8x8

8x8 SIP Trunking

Interface Specification

Version 2.0

Table of Contents

Introduction

This document outlines the requirements for interoperability with the 8x8 SIP trunking interface and services.

Feature Set

The 8x8 SIP trunking service provides the following features:

- Call termination (domestic and international)
- Call origination (domestic DIDs and international DIDs for over 15 countries)
- Virtual numbers
- Toll-free numbers
- e911
- 411/DA services
- CNAM completion (caller ID with name on origination calls)
- Call forwarding (redirection of origination calls)
- DID rollover
- Route Advance (failover to another carrier in the event of a call failure)
- Directory listing service

As this time, the 8x8 SIP trunking service does not provide any voicemail features.

SIP Interface

This section details the 8x8 SIP trunking interface interoperability requirements.

Supported Standards

The 8x8 SIP trunking interface supports the following SIP standards:

- RFC3261 (SIP)
- RFC3263 (Locating SIP Servers)
- RFC3264 (Offer/Answer model for SDP)
- RFC3311 (UPDATE method)
- RFC3581 (Symmetric Response Routing)
- RFC4028 (SIP Session Timer)
- RFC2806 (tel URL)
- draft-ietf-sip-privacy-04.txt (Remote-Party-ID header)

Supported SIP methods

The 8x8 SIP trunking interface supports the following SIP methods:

INVITE, UPDATE, CANCEL, BYE, ACK

Note: The 8x8 SIP trunking interface does not provide any registration support. There is no registrar and the REGISTER method is not supported.

Additional Supported SIP Headers

In addition to the standard SIP (RFC3261) header definitions, the following additional SIP headers are supported:

- Remote-Party-ID (draft-ietf-sip-privacy-04.txt)
- Session-Expires (RFC4028)
- Min-SE (RFC4028)

Supported SIP Transport Protocols

The 8x8 SIP trunking interface supports UDP. At this time, TCP and TLS are not currently supported.

SIP Session Timer

Use of the SIP Session Timer is highly recommended. This specification prevents "infinite calls" and minimizes the chance of over-billing of calls in the event of network problems.

The 8x8 SIP trunking interface supports both UAC and UAS session timer refresher modes as described in RFC4028. The session timers may be refreshed via either a re-INVITE or an UPDATE message.

Caller ID

Caller-ID information will be conveyed in the Remote-Party-ID header field as described in draft-ietf-sip-privacy-04. Here are some examples:

```
Remote-Party-ID: “John Doe” <sip:15558881234@209.247.17.37>;
  party=calling;privacy=off;screen=yes
Remote-Party-ID: <sip:5551234@209.247.17.37>;
  party=calling;privacy=full;screen=yes
Remote-Party-ID: <sip:5551234@packet8.net>;
  party=calling;privacy=off;screen=yes
```

Media

This section details the supported media types, CODECs, and media interoperability requirements.

Supported Media Types

The 8x8 SIP trunking interface supports RTP for voice relay

The following audio/fax CODECs and media formats are supported:

- G.711 uLaw (default RTP payload 0)
- G.729 (default RTP payload 18)
- DTMF relay (RFC2833)

Here is an example of a compliant Session Description Protocol (SDP) for a voice call:

```
v=0
o=rtp 1219179360 1219179360 IN IP4 192.84.13.227
s=-
c=IN IP4 192.84.13.227
t=0 0
m=audio 28000 RTP/AVP 0 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Note: The PSTN gateway providers used by the 8x8 network do not support RTCP. They will ignore RTCP packets sent to them, and they will not send RTCP packets.

DTMF relay

DTMF relay may be performed in-band (DTMF tones are encoded into the audio stream), or out-of-band (by using a “telephone-event” payload as defined in RFC2833). The preferred method is to use the out-of-band relay method defined in RFC2833. The SIP Session Description Protocol (SDP) must provide the appropriate “telephone-event” payload mapping, example:

```
m=audio 60566 RTP/AVP 18 0 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Supported Media Transport Protocols

Currently, the only supported transport protocol for media traffic is UDP (RTP/AVP for voice traffic.)

NAT Traversal

The 8x8 SIP trunking service does not offer any media switching capabilities. That is, the 8x8 SIP trunking interface is not a Session Border Controller (SBC). It is the customer's responsibility to provide NAT traversal services for SIP and media traffic. This can be achieved by using one of the following:

- A publicly addressable static IP address (preferable)
- A STUN server (this will only work if your SIP device(s) supports STUN and is behind a non-symmetrical NAT/firewall)
- A TURN server

All media IP addresses presented in the Session Description Protocol (SDP) MUST be publicly addressable.

Authentication

Authentication with the 8x8 SIP trunking interface is achieved by satisfying the following criteria:

- SIP traffic must be received from a pre-registered static publicly addressable IP address. The 8x8 service will reject SIP traffic from unknown IP addresses.
- SIP traffic will be challenged using standard SIP digest authentication procedures as outlined in RFC3261. The 8x8 service will challenge all call request INVITE messages with a 407 response. The SIP trunk UAC must resend the INVITE using the username and password credentials supplied by 8x8.

Request-URI, To and From Header Field Requirements

The 8x8 SIP trunking service will only accept full E.164 compliant telephone numbers. It does not support 7 or 10 digit dialing. All domestic US numbers must contain all 11 digits. The 8x8 interface will accept domestic US numbers with or without a pre-pended "+".

For call termination, the 8x8 service will only accept INVITE "Request-URI", "To" and "From" header fields that appear in this E.164 format. The 8x8 service supports both "sip" (RFC3261) and "tel" (RFC2806) URI formats. For example, to dial "966-555-1234", any one of the following Request-URIs may be sent to the 8x8 SIP trunking interface:

```
sip:+19665551234@packet8.net
sip:19665551234@packet8.net
tel:+19665551234
tel:19665551234
```

Here are some examples of valid requests to the 8x8 SIP trunking interface:

```
INVITE sip:+19665551234@tg.packet8.net;transport=UDP;user=phone SIP/2.0
f: “John Doe” <sip:14665554321@tg.packet8.net>;tag=c0541341-13c4
t: 19665551234 <sip:+19665551234@tg.packet8.net>

INVITE sip:19665551234@63.209.0.77;transport=UDP SIP/2.0
From: <sip:14665554321@63.209.0.77>;tag=c0541341-13c4
To: <sip:19665551234@63.209.0.77>

INVITE tel:+19665551234;transport=UDP SIP/2.0
From: <sip:14665554321@63.209.0.77>;tag=c0541341-13c4
To: <tel:+19665551234>

INVITE tel:19665551234;transport=UDP SIP/2.0
f: <sip:14665554321@63.209.0.77>;tag=c0541341-13c4
t: <tel:19665551234>
```

The From header field MUST contain one of the E.164 telephone numbers assigned to the SIP trunking account. For example, if the SIP trunking account has three telephone numbers (DIDs) for inbound calls, you may send any one of the three numbers (formatted as an E.164 number) in the user parameter of the From header, as shown in the examples above (examples use the phone number 1-466-555-4321).

For call origination, the 8x8 service will always send INVITE messages in which the INVITE “Request-URI” and “To” header fields contain phone numbers in the E.164 format. The 8x8 service will always send the phone number using the “sip” URI format in the Request-URI, and the number will always be pre-pended with a “+”. Here is an example of a SIP INVITE sent by the 8x8 SIP trunking interface:

```
INVITE sip:+14665554321@192.84.19.65:5060;transport=udp;user=phone SIP/2.0
f: <sip:15551231234@209.247.17.37>;tag=bp3FaT3Uk4JqK
t: <sip:+14665554321@acmetrunk.packet8.net.;user=phone>
```

e911 Support

The 8x8 SIP trunking interface supports e911. Emergency services can be contacted by dialing “911”. The Request-URI MUST be formatted as an E.164 number “911” or “+1911”. Example:

```
INVITE sip:911@63.209.0.77;transport=UDP SIP/2.0
From: “John Joe” <sip:14665554321@63.209.0.77>;tag=c0541341-13c4
To: 911 <sip:911@63.209.0.77>
```

Call Flow Examples

This section provides example SIP call signaling for an outbound call (SIP trunking client to 8x8 SIP trunking interface), and an inbound call (8x8 SIP trunking interface to SIP trunking client). In both examples, the SIP trunking client is located at 192.84.19.65:5060, and the 8x8 SIP trunking interface is at 63.209.0.77:5060.

Outbound call to 555-987-1234

```
192.84.19.65:5060-->63.209.0.77:5060
INVITE sip:15559871234@63.209.0.77;transport=UDP SIP/2.0
f: “Line 4” <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 1 INVITE
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07046-ad792eb-6a1b2ad
Max-Forwards: 70
k: timer, replaces
User-Agent: AcmeUAC/1.6.0.34
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REFER
m: <sip:14665554321@192.84.19.65:40833;transport=UDP>
x: 1800
c: application/sdp
l: 192

v=0
o=rtp 1219522629 1219522629 IN IP4 192.84.19.65
s=-
c=IN IP4 192.84.19.65
t=0 0
m=audio 28014 RTP/AVP 0 101
a=fmtp:101 0-15
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

63.209.0.77:5060-->192.84.19.65:40833

```
SIP/2.0 100 Trying
CSeq: 1 INVITE
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07046-ad792eb-6a1b2ad
f: “Line 4” <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>
Server: eSLEE/0.12.83
l: 0
```

63.209.0.77:5060-->192.84.19.65:40833

```
SIP/2.0 407 Proxy Authentication Required
f: “Line 4” <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>;tag=bZboFdy65AcY
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 1 INVITE
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07046-ad792eb-6a1b2ad
Record-Route: <sip:bHIMgqMCGTN20VDhUId@63.209.0.77:5060;lr>
Server: Packet8/1.1.126 (AAATrunking) eSLEE/0.12.83
l: 0
Proxy-Authenticate: Digest realm=”packet8.net”, nonce=”SLBwRxaSEt8cYNjOiew8yKvO0hUA”
```

192.84.19.65:40833-->63.209.0.77:5060

```
ACK sip:15559871234@63.209.0.77;transport=UDP SIP/2.0
f: “Line 4” <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>;tag=bZboFdy65AcY
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 1 ACK
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07046-ad792eb-6a1b2ad
Max-Forwards: 70
User-Agent: AcmeUAC/1.6.0.34
m: <sip:14665554321@192.84.19.65:40833;transport=UDP>
l: 0
```

192.84.19.65:40833-->63.209.0.77:5060

```
INVITE sip:15559871234@63.209.0.77;transport=UDP SIP/2.0
f: “Line 4” <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 2 INVITE
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07046-ad7931f-7d247173
Max-Forwards: 70
k: timer, replaces
User-Agent: AcmeUAC/1.6.0.34
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REFER
m: <sip:14665554321@192.84.19.65:40833;transport=UDP>
Proxy-Authorization: Digest username=”045401020304”, realm=”packet8.net”, nonce=”SLBwRxaSEt8cYNjOiew8
yKvO0hUA”, uri=”sip:15559871234@63.209.0.77;transport=UDP”, response=”1db71e987550aa0233303b42a6b24b8c”,
algorithm=MD5
x: 1800
c: application/sdp
l: 192

v=0
o=rtp 1219522629 1219522629 IN IP4 192.84.19.65
s=-
c=IN IP4 192.84.19.65
t=0 0
m=audio 28014 RTP/AVP 0 101
a=fmtp:101 0-15
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

63.209.0.77:5060-->192.84.19.65:40833

```
SIP/2.0 100 Trying
CSeq: 2 INVITE
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07046-ad7931f-7d247173
f: “Line 4” <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>
Server: eSLEE/0.12.83
l: 0
```

63.209.0.77:5060-->192.84.19.65:40833

```
SIP/2.0 180 Ringing
f: “Line 4” <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>;tag=bdCnel2W8IWJ
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 2 INVITE
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07046-ad7931f-7d247173
Record-Route: <sip:blTXE4RCGTN20VDhUId@63.209.0.77:5060;lr>
Server: eSLEE/0.12.83
l: 0
m: <sip:bVWIo2RCGTN20VDhUId@63.209.0.77:5165>
```

63.209.0.77:5060-->192.84.19.65:40833

```
SIP/2.0 200 OK
f: "Line 4" <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>;tag=bdCnel2W8IWJ
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 2 INVITE
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07046-ad7931f-7d247173
Record-Route: <sip:blTXE4RCGTN20VDhUId@63.209.0.77:5060;lr>
Server: Packet8/1.1.126 (InTrunkGateway) eSLEE/0.12.83
l: 210
c: application/sdp
m: <sip:bVWIo2RCGTN20VDhUId@63.209.0.77:5165>
x: 1800;refresher=uas

v=0
o=mycall 0 0 IN IP4 192.168.89.180
s=-
c=IN IP4 63.209.12.152
t=0 0
m=audio 49337 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
```

192.84.19.65:40833-->63.209.0.77:5060

```
ACK sip:bVWIo2RCGTN20VDhUId@63.209.0.77:5165 SIP/2.0
f: "Line 4" <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
t: 15559871234 <sip:15559871234@63.209.0.77>;tag=bdCnel2W8IWJ
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 2 ACK
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07049-ad7a00e-55078830
Max-Forwards: 70
User-Agent: AcmeUAC/1.6.0.34
m: <sip:14665554321@192.84.19.65:40833;transport=UDP>
Route: <sip:blTXE4RCGTN20VDhUId@63.209.0.77:5060;lr>
Proxy-Authorization: Digest username="045401020304", realm="packet8.net", nonce="SLBwRxaSEt8cYNjOiew8
yKvO0hUA", uri="sip:15559871234@63.209.0.77;transport=UDP", response="1db71e987550aa0233303b42a6b24b8c",
algorithm=MD5
l: 0
```

63.209.0.77:5060-->192.84.19.65:40833

```
BYE sip:14665554321@192.84.19.65:40833;transport=UDP SIP/2.0
f: 15559871234 <sip:15559871234@63.209.0.77>;tag=bdCnel2W8IWJ
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 1899411493 BYE
t: "Line 4" <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
m: <sip:bVWIo2RCGTN20VDhUId@63.209.0.77:5165>
Max-Forwards: 70
k: timer, histinfo
l: 0
User-Agent: Packet8/1.1.126 (InTrunkGateway) eSLEE/0.12.83
v: SIP/2.0/UDP 63.209.0.77:5060;branch=z9hG4bKaBFzgmv7dGne, SIP/2.0/TCP 63.209.0.77:5165;branch=z9hG4bKaL
X4sAAfJ28a
Record-Route: <sip:blTXE4RCGTN20VDhUId@63.209.0.77:5060;lr>
```

```
192.84.19.65:40833-->63.209.0.77:5060
SIP/2.0 200 OK
f: 15559871234 <sip:15559871234@63.209.0.77>;tag=bdCnel2W8IWJ
t: "Line 4" <sip:14665554321@63.209.0.77>;tag=c0541341-13c4-48b07046-ad792eb-7e4cf3c4
i: 8bf4c4-c0541341-13c4-48b07046-ad792eb-2bfd4e56@63.209.0.77
CSeq: 1899411493 BYE
v: SIP/2.0/UDP 63.209.0.77:5060;branch=z9hG4bKaBFzgmv7dGne, SIP/2.0/TCP 63.209.0.77:5165;branch=z9hG4bKaL
X4sAAfJ28a
k: timer, replaces
Server: AcmeUAC/1.6.0.34
l: 0
```

Inbound call from 555-123-1234 to 444-789-5432

```
63.209.0.77:5060-->192.84.19.65:5060
INVITE sip:+14447895432@192.84.19.65:5060;transport=udp;user=phone SIP/2.0
f: <sip:15551231234@209.247.17.37>;tag=bp3FaT3Uk4JqK
t: <sip:+14447895432@acmetrunk.packet8.net.;user=phone>
i: SFOMGC01200808232034510082 57@209.244.63.12
CSeq: 1900462892 INVITE
Max-Forwards: 69
k: timer, histinfo
l: 175
Remote-Party-ID: "John Doe"<sip:15551231234@209.247.17.37>;
party=calling;privacy=off;screen=yes
User-Agent: Packet8/1.1.126 (OutTrunkGateway) eSLEE/0.12.83
c: application/sdp
x: 1854
v: SIP/2.0/UDP 63.209.0.77:5060;branch=z9hG4bKav8qDFo7Ql1984a4727435748e6fd2dce565d0a9b3e, SIP/2.0/TCP
63.209.0.77:5164;branch=z9hG4bKa4eupwMN0hti
m: <sip:bnKgZUBxRanAnUDhUId@63.209.0.77:5164>
Record-Route: <sip:bT9rRXPxRanAnUDhUId@63.209.0.77:5060;lr>

v=0
o=- 1219523691 1219523696 IN IP4 209.247.23.129
s=-
c=IN IP4 209.247.23.129
t=0 0
m=audio 60176 RTP/AVP 18 0 101
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

```
192.84.19.65:5060-->63.209.0.77:5060
SIP/2.0 100 Trying
f: <sip:15551231234@209.247.17.37>;tag=bp3FaT3Uk4JqK
t: <sip:+14447895432@acmetrunk.packet8.net.;user=phone>;tag=c0541341-13c4-48b07469-ae7bdf7-994f75c
i: SFOMGC01200808232034510082570209.244.63.12
CSeq: 1900462892 INVITE
v: SIP/2.0/UDP 63.209.0.77:5060;branch=z9hG4bKav8qDFo7Ql1984a4727435748e6fd2dce565d0a9b3e, SIP/2.0/TCP
63.209.0.77:5164;branch=z9hG4bKa4eupwMN0hti
k: timer, replaces
Server: AcmeUAS/1.6.0.34
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REFER
m: <sip:14447895432@192.84.19.65:40833;transport=udp;user=phone>
l: 0

192.84.19.65:5060-->63.209.0.77:5060
SIP/2.0 180 Ringing
f: <sip:15551231234@209.247.17.37>;tag=bp3FaT3Uk4JqK
t: <sip:+14447895432@acmetrunk.packet8.net.;user=phone>;tag=c0541341-13c4-48b07469-ae7bdf7-994f75c
i: SFOMGC01200808232034510082570209.244.63.12
CSeq: 1900462892 INVITE
v: SIP/2.0/UDP 63.209.0.77:5060;branch=z9hG4bKav8qDFo7Ql1984a4727435748e6fd2dce565d0a9b3e, SIP/2.0/TCP
63.209.0.77:5164;branch=z9hG4bKa4eupwMN0hti
k: timer, replaces
Server: AcmeUAS/1.6.0.34
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REFER
m: <sip:14447895432@192.84.19.65:40833;transport=udp;user=phone>
Record-Route: <sip:bT9rRXPxRanAnUDhUId@63.209.0.77:5060;lr>
l: 0

192.84.19.65:5060-->63.209.0.77:5060
SIP/2.0 200 OK
f: <sip:15551231234@209.247.17.37>;tag=bp3FaT3Uk4JqK
t: <sip:+14447895432@acmetrunk.packet8.net.;user=phone>;tag=c0541341-13c4-48b07469-ae7bdf7-994f75c
i: SFOMGC01200808232034510082570209.244.63.12
CSeq: 1900462892 INVITE
v: SIP/2.0/UDP 63.209.0.77:5060;branch=z9hG4bKav8qDFo7Ql1984a4727435748e6fd2dce565d0a9b3e, SIP/2.0/TCP
63.209.0.77:5164;branch=z9hG4bKa4eupwMN0hti
k: timer, replaces
Server: AcmeUAS/1.6.0.34
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REFER
m: <sip:14447895432@192.84.19.65:40833;transport=udp;user=phone>
Record-Route: <sip:bT9rRXPxRanAnUDhUId@63.209.0.77:5060;lr>
x: 1800;refresher=uas
c: application/sdp
l: 175

v=0
o=rtp 1219523689 1219523689 IN IP4 192.84.19.65
s=-
c=IN IP4 192.84.19.65
t=0 0
m=audio 28002 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```

63.209.0.77:5060-->192.84.19.65:40833

```
ACK sip:+14447895432@192.84.19.65:40833;transport=udp;user=phone SIP/2.0
f: <sip:15551231234@209.247.17.37>;tag=bp3FaT3Uk4JqK
t: <sip:+14447895432@acmetrunk.packet8.net.;user=phone>;tag=c0541341-13c4-48b07469-ae7bdf7-994f75c
i: SFOMGC0120080823203451008257@209.244.63.12
CSeq: 1900462892 ACK
Max-Forwards: 70
User-Agent: Packet8/1.1.126 (OutTrunkGateway) eSLEE/0.12.83
l: 0
v: SIP/2.0/UDP 63.209.0.77:5060;branch=z9hG4bKa3S00aebT0l5, SIP/2.0/TCP 63.209.0.77:5164;branch=z9hG4bKaM
LPj4TQyeod
m: <sip:bnKgZUBxRanAnUDhUId@63.209.0.77:5164>
Record-Route: <sip:bT9rRXPxRanAnUDhUId@63.209.0.77:5060;lr>
```

192.84.19.65:40833-->63.209.0.77:5060

```
BYE sip:bnKgZUBxRanAnUDhUId@63.209.0.77:5164 SIP/2.0
f: <sip:+14447895432@acmetrunk.packet8.net.;user=phone>;tag=c0541341-13c4-48b07469-ae7bdf7-994f75c
t: <sip:15551231234@209.247.17.37>;tag=bp3FaT3Uk4JqK
i: SFOMGC0120080823203451008257@209.244.63.12
CSeq: 1 BYE
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07470-ae7d979-1efae33a
Max-Forwards: 70
k: timer, replaces
User-Agent: AcmeUAS/1.6.0.34
Route: <sip:bT9rRXPxRanAnUDhUId@63.209.0.77:5060;lr>
l: 0
```

63.209.0.77:5060-->192.84.19.65:40833

```
SIP/2.0 200 OK
f: <sip:+14447895432@acmetrunk.packet8.net.;user=phone>;tag=c0541341-13c4-48b07469-ae7bdf7-994f75c
t: <sip:15551231234@209.247.17.37>;tag=bp3FaT3Uk4JqK
i: SFOMGC0120080823203451008257@209.244.63.12
CSeq: 1 BYE
v: SIP/2.0/UDP 192.84.19.65:40833;branch=z9hG4bK-48b07470-ae7d979-1efae33a
Record-Route: <sip:bT9rRXPxRanAnUDhUId@63.209.0.77:5060;lr>
Server: Packet8/1.1.126 (OutTrunkGateway) eSLEE/0.12.83
l: 0
m: <sip:bnKgZUBxRanAnUDhUId@63.209.0.77:5164
```

WARNING

Toll fraud is committed when individuals unlawfully gain access to a customers telecommunication system. This is a criminal offense. Currently, we do not know of any telecommunications system that is immune to this type of criminal activity. 8x8 will not accept liability for any damages, including long distance charges, which result from unauthorized and/or unlawful use. Although 8x8 has designed security features into its products and services, it is your sole responsibility to use the security features and to establish security practices within your organization, including training, security awareness, and call auditing to eliminate security risks.

NOTICE

While every effort has been made to ensure accuracy, 8x8 will not be liable for technical or editorial errors or omissions contained within the documentation. The information contained in this documentation is subject to change without notice. This documentation may be used only in accordance with the terms of the 8x8 License Agreement.

8x8

NASDAQ: EGHT
www.8x8.com