



Testing SIP Aware Routers

white paper

Introduction

This document discusses the importance of testing SIP aware CPE routers using the CDRouter test solution as part of an over-all Voice over IP test strategy. CDRouter offers comprehensive functional testing of SIP aware routers using a real world test setup. Using the CDRouter SIP test module, network and QA engineers can quickly verify the behavior of a SIP aware device and avoid costly interoperability problems.

SIP and NAT

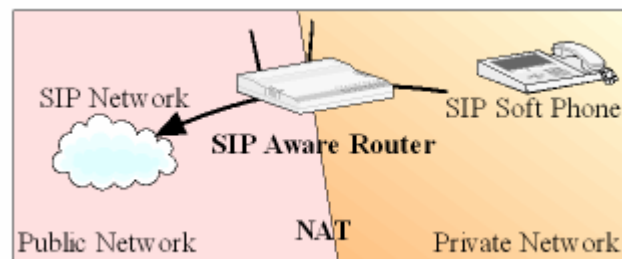
In the last couple of years, SIP has become the leading signaling protocol for establishing Voice over IP calls between soft-phones and other VoIP applications. Major VoIP carriers are now deploying SIP based networks. However, many broadband users who are trying to take advantage of the new SIP services are also deploying NAT on their CPE router. Are SIP and NAT compatible? Unfortunately, no. While some SIP clients attempt to detect NAT and work around it, many existing SIP applications do not work correctly with NAT. To make matters worse, most SIP aware routers are not compatible with SIP clients using STUN techniques. To work gracefully with SIP, a CPE router needs to be SIP aware.

Today, most CPE vendors are building SIP aware functionality into the CPE router. The implementation may take the form of an ALG (Application Layer Gateway) or the implementation may act like an additional SIP proxy. In either case, the SIP aware router should allow the end user to interoperate with a SIP based network while deploying NAT on the local network.

Inside the Headers

SIP aware devices must understand the protocol messages used by SIP. Several of the headers used in a SIP message contain information about the local IP address and port. Some SIP messages also contain SDP information (Session Description Protocol) describing the media stream that will transport the actual audio or video data. A SIP aware router must understand the SIP and SDP information passing through the router. The IP address and port numbers need to be translated from the private network to

the public side of the network. The router must also open port mappings allowing the media stream to flow through the router.



CDRouter and SIP

CDRouter offers a functional test module to verify the behavior of a SIP aware router. Using a single PC loaded with CDRouter software, SIP clients and proxy servers can be created to reflect the typical usage of SIP in a CPE router setup. Using CDRouter's built-in SIP client and server, inbound and outbound SIP calls are created along with real RTP media streams. At each step of the way, CDRouter can validate the expected changes in protocol packets, and verify that the media streams are flowing in both directions.

All CDRouter test cases are fully automated. The software needed to run SIP clients and servers is built directly into CDRouter. This allows CDRouter to quickly cycle through several call scenarios without having to install and troubleshoot third party SIP software. In a matter of minutes, CDRouter will report how well the SIP aware router supports SIP call functionality.

Something Goes Wrong

Implementation bugs in the SIP aware router are a leading cause of interoperability problems between a specific SIP phone and a VoIP service provider. A wide range of problems can occur at the user level including audio in one direction only, no audio, no inbound calls, or calls that go dead.

Without looking at both sides of a SIP aware router, these problems can be difficult to diagnose. CDRouter can help detect these problems early on during the development and testing phase of production.

Example Implementation bugs

The following examples illustrate the types of functional implementation bugs that CDRouter can detect. These problems were discovered on shipping CPE routers running the CDRouter SIP test module.

1. Illegal port number values in translation of 'Contact' header

When a SIP REGISTER or INVITE message passes through NAT, the size of the message may change based on changes to the IPv4 address or port number. In the example below, the SIP aware router translates the IP port information to an illegal IP port on the public side of the network. The SIP proxy server receiving these messages will be unable to respond correctly since the port does not exist. Unfortunately, some SIP proxy servers will accept this faulty REGISTER message. The end user will not be able to receive incoming SIP calls.

Here is the initial REGISTER packet on the private LAN:

```
REGISTER sip:3.3.3.3 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.19:5060
Content-Length: 0
Contact: <sip:+1-978-200-0002@192.168.0.19:14265>;expires=3600
Call-ID: e88740b8-15@192.168.0.19
Max-Forwards: 70
From: <sip:+1-978-200-0002@3.3.3.3:5060>
CSeq: 47 REGISTER
To: <sip:+1-978-200-0002@3.3.3.3:5060>
User-Agent: CDRouter SIP Client 1.0
```

The router then translates the Contact header in the REGISTER message. Here is the REGISTER packet on the public WAN:

```
REGISTER sip:3.3.3.3 SIP/2.0
Via: SIP/2.0/UDP 192.168.200.2:30913
Content-Length: 0
Contact: <sip:+1-978-200-0002@192.168.200.2:309135>;expires=3600
Call-ID: e88740b8-15@192.168.0.19
Max-Forwards: 70
From: <sip:+1-978-200-0002@3.3.3.3:5060>
CSeq: 47 REGISTER
To: <sip:+1-978-200-0002@3.3.3.3:5060>
User-Agent: CDRouter SIP Client 1.0
```

In the above example, the port number in the Contact header on the WAN side has the illegal value 309135. The SIP server will be

unable to direct incoming calls to the correct port since port 309135 does not exist.

2. No support for compact header formats

Many SIP headers support a compact form that can be used by a SIP client or proxy when the SIP message size is an issue. Many SIP clients allow the user to configure the use of compact headers. Any SIP aware router must be able to understand both the normal header format and the compact header format.

In the example below, the SIP client sends an INVITE message using compact headers through the SIP aware router.

```
INVITE sip:cdrouter@3.3.3.3 SIP/2.0
v: SIP/2.0/UDP 192.168.0.19:5060
f: "+1-978-200-0001" <sip:+1-978-200-0001@192.168.0.19>
m: <sip:+1-978-200-0001@192.168.0.19:5060>
t: <sip:cdrouter@3.3.3.3>
i: 8e0db03d-2@192.168.0.19
CSeq: 3 INVITE
User-Agent: CDRouter SIP Client 1.0
c: application/sdp
l: 276

v=0
o=Registered_User 0 0 IN IP4 192.168.0.19
s=session
c=IN IP4 192.168.0.19
b=CT:1000
t=0 0
m=audio 13194 RTP/AVP 97 0 8 4 101
a=rtpmap:97 red/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:4 G723/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

While the router does update the SDP information, it fails to recognize the compact form of the Contact and Via headers in the INVITE message. These headers are not translated to the publish side IP address still contain the private IP address from the LAN side.

```
INVITE sip:cdrouter@3.3.3.3 SIP/2.0
v: SIP/2.0/UDP 192.168.0.19:5060
f: "+1-978-200-0001" <sip:+1-978-200-0001@192.168.0.19>
m: <sip:+1-978-200-0001@192.168.0.19:5060>
t: <sip:cdrouter@3.3.3.3>
i: 8e0db03d-2@192.168.0.19
CSeq: 3 INVITE
User-Agent: CDRouter SIP Client 1.0
c: application/sdp
```

```
1: 276

v=0
o=Registered_User 0 0 IN IP4 192.168.0.19
s=session
c=IN IP4 192.168.200.2
b=CT:1000
t=0 0
m=audio 38890 RTP/AVP 97 0 8 4 101
a=rtpmap:97 red/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:4 G723/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

3. SIP retransmissions

Some SIP aware devices are not careful about processing SIP retransmissions. Retransmitted SIP packets containing SDP information can end up with multiple port mappings created for a single RTP stream. In the example below, the original INVITE packet has a SDP source port of 13078. Later, when the INVITE is retransmitted with the same Call-ID and branch, the SDP port is changed to 12283. Even worse, this SIP aware device did not preserve the “even port property” of RTP ports and translated the RTP port to an odd value.

First translated INVITE packet:

```
INVITE sip:cdrouter@3.3.3.3 SIP/2.0
Via: SIP/2.0/UDP 192.168.200.2:12282;branch=z9hG4bK448e3f4b
From: "+1-978-200-0001" <sip:+1-978-200-0001@192.168.200.2>
Contact: <sip:+1-978-200-0001@192.168.200.2:12282>
To: <sip:cdrouter@3.3.3.3>
Call-ID: 44207a9d-2@lan.cdrouter.com
CSeq: 3 INVITE
User-Agent: CDRouter SIP Client 1.0
Content-Type: application/sdp
Content-Length: 278

v=0
o=Registered_User 0 0 IN IP4 192.168.1.109
s=session
c=IN IP4 192.168.200.2
b=CT:1000
t=0 0
m=audio 13078 RTP/AVP 97 0 8 4 101
a=rtpmap:97 red/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:4 G723/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

Retransmitted INVITE packet:

```
INVITE sip:cdrouter@3.3.3.3 SIP/2.0
Via: SIP/2.0/UDP 192.168.200.2:12282;branch=z9hG4bK448e3f4b
From: "+1-978-200-0001" <sip:+1-978-200-0001@192.168.200.2>
Contact: <sip:+1-978-200-0001@192.168.200.2:12282>
To: <sip:cdrouter@3.3.3.3>
Call-ID: 44207a9d-2@lan.cdrouter.com
CSeq: 3 INVITE
User-Agent: CDRouter SIP Client 1.0
Content-Type: application/sdp
Content-Length: 278

v=0
o=Registered_User 0 0 IN IP4 192.168.1.109
s=session
c=IN IP4 192.168.200.2
b=CT:1000
t=0 0
m=audio 12283 RTP/AVP 97 0 8 4 101
a=rtpmap:97 red/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:4 G723/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

4. Firewall interoperability

Besides the SIP ALG function of the router, some routers also contain advanced firewall functions that must work gracefully with the SIP ALG. Using CDRouter the maximum number of outgoing and incoming SIP calls can be tested. This type of testing has shown routers that confuse multiple RTP over UDP packets as port scan attempts. When multiple calls are created between the same end user and SIP proxy (such as a multi-party call), the router detects a port scan and then closes the RTP ports, preventing communication in one direction.

5. Using the MUTE function

The MUTE function on a SIP soft-phone can interact poorly with some SIP ALGs. To implement MUTE, some SIP clients stop sending RTP traffic to the remote SIP endpoint. If the ALG depends on out-going RTP traffic to establish and maintain the NAT port mapping, enabling the MUTE function on the phone behind NAT can cause the port mapping to eventually be deleted. The common NAT timeout for UDP NAT connections is 5 minutes. So after 5 minutes, the RTP stream from the other SIP endpoint may fail to make it through NAT from the WAN.

CDRouter can verify that the NAT port mappings are created based on the SIP call state, not the actual RTP packets. This allows RTP to flow in both directions regardless of the MUTE function on the phone.

Conclusion

CDRouter is part of the Voice over IP test solution for SIP aware routers during the development and testing phase of production. Using CDRouter, network vendors can quickly check for NAT interoperability issues before deploying a SIP aware router. CDRouter makes it easy and quick to cycle through several interoperability test cases before field trials with a real service.

Poorly tested SIP ALG functionality can lead to many interoperability issues that affect some of the largest SIP based networks today. CDRouter can help eliminate some of these common problems in a controlled test environment.

NOTICE

CDRouter™ is a registered trademark of QA Cafe. With out the prior written consent of QA Cafe, no part of the document may be reproduced by any means.

Additional Information

For additional information, contact:

QA Cafe
155 Fleet Street
Portsmouth, NH 03801
Tel: (877) 332 0784
Email: info@qacafe.com