

VoIP中的NAT

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[靜態NAT](#)

[動態NAT](#)

[NAT過載\(PAT\)](#)

[NAT命令選項](#)

[NAT針孔](#)

[VoIP中的NAT](#)

[ALG](#)

[閘道](#)

[CME](#)

[本地](#)

[本地到遠端](#)

[遠端工作人員](#)

[帶有公共裝置的遠端電話\(讀：可路由\)IP地址](#)

[具有私有IP地址的遠端電話](#)

[遠端SIP電話](#)

[立方體](#)

[託管NAT穿越](#)

[NAT SBC](#)

[維護和運作技術筆記](#)

[組態](#)

[使用SBC NAT的呼叫流](#)

[SIP註冊](#)

[CUSP](#)

[疑難排解](#)

[症狀](#)

[Show和debug命令](#)

[要檢查的事項](#)

[案例](#)

[基本NAT](#)

[SIP ALG](#)

[參考資料](#)

簡介

本檔案將說明作為CUBE (思科整合邊界元件)、CME或CUCME (思科整合通訊管理員

Express)、闡道與CUSP (思科整合SIP代理) 的路由器中的NAT(網路位址轉譯)行為。

必要條件

需求

思科建議您瞭解以下主題：

- SIP (作業階段啟始通訊協定)
- IP語音 (Internet協定)
- 路由通訊協定

採用元件

本檔案中的資訊是根據

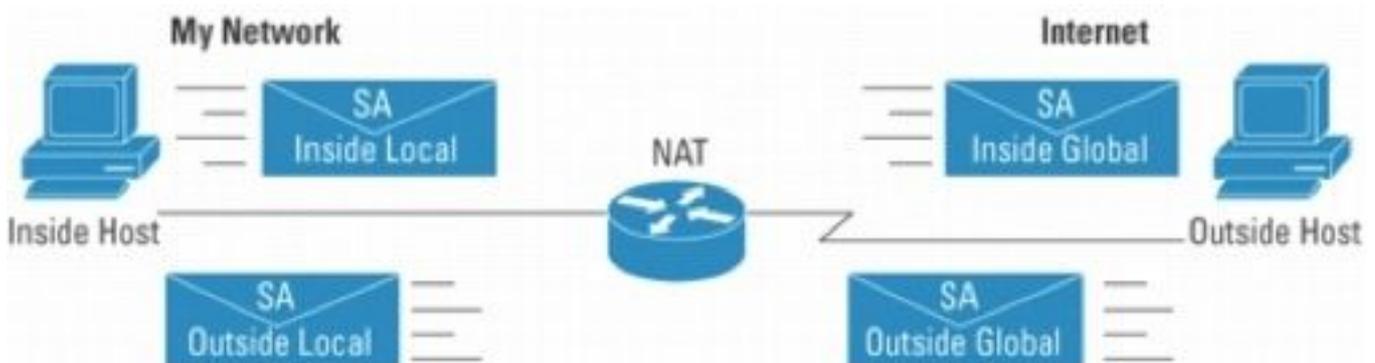
- 任何IOS版本12.4T及更高版本。
- 任何CME版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

網路地址轉換是一種常用的技術，用於在使用不同地址空間的網路之間傳輸的資料包上轉換IP地址。本文的目的不是複習NAT。相反，本文檔旨在對NAT在思科VoIP網路中使用的方式進行全面的審查。此外，範圍僅限於組成MS-Voice技術的元件。

- NAT基本上用不同的IP地址替換資料包中的IP地址
- 使專用子網中的多台主機能夠共用 (即像這樣) 單個公有IP地址，以訪問Internet。
- 通常，NAT配置僅更改內部主機的IP地址
- NAT是雙向的 — 如果A在內部介面上轉換為B，到達外部介面的B將轉換為A!
- RFC1631



An IP address is either local or global
Local IP addresses are seen in the inside network
Global IP addresses are seen in the Outside network

注意:將NAT視為使用私有地址空間將IP資料包路由進和路由出網路的輔助手段可能有所幫助。換句話說，NAT使不可路由的地址可路由

圖2顯示後面圖中所引用的拓撲。

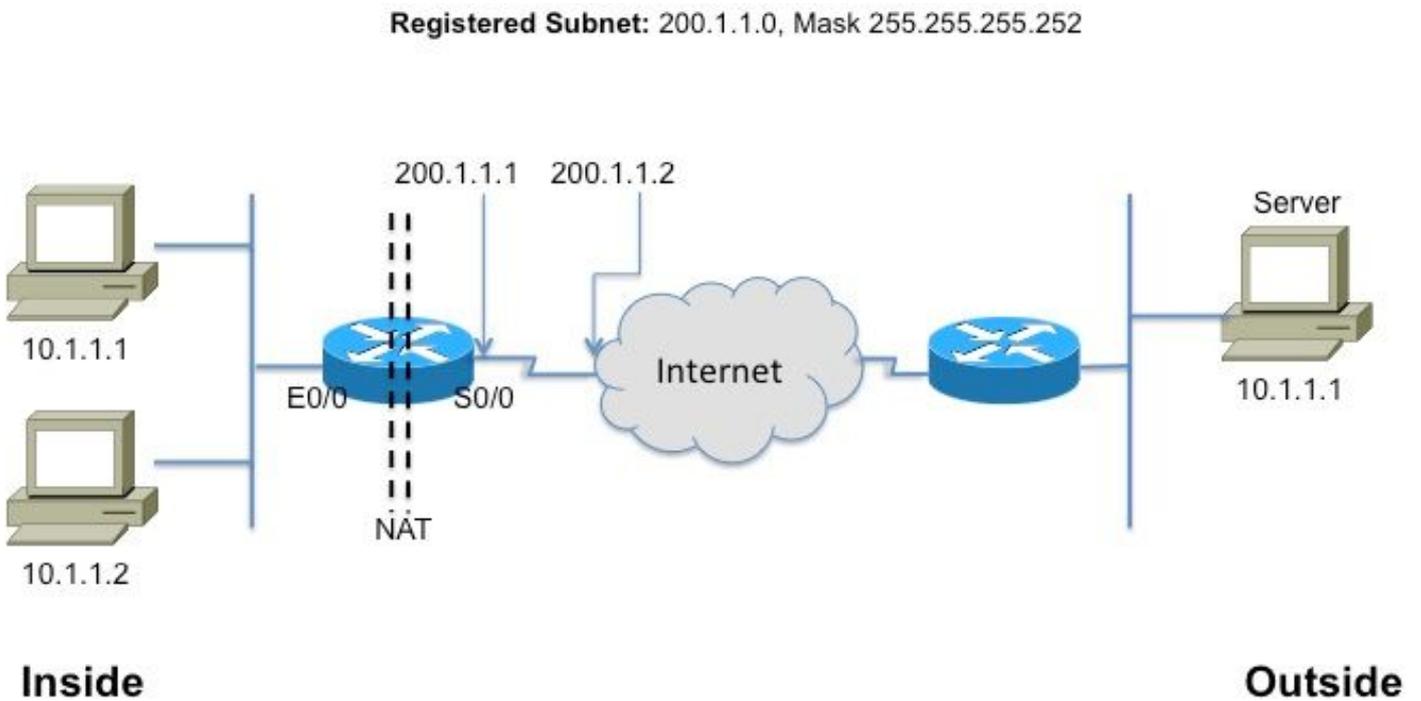


圖2

本術語表是瞭解和描述NAT的基礎

- **內部本地地址** — 分配給內部網路上主機的IP地址。通常，地址來自私有地址空間。
- **內部全域性地址** — 由NIC或服務提供商分配的可路由IP地址，代表一個或多個外部的內部本地IP地址。
- **外部本地地址** — 外部主機對內部網路顯示的IP地址。不一定是合法地址，它從內部可路由的地址空間分配。
- **外部全域性地址** — 主機所有者分配給外部網路上主機的IP地址。地址從全域性可路由地址或網路空間分配。

注意:適應這些術語。有關NAT的任何備註或文檔一定參考它們

靜態NAT

這是最簡單的NAT形式，其中每個內部地址被靜態轉換為外部地址（反之亦然）。

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

圖3

上述轉換的CLI配置如下

```
interface Ethernet0/0
```

```
ip address 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 < — 必需！ [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
```

動態NAT

在動態NAT中，每個內部主機都對映到一個地址池中的地址。

- 從內部全域性地址池中分配IP地址。
- 如果新資料包從另一台內部主機到達，並且需要NAT條目，但所有池化IP地址都在使用中，則路由器只會丟棄該資料包。
- 實質上，內部全域性地址池的大小需要與同時需要使用Internet的最大併發主機數量相同

以下CLI說明了配置動態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過載(PAT)

當IP地址池小於需要轉換的地址集時，此功能非常方便。

- 多個內部地址NAT僅轉換為一個或多個外部地址
- PAT (埠地址轉換) 使用內部全域性IP地址上的唯一源埠號來區分轉換。由於埠號採用16位編碼，因此理論上，每個IP地址的總埠數可能高達65,536。如果此源埠已分配，則PAT將嘗試保留原始源埠，PAT將嘗試查詢第一個可用埠號

- NAT過載可使用超過65,000個埠，使其可以很好地擴展，而無需多個註冊IP地址，在許多情況下，只需要一個外部全域性IP地址。

圖4說明PAT。

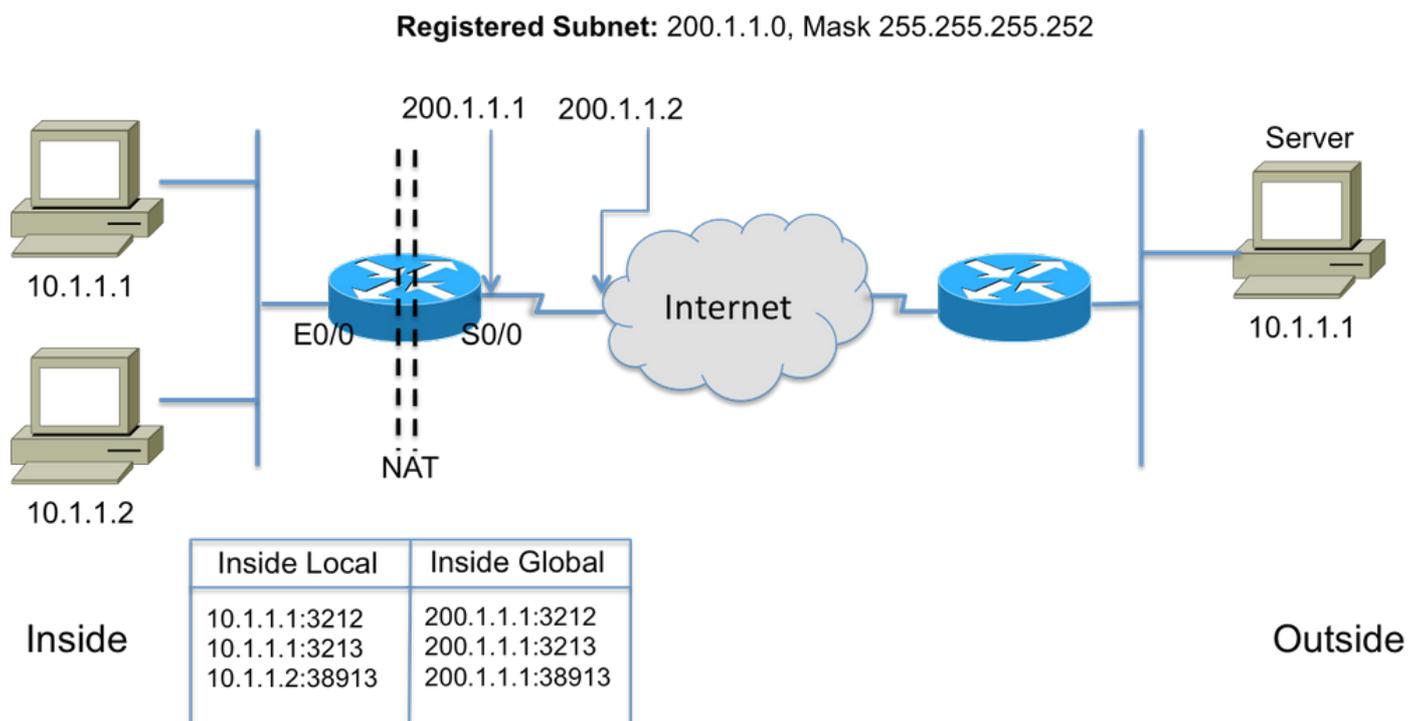


圖4

NAT命令選項

Cisco NAT實施功能非常多用，有許多選項。下面列出了一些增強，但請參閱 http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html以瞭解有關增強功能的完整清單的詳細資訊。

- 帶有埠的靜態轉換 — 傳送到特定埠(例如 埠25 (用於SMTP伺服器) 傳送到特定伺服器。
- 支援路由對映 — 靈活配置過濾器/ACL
- 更靈活的池配置 — 允許不連續的地址範圍。
- 主機號保留 — 轉換「網路」部分，保留「主機」部分。

NAT針孔

NAT術語中的針孔是指<主機IP，埠>和<全域性地址，全域性埠>元組之間的對映。它允許NAT裝置使用傳入消息的目標埠號(將為全域性埠)將目標對映回發起會話的主機IP和埠。必須注意的是，針孔在不使用一段時間後超時，並且公有地址將返回到NAT池。

VoIP中的NAT

那麼，VoIP網路中的NAT有哪些問題和顧慮？請回想一下，我們目前討論的NAT(更確切地說是基本NAT)只轉換IP資料包報頭中的IP地址，當然還會重新計算校驗和，但VoIP信令攜帶嵌入信令消息正文的IP地址。換句話說，在第5層

圖5說明了保留未轉換的嵌入式IP地址的效果。呼叫信令成功完成，但服務提供商的SIP代理無法嘗試將媒體(RTP)資料包路由到呼叫代理傳送的媒體地址！

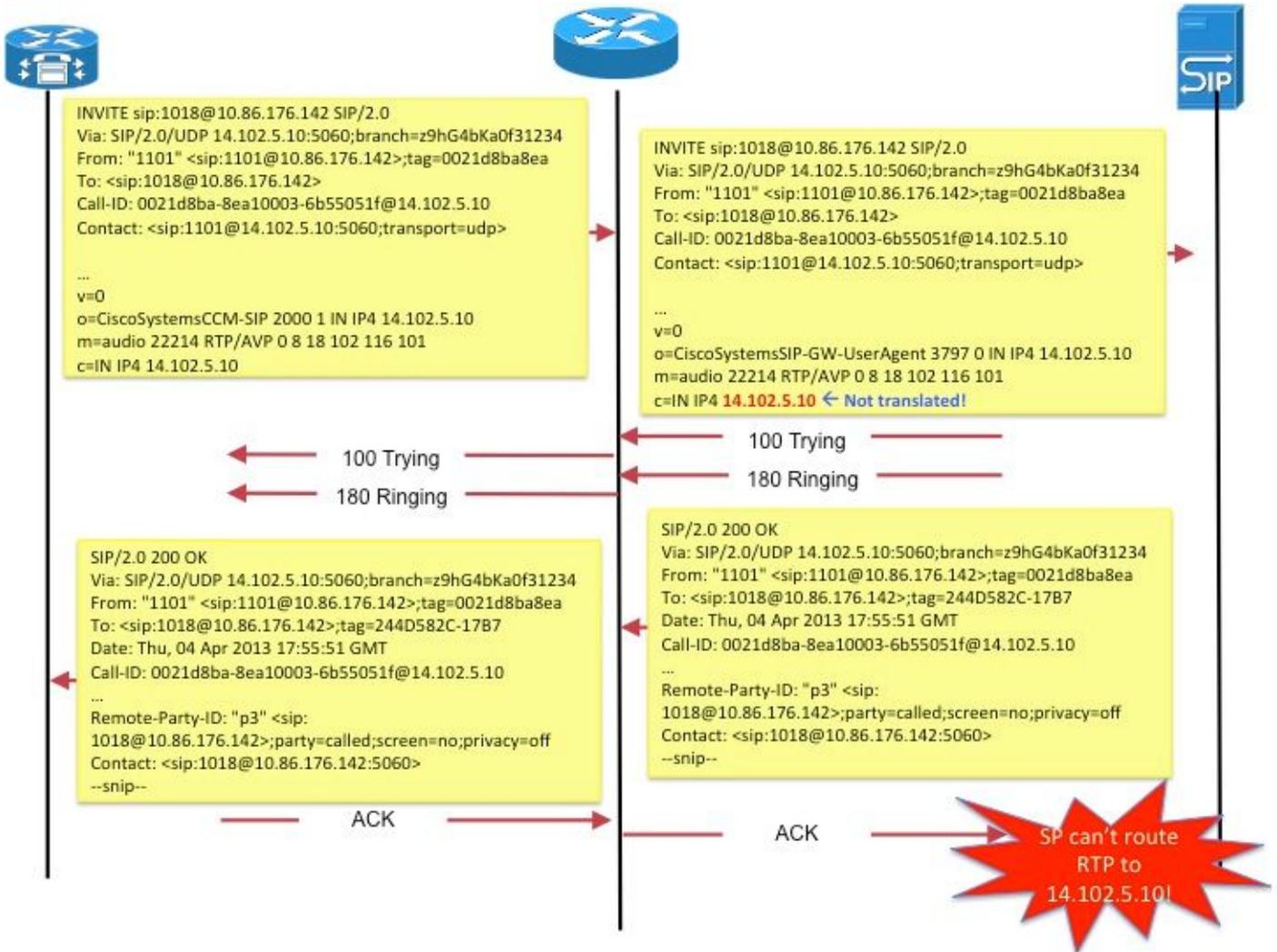


圖5

另一個示例是SIP終端使用 **Contact:**欄位，用於傳達終端希望接收新請求信令消息的地址。

這些問題可通過稱為應用層網關(ALG)的功能來解決。

ALG

ALG瞭解其支援的特定應用（例如SIP）使用的協定，並對通過該協定的流量執行協定資料包檢查和「修復」。有關如何為SIP呼叫信令修復各個欄位的詳細說明，請參閱<http://www.voip-info.org/wiki/view/Routers+SIP+ALG>。

在Cisco路由器上，在標準TCP埠5060上預設啟用對ALG SIP的支援。可以將ALG配置為支援用於SIP信令的非標準埠。請參閱http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html。

注意:小心！沒有RFC或其他標準規定應該為各種VoIP協定轉換哪些嵌入式欄位。因此，不同裝置供應商的實施各不相同，導致互操作問題（和TAC案例）。

闡道

由於根據定義，網關不是ip到ip裝置，因此NAT不適用。

CME

本文檔的此部分使用CME檢視呼叫方案，以瞭解為什麼必須使用NAT。

案例1.本地電話

案例2.遠程電話 (具有公用IP地址)

案例3.遠端遠端員工

注意：在所有情況下，為了讓音訊流通，CME IP地址都需要可路由

本地

在此情境 (圖6) 中，呼叫中涉及的兩部電話是具有私有IP地址的小型電話。



圖6

注意：請記住，在與同一CME系統中的另一部瘦電話進行呼叫時連線的瘦電話會將其媒體資料包直接傳送到另一部電話；即本地電話到本地電話的RTP不會通過CME。

因此，在這種情況下，NAT不適用或不需。

註：CME根據呼叫中涉及的兩種電話是否都較薄且位於同一網段，確定是否應直接確定介質 (RTP)。否則，CME會將自身插入RTP路徑中。

本地到遠端

在此場景中 (圖7)，CME將自身插入RTP流，這樣來自電話的RTP將在CME上終止。CME會將資料流重新發起到另一台電話。由於CME位於內部 (專用) 網路和外部網路上，並將其內部地址傳送到內部電話，並將外部 (公共) 地址傳送到外部電話，因此這裡也不需要NAT。

但是請注意，遠端IP電話和CME源IP地址之間的UDP/TCP埠（信令以及RTP）必須開啟。這表示防火牆或其他篩選裝置已設定為允許相關連線埠。

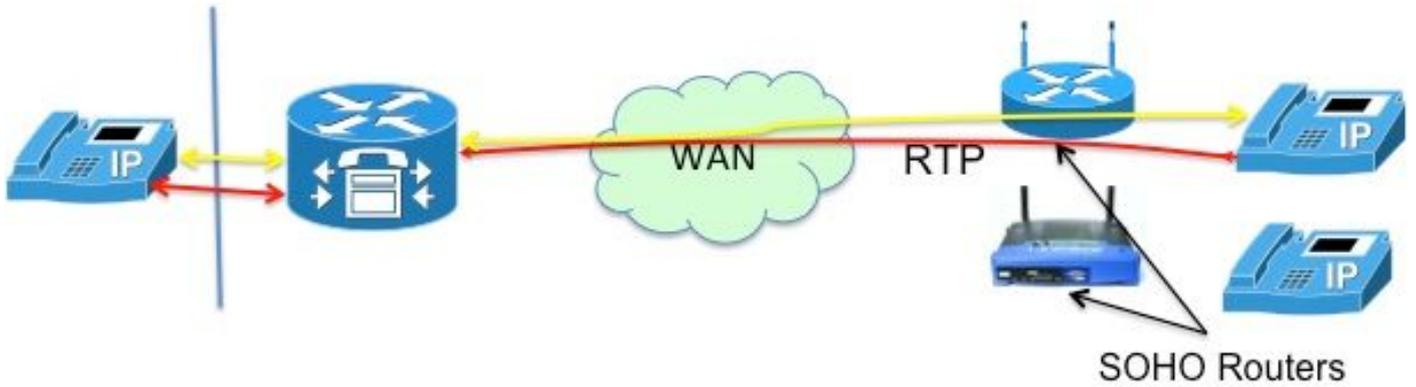


圖7

注意:請注意，在CM上始終終止訊號[消息]

遠端工作人員

這是指通過WAN連線到CME的IP電話，用於支援辦公室與CME路由器相隔遙遠的遠端工作人員。最常見的設計涉及具有可路由IP地址的電話和具有私有IP地址的電話。

帶有公共裝置的遠端電話(讀：可路由)IP地址

如果呼叫中涉及的兩台電話都配置了公共的可路由IP地址，則媒體可以在電話之間直接流動（圖8）。因此，再次說明，無需NAT！

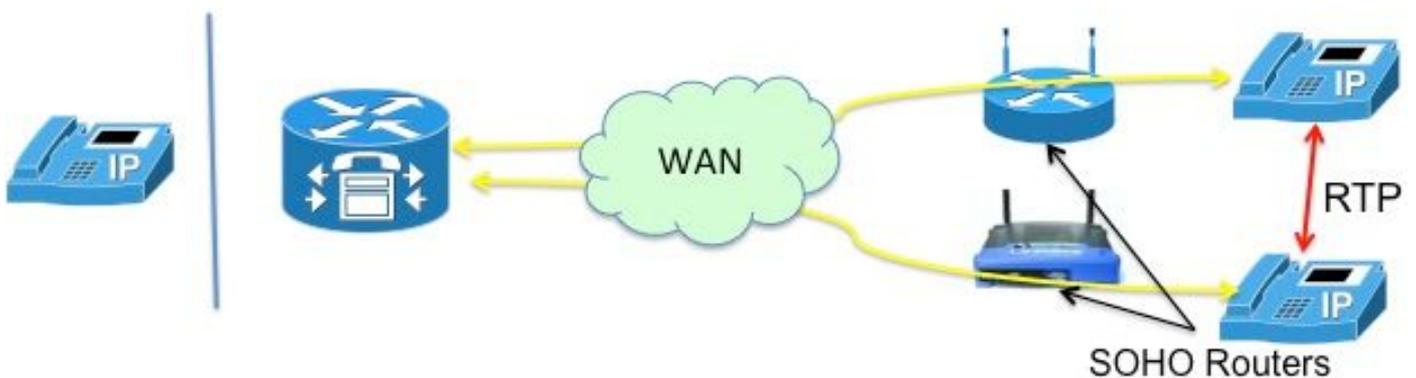


圖8

具有私有IP地址的遠端電話

在此場景中，呼叫會在配置有私有IP地址的小型電話之間發出訊號。一般而言，家庭辦公室(SOHO)路由器往往不具有「SCCP意識」。即無法轉換SCCP消息中嵌入的IP地址。這意味著，在呼叫建立完成後，電話會以彼此的私有IP地址結尾。由於兩部電話都是私密的，CME將發出它們之間的呼叫訊號，以便音訊直接在電話之間傳輸。但是，這將導致單向或單向音訊（因為根據定義，私有IP地址不能路由到Internet！），除非實施以下一種解決方法-

·在SOHO路由器上配置靜態路由

·建立到電話的IPsec VPN連線

解決此問題的更好方法是配置「mtp」。mtp命令可確保來自遠端電話的媒體(RTP)資料包通過CME路由器(圖9)。

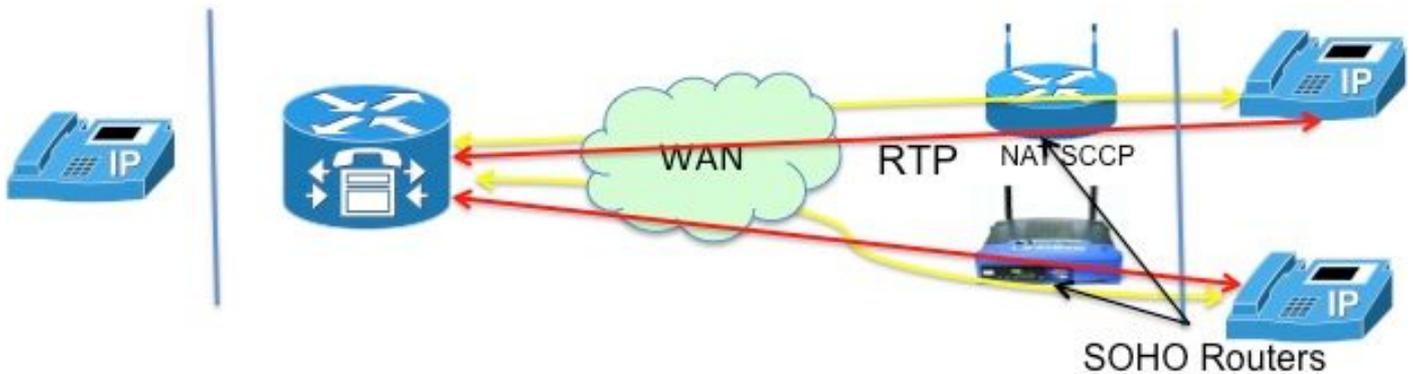


圖9

由於開放防火牆埠存在一些複雜問題，因此「mtp」解決方案更好。通過WAN傳輸的媒體資料包可能被防火牆阻擋。這表示您需要在防火牆上開啟連線埠，但需使用哪些連線埠？通過CME中繼音訊，可以輕鬆配置防火牆以傳遞RTP資料包。CME路由器對媒體封包使用特定的UDP埠(2000!)。因此，僅允許資料包進出埠2000，就可以傳輸所有RTP流量。

圖10說明了如何配置mtp。

```
ephone 1
  mac 1111.2222.3333
  type 7965
  mtp
  1:1
```

圖10

使用mtp並非一切美好。在某些情況下，mtp可能不可取

- MTP對CPU利用率不溫和
- 組播MOH通常無法通過WAN轉發 — 組播MOH功能檢查電話是否啟用了MTP，如果啟用，則不會將MOH傳送到該電話。

因此，如果您的WAN配置可以轉發組播資料包，並且您可以允許RTP資料包通過防火牆，則可以決定不使用MTP。

遠端SIP電話

請注意，上述場景中未提及SIP電話。這是因為如果其中一個電話是SIP電話，CME會將自身插入音訊路徑。然後就變為前面所述的本地到遠端場景，其中不需要NAT。

立方體

CUBE在終止和重新發起所有會話時本身執行NAT和PAT功能。CUBE將其自身的地址替換為其通訊的任何終端的地址，從而有效地隱藏（轉換）該終端的地址。

因此，CUBE函式不需要NAT。在VoIP服務場景中，CUBE上需要NAT，如下一節所述。

託管NAT穿越

有關託管電話服務的簡要背景資料將有助於瞭解此功能的原理。

託管電話服務是一種新的VoIP服務形式，其中大多數裝置位於服務提供商的位置。它們與僅實施基本NAT（即L3/L4的NAT）的家庭網關(HGW)配合工作。例如，Verizon安裝了光纖網路終端(ONT)，該終端在家中提供FiOS服務；使用ONT中內建的SIP進程發出語音呼叫訊號。SIP訊號是透過Verizon的私人IP網路向新的軟交換器發出的，而新的軟交換器則提供服務和控制，以與其他FiOS數位語音客戶或傳統電話客戶建立語音通訊。

託管電話服務的主要提供商要求包括：

- 遠端NAT穿越：利用NAT（只能執行NAT第3層！）和防火牆裝置（通過遠端執行「ALG！」）向終端提供5類服務的能力。
- 聯合媒體支援：在位於同一位置的裝置之間傳送介質的功能，在這種裝置中將介質路由回到IP網路沒有意義
- 無需新增裝置，無需新增任何CPE。

鑑於上述情況，實施此類服務有哪些選項？

- 用昂貴的ALG更換HGW，
- 使用會話邊界控制器(SBC)修改資料包的嵌入式SIP報頭。這涉及網路託管的運營商級產品，它以非常安全、容錯的配置支援SIP。此解決方案稱為NAT SBC。

NAT SBC選項滿足上面列出的提供商要求。

NAT SBC

NAT SBC的工作方式如下（圖11）

1. 接入路由器僅轉換L3/L4 IP地址
2. SIP消息中的IP地址未轉換
3. SBC NAT攔截並轉換嵌入式IP地址。當SBC看到目的地為200.200.200.10的SIP資料包時，它會進入nat-sbc代碼。
4. 介質不進行轉換，直接在電話之間傳輸[5]

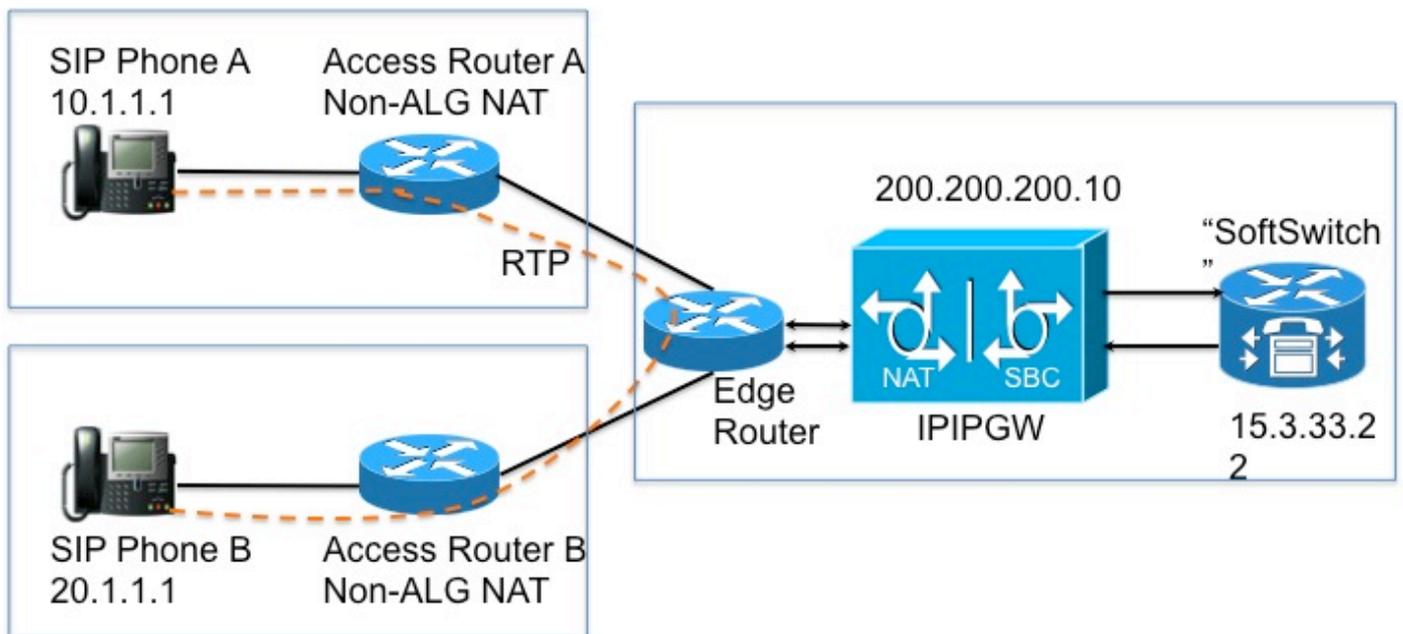


圖11

維護和運作技術筆記

- IP地址200.200.200.10 (圖12) 未分配給NAT SBC上的任何介面。它被配置為SIP電話A和SIP電話B向其傳送信令消息的「代理」的地址。
- 家庭裝置不轉換某些SIP/SDP *address-only* 欄位(例如Call-Id:,O= , 警告: headers & branch=引數。maddr=和received=引數僅在特定情況下處理。) 這些欄位由NAT SBC處理, 代理授權和授權轉換除外, 因為這些欄位將中斷身份驗證。
- 如果家庭裝置配置為執行PAT, 則使用者代理(電話和代理)必須支援對稱信令[6]以及對稱和早期媒體。您必須在NAT SBC路由器上配置覆蓋埠。
- 如果不支援對稱信令以及對稱和早期介質, 則必須在沒有PAT的情況下配置中間路由器, 並且應在NAT SBC中配置覆蓋地址。

組態

以下是典型NAT SBC的配置示例。

```

ip nat sip-sbc

200.200.200.10 5060 15.3.33.22 5060udp

call-id-pool call-id-pool

session-timeout 300

mode allow-flow-around

!

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 1.1.1.255.254 netmask 255.255.0.0

```

```
ip nat pool outside-pool 200.200.200.100 200.200.200.200 netmask 255.255.255.0

ip nat inside source list 1 pool sbc1 overload

ip nat inside source list 2 pool sbc2

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

ip nat inside source list 4 pool call-id-pool

!

access-list 1 permit 10.1.1.0 0.0.0.255

access-list 1 permit 171.1.1.0 0.0.0.255

access-list 2 permit 20.1.1.0 0.0.0.255

access-list 2 permit 172.1.1.0 0.0.0.255

access-list 3 permit 15.4.0.0 0.0.255.255

access-list 3 permit 15.5.0.0 0.0.255.255

access-list 4 permit 10.1.0.0 0.0.255.255

access-list 4 permit 20.1.0.0 0.0.255.255
```

使用SBC NAT的呼叫流

圖13和圖14從轉換的角度說明了呼叫流程。應注意到以下幾點 —

- 註冊後，軟交換機將兩台電話記為
 - SIP電話A - 15.3.33.62 2001
 - SIP電話B - 15.3.33.62 2002
- 在此呼叫流程中，SBC NAT有效地使介質IP地址未轉換。

Call Flow – Media Flow-Around Phone A Calls Phone B

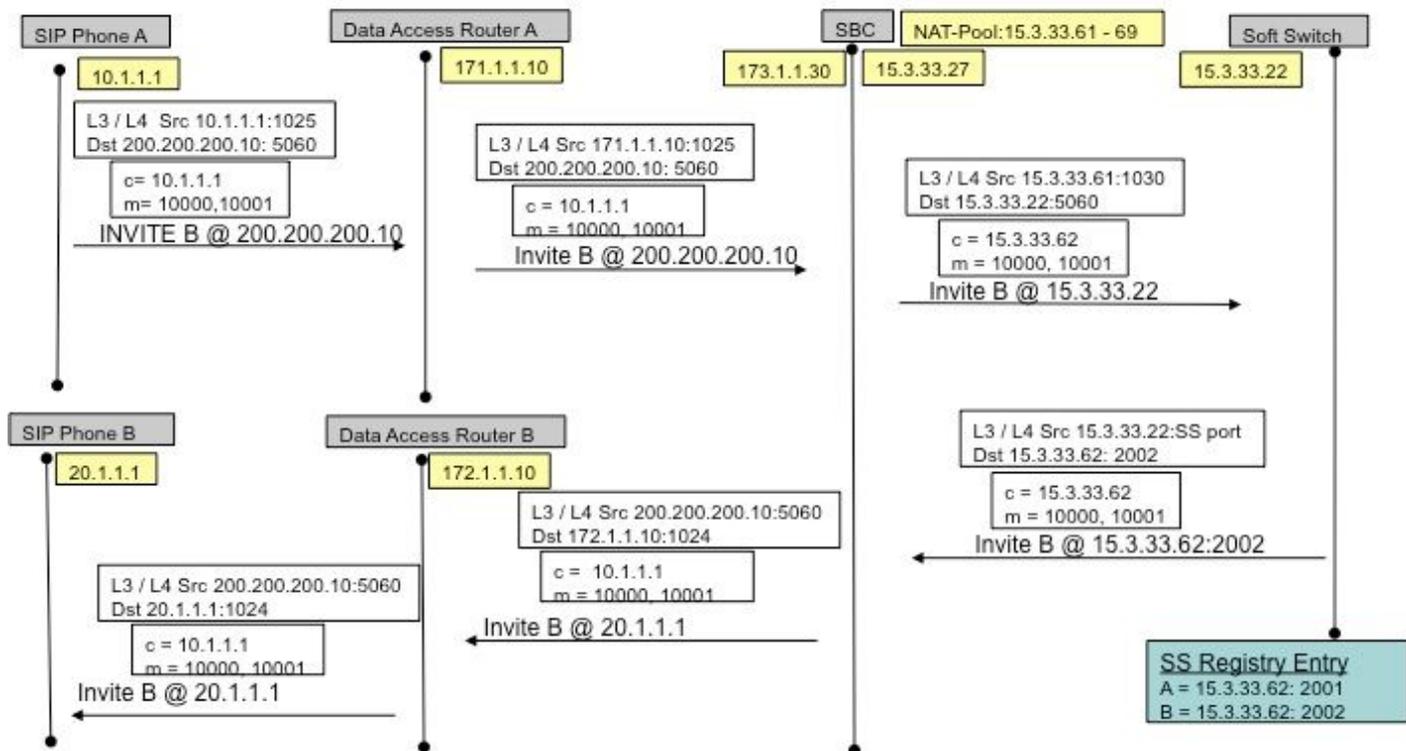


圖13

Call Flow – Media Flow-Around (Cont' d) Phone A Calls Phone B

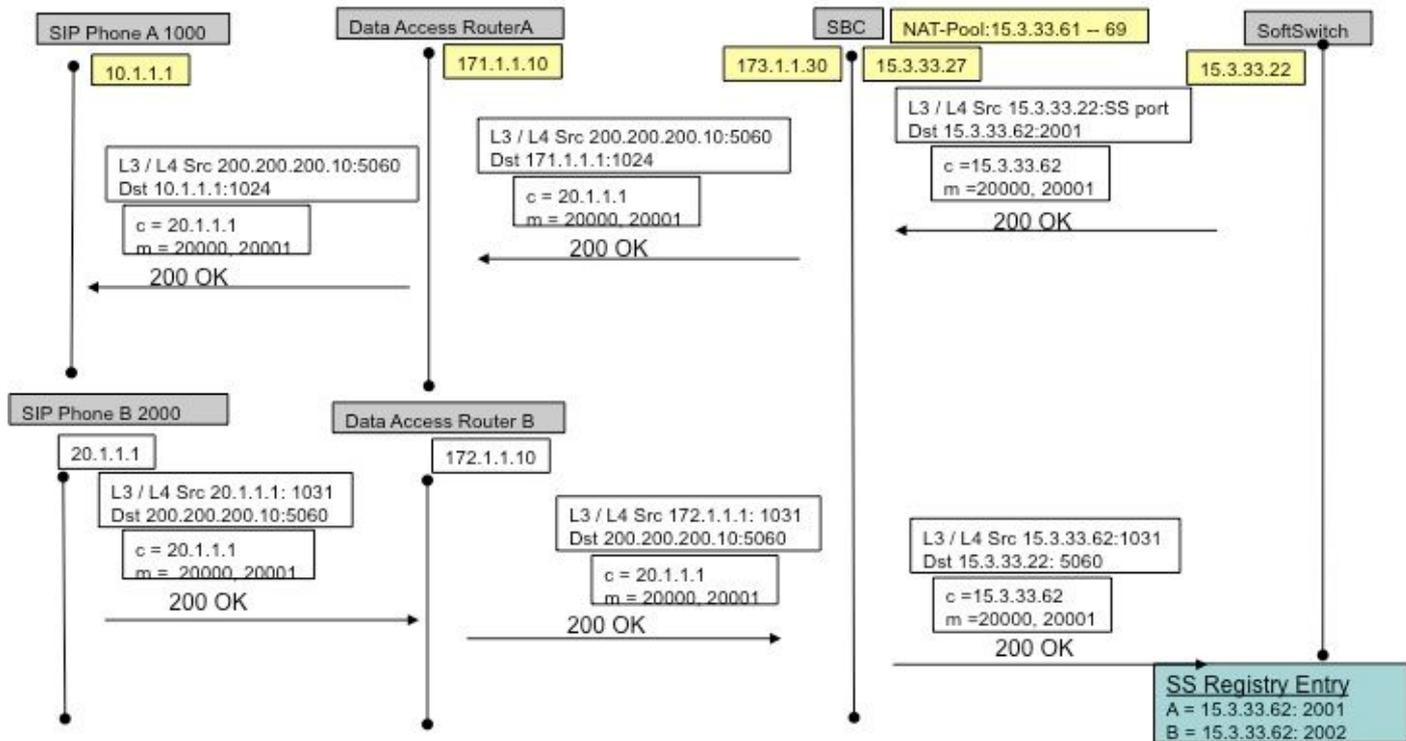


圖14

SIP註冊

在早期版本(SBC NAT)中，SIP終端必須傳送`keep-alive`資料包，以保持SIP註冊針孔開啟（允許流出>傳入流量，例如入站呼叫）。`keep-alive`資料包可以是終端或註冊器（軟交換機）傳送的任何SIP資料包。最新版本不再需要此功能，因為NAT-SBC本身（相對於軟交換機）會強制終端頻繁重新註冊，以使針孔保持開啟。

附註：註冊針孔失效的症狀可能難以發現，隨機呼叫信令失敗。

CUSP

CUSP具有邏輯網路的概念，它是指對本地介面進行類似處理(例如 介面、埠、用於偵聽的傳輸)路由目的。在CUSP上配置邏輯網路時，可以將其配置為使用NAT。配置後，SIP ALG將自動啟用。這在特定邏輯網路時很有用。

疑難排解

症狀

一個明顯的症狀可能是呼叫在一個或兩個方向上失敗。不太明顯的症狀可能包括，

- 單向音訊
- 傳送時的單向音訊
- 單向音訊
- 丟失SIP註冊

Show和debug命令

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

要檢查的事項

- 確保配置包括`ip nat inside` 或 `ip nat outside` 介面子命令。這些命令在介面上啟用NAT，而內部/外部指定非常重要。
- 對於靜態NAT，請確保`ip nat source static` 命令首先列出內部本地地址，然後列出內部全域性IP地址。
- 對於動態NAT，請確保在進行NAT轉換之前，配置為匹配內部主機傳送的資料包的ACL與該主機的資料包匹配。例如，如果內部本地地址10.1.1.1應轉換為200.1.1.1，請確保ACL匹配源地址10.1.1.1，而不是200.1.1.1。
- 對於沒有PAT的動態NAT，請確保池具有足夠的IP地址。地址不足的症狀包括`show ip nat statistics` 命令輸出中的第二個未命中計數器的值不斷增大，以及在動態轉換清單中看到NAT池中定義範圍內的所有地址。
- 對於PAT，很容易忘記在`ip nat inside source list` 命令上新增`overload` 選項。如果沒有它，NAT可以工作，但PAT不起作用，通常會導致使用者的資料包無法轉換，主機無法訪問

Internet。

- 可能正確配置了NAT，但其中一個介面上存在ACL，丟棄了資料包。請注意，對於進入介面的資料包，IOS在NAT之前處理ACL，對於從介面離開的資料包轉換地址之後處理ACL。
- 不要忘記在面向WAN的介面上配置「ip nat outside」（即使沒有轉換外部地址）！
- 配置NAT後，show ip nat translations不會顯示任何內容。Ping一次，然後再次檢查。
- 在NAT-SBC的內部和外部介面上捕獲wireshark跟蹤

案例

下面顯示了幾種情況的調試輸出。它們基本上不言自明！

基本NAT

基本NAT的配置和調試行如下所示。

```
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

顯示debug ip nat sip的輸出行。在這種情況下，傳出資料包上的嵌入式IP地址將被轉換。

```
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:
```

參考資料

概觀:

- http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html
- 解剖學 : 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和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功能表

- 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

託管的NAT穿越：

- 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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。