

# VoIP의 NAT

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[고정 NAT](#)

[동적 NAT](#)

[NAT 오버로드\(PAT\)](#)

[NAT 명령 옵션](#)

[NAT 핀홀](#)

[VoIP의 NAT](#)

[알그](#)

[게이트웨이](#)

[CME](#)

[로컬](#)

[로컬에서 원격으로](#)

[원격 재택근무자](#)

[공용 원격 전화\(읽기: 라우팅 가능\) IP 주소](#)

[개인 IP 주소가 있는 원격 전화](#)

[원격 SIP 전화](#)

[입방체](#)

[호스팅된 NAT 통과](#)

[NAT SBC](#)

[디자인 노트](#)

[설정](#)

[SBC NAT를 사용한 통화 흐름](#)

[SIP 등록](#)

[교두](#)

[문제 해결](#)

[증상](#)

[Show 및 debug 명령](#)

[확인 사항](#)

[시나리오](#)

[기본 NAT](#)

[SIP ALG](#)

[참조](#)

## 소개

이 문서에서는 CUBE(Cisco Unified Border Element), CME 또는 CUCME(Cisco Unified

Communications Manager Express), 게이트웨이 및 CUSP(Cisco Unified SIP Proxy)로 작동하는 라우터의 NAT(Network Address Translation) 동작에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SIP(Session Initiation Protocol)
- VoIP(인터넷 프로토콜)
- 라우팅 프로토콜

### 사용되는 구성 요소

이 문서의 정보는

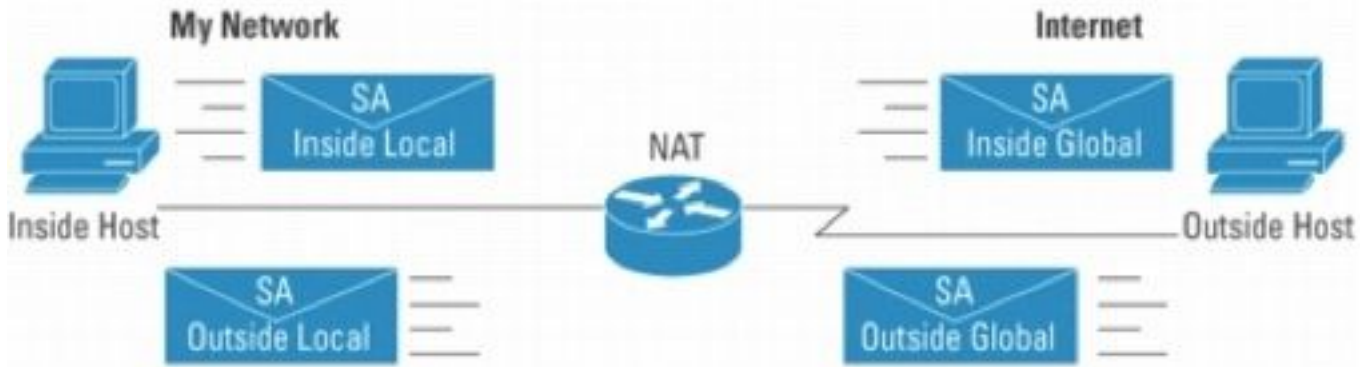
- 모든 IOS 버전 12.4T 이상
- 모든 CME 버전

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

Network Address Translation은 서로 다른 주소 공간을 사용하여 네트워크 간에 흐르는 패킷의 IP 주소를 변환하는 데 일반적으로 사용되는 기술입니다. 이 문서의 목적은 NAT를 검토하는 것이 아닙니다. 이 문서에서는 NAT가 Cisco의 VoIP 네트워크에서 사용될 때 이에 대한 종합적인 검토를 제공합니다. 또한 MS-Voice 기술을 구성하는 구성 요소로 범위가 제한됩니다.

- NAT는 기본적으로 패킷 내의 IP 주소를 다른 IP 주소로 교체합니다
- 사설 서브넷의 여러 호스트가 단일 공용 IP 주소를 공유(예: 처럼 표시)하여 인터넷에 액세스할 수 있도록 합니다.
- 일반적으로 NAT 컨피그레이션은 내부 호스트의 IP 주소만 변경합니다
- NAT는 양방향입니다. A가 내부 인터페이스에서 B로 변환되면 외부 인터페이스에 도착하는 B는 A!
- RFC1631



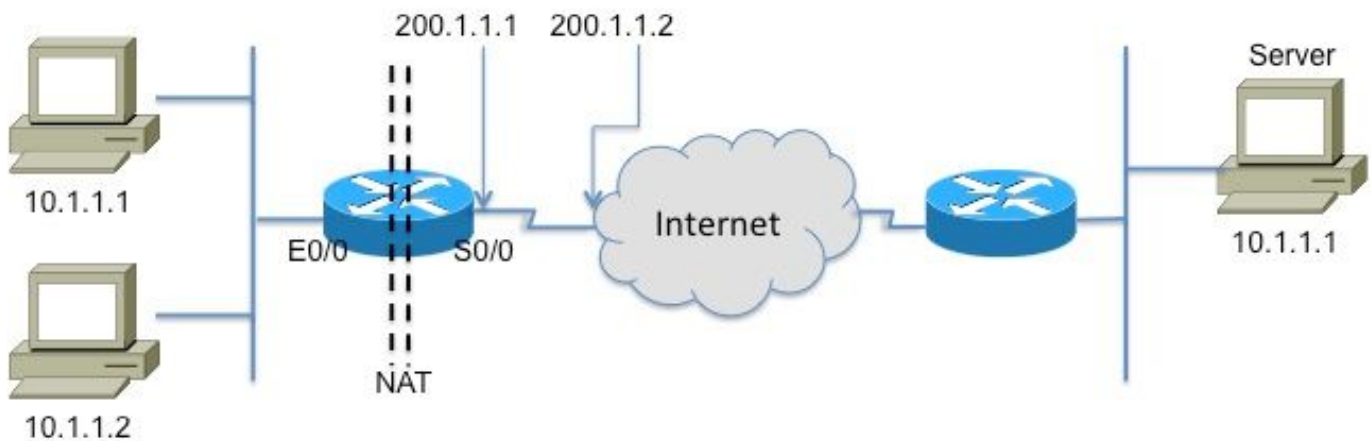
An IP address is either local or global  
 Local IP addresses are seen in the inside network  
 Global IP addresses are seen in the Outside network

그림 1

참고: NAT를 사설 주소 공간을 사용하여 네트워크 안팎으로 IP 패킷을 라우팅하는 데 도움이 될 수 있습니다. 즉, NAT는 라우팅 불가능한 주소를 라우팅 가능하게 만듭니다

그림 2는 다음 그림에서 참조하는 토폴로지를 보여줍니다.

Registered Subnet: 200.1.1.0, Mask 255.255.255.252



Inside

Outside

그림 2

이 용어집은 NAT를 이해하고 설명하는 데 필수적입니다

- **Inside local address**(내부 로컬 주소) - 내부 네트워크의 호스트에 할당된 IP 주소입니다. 일반적으로 주소는 전용 주소 공간에서 옵니다.
- **Inside global address**(내부 전역 주소) - NIC 또는 서비스 공급자가 할당한 라우팅 가능한 IP 주소로서 외부에 대한 하나 이상의 내부 로컬 IP 주소를 나타냅니다.
- **Outside local address**(외부 로컬 주소) - 내부 네트워크에 나타나는 외부 호스트의 IP 주소입니다.

- 다. 반드시 합법적인 주소일 필요는 없으며 내부에서 라우팅 가능한 주소 공간에서 할당됩니다.
- **Outside global address**(외부 전역 주소) - 호스트 소유자가 외부 네트워크의 호스트에 할당한 IP 주소입니다. 주소는 전역 라우팅 가능한 주소 또는 네트워크 공간에서 할당됩니다.

**참고:** 이 약관을 숙지하십시오. NAT의 모든 메모 또는 문서는 해당 항목을 참조해야 합니다

## 고정 NAT

이는 가장 간단한 형식의 NAT로서, 각 내부 주소에서 외부 주소로(또는 그 반대로) 정적으로 변환됩니다.

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

그림 3

위 변환을 위한 컨피그레이션에 대한 CLI는 다음과 같습니다

인터페이스 Ethernet0/0

ip 주소 10.1.1.3 255.255.255.0

ip nat 내부

!

인터페이스 Serial0/0

ip 주소 200.1.1.251 255.255.255.252

ip nat outside ← 필수![\[2\]](#)

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

## 동적 NAT

동적 NAT에서 각 내부 호스트는 주소 풀의 주소에 매핑됩니다.

- 내부 전역 주소 풀에서 IP 주소를 할당합니다.
- 새 패킷이 또 다른 내부 호스트에서 도착하고 NAT 항목이 필요하지만 풀링된 모든 IP 주소가 사용 중인 경우 라우터는 패킷을 무시합니다.
- 기본적으로 내부 글로벌 주소의 풀은 인터넷을 동시에 사용해야 하는 동시 호스트의 최대 개수 만큼 커야 합니다

다음 CLI는 동적 NAT 구성을 보여줍니다

```
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 오버로드(PAT)

풀(IP 주소)이 변환해야 하는 주소 세트보다 작으면 이 기능이 유용합니다.

- 하나 또는 소수의 외부 주소에만 NAT되는 여러 내부 주소
- PAT(Port Address Translation)는 내부 **글로벌** IP 주소에서 고유한 소스 포트 번호를 사용하여 변환을 구분합니다. 포트 번호는 16비트로 인코딩되므로 이론상 총 IP 주소당 최대 65,536개일 수 있습니다. PAT는 원래 소스 포트를 유지하려고 시도합니다. 이 소스 포트가 이미 할당된 경우 PAT는 사용 가능한 첫 번째 포트 번호를 찾으려고 시도합니다
- NAT 오버로드는 65,000개 이상의 포트를 사용할 수 있으므로 많은 등록된 IP 주소 없이(대부분의 경우 하나의 외부 글로벌 IP 주소만 필요) 원활하게 확장할 수 있습니다.

그림 4는 PAT를 보여줍니다.

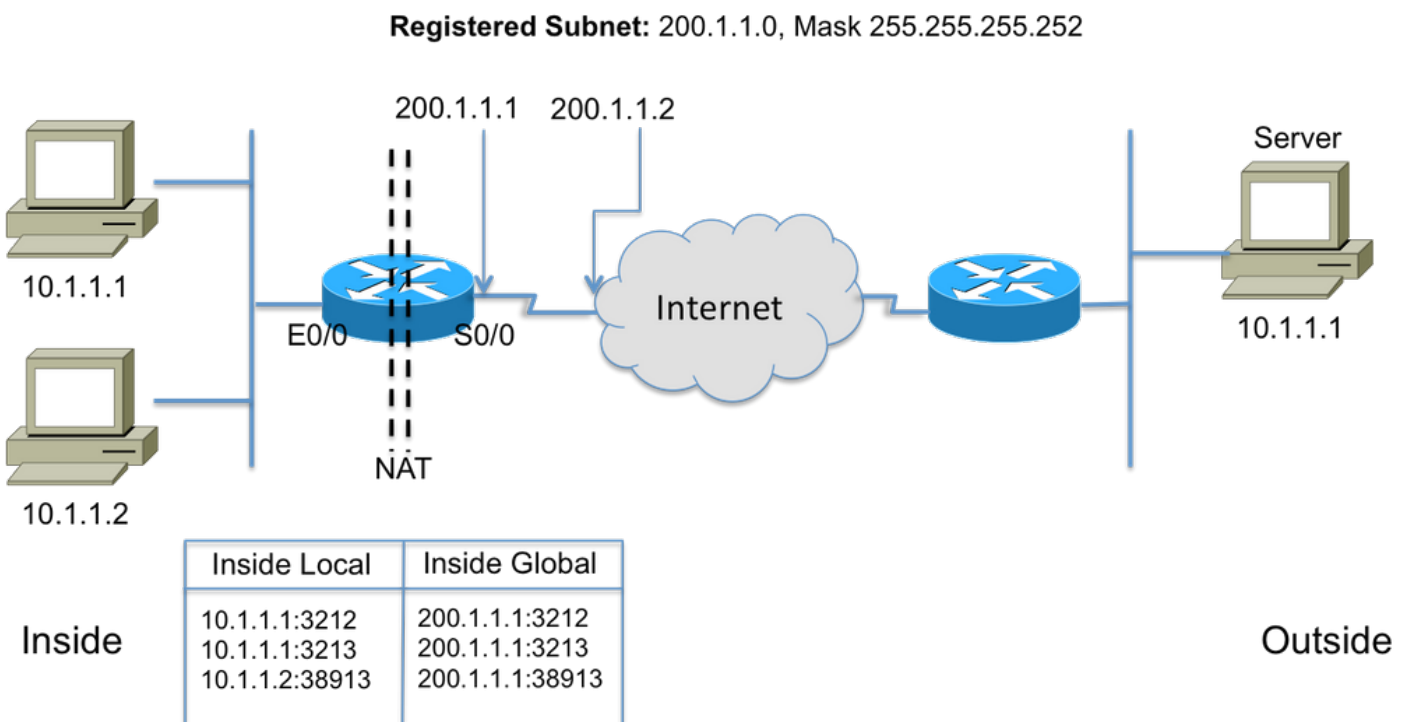


그림 4

## NAT 명령 옵션

Cisco NAT 구현은 다양한 옵션과 매우 다용적입니다. 몇 가지 개선 사항이 아래에 나열되어 있지만, 전체 개선 사항 [목록](http://www.cisco.com)에 대한 자세한 내용은 [http:// www.cisco.com](http://www.cisco.com)

/en/US/partner/technologies/tk648/tk361/tk438/technologies\_white\_paper09186a0080091cb9.html  
을 참조하십시오.

- 포트를 통한 정적 변환 - 특정 포트로 주소가 지정된 수신 패킷(예: 포트 25(SMTP 서버의 경우))가 특정 서버로 전송되었습니다.
- 경로 맵 지원 - 필터/ACL 구성의 유연성
- 더 유연한 풀 컨피그레이션 - 주소의 불연속 범위를 허용합니다.
- 호스트 번호 보존 - "네트워크" 부분을 변환하고 "호스트" 부분을 보존합니다.

## NAT 핀홀

NAT 패런스의 핀홀은 <host IP, port> 및 <global address, global port> 튜플 간의 매핑을 의미합니다. 이를 통해 NAT 디바이스는 수신 메시지의 목적지 포트 번호(글로벌 포트)를 사용하여 목적지를 세션을 시작한 호스트 IP 및 포트에 다시 매핑할 수 있습니다. 사용하지 않는 기간이 지나면 핀홀이 시간 초과되고 공용 주소가 NAT 풀로 반환된다는 점에 유의해야 합니다.

## VoIP의 NAT

그렇다면 VoIP 네트워크의 NAT와 관련된 문제와 우려 사항은 무엇입니까? 지금까지 설명한 NAT(기본 NAT라고도 함)는 IP 패킷 헤더의 IP 주소를 변환하고 체크섬을 다시 계산하지만, VoIP 시그널링은 시그널링 메시지의 본문에 포함된 주소를 전달합니다. 즉, 레이어 5에서

그림 5는 임베디드 IP 주소를 변환하지 않은 상태로 두는 효과를 보여줍니다. 통화 신호 처리가 성공적으로 완료되지만 서비스 공급자의 SIP 프록시가 RTP(미디어) 패킷을 통화 에이전트가 전송한 미디어 주소로 라우팅하지 못합니다.

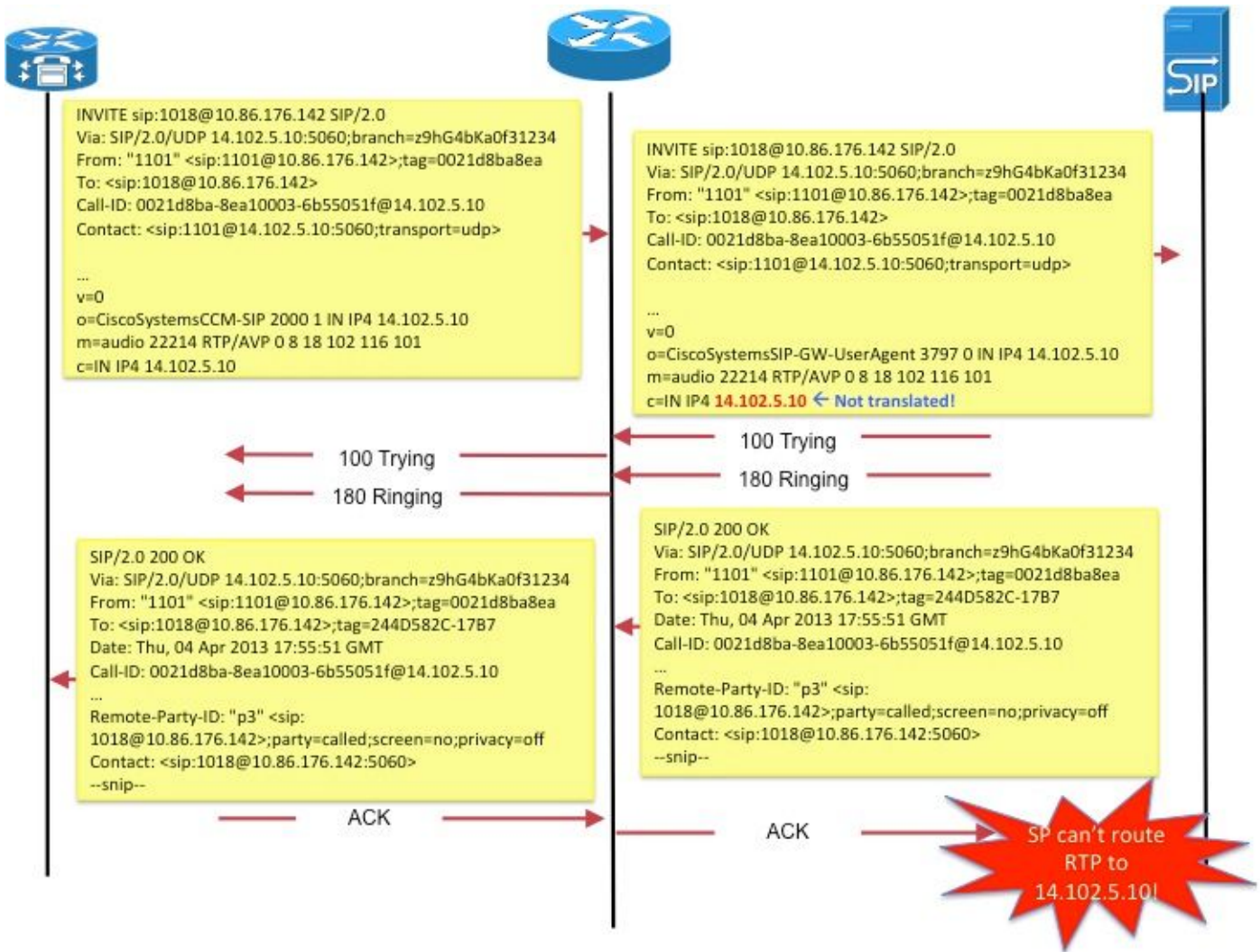


그림 5

또 다른 예는 SIP 엔드포인트의 **연락처** 사용입니다. SDP의 필드입니다. 새 요청에 대한 신호 메시지를 받을 엔드포인트의 주소입니다.

이러한 문제는 ALG(Application Layer Gateway)라는 기능으로 해결됩니다.

## 알그

ALG는 지원하는 특정 애플리케이션(예: SIP)에서 사용하는 프로토콜을 이해하며, 이를 통해 트래픽을 "고정"하고 패킷 검사를 수행합니다. SIP 통화 시그널링에 대한 다양한 필드의 고정 방식에 대한 자세한 내용은 <http://www.voip-info.org/wiki/view/Routers+SIP+ALG>를 **참조하십시오**.

Cisco 라우터에서 ALG SIP 지원은 기본적으로 표준 TCP 포트 5060에서 활성화됩니다. SIP 시그널링용 비표준 포트를 지원하도록 ALG를 구성할 수 있습니다. [http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr\\_nat/configuration/15-mt/nat-tcp-sip-alg.html](http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html)을 **참조하십시오**.

**주의:** 주의! 다양한 VoIP 프로토콜에 대해 어떤 임베디드 필드를 변환해야 하는지 알려주는 RFC 또는 기타 표준은 없습니다. 그 결과, 장비 공급업체마다 구현이 다르므로 interoper 문제 (및 TAC 사례)가 발생합니다.

## 게이트웨이



게이트웨이는 정의상 ip-to-ip 디바이스가 아니므로 NAT를 적용할 수 없습니다.

## CME

이 섹션에서는 NAT를 사용해야 하는 이유를 파악하기 위해 CME를 사용하는 통화 시나리오를 검토합니다.

시나리오 1. 로컬 전화

시나리오 2. 원격 전화(공용 IP 주소 포함)

시나리오 3. 원격 재택근무자

**참고:** 모든 경우 오디오가 흐르려면 CME IP 주소를 라우팅 가능해야 합니다

## 로컬

이 시나리오(그림 6)에서는 통화에 포함된 두 개의 전화기가 개인 IP 주소가 있는 마른 전화기입니다.



그림 6

**참고:** 동일한 CME 시스템의 다른 스키니 폰과의 통화에서 연결된 스키니 폰은 미디어 패킷을 다른 폰으로 직접 전송합니다. 즉, 로컬 폰에서 로컬 폰으로의 RTP가 CME를 통해 흐르지 않습니다.

따라서 이 경우에는 NAT가 적용되지 않거나 필요하지 않습니다.

**참고:** CME는 통화에 포함된 두 전화기가 모두 마른 전화기와 동일한 네트워크 세그먼트에 있는지 여부에 따라 미디어(RTP)가 직접 실행되어야 하는지 여부를 결정합니다. 그렇지 않으면 CME가 RTP 경로에 삽입됩니다.

## 로컬에서 원격으로

이 시나리오(그림 7)에서는 CME가 RTP 스트림에 삽입되므로 전화기의 RTP가 CME에서 종료됩니다. CME는 스트림을 다른 전화기로 다시 시작합니다. CME는 내부(사설) 네트워크와 외부 네트워크



크에 모두 위치하여 내부 주소를 내부 전화기로 보내고 외부(공용) 주소를 외부 전화기로 보내기 때문에 여기서도 NAT가 필요하지 않습니다.

그러나 원격 IP Phone과 CME 소스 IP 주소 간에 UDP/TCP 포트(신호 및 RTP)가 열려 있어야 합니다. 이는 방화벽 또는 기타 필터링 장치가 문제의 포트를 허용하도록 구성되었음을 의미합니다.

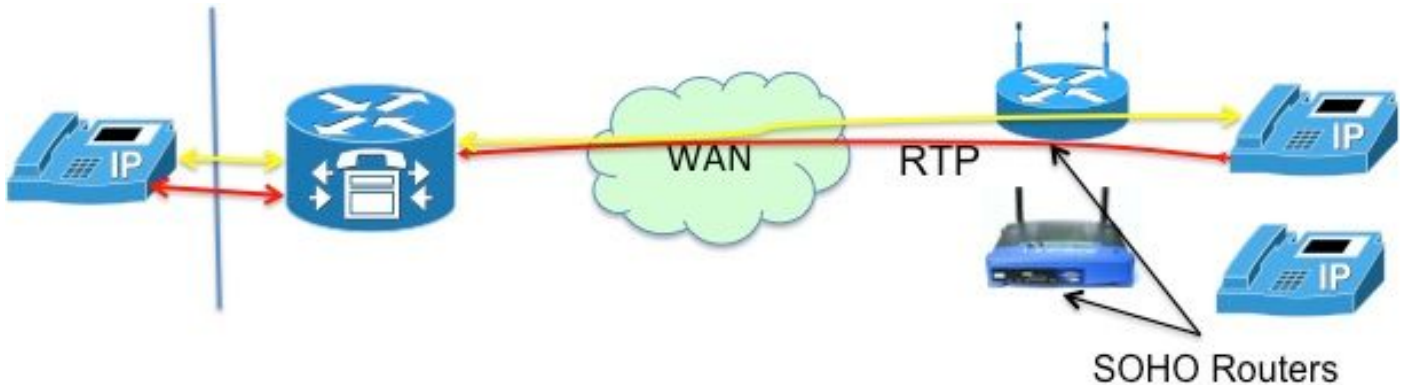


그림 7

참고: 신호 [메시지]는 항상 CM에서 종료됩니다.

## 원격 재택근무자

이는 CME 라우터에서 멀리 떨어진 사무실이 있는 재택근무자를 지원하기 위해 WAN을 통해 CME에 연결하는 IP 전화를 말합니다. 가장 일반적인 설계는 라우팅 가능한 IP 주소가 있는 전화기와 전용 IP 주소가 있는 전화기가 포함된 것입니다.

### 공용 원격 전화(읽기: 라우팅 가능) IP 주소

통화에 포함된 두 전화기 모두 라우팅 가능한 공용 IP 주소로 구성된 경우 전화기 간에 미디어가 직접 흐를 수 있습니다(그림 8). 따라서 다시 한 번 NAT가 필요 없습니다!

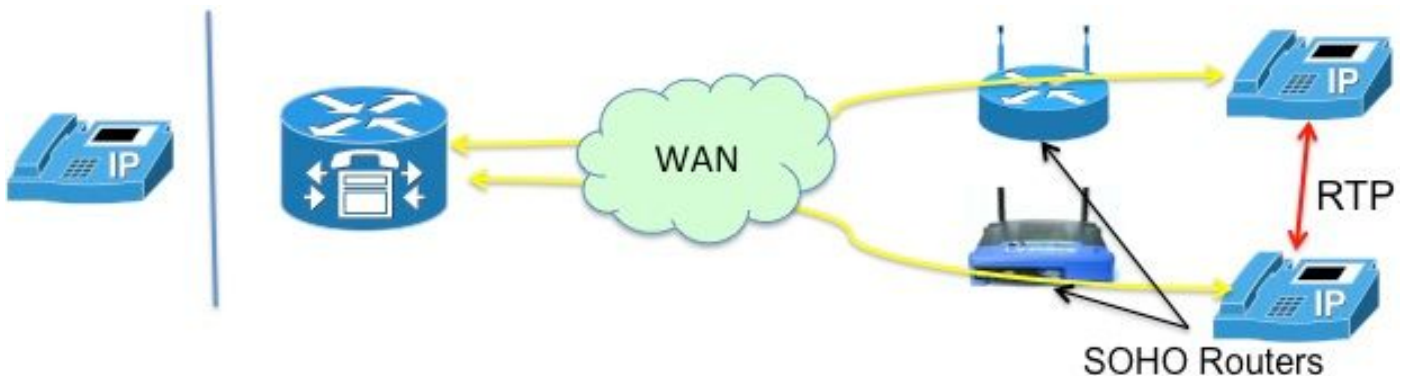


그림 8

### 개인 IP 주소가 있는 원격 전화

이 시나리오에서 통화는 개인 IP 주소로 구성된 skinny phone 사이에서 신호를 보냅니다. 홈 오피스(SOHO) 라우터는 일반적으로 "SCCP 인식"이 되지 않는 경향이 있습니다. 즉, SCCP 메시지에 포함된 IP 주소를 변환할 수 없습니다. 즉, 통화 설정이 완료되면 전화기가 서로의 개인 IP 주소로

종료됩니다. 두 전화기 모두 비공개이므로 CME는 오디오가 전화기 간에 직접 흐르도록 둘 사이의 통화를 시그널링합니다. 그러나 다음과 같은 해결 방법 중 하나가 구현되지 않는 한 단방향 또는 비양방향 오디오가 발생합니다(정의상 사실 IP 주소는 인터넷에서 라우팅할 수 없기 때문).

·SOHO 라우터에서 고정 경로 구성

·전화기에 대한 IPsec VPN 연결 설정

이를 해결하는 더 좋은 방법은 "mtp"를 구성하는 것입니다. mtp 명령은 원격 전화기의 미디어(RTP) 패킷이 CME 라우터를 통해 전달되도록 합니다(그림 9).

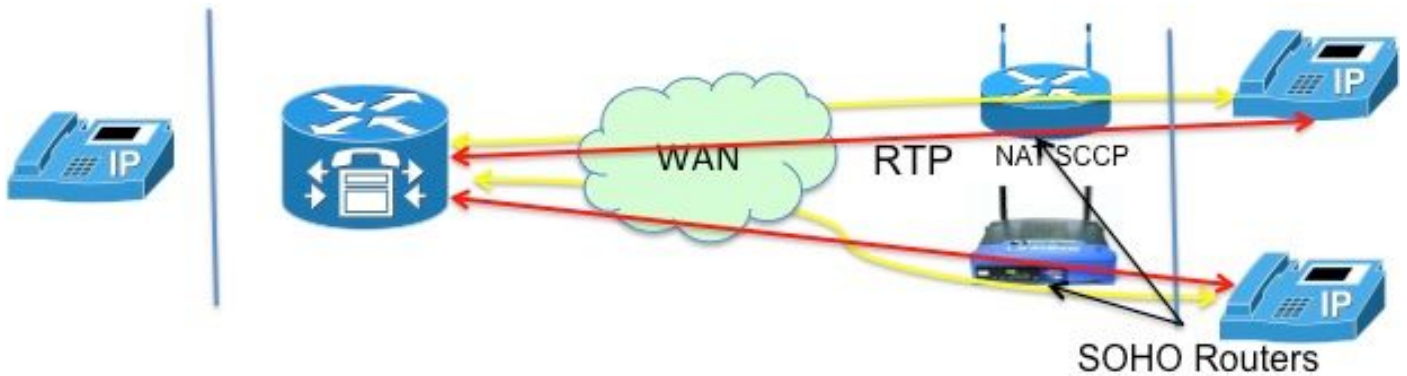


그림 9

"mtp" 솔루션은 방화벽 포트 개방과 관련된 복잡성 때문에 더 우수합니다. WAN을 통해 흐르는 미디어 패킷은 방화벽에 의해 차단될 수 있습니다. 즉, 방화벽에서 포트를 열어줘야 하지만 어떤 포트가 필요합니까? CME가 오디오를 릴레이하면 RTP 패킷을 전달하도록 방화벽을 쉽게 구성할 수 있습니다. CME 라우터는 미디어 패킷에 특정 UDP 포트(2000!)를 사용합니다. 따라서 포트 2000에서 들어오고 나가는 패킷만 허용하면 모든 RTP 트래픽을 전달할 수 있습니다.

그림 10은 mtp 구성 방법을 보여줍니다.

```

1
mac 1111.2222.3333

7965

mtp

1:1

```

그림 10

모든 것이 mtp로 훌륭하지 않습니다. mtp가 바람직하지 않을 수 있는 상황이 있다

- MTP는 CPU 사용률이 낮지 않음
- 멀티캐스트 MOH는 일반적으로 WAN을 통해 전달될 수 없습니다. - 멀티캐스트 MOH 기능은 MTP가 전화기에 대해 활성화되었는지 확인하고, 활성화된 경우 MOH를 해당 전화기로 전송하지 않습니다.

따라서 멀티캐스트 패킷을 전달할 수 있는 WAN 컨피그레이션이 있고 방화벽을 통해 RTP 패킷을 허용할 수 있는 경우 MTP를 사용하지 않기로 결정할 수 있습니다.

## 원격 SIP 전화

SIP 전화기는 위 시나리오에서 언급되지 않았습니다. 전화기 중 하나가 SIP 전화기인 경우 CME가 오디오 경로에 삽입되기 때문입니다. 그러면 앞에서 설명한 로컬-원격 시나리오가 되며, 여기서 NAT는 필요하지 않습니다.

## 입방체

CUBE는 모든 세션을 종료하고 다시 시작할 때 NAT 및 PAT 기능을 기본적으로 수행합니다. CUBE는 자체 주소를 통신하는 엔드포인트의 주소로 대체하므로 해당 엔드포인트의 주소를 효과적으로 숨깁니다(변환).

따라서 NAT는 CUBE 기능과 함께 필요하지 않습니다. 다음 섹션에 설명된 대로 CUBE에 NAT가 필요한 VoIP 서비스 시나리오가 있습니다.

## 호스팅된 NAT 통과

호스티드 텔레포니 서비스에 대한 간략한 배경은 이 기능의 이유를 이해하는 데 도움이 될 것입니다.

호스티드 텔레포니 서비스는 대부분의 장비가 통신 사업자의 위치에 상주하는 새로운 형태의 VoIP 서비스입니다. 기본 NAT(예: L3/L4의 NAT)만 구현하는 홈 게이트웨이(HGW)와 함께 작동합니다. 예를 들어 Verizon은 가정에서 FiOS 서비스를 제공하는 ONT(Optical Network Terminal)를 설치합니다. 음성 통화는 ONT에 내장된 SIP 프로세스를 사용하여 신호를 보냅니다. SIP 시그널링은 Verizon의 프라이빗 IP 네트워크를 통해 다른 FiOS Digital Voice 고객 또는 기존 전화 고객에게 음성 통신을 설정하는 서비스와 제어를 제공하는 새로운 소프트웨어 스위치에 전달됩니다.

호스티드 텔레포니 서비스의 주요 공급자 요구 사항에는 다음이 포함됩니다.

- 원격 NAT 통과: nat(NAT 레이어 3!만 가능) 및 방화벽 디바이스를 사용하여(원격으로 "ALG"를 수행하여) 엔드포인트에 클래스 5 서비스를 제공하는 기능!
- 공동 미디어 지원: IP 네트워크로 미디어를 다시 라우팅하는 것이 적합하지 않은 경우, 함께 배치된 디바이스 간에 미디어를 전송하는 기능
- 추가된 장비가 없으므로 CPE를 추가할 필요가 없습니다.

위에서 설명한 대로, 그러한 서비스를 구현하기 위한 옵션은 무엇입니까?

- HGW를 값비싼 ALG로 교체하고
- 패킷의 포함된 SIP 헤더를 수정하려면 SBC(Session Border Controller)를 사용합니다. 여기에는 매우 안전한 내결함성 구성에서 SIP를 지원하는 네트워크 호스팅 캐리어급 제품이 포함됩니다. 이 솔루션을 NAT SBC라고 합니다.

NAT SBC 옵션은 위에 나열된 공급자 요구 사항을 충족합니다.

## NAT SBC

NAT SBC는 다음과 같이 작동합니다(그림 11)

1. 액세스 라우터는 L3/L4 IP 주소만 변환합니다
2. SIP 메시지의 IP 주소가 변환되지 않음

3. SBC NAT는 포함된 IP 주소를 가로채고 변환합니다. SBC에서 200.200.200.10으로 향하는 SIP 패킷을 확인하는 순간 nat-sbc 코드가 시작됩니다.
4. 미디어는 번역되지 않으며 전화기 간에 직접 이동됩니다[5]

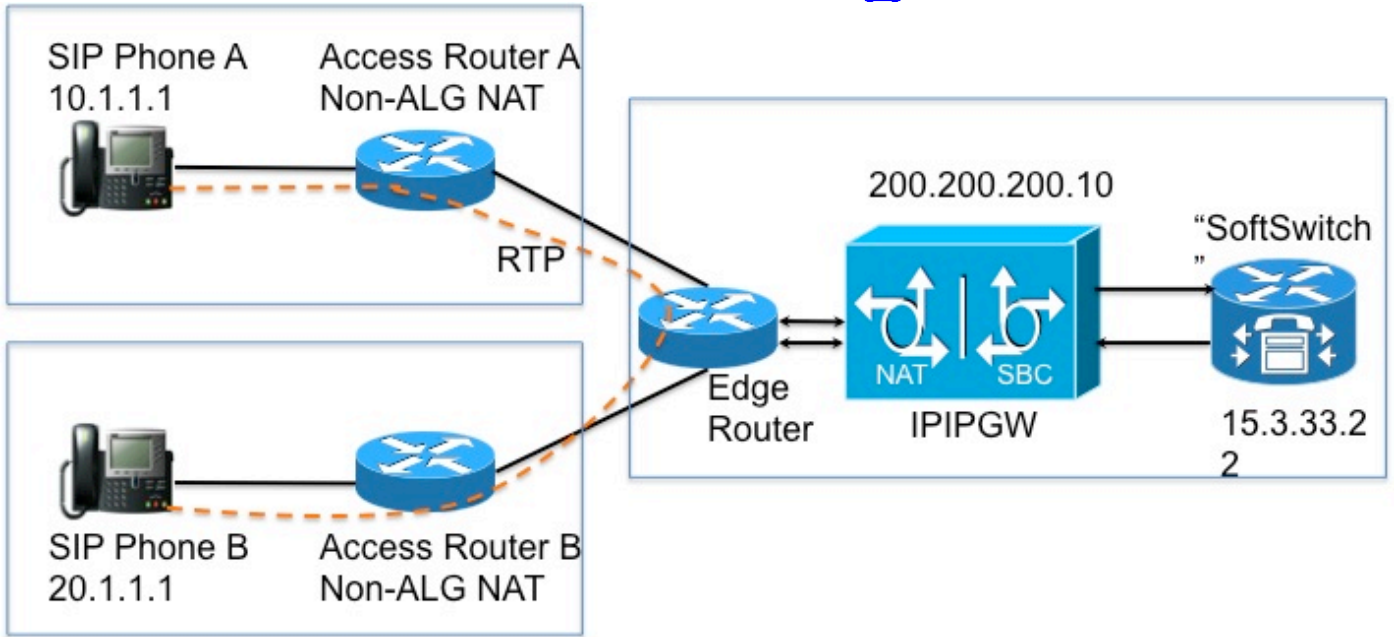


그림 11

## 디자인 노트

- IP 주소 200.200.200.10(그림 12)은 NAT SBC의 어떤 인터페이스에도 할당되지 않습니다. SIP Phone A 및 SIP Phone B가 신호 메시지를 보내는 "프록시"의 주소로 구성됩니다.
- 홈 디바이스는 특정 SIP/SDP 주소 전용 필드(예: Call-Id: , O= , 경고: headers & branch= 매개 변수. maddr= 및 received= 매개 변수는 특정 시나리오에서만 처리되었습니다.) 이러한 필드는 프록시-권한 부여 및 권한 부여 변환을 제외하고 NAT SBC에서 처리됩니다. 이러한 변환은 인증을 중단하기 때문입니다.
- 홈 디바이스가 PAT를 수행하도록 구성된 경우 사용자 에이전트(전화기 및 프록시)는 대칭 시그널링[6]과 대칭 및 조기 미디어를 지원해야 합니다. NAT SBC 라우터에서 재정의의 포트를 구성해야 합니다.
- 대칭 시그널링 및 대칭 및 조기 미디어가 지원되지 않는 경우 중간 라우터는 PAT 없이 구성해야 하며 재정의의 주소는 NAT SBC에서 구성해야 합니다.

## 설정

일반적인 NAT SBC의 샘플 컨피그레이션은 다음과 같습니다.

```
ip nat sip-sbc
    200.200.200.10 5060 15.3.33.22 5060  udp
call-id-pool call-id-pool
session-timeout 300
allow-flow-around
```

```
ip nat sbc1 15.3.33.61 15.3.33.69 255.255.0.0

ip nat sbc2 15.3.33.91 15.3.33.99 255.255.0.0

ip nat pool call-id-pool 1.1.1 1.1.255.254 255.255.0.0

ip nat 200.200.200.100 200.200.200.200 255.255.255.0

ip nat inside source list 1 sbc1

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
```

## SBC NAT를 사용한 통화 흐름

그림 13과 그림 14는 통화 흐름을 번역 측면에서 보여줍니다. 다음 사항에 유의해야 합니다.

- 등록 시 소프트웨어 스위치는 두 전화기를 다음과 같이 기록합니다.
  - SIP Phone A - 15.3.33.62 2001
  - SIP Phone B - 15.3.33.62 2002
- 이 통화 흐름에서 SBC NAT는 미디어 IP 주소를 변환되지 않은 상태로 효과적으로 돕니다.

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

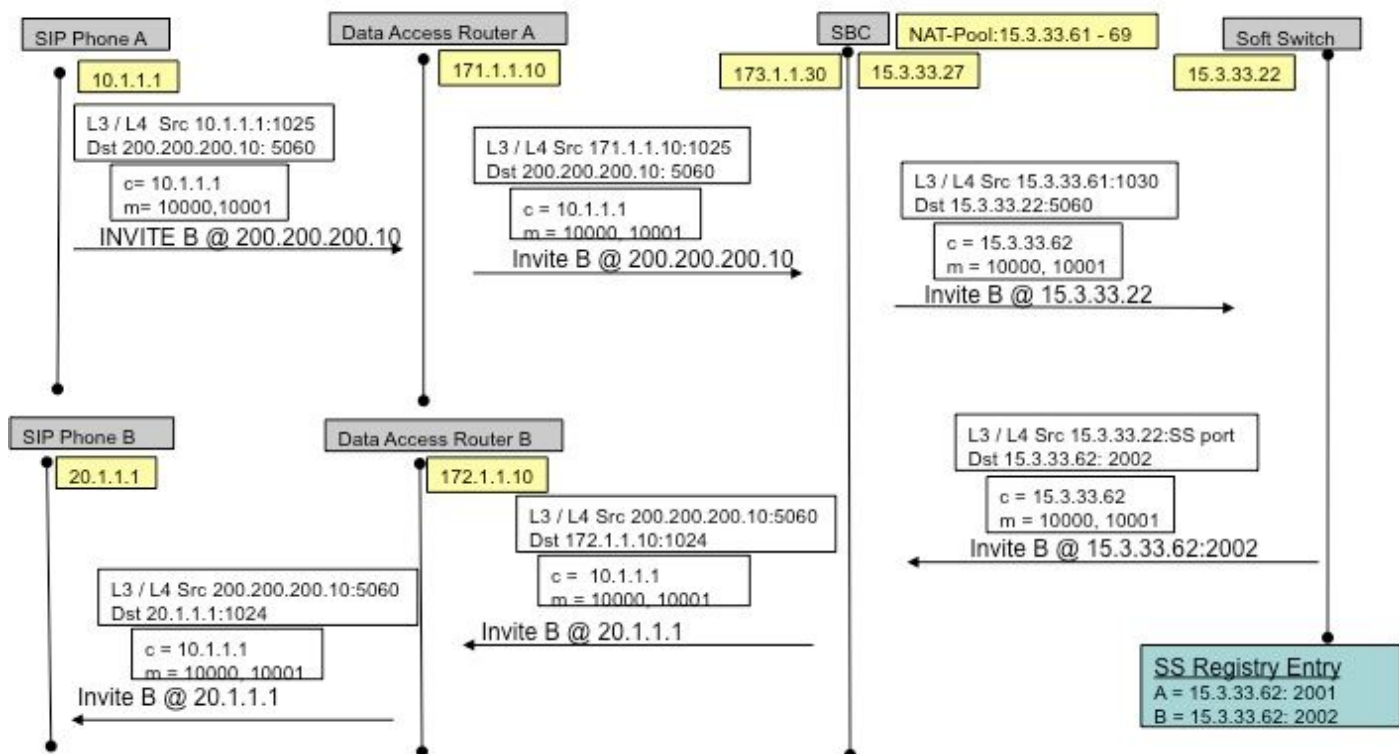


그림 13

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

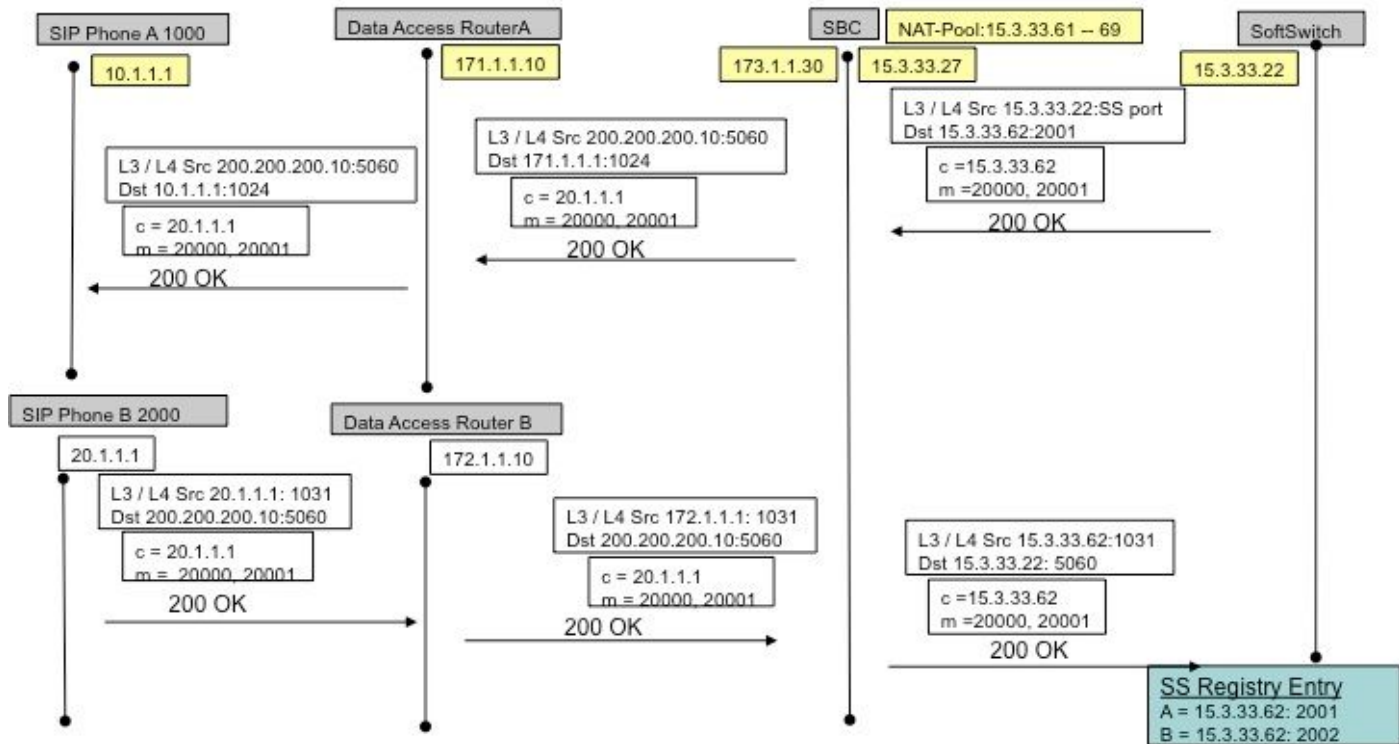


그림 14

## SIP 등록

이전 버전(SBC NAT)에서는 SIP 엔드포인트가 킵얼라이브 패킷을 보내 SIP 등록 핀홀을 열어 유지해야 합니다(아웃->인 트래픽의 흐름(예: 인바운드 통화) 허용). 킵얼라이브 패킷은 엔드포인트 또는 등록자(소프트 스위치)가 보낸 모든 SIP 패킷일 수 있습니다. 최근 버전에서는 NAT-SBC 자체(소프트 스위치와 반대)가 엔드포인트를 자주 재등록하여 핀홀이 열려 있도록 하므로 이러한 필요성이 없어졌습니다.

**참고:** 만료된 등록 핀홀의 증상은 모호할 수 있으며, 임의 통화 시그널링 실패가 발생할 수 있습니다.

## 교두

CUSP는 논리적 네트워크라는 개념이 있으며, 이는 (예: 인터페이스, 포트, 수신 목적의 전송) 라우팅 CUSP에서 논리적 네트워크를 구성할 때 NAT를 사용하도록 구성할 수 있습니다. 구성이 완료되면 SIP ALG가 자동으로 활성화됩니다. 이는 특정 논리적 네트워크에서 유용합니다.

## 문제 해결

### 증상

분명한 증상은 한 방향 또는 두 방향으로 통화가 실패하는 것일 수 있습니다. 덜 확실한 증상으로는

- 단방향 오디오
- 단방향 오디오 전송 중
- 무방향 오디오
- SIP 등록 손실

### Show 및 debug 명령

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

### 확인 사항

- 컨피그레이션에 `ip nat inside` 또는 `ip nat outside interface` 하위 명령이 포함되는지 확인합니다. 이러한 명령은 인터페이스에서 NAT를 활성화하며 내부/외부 지정이 중요합니다.
- 고정 NAT의 경우 `ip nat source static` 명령이 내부 로컬 주소를 먼저 나열하고 내부 전역 IP 주소를 두 번째로 나열하는지 확인합니다.
- 동적 NAT의 경우 NAT 변환이 발생하기 전에 내부 호스트에서 전송한 패킷과 일치하도록 구성된 ACL이 해당 호스트의 패킷과 일치하는지 확인합니다. 예를 들어 내부 로컬 주소 10.1.1.1을 200.1.1.1로 변환해야 하는 경우 ACL이 소스 주소 200.1.1.1이 아니라 10.1.1.1과 일치하는지 확인합니다.
- PAT가 없는 동적 NAT의 경우 풀에 충분한 IP 주소가 있는지 확인합니다. 주소가 충분하지 않으면 `show ip nat statistics` 명령 출력의 두 번째 miss 카운터에서 증가하는 값과 동적 변환 목록



의 NAT 풀에 정의된 범위의 모든 주소가 표시되는 증상이 나타납니다.

- PAT의 경우 **ip nat inside source list** 명령에서 **overload** 옵션을 추가하기가 쉽습니다. 이 기능이 없으면 NAT는 작동하지만 PAT는 작동하지 않으므로 사용자의 패킷이 변환되지 않고 호스트가 인터넷에 연결할 수 없는 경우가 많습니다.
- NAT가 올바르게 구성되었을 수 있지만 ACL이 인터페이스 중 하나에 있으므로 패킷이 삭제됩니다. IOS는 인터페이스에 들어오는 패킷에 대해 NAT 전에, 그리고 인터페이스에서 나가는 패킷에 대해 주소를 변환한 후에 ACL을 처리합니다.
- 외부 주소를 변환하지 않더라도 WAN을 향하는 인터페이스에 "ip nat outside"를 구성해야 합니다.
- NAT가 구성되는 즉시 show ip nat translations에 아무 것도 표시되지 않습니다. Ping을 한 번 실행한 다음 다시 확인합니다.
- NAT-SBC의 내부 및 외부 인터페이스에서 wireshark 추적 수집

## 시나리오

몇 가지 시나리오에 대한 디버그 출력이 아래에 나와 있습니다. 그들은 대부분 자명합니다!

## 기본 NAT

기본 NAT의 컨피그레이션 및 디버그 행은 아래에 나와 있습니다.

```
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

디버그 ip nat sip의 출력 줄이 표시됩니다. 이 경우 발신 패킷의 포함된 IP 주소가 변환됩니다.

```
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:
```

## 참조

### 개요:

- [http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies\\_white\\_paper09186a0080091cb9.html](http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html)
- 해부학: [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_7-3/anatomy.html](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](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml)

### VoiP 및 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 기능 매트릭스

- [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080b17919.shtml](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/technologies/tk648/tk361/tk438/technologies_white_paper09186a00801af2b9.html)
- [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080b17919.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919.shtml)

## 호스팅된 NAT 통과:

- [www.tmcnet.com/it/0804/FKagoor.htm](http://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.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](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/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](http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc_cucm.html)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.