

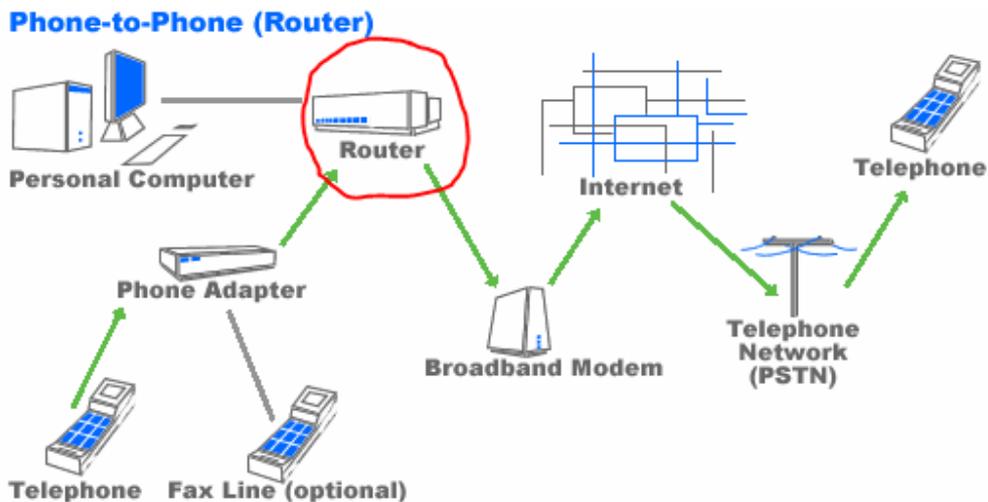
What is Router SIP ALG?

Many of today's commercial routers implement [SIP](#) ALG (Application-level gateway), coming with this feature enabled by default. While ALG could help in solving [NAT](#) related problems, the fact is that many routers' ALG implementations are wrong and break SIP.

There are various solutions for SIP clients behind NAT, some of them in the client side ([STUN](#), [TURN](#), [ICE](#)), others in the server side (Proxy RTP as [RtpProxy](#), [MediaProxy](#)). ALG works typically in the client LAN router or gateway. In some scenarios some client side solutions are not valid; for example, STUN with symmetrical NAT router. If the SIP proxy doesn't provide a server side NAT solution, then an ALG solution could have a place.

An ALG understands the protocol used by the specific applications that it supports (in this case SIP) and does a protocol packet-inspection of traffic through it. A NAT router with a built-in SIP ALG can re-write information within the SIP messages (SIP headers and SDP body) making signaling and audio traffic

Figure 1



Notice in Figure 1 the red circle is where SIP ALG takes place; please disable it on your router .

SIP ALG example

- Caller behind NAT with private IP 192.168.1.33
- Caller router public IP 192.0.2.200
- SIP proxy in internet with domain "example.com"

INVITE from the LAN client (with private IP)

```
INVITE sip:destino@example.com SIP/2.0
Via: SIP/2.0/UDP 192.168.1.33:5060;branch=z9hG4bKjyofqmp
Max-Forwards: 70
To: <sip:destino@example.com>
From: "Iñaki" <sip:ibc@example.com>;tag=nrrrx
Call-ID: xetazdjyktlpsfo@192.168.1.33
CSeq: 800 INVITE
Contact: <sip:ibc@192.168.1.33:5060>
Content-Type: application/sdp
Allow:
INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO,MESSAGE
Supported: replaces,norefersub,100rel
User-Agent: Twinkle/1.1
Content-Length: 312
```

```
v=0
o=ibc 1090098764 894503441 IN IP4 192.168.1.33
s=-
c=IN IP4 192.168.1.33
t=0 0
m=audio 8000 RTP/AVP 98 97 8 0 3 101
a=rtpmap:98 speex/16000
a=rtpmap:97 speex/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=zrtp
```

Note that text in **red** needs to be fixed before it arrives to the proxy (in case our proxy doesn't provide us a NAT server solution). If not, the proxy reply will not arrive at the client (caller):

- The caller couldn't receive in-dialog/sequential messages (ACK for the INVITE, BYE, REFER, re-INVITE...) since the address in "Contact" is not routable outside their network.
- Unidirectional audio - since the caller told the callee to send audio to a non-routable address and port (so the caller won't hear the callee).

The text in [blue](#) doesn't need to be fixed since SIP already handles it (the server adds the parameter "received=REAL_SOURCE_IP" to the "Via" header and sends the replies to that address). Some ALG implementations also change this value.

The same INVITE modified by the ALG router:

```

INVITE sip:destino@example.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.200:12345;branch=z9hG4bKjyfofoqmp
Max-Forwards: 70
To: <sip:destino@example.com>
From: "Iñaki" <sip:ibc@example.com>;tag=nrrrx
Call-ID: xetazdjyktlpsfo@192.168.1.33
CSeq: 800 INVITE
Contact: <sip:ibc@192.0.2.200:12345>
Content-Type: application/sdp
Allow:
INVITE,ACK,BYE,CANCEL,OPTIONS,PRACK,REFER,NOTIFY,SUBSCRIBE,INFO,MESSAGE
Supported: replaces,norefersub,100rel
User-Agent: Twinkle/1.1
Content-Length: 312

v=0
o=ibc 1090098764 894503441 IN IP4 192.168.1.33
s=-
c=IN IP4 192.0.2.200
t=0 0
m=audio 33445 RTP/AVP 98 97 8 0 3 101
a=rtpmap:98 speex/16000
a=rtpmap:97 speex/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=zrtp

```

The ALG has fixed the NAT related problem by:

- Replacing IP in "Via" header with the public IP and port.
- Replacing "Contact" with mapped public IP and port.
- Replacing SDP media address with public IP and port.

SIP ALG problems

The main problem is the poor implementation at SIP protocol level of most commercial routers and the fact that this technology is just useful for outgoing calls, but not for incoming calls:

- Lack of incoming calls: When a UA is switched on, it sends a REGISTER to the proxy in order to be localizable and receive incoming calls. This REGISTER is modified by the ALG feature (if not, the user wouldn't be reachable by the proxy since it indicates a private IP in REGISTER "Contact" header). Common routers just maintain the UDP "connection" open for a while (30-60 seconds), so after that time the port forwarding is ended and incoming packets are discarded by the router. Many SIP proxies maintain the UDP keepalive by sending OPTIONS or NOTIFY messages to the UA, but they just do it when the UA has been detected as natted during the registration. A SIP ALG router rewrites the REGISTER request so the proxy doesn't detect the NAT and doesn't maintain the keepalive (so incoming calls will be not possible).
- Breaking SIP signaling: Many of the actual common routers with inbuilt SIP ALG modify SIP headers and the SDP body incorrectly, breaking SIP and making communication impossible. Some of them do a whole replacing by searching a private address in **all** SIP headers and body and replacing them with the router public mapped address (for example, replacing the private address if it appears in "Call-ID" header, which makes no sense at all). Many SIP ALG routers corrupt the SIP message when writing into it (i.e. missed semi-colon ";" in header parameters). Writing incorrect port values greater than 65536 is also common in many of these routers.
- Disallows server side solutions: Even if you don't need a client side NAT solution (your SIP proxy gives you a server NAT solution), if your router has SIP ALG enabled that breaks SIP signaling, it will make communication with your proxy impossible.

List of routers with SIP ALG enabled

The following is a list containing SIP ALG router models, their issues and how to disable SIP ALG (enabled by default in most of the cases).

Dlink

Models: DIR-655

Motorola

Models: **SBG6580** (SurfBoard Extreme Wireless Cable Modem Gateway)

- No Registration possible behind NAT as the device changes Call-ID and causes the responses to be discarded by SIP clients/ATAs
- No Solution at this time (SIP ALG, called SIP Pass Through, cannot be disabled).
- Must disable NAT and put the device in bridge mode. ([See this guide](#))

SpeedTouch

Models: **ST530 v6** (*firmware* $\geq 5.4.0.13$) comes with SIP ALG enabled by default.

NAT type: symmetrical

Issues:

- No incoming calls.
- It replaces the private IP appearing in SIP headers with the public IP using a dumb text replacement. If for example the private IP appears in the "Call-ID", it replaces it too (that it's completely unnecessary).

To disable SIP ALG:

```
~# telnet router
```

```
-> connection unbind application=SIP port=5060
```

```
-> saveall
```

Zyxel

Models: **660 family** comes with SIP ALG enabled by default.

NAT type: symmetrical

Issues:

- No incoming calls.
- SIP protocol broken, making 50% of outgoing calls impossible because the wrong values are inserted into SIP headers.

To disable SIP ALG:

```
~# telnet router
```

```
Menu option "24. System Maintenance".
```

```
Menu option "8. Command Interpreter Mode".
```

```
ip nat service sip active 0
```

Netgear

Models: WGR614v9 Wireless-G Router, DGN2000 Wireless-N ADSL2+ Modem Router
Firmware V1.0.18_8.0.9NA

To disable SIP ALG: From Wan Setup Menu, NAT Filtering, uncheck the box next to "Disable SIP ALG"

SMC

Models: **ToDo**

NAT type: No symmetrical

Issues:

- The ALG doesn't replace the private address in "Call-ID" header (that is correct). but it does replace the "Call-ID" value in "Refer-To" header so SIP transfer is broken.

To disable SIP ALG: **ToDo** no ALG related options found via web and telnet. No idea of how to disable it.

Linksys

Models: WRV200, WRT610N

NAT type: Symmetrical

Issues:

- The ALG replaces the private address in "Call-ID" header (not needed at all). Some phones (as Linksys with latest firmware) encode the "Call-ID" value in the "Refer-To" header (by escaping the dots) so the private IP appearing there is not replaced with the public IP. This causes the call transfer to fail since the proxy/PBX/endpoint will not recognize the dialog info.

To disable SIP ALG: **ToDo** no ALG related options found via web and telnet. No idea of how to disable it.

To disable SIP ALG on WRT610N: Web Interface: Administration, Management, under side heading 'Advanced Features' SIP ALG, can be disabled.

[Peplink Multi-WAN routers](#)

Models: All multi-WAN models

To disable SIP ALG, go to <http://<router.LAN.IP>/cgi-bin/MANGA/support.cgi>

Click the "Disable" button under "SIP ALG Support"

Issues:

- Not aware of any SIP ALG issues, but if you just want to turn it off, here you go.

Fortinet

Models: All models come with SIP Helper enabled by default.

To disable SIP helper:

```
~# telnet firewall
config system settings
set sip-helper disable
set sip-nat-trace disable
end
```

```
config system session-helper
show <---- use this to find out which entry is configured for typically 12 or 13
delete 12
end
```

The preferred solution is to configure the SIP ALG. Policies that use the SIP ALG will not use SIP helper. Full documentation at <http://docs.fortinet.com>, then pick FortiOS for the version on your device, then VoIP solutions: SIP.

Cisco

Models: 800 Series

To disable the NAT services for SIP in IOS, just run these commands:

```
no ip nat service sip tcp port 5060
no ip nat service sip udp port 5060
```

Juniper / Netscreen

Models: SSG Series

To disable SIP ALG:

In the Web interface: Security -> ALG