



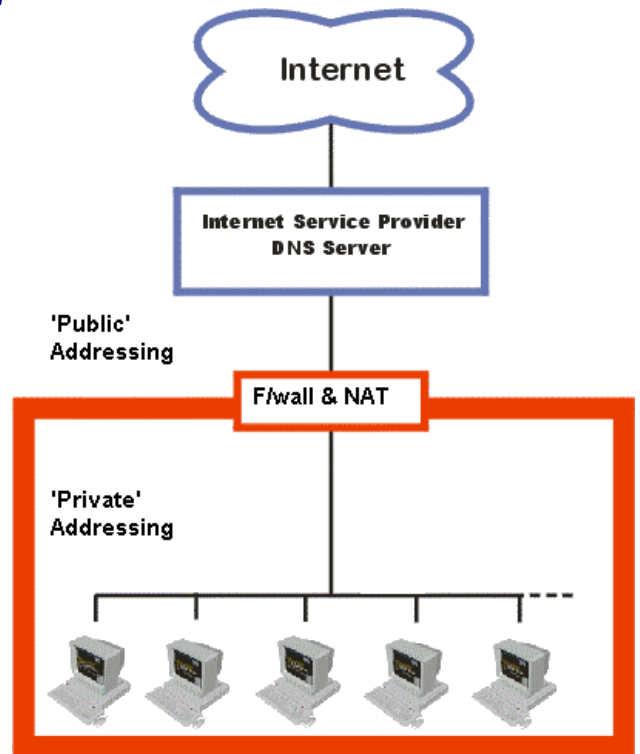
VoIP and Network Address Translation (NAT)

What is Network Address Translation (NAT)?

NAT stands for Network Address Translation. NAT resolves IP address conflicts by replacing unregistered addresses with registered ones in IP packets. Registered addresses are routable IP addresses over the internet (also referred to as **public** IP addresses). Unregistered, or **private** IP addresses are non-routable IP addresses.

NAT functionality is built into devices such as network routers, firewalls, ISDN routers and standalone NAT devices. NAT devices maintain state tables that map private IP addresses on one side of the devices to public addresses on the other side. See opposite diagram.

Most (if not all) enterprise businesses through to home individuals use NAT to provide IP address capacity behind NAT whilst allowing 'public' connectivity through NAT (an on demand, many to one type arrangement)



Types of NAT

There are effectively three kinds of NAT: **static NAT**, **pooled NAT** and **port-level NAT** (sometimes referred to as Port Address Translation, or PAT). Static NAT is the simplest to set up. Each host on the internal network is permanently mapped to an address on the external network. Pooled NAT defines a pool of addresses on the external network that are allocated dynamically to internal hosts. PAT maps internal connections to a single IP address on the external network, but with a TCP port number selected by the NAT device. Depending on what you want to accomplish, each strategy has advantages and disadvantages

NAT at work

- NATs work at Layer 3 (IP layer)
- NATs modify the source/destination IP address
- NATs do not modify Layer 4, Layer 5, Layer 6, and Layer 7 addresses embedded within the IP Payload
- Many applications (like VoIP) embed IP addresses at Layer 4 through Layer 7
- NAT breaks the end-to-end model of IP for routability, encryption, and so on, due to the embedded Layer 4 through Layer 7 IP addresses

VoIP and NAT – The Problem

Like other applications, VoIP (H.323 and SIP), embed IP addresses above layer 3 (headers and payload). As NAT only modifies IP addresses at layer 3, it cannot modify these addresses and a 'mismatch' occurs as a result. (see below).

```
value RasMessage = registrationRequest
{
  requestSeqNum 3923
  protocolIdentifier {0 0 8 2250 0 2 }
  discoveryComplete FALSE
  callSignalAddress
  {
  }
  rasAddress
  {
  ipAddress
  {
  ip '8DF52B03'H
  port 54338
  }
  }
  terminalType
  {
  mc FALSE
  undefinedNode FALSE
  }
  gatekeeperIdentifier ("Exl-GK")
  endpointVendor
}
```

Embedded IP addresses within H.323 signalling

141.245.43.3:54338
IP Address:Port embedded in H.323 signalling

Embedded IP addresses within SIP signalling

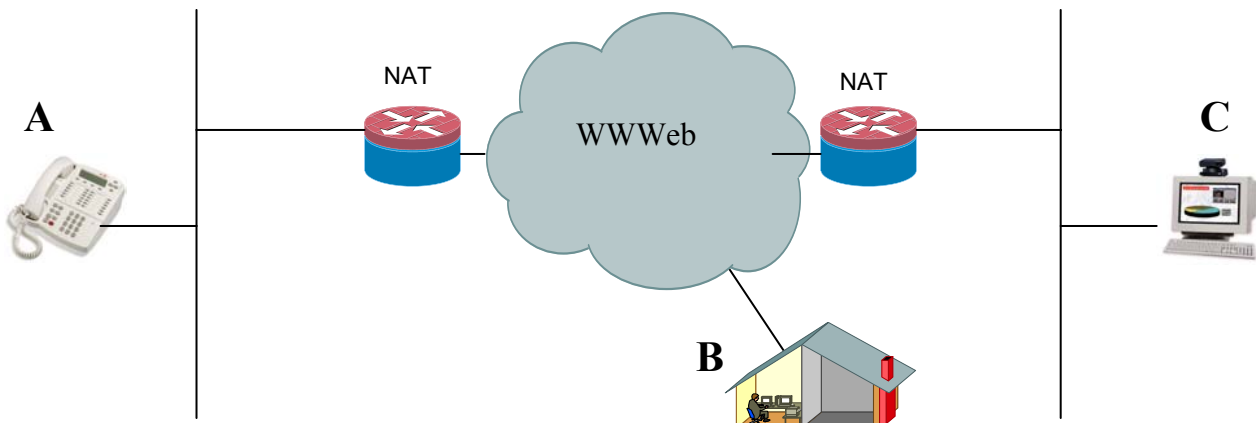
```
SIP Signaling
INVITE sip:23198@172.17.207.91:5060 SIP/2.0
Expires: 180
Content-Type: application/sdp
Via: SIP/2.0/UDP 172.18.192.232:5060;branch=1FV1xhfvxGJOK9rWcKdAKOA
Via: SIP/2.0/UDP 10.80.17.134:5060
To: <sip:23198@172.18.192.232>
From: sip:15691@10.80.17.134
Call-ID: c2943000-50405d-6af10a-382e3031@10.80.17.134
CSeq: 100 INVITE
Contact: sip:15691@10.80.17.134:5060
Content-Length: 219
User-Agent: Cisco IP Phone/ Rev. 1/ SIP enabled
Accept: application/sdp
Record-Route: <sip:23198@172.18.192.232:5060;maddr=172.18.192.232>

SDP Signaling
v=0
o=CiscoSystemsSIP-IPPhone-UserAgent 17045 11864 IN IP4 10.80.17.134
s=SIP Call
c=IN IP4 10.80.17.134
t=0
m=audio 29118 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
```

10.80.17.134:5060
IP Address:Port embedded in SIP & SDP signaling

VoIP and NAT – The Problem in practice

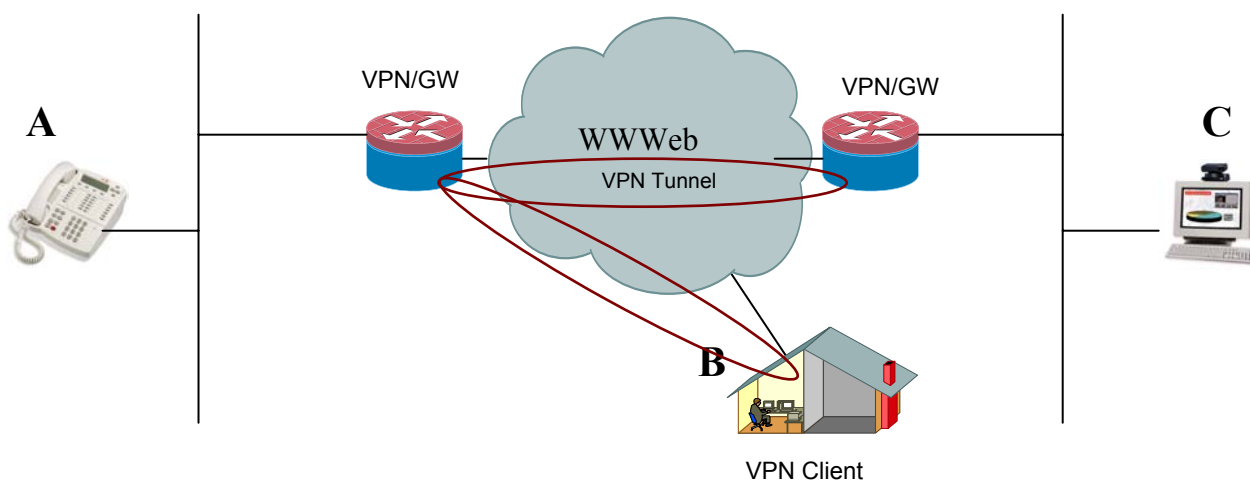
Refer to the below diagram. Let's say A calls B. The NAT at A allows access to the web, and translates A's address to a public, 'routable' address. B then gets call request from A (via NAT), but tries to respond to embedded IP address (not to the NAT address). The result, B responds to A's private address, which the web cannot route, and the call fails. Call scenario A to C (private to private NAT) also fails in the same way.



VoIP and NAT – The Answers

The following are various options available to negate or traverse NAT's to allow for public and private call scenarios:

- Place IP Telephones outside of NAT and provide public addresses. This would work, but is not practical, and undermines the concept of needing NAT in the first place. Not Recommended.
- Create 'Static' NAT mapping for IP telephones. Again, this would work but not practical, particularly for Softphones and DHCP environments. Administration increases also. Not Recommended.
- Create secure VPN tunnels from site to site or even home to office (see below). A VPN tunnel simply encapsulates traffic from site to site / place to place, routing is supplied by the VPN IP addressing, and the traffic is simply left non-NAT'ed. Recommended where ever suitable.



- Use 'Application Aware' NAT's – Often termed Application Level Gateways (ALG's), these devices (normally VPN, F/wall and NAT all in one), are able to extend NAT's into L4 and above, meaning they are able to modify the embedded IP addressing at L4 and above. This works very successfully, but often means replacing customer equipment – perhaps expensive. Going forward though, this option is expected to become the chosen option for new and upgrade opportunities. Recommended.
- Use 'Application Proxy' – H.323 and SIP both initiate signalling and communications on well known TCP ports. This makes it possible for rule writing on most firewalls to pass the transaction and call over to a proxy to handle further. The proxy can perform a re-write of the embedded addresses as described above with the ALG's or can do something different. There is the possibility to create two calls at this point (a public call and a private call), for a single call scenario. This effectively negates the NAT problem and the proxy handles the two calls independently – the users are unaware. We would recommend this solution where cost was an issue, and the customer wanted to retain the existing f/wall and NAT arrangement.

We can see that NAT's can create a real problem for VoIP calling scenarios. In reality though we will see most issues negated by using secure VPN tunnelling for site to site communications, and foresee ALG's as the best route to resolve this issue outside of this.