

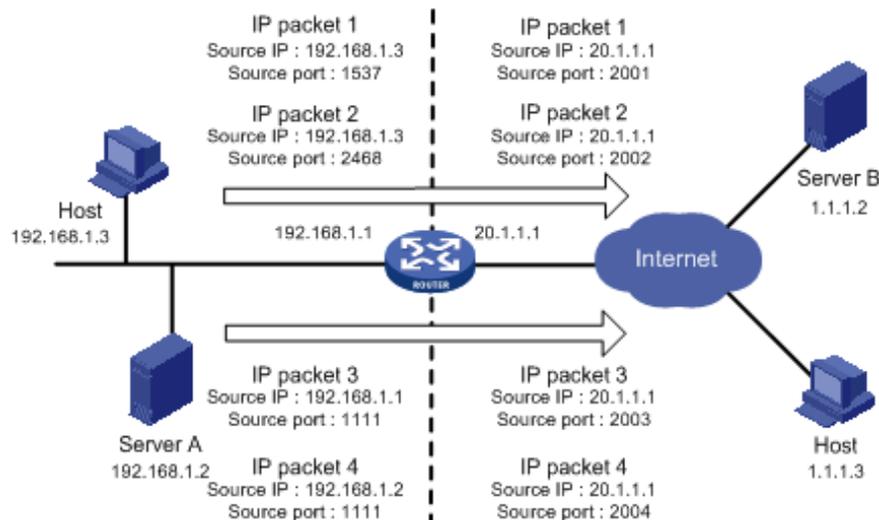
SCOPSERV
INTERNATIONAL INC.

ScopTEL™ IP PBX Software

Configuring ScopTEL for NAT

What is NAT?

Network address translation (NAT) is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network. (Source: https://en.wikipedia.org/wiki/Network_address_translation)



NAT routers assign internal and external port numbers to egress source host packets and maintain a cache of this data to re-route returned packets to the correct internal source IP address.





The VIA header

Whenever ScopTEL is behind a third party NAT router an external IP address must be defined so that Asterisk can rewrite the SIP VIA header with the public IP address of the router. Other technologies such as STUN can discover the public IP address of the router both server and client side. However it is easiest to configure the public IP address or Fully Qualified Domain Name manually on the server. Since ScopTEL does this natively the usage of any third party router employing a SIP ALG is NOT recommended.

The VIA Header: Every proxy in the request path adds the “Via” the address and port on which it received the message, than forwards it onwards. When processing responses, each proxy in the return path processes the contents of the “Via” field in reverse order, removing its address from the top.

Here is what the SIP INVITE from a remote NAT extension looks like when calling an internal extension on the same server.

```
[2016-04-27 10:25:58] INVITE sip:501@fqdn:5060 SIP/2.0
```

```
[2016-04-27 10:25:58] Accept: application/conference-info+xml, application/sdp, message/sipfrag, multipart/mixed
```

```
[2016-04-27 10:25:58] Via: SIP/2.0/UDP 10.35.25.71:5062;branch=z9hG4bKd0ac118bea34ac054;rport
```

```
[2016-04-27 10:25:58] Max-Forwards: 70
```

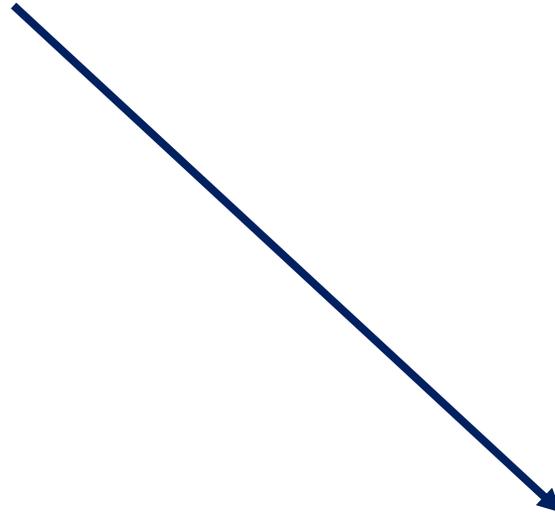
```
[2016-04-27 10:25:58] From: "244" <sip:244@fqdn:5060>;tag=5efba267c4
```

```
[2016-04-27 10:25:58] To: <sip:501@fqdn:5060>
```



Setting all extensions to use NAT settings

This will configure all extensions to use 'nat = force_rport,comedia'



Telephony Settings: Channels

Configuration Channels Language Time Zones Asterisk Manager External API Monitoring Scheduled Tasks Hangup Causes Synchronization

Channels

General RTP Options Codecs SIP Channel IAX Channel ENUM Jitter Buffer Media Transcoding Guest Account

Port (UDP): 5060
Default: 5060
Bind Address (UDP):

Enable support for SIP TCP?: Yes
Port (TCP): 5060
Default: 5060
Bind Address (TCP):

Enable support for SIP TLS (secure)?: Yes
Port (TLS): 5061
Default: 5061
Bind Address (TLS):
Certificate: master88sha1
Certificate Chain: master88sha1 chain

Enable Outbound Proxy support?: No
When enabled, the server will send outbound signalling to the specified server, not directly to devices.

SIP Options

Realm for Digest Authentication: scopserv
Default: scopserv
User Agent: Asterisk PBX (ScopServ)
Default: Asterisk PBX (ScopServ)
Record SIP History: No
Auto-create Peers: Yes
Enable RTP Auto Framing?: No
If set, then all calls will try to set the packetization based on the remote endpoint's preferences.
Enable DNS SRV lookups on outbound calls: Yes
Default: True
Max length of incoming registration: 3600
Default: 3600
Default length of incoming/outgoing registration: 120
Default: 120
Enable Pedantic checking for strict SIP compatibility: No
Turn on support for SIP Video: Yes
Default: True
Use Direct RTP media path?: No
This will cause Asterisk to behave more like a proxy does with respect to media and simply pass the SDP payloads as received to both endpoints.
Always assume NAT for ALL devices?: Yes
When unchecked, you can control this option on a per-extension basis. If your server is on a public IP and communicating with devices hidden behind a NAT device (broadband router).



Setting the SIP Trunk to use NAT settings

This will configure the trunk to use 'nat = force_rport,comedia'

Interfaces Manager: VoIP Accounts

Digital Interfaces Analog Interfaces **VoIP Accounts** Interface Group Jabber (XMPP) Shared Line Appearance

VoIP Accounts

General Server **Network** Options Billing Incoming Calls Outgoing Calls

Transport Mode: UDP

Trunk behind NAT ?

Enable Interactive Connectivity Establishment (ICE) ? This require a STUN and/or TURN server defined in Settings -> Channels -> RTP settings.

Enable Outbound Proxy support ? When enabled, the server will send outbound signalling to the specified server, not directly to devices.

Insecure: Port Invite
Select all, Select none, Invert selection
- Port: Allow matching of peer by IP address without matching port number
- Invite: Do not require authentication of incoming INVITES

Enable SRTP encryption ? Calls will fail with if the peer does not support SRTP. Defaults to no.

Qualify ? Default: True

Qualify Time (in ms): 300 Default: 300

Qualify Frequency (in seconds): 60 Default: 60

Keepalive Interval: 20 Interval at which keepalive packets should be sent to a peer (value in seconds).

RTP Timeout

Use Custom values for RTP timeout/activity ?



The externalhost setting is used to replace the VIA header

- Check the box to enable 'Server behind NAT' ONLY if the ScopTEL Server is behind a NAT router. This will set any SIP packets not in the Local Network list to use the externalhost in the SIP VIA header. If the ScopTEL server has a direct public interface this option is not required.
- External IP or Hostname = fullyqualifieddomainnamegoeshere
- Any local hosts must have their Local Networks defined so that they DO NOT use the externalhost in the VIA header. This includes any local networks, VLAN's, or remote VPN subnets, and often applies to ITSP SIP trunks using a private network such as a dedicated MPLS interface for the trunk! Failure to include all local networks will result in the public IP address being used for all local SIP signalling and these calls will fail.

The screenshot shows the 'Configuration' page for ScopTEL. The 'Server behind NAT' checkbox is checked. The 'External IP or Hostname' field contains the placeholder text 'fullyqualifieddomainnamegoeshere'. The 'Local Network' field contains a list of IP ranges: 192.168.192.0/24, 172.16.88.0/24, 172.16.78.0/24, 172.16.79.0/24, 192.168.108.0/24, and 192.168.8.0/24. A note at the bottom states: 'You can add multiple 'network/subnet' if separated by a space.'

Configuration	
Default Language:	English Default: English
Tone Indication:	United States / North America Default: United States / North America
Server behind NAT ?	<input checked="" type="checkbox"/>
External IP or Hostname:	fullyqualifieddomainnamegoeshere
How often to refresh Hostname if used ?:	10 Default: 10
Local Network:	192.168.192.0/24 172.16.88.0/24 172.16.78.0/24 172.16.79.0/24 192.168.108.0/24 192.168.8.0/24

You can add multiple 'network/subnet' if separated by a space.

