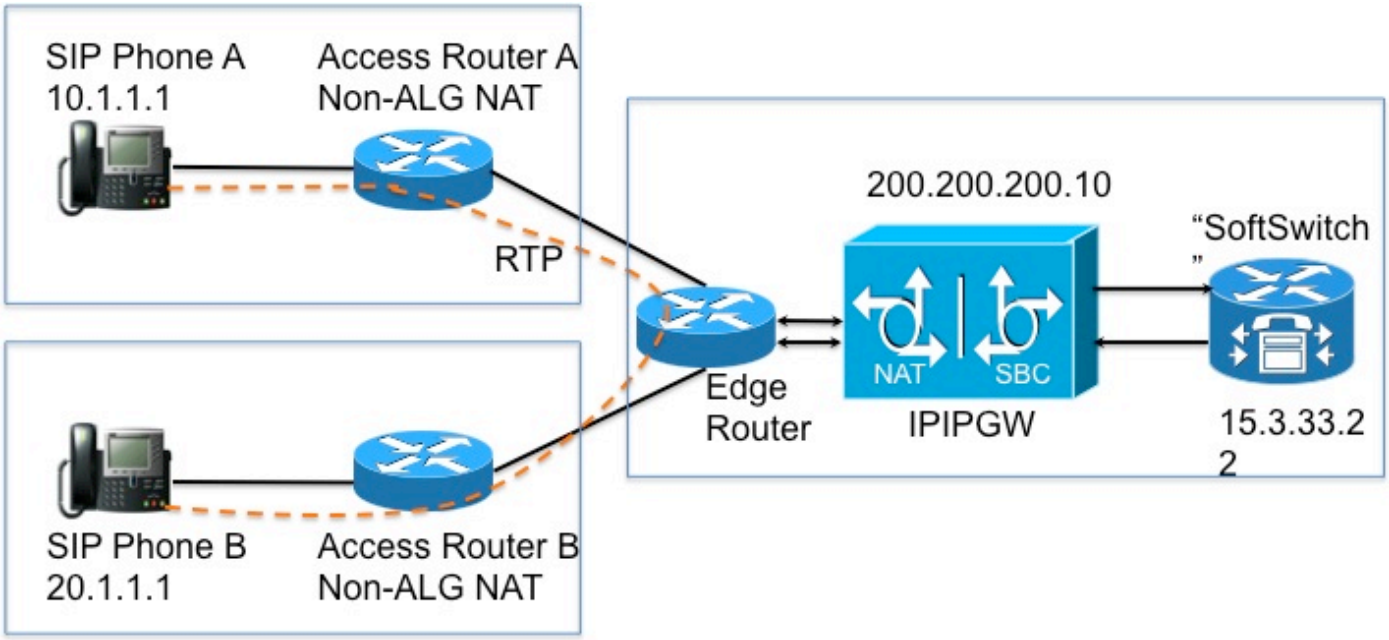

Abbildung 11

Design-Hinweise

- Die IP-Adresse **200.200.200.10** (Abbildung 12) wird keiner Schnittstelle auf dem NAT-SBC zugewiesen. Sie wird als die Adresse des "Proxys" konfiguriert, an den SIP-Telefon A und SIP-Telefon B Signalisierungsnachrichten senden.
- Heimgeräte übersetzen bestimmte *reine* SIP/SDP-Adressfelder nicht (z. B. Anruf-ID: ‚O= , Warnung: headers & branch= Parameter. maddr= und received= wurden nur in bestimmten Szenarien behandelt.) Diese Felder werden vom NAT-SBC verarbeitet. Eine Ausnahme bilden die Proxy-Autorisierung und die Autorisierungsübersetzung, da die Authentifizierung hierdurch unterbrochen wird.
- Wenn die Heimgeräte für PAT konfiguriert sind, müssen die Benutzeragenten (Telefone und Proxy) eine symmetrische Signalisierung [6] sowie symmetrische und Early Media unterstützen. Sie müssen den Überschreibungsport auf dem NAT-SBC-Router konfigurieren.
- Da symmetrische Signalisierung sowie symmetrische und Early Media nicht unterstützt werden, müssen die zwischengeschalteten Router ohne PAT konfiguriert werden, und die Außerkraftsetzungsadresse muss im NAT-SBC konfiguriert werden.

Konfiguration

Nachfolgend finden Sie eine Beispielkonfiguration für einen typischen NAT-SBC.

```
ip nat sip-sbc

  Proxy 200.200.200.10 5060 15.3.33.22 5060 Protokoll udp

  Anruf-ID-Pool Anruf-ID-Pool

  Sitzungs-Timeout 300

  Betriebszuflussbegrenzung

  Überschreibport

!
```

```
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 innerhalb der Quellliste 1 pool sbc1 overload

ip nat innerhalb der Quellliste 2 pool sbc2

ip nat outside source list 3 pool outside-pool add-route

ip nat inside source list 4 pool anruf-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
```

Anrufablauf mit SBC NAT

Abbildung 13 und Abbildung 14 zeigen den Anruffluss in Bezug auf die Übersetzungen. Folgende Punkte sind zu beachten:

- Bei der Registrierung merkt der Soft-Switch an, dass die beiden Telefone
  — SIP-Telefon A - 15.3.33.62 2001

  — SIP-Telefon B - 15.3.33.62 2002

- Bei diesem Anruffluss lässt SBC NAT die Medien-IP-Adresse praktisch unübersetzt.

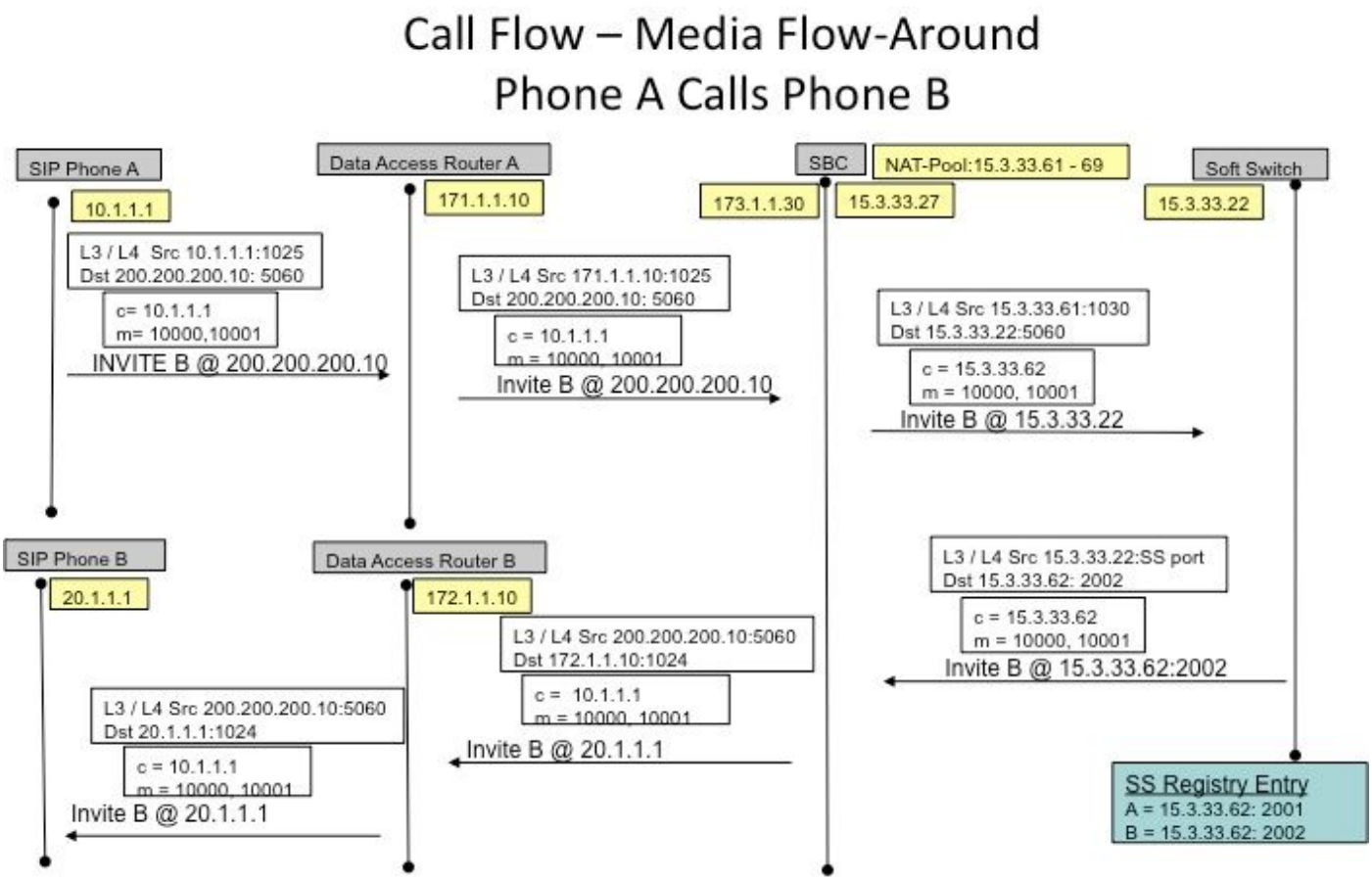

Abbildung 13

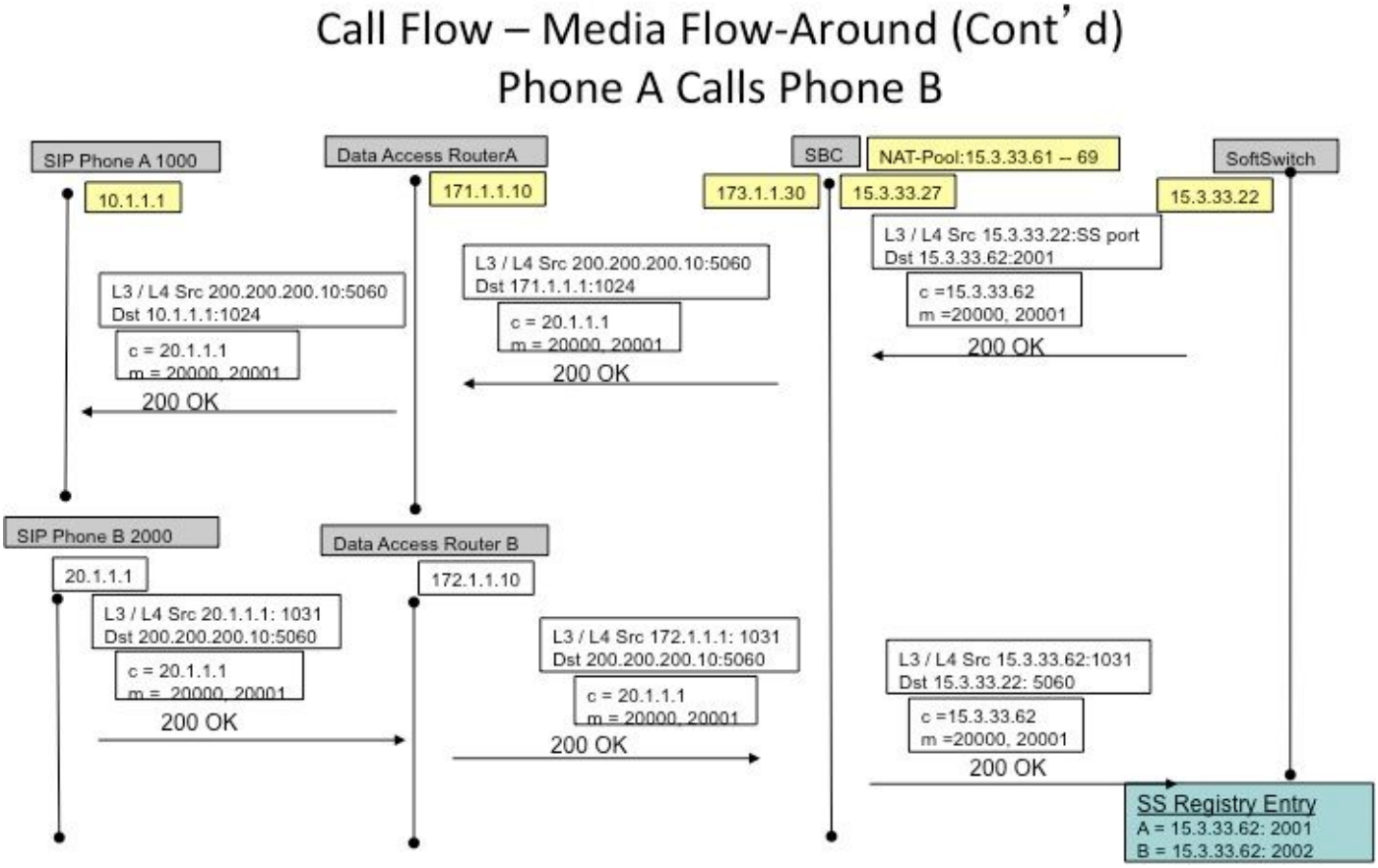

Abbildung 14

SIP-Registrierung

In früheren Versionen (von SBC NAT) mussten SIP-Endpunkte *Keep-Alive*-Pakete senden, um das Pinhole der SIP-Registrierung offen zu halten (damit Out->in-Datenverkehr fließen kann, z. B. eingehende Anrufe). *Keep-Alive*-Pakete können vom Endpunkt oder vom Registrar gesendete SIP-Pakete sein (Soft-Switch). Neuere Versionen machen dies überflüssig, da der NAT-SBC selbst (im Gegensatz zu Soft-Switches) die Endpunkte zwingt, sich häufig neu zu registrieren, um die Pinholes offen zu halten.

> **Anmerkung:** Die Symptome eines abgelaufenen Registrierungsstiftlochs können unklar sein und zufällige Anrufsignalisierungsfehler aufweisen.

CUSP

Der CUSP hat den Begriff eines logischen Netzwerks, der sich auf eine Reihe von lokalen Schnittstellen bezieht, die ähnlich behandelt werden (z. Schnittstelle, Port, Transport zum Abhören). Wenn Sie ein logisches Netzwerk auf CUSP konfigurieren, können Sie es für die Verwendung von NAT konfigurieren. Nach der Konfiguration wird SIP ALG automatisch aktiviert. Dies ist nützlich, wenn bestimmte logische Netzwerke verwendet werden.

Fehlerbehebung

Symptome

Ein offensichtliches Symptom kann sein, dass ein Anruf in eine oder beide Richtungen fehlschlägt. Zu den weniger offensichtlichen Symptomen gehören

- Einweg-Audio
- Einweg-Audio bei Übertragung
- Freier Ton
- Verlust der SIP-Registrierung

Befehle anzeigen und debuggen

- `deb ip nat [sip] | mager]`
- `ip nat statistik anzeigen`
- `show ip nat übersetzungen`

Zu prüfende Punkte

- Stellen Sie sicher, dass die Konfiguration den Unterbefehl **ip nat inside** oder **ip nat outside** interface enthält. Diese Befehle aktivieren NAT an den Schnittstellen, und die Kennzeichnung "inside/outside" ist wichtig.
- Stellen Sie bei statischer NAT sicher, dass der Befehl **ip nat source static** zuerst die interne lokale Adresse und dann die interne globale IP-Adresse angibt.
- Bei dynamischer NAT stellen Sie sicher, dass die ACL, die so konfiguriert ist, dass sie mit den vom internen Host gesendeten Paketen übereinstimmt, mit den Paketen des Hosts

übereinstimmt, bevor eine NAT-Umwandlung erfolgt ist. Wenn beispielsweise eine interne lokale Adresse von 10.1.1.1 in 200.1.1.1 übersetzt werden soll, stellen Sie sicher, dass die ACL mit der Quelladresse 10.1.1.1 übereinstimmt und nicht mit der Quelladresse 200.1.1.1.

- Bei einer dynamischen NAT ohne PAT stellen Sie sicher, dass der Pool über genügend IP-Adressen verfügt. Zu den Symptomen, dass nicht genügend Adressen vorhanden sind, gehören ein wachsender Wert im zweiten Zähler für fehlende Nachrichten in der Ausgabe des Befehls **show ip nat statistics** sowie die Anzeige aller Adressen in dem im NAT-Pool definierten Bereich in der Liste der dynamischen Übersetzungen.
- Für PAT ist es leicht zu vergessen, die **Overload-**Option auf dem **Befehl ip nat inside source list** hinzuzufügen. Ohne diese Funktion funktioniert NAT, PAT jedoch nicht. Häufig werden Benutzerpakete nicht übersetzt, und Hosts können nicht auf das Internet zugreifen.
- Möglicherweise wurde NAT richtig konfiguriert, aber eine ACL ist auf einer der Schnittstellen vorhanden und verwirft die Pakete. Beachten Sie, dass IOS ACLs vor NAT für Pakete verarbeitet, die in eine Schnittstelle eingehen, und nach der Übersetzung der Adressen für Pakete, die eine Schnittstelle verlassen.
- Vergessen Sie nicht, "ip nat outside" auf der Schnittstelle zum WAN zu konfigurieren (auch wenn dies keine externe Adresse übersetzt)!
- Sobald NAT konfiguriert ist, zeigt show ip nat translation not show Nothing. Ping einmal und dann wieder überprüfen.
- Ermitteln von **Wireshark-Traces** an internen und externen Schnittstellen des NAT-SBC

Szenarien

Die Debug-Ausgabe für einige Szenarien ist unten dargestellt. Sie sind meist selbsterklärend!

Grundlegende NAT

Konfigurations- und Debug-Zeilen für grundlegende NAT sind unten dargestellt.

```
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

Ausgabeleitungen von **debug ip nat sip** werden angezeigt. In diesem Fall wird die eingebettete IP-Adresse eines ausgehenden Pakets übersetzt.

```
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:
```

Referenzen

Übersicht:

- http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.HTML
- **Anatomie:** http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html
- http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml

VoiP und NAT

- https://supportforums.cisco.com/docs/DOC-5406
- http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-security/id-60290.HTML

NAT-Funktionsmatrix

- 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_note09186a0080b17919sht

ml

Gehostete NAT-Überbrückung:

- 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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.