Copyright (C) 2019 Gaman SP z o.o

<https://gaman-gt.com>

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Twilio Cloud Connect with Cisco Cloud Service Router 1000V in AWS

Table of Contents

[General Overview 3](#_Toc1898877)

[Test environment 4](#_Toc1898878)

[Configuration procedure 5](#_Toc1898879)

[Configure and Add Security Group to your VPC 5](#_Toc1898880)

[Check the Cloud Connect Configuration on Twilio Console 6](#_Toc1898881)

[Create Elastic SIP Trunk on Twilio 6](#_Toc1898882)

[vRouter (vCube) Configuration 10](#_Toc1898883)

[SIP Call flow 11](#_Toc1898884)

[Troubleshooting 13](#_Toc1898885)

[Twilio Cloud Connect doesn’t respond to the SIP INVITE message 13](#_Toc1898886)

[Twilio Cloud Connect sends SIP 404 - Not a valid Twilio domain 14](#_Toc1898887)

[No audio issues 15](#_Toc1898888)

[Call is successful connected but dropped after 20-30 seconds 17](#_Toc1898889)

[Contact information 20](#_Toc1898890)

[Appendix 1 - vRouter licensing and pricing models on AWS 21](#_Toc1898891)

[Appendix 2 – Detailed SIP Log Reference 23](#_Toc1898892)

# General Overview

If look at the Twilio cloud services, you will find one called Cloud Connect. General description can be found here: <https://www.twilio.com/docs/interconnect/cloud-connect>. In general Cloud Connect allows you to connect your SIP infrastructure that resides in AWS with dedicated link with Twilio. High level of the solution is provided on Twilio webpage and looks like this:



The link between your VPC and the Twilio is done AWS backbone network. What limits you is the bandwidth assigned to the Cloud Connect link.

Before you consider this solution, you will need to verify the basic requirements, including:

* Your border devices (e.g. IP-PBX, SIP-PRI IAD, Session Border Controller, NAT gateway, etc.) will need to be assigned IPv4 addresses. The addresses must be public IPs - as opposed to [RFC 1918](https://tools.ietf.org/html/rfc1918) address ranges - to avoid conflicts with other networks that Twilio platform is peered with.
* You will need to add Twilio's IP ranges (Twilio Interconnect exchange) to the access control list on your firewall (e.g. AWS Network ACL) to allow your and Twilio's platform elements to talk to each other. The ranges vary and are assigned to location of the Twilio Interconnect exchange service.
* You will need to decide what bandwidth is needed for the communication. At this moment Twilio offers 10-Mbps, 100-Mbps, 500-Mbps (available in London & Singapore), 1-Gbps connection.
* You will need to consider the availability of the service in the AWS regions. At this moment the following regions are supported:
	+ AWS US East (Virginia) via Interconnect Exchange in Ashburn, Virginia
	+ AWS US West (Oregon) via Interconnect Exchange in San Jose, California
	+ AWS EU (Ireland) via Interconnect Exchange in London, United Kingdom
	+ AWS Asia Pacific (Singapore) via Interconnect Exchange in Singapore
* You will need to contact Twilio so they can prepare Cloud Connect service for you. During the setup process you will need to present to Twilio the public IP address of your border device.

Considering above requirements Gaman team started to build test environment.

# Test environment

To test the service Gaman team build up a test environment which is presented on the diagram below.



Our infrastructure is built with:

1. On premise infrastructure that consist of:
	1. Cisco Router acting as a VPN tunnel termination point and as a CUBE
	2. Voice infrastructure build with CUCM and UCCX
2. AWS infrastructure
	1. Cisco Cloud Service Router 1000V EC2 instance used as a CUBE – interconnection between on premise infrastructure and Twilio cloud connect service. In the next chapters this device will be called vRouter or vCube.

The main objective was to build setup that would allow calls originated from Gaman on premise infrastructure do out to PSTN through Twilio Cloud Connect service. To rise the bar even higher we assumed that this setup should work with UCCX outbound dialer.

In the next chapters you will find results of our tests. At the end UCCX dialer calls were delivered to PSTN without any delay.

# Configuration procedure

### Configure and Add Security Group to your VPC

Twilio Cloud Connect communicates directly with the border device of your infrastructure. In our test environment this is the VRouter which acts as a virtual CUBE. This CUBE is in the AWS VPC. The simplest way to enable communication between those 2 components is to add firewall rules under VPC. We recommend to create a new Security Group dedicated for Twilio Cloud Connect that will be assigned to your VPC.

Below is a sample of the configuration of the security group in our test environment. Our Twilio Cloud Connect Service was in US (Virginia) region.

Inbound security group



Outbound security group



Blow is the table that gathers all IP addresses that were published and need to be added as a firewall security groups based on the location.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Region** | **Type** | **IP ranges** | **Ports** | **Protocol** |
| US East (Virginia) | Signaling | 208.78.112.64208.78.112.65208.78.112.66 | 5060 | UDP/TCP |
| 5061 | TLS |
| Media | 208.78.112.64/26 | 10000 - 20000 | UDP |
| US West (Oregon) | Signaling | 67.213.136.6467.213.136.6567.213.136.66 | 5060 | UDP/TCP |
| 5061 | TLS |
| Media | 67,213.136.64/26 | 10000 - 20000 | UDP |
| AWS EU (Ireland) | Signaling | 185.187.132.68185.187.132.69185.187.132.70 | 5060 | UDP/TCP |
| 5061 | TLS |
| Media | 185.187.132.64/26 | 10000 - 20000 | UDP |
| AWS Asia Pacific (Singapore) | Signaling | 103.75.151.68103.75.151.69103.75.151.70 | 5060 | UDP/TCP |
| 5061 | TLS |
| Media | 103.75.151.64/26 | 10000 - 20000 | UDP |

### Check the Cloud Connect Configuration on Twilio Console

Twilio Cloud Connect Service is created by Twilio engineer. Before you will have the ability to deep dive in the configuration you will need to contact Twilio and provide them basic information. Remember that one of the is the public IP address of your edge device (visible as IP ROUTES on the Cloud Connect Information panel).

Once Twilio is done with the configuration you will receive basic information about your private service. To see it please log into your Twilio Console and navigate to: **All Products & Services > Super Network > Interconnect**. From the list select your Cloud Connect service. Details will be presented.



Note down the SID value (highlighted in red) – it will be needed in the voice gateway configuration section.

Base on the information above – Exchange – select your base URI using below table:

|  |  |  |
| --- | --- | --- |
| **Region** | **Exchange** | **URI** |
| US East (Virginia) | Ashburn, Virginia | {example}.pstn.us1-ix.twilio.com |
| US West (Oregon) | San Jose, California | {example}.pstn.us2-ix.twilio.com |
| AWS EU (Ireland) | London, United Kingdom | {example}.pstn.ie1-ix.twilio.com |
| AWS Asia Pacific (Singapore) | Singapore | {example}.pstn.sg1-ix.twilio.com |

Having valid URI replace the {example} section with the name of the Cloud Connect service. In our case the we used US East (Virginia) region and our trunk name was Gaman-Cloud. At the end we received the URI:

**Gaman-Cloud.pstn.us1-ix.twilio.com**

Note down this URI – it will be needed in the voice gateway configuration section.

### Create Elastic SIP Trunk on Twilio

Please use the below procedure to configure domain name (Elastic Sip Trunk) for your Twilio Cloud Connect Service.

1. Please navigate to **Super Network > Elastic SIP Trunking** section of the Twilio control panel.



1. Elastic SIP trunking requires configuration of the following elements:
	1. Authentication > IP Access Control List
	2. Trunks

**NOTE**

There is no need to create Authentication > Credential List as Twilio Cloud Connect Service uses different method of authentication – via tnx hash/SIP value in SIP Request URI header.

1. Click on the **Elastic SIP Trunking > Authentication** to expand the list to see all available options:



1. Navigate to **IP Access Control List** sub menu. New window will appear



1. Click the  button to add new ACL
2. New popup window will be presented



1. Fill in fields keeping in mind that
* Properties > Friendly Name is the name of the ACL. Name should directly indicate the user/organization that is assigned to this ACL
* IP Address Range > CIDR Network/Address is the public IP address/IP ranges of the network where vRouter (CUBE) resides.
* IP Address Range > Friendly Name (Optional) is the name of the range.

Once all fields are filled click Create ACL button  .

1. Navigate to **Trunks** menu. New window will appear



1. Click the  button to add new credentials. New window will appear.



1. Please enter a Friendly name – name assigned to trunk in Twilio. In our test example this name is set to: Gaman. Once entered click Create button .
2. New window will appear
3. Sip trunk configuration is split into 4 tabs: **General, Termination, Origination, Numbers**. All the elements can be found on sub menu.
4. **General** sub menu

Ensure that the following settings are set:

* Trunk name – is the name entered in step 14.
* Call Recording – if needed this option can be enabled (additional fees will be charged). Recording will be stored on Twilio cloud. In general please select “Do not Record” option from drop down list
* Secure Trunking – if needed signaling and media may be encrypted by enabling this feature (additional fees will be charged). In general to avoid issues leave this setting to Disabled.
* Call Transfer – leave setting on default, as enabled
* Allow Call Transfers to the PSTN via your Trunk – leave setting on default unchecked

When done click Save button .

1. **Termination** sub menu

Ensure that the following settings are set:

* Termination SIP URI – please enter the name of the SIP URI that will be used on the voice gateway configuration. Best practice is to create a dedicated URI for each customer. The format will always be: **<uri name>.pstn.twilio.com**

In our example the Elastic SIP Domain is: **gaman.pstn.twilio.com**

* IP Access control list – please add the ACL created in the steps above
* Credential list – leave credential list empty

When done click Save button .

1. **Numbers** sub menu



1. Click the  button. System will expand an additional menu



* **Add an Existing Number** – add one of the numbers that are already owned by your organization
* **Bulk Ass Existing Numbers** – add multiple numbers that are already owned by your organization
* **Buy a Number**
1. Click **Add an Existing Number**. New popup window will appear



1. From the list select the number and once done click Add Selected button .
2. Trunk configuration is done.

### vRouter (vCube) Configuration

Let’s start with the voice service voip section. To allow traffic from and to Twilio Media Gateway add the ip addresses ranges under ip address trusted list. Please use the IP range (taken from table available in [Configure and Add Security Group to your VPC](#_Configure_and_Add) section of this document) that matches your Cloud Connect location. Below sample is for US East (Virginia) region:

|  |
| --- |
| voice service voip ip address trusted list ipv4 208.78.112.64 ipv4 208.78.112.65 ipv4 208.78.112.66 ipv4 208.78.112.64 255.255.255.192 |

**NOTE**

Twilio uses different port ranges that are by default used by Cisco devices:

* For Twilio by default port range is from 10000 to 20000
* For Cisco by default port range is from 16384 to 32767

To extend the port range on Cisco vRouter please issue the following command under voice service voip (it should not be needed as CUBE should accept or connections but it’s good to add it):

|  |
| --- |
| rtp-port range 10000 32767 |

Once the voice service voip is configured, it is time to configure the sip-profile and adjust the SIP Header to the required by Twilio. Below is the example of SIP Header translation for our domain:

|  |
| --- |
| voice class sip-profiles 1 request ANY sip-header SIP-Req-URI modify "Gaman-Cloud.pstn.us1-ix.twilio.com" "gaman.pstn.twilio.com" request INVITE sip-header SIP-Req-URI modify "sip:((.\*)((@)(.\*))|((.\*):5060)) (SIP\/2.0)" "sip:\1;tnx=TN01011XXXXXXXXXXXXXXXXXXXXXXXXXXX \8" |

When applying this configuration please have in mind:

1. Gaman-Cloud.pstn.us1-ix.twilio.com is the Twilio Cloud Connect service name It should be replaced with the one that you received from Twilio. Please refer to [Check the Cloud Connect Configuration on Twilio Console](#_Check_the_Cloud) section of this document.
2. gaman.pstn.twilio.com is the name of the Elastic SIP Trunking service name configured under the Twilio console. Please refer to [Create Elastic SIP Trunk on Twilio](#_Create_Elastic_SIP) section of this document.
3. TN01011XXXXXXXXXXXXXXXXXXXXXXXXXXX is the hash/SID identifying your Twilio Cloud Connect Service. Please refer to [Check the Cloud Connect Configuration on Twilio Console](#_Check_the_Cloud) section of this document.
4. Remember to adjust the sip-profile number

Once this step is completed you can move forward to the last section – dial-peer configuration. Below is a sample of dial-peer configuration for the NANP numbering plan. This dial peer points out to the Twilio Cloud Connect Service.

|  |
| --- |
| dial-peer voice 2000 voip description -= Calls from vCUBE to Twilio =- translation-profile outgoing E164-Out destination-pattern [2-9]..[2-9]...... session protocol sipv2 session target dns:Gaman-Cloud.pstn.us1-ix.twilio.com session transport tcp voice-class sip early-offer forced voice-class sip profiles 1 dtmf-relay rtp-nte codec g711ulaw no vad |

When applying this configuration please keep in mind:

1. session target dns:Gaman-Cloud.pstn.us1-ix.twilio.com - replace the DNS name with the value provided by Twilio (Cloud Connect Service DNS name).
2. voice-class sip profiles 1 - assign the valid sip-profile to the outgoing dial-peer (number must match the id configured in the previous step).
3. session transport tcp – set the SIP transport protocol. In our case we had to use TCP. Tread more in the [Call is successful connected but dropped after 20-30 seconds](#_Call_is_successful) chapter of this document.
4. voice-class sip early-offer forced – early offer is required for most Internet SIP providers. This setting can be added under voice service voip level or here under dial-peer level.

### SIP Call flow

Sometimes it is good to visualize the signaling messages that come across systems in communication. Based on the logs gathered during the implementation process we created the below flowchart for SIP messages. On the diagram – 3 messages are marked with numbers. You will find explanation to those numbers in the [Troubleshooting](#_Troubleshooting) section of this document.

If you need to see entire SIP communication, please navigate to the [Appendix - Detailed SIP Log Reference](#_Appendix_2_–)



# Troubleshooting

Please look at the tips that may be useful when troubleshooting Cloud Connect link.

In the guides we used following convention for SIP Messages:

* Red – all messages send from vRouter to Twilio
* Blue – all messages received by vRouter from Twilio

### Twilio Cloud Connect doesn’t respond to the SIP INVITE message

Connecting to Twilio Cloud Connect can be tricky. The configuration of the service is different in different locations. During our tests, we tried to check the network connection using ICMP Ping. Results were interesting, some of the locations responded but some of them (like US East (Virginia)) did not. Conclusion is simple, using ping to check connectivity is not a good idea. Having that in mind we moved our checks to the SIP word. Because Twilio documentation is not so good we started with the following SIP INVITE structure - marked as on the sip diagram (SDP part of SIP frame is removed for clearance):

Sent:

INVITE sip:+1647XXXXXXX@gaman.pstn.twilio.com:5060 SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK14FB20AB

Remote-Party-ID: <sip:1648XXXXXXX@172.YYY.YYY.YYY>;party=calling;screen=no;privacy=off

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>

Date: Tue, 12 Feb 2019 08:02:41 GMT

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Supported: 100rel,timer,resource-priority,replaces,sdp-anat

Min-SE: 1800

Cisco-Guid: 1426215482-0270341829-1440371967-1355394071

User-Agent: Cisco-SIPGateway/IOS-16.9.1

Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER

CSeq: 101 INVITE

Timestamp: 1549958561

Contact: <sip:1648XXXXXXX@172.YYY.YYY.YYY:5060;transport=tcp>

Expires: 180

Allow-Events: telephone-event

Max-Forwards: 68

Session-ID: d9f4f55c15b558a18306f14451d81b7d;remote=00000000000000000000000000000000

Content-Type: application/sdp

Content-Disposition: session;handling=required

Content-Length: 249

What happened – Twilio didn’t respond. This was interesting, so we deep dived into the problem. The root cause was the structure of the SIP Request URI. When working with Twilio Cloud Connect, SIP Request URI must be built:

1. With a valid configured domain recognized by Twilio
2. With an additional parameter called tnx= - it is used as a authentication hash to allow entry to the Twilio infrastructure.

Having that in mind the valid SIP Request URI should look like this:

Sent:

INVITE sip:+1647XXXXXXX@gaman.pstn.twilio.com:5060;tnx=TN01011XXXXXXXXXXXXXXXXXXXXXXXXXXX SIP/2.0

What is also interesting if you send an SIP INVITE with the following structure (without tnx= and with the domain equal to the DNS name of the Twilio Cloud Connect Service servers:

Sent:

INVITE sip:+16475607805@Gaman-Cloud.pstn.us1-ix.twilio.com:5060 SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK148F196A

Remote-Party-ID: <sip:1648XXXXXXX@172.YYY.YYY.YYY>;party=calling;screen=no;privacy=off

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=CEFCDE64-1628

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>

Date: Tue, 12 Feb 2019 01:37:20 GMT

Call-ID: 92DA5966-2D9D11E9-98FDC3D9-6221335B@172.YYY.YYY.YYY

Supported: 100rel,timer,resource-priority,replaces,sdp-anat

Min-SE: 1800

Cisco-Guid: 0462048170-2102600894-1658044365-0965779260

User-Agent: Cisco-SIPGateway/IOS-16.9.1

Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER

CSeq: 101 INVITE

Timestamp: 1549935440

Contact: <sip:1648XXXXXXX@172.YYY.YYY.YYY:5060;transport=tcp>

Expires: 180

Allow-Events: telephone-event

Max-Forwards: 68

Session-ID: 676e6635daf85c34803d08aa8b326a59;remote=00000000000000000000000000000000

Content-Type: application/sdp

Content-Disposition: session;handling=required

Content-Length: 248

Twilio will respond but this this may lead to the 404 error described in the next section of this document.

### Twilio Cloud Connect sends SIP 404 - Not a valid Twilio domain

Please look at the following SIP call flow:

Sent:

INVITE sip:+16475607805@Gaman-Cloud.pstn.us1-ix.twilio.com:5060;tnx=TN01011XXXXXXXXXXXXXXXXXXXXXXX SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK148F196A

Remote-Party-ID: <sip:1648XXXXXXX@172.YYY.YYY.YYY>;party=calling;screen=no;privacy=off

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=CEFCDE64-1628

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>

Date: Tue, 12 Feb 2019 01:37:20 GMT

Call-ID: 92DA5966-2D9D11E9-98FDC3D9-6221335B@172.YYY.YYY.YYY

Supported: 100rel,timer,resource-priority,replaces,sdp-anat

Min-SE: 1800

Cisco-Guid: 0462048170-2102600894-1658044365-0965779260

User-Agent: Cisco-SIPGateway/IOS-16.9.1

Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER

CSeq: 101 INVITE

Timestamp: 1549935440

Contact: <sip:1648XXXXXXX@172.YYY.YYY.YYY:5060;transport=tcp>

Expires: 180

Allow-Events: telephone-event

Max-Forwards: 68

Session-ID: 676e6635daf85c34803d08aa8b326a59;remote=00000000000000000000000000000000

Content-Type: application/sdp

Content-Disposition: session;handling=required

Content-Length: 248

v=0

o=CiscoSystemsSIP-GW-UserAgent 9175 411 IN IP4 34.XXX.XXX.XXX

s=SIP Call

c=IN IP4 34.XXX.XXX.XXX

t=0 0

m=audio 8100 RTP/AVP 0 101

c=IN IP4 34.XXX.XXX.XXX

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-15

a=ptime:20

Received:

SIP/2.0 100 Giving a try

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;received=34.XXX.XXX.XXX;rport=28777;branch=z9hG4bK148F196A

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=CEFCDE64-1628

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>

Call-ID: 92DA5966-2D9D11E9-98FDC3D9-6221335B@172.YYY.YYY.YYY

CSeq: 101 INVITE

Server: Twilio Gateway

Content-Length: 0

Received:

SIP/2.0 404 Not a valid Twilio domain

CSeq: 101 INVITE

Call-ID: 92DA5966-2D9D11E9-98FDC3D9-6221335B@172.YYY.YYY.YYY

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=CEFCDE64-1628

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=25983233\_6772d868\_04ebabe6-fef9-4a10-9d8a-fdb0fbb390a2

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;rport=28777;received=34.XXX.XXX.XXX;branch=z9hG4bK148F196A

Timestamp: 1549935440

Server: Twilio

Contact: <sip:172.18.40.157:5060>

Content-Length: 0

If this call flow we highlighted 2 lines:

1. SIP Request URI from the first INVITE (marked as on the sip diagram).
2. Response code and message that we got from Twilio

Why is this happening?

As you can see SIP Request URI points to the domain Gaman-Cloud.pstn.us1-ix.twilio.com. This domain is only used to get the IP addresses of Twilio Cloud Connect service based on the location. Twilio expects that in this place it will get a domain configured under Elastic SIP Trunking on the Twilio console.

In our case – it is the gaman.pstn.twilio.com. So the SIP Request URI should look like this:

Sent:

INVITE sip:+1647XXXXXXX@gaman.pstn.twilio.com:5060;tnx=TN01011XXXXXXXXXXXXXXXXXXXXXXXXXXX SIP/2.0

Please verify this before you do further troubleshooting.

### No audio issues

When you experience no audio issues please check if:

1. All communication ports for media are added for firewall rules. Please refer to the table in the [Configure and Add Security Group to your VPC](#_Configure_and_Add) section in this document.
2. Check the SDP headers for SIP messages that are going out to the Twilio. If your border device uses 2 NIC’s (one for Internet access, one for internal communication) it may happen that IP addresses in SDP are invalid. To check that please look at the first SIP INVITE (marked as on the sip diagram). In SDP you will always need to see public IP’s not private ones.

Below is a sample of invalid SIP message with SDP. The invalid IP addresses were highlighted in yellow:

Sent:

INVITE sip:+1647XXXXXXX@gaman.pstn.twilio.com:5060;tnx=TN01011XXXXXXXXXXXXXXXXXXXXXXXXXXX SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK14FB20AB

Remote-Party-ID: <sip:1648XXXXXXX@172.YYY.YYY.YYY>;party=calling;screen=no;privacy=off

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>

Date: Tue, 12 Feb 2019 08:02:41 GMT

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Supported: 100rel,timer,resource-priority,replaces,sdp-anat

Min-SE: 1800

Cisco-Guid: 1426215482-0270341829-1440371967-1355394071

User-Agent: Cisco-SIPGateway/IOS-16.9.1

Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER

CSeq: 101 INVITE

Timestamp: 1549958561

Contact: <sip:1648XXXXXXX@172.YYY.YYY.YYY:5060;transport=tcp>

Expires: 180

Allow-Events: telephone-event

Max-Forwards: 68

Session-ID: d9f4f55c15b558a18306f14451d81b7d;remote=00000000000000000000000000000000

Content-Type: application/sdp

Content-Disposition: session;handling=required

Content-Length: 249

v=0

o=CiscoSystemsSIP-GW-UserAgent 4922 9570 IN IP4 172.YYY.YYY.YYY

s=SIP Call

c=IN IP4 172.YYY.YYY.YYY

t=0 0

m=audio 8130 RTP/AVP 0 101

c=IN IP4 172.YYY.YYY.YYY

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-15

a=ptime:20

To resolve this issue additional translations are needed. They must be added to the voice class sip-profiles object on the voice gateway. Here are recommended translations:

|  |
| --- |
| response ANY sdp-header Audio-Connection-Info modify "172.YYY.YYY.YYY" "34.XXX.XXX.XXX"response ANY sdp-header Connection-Info modify "172.YYY.YYY.YYY" "34.XXX.XXX.XXX"response ANY sdp-header Session-Owner modify "172.YYY.YYY.YYY" "34.XXX.XXX.XXX"request ANY sdp-header Audio-Connection-Info modify "172.YYY.YYY.YYY" "34.XXX.XXX.XXX"request ANY sdp-header Connection-Info modify "172.YYY.YYY.YYY" "34.XXX.XXX.XXX"request ANY sdp-header Session-Owner modify "172.YYY.YYY.YYY" "34.XXX.XXX.XXX" |

**IMPORTANT!!!**

Before you apply the following rules please change the IP’s:

* 172.YYY.YYY.YYY – to your internal IP address
* 34.XXX.XXX.XXX – to your public IP address (Internet)

### Call is successful connected but dropped after 20-30 seconds

If you review Twilio troubleshooting guide you will find this problem as a one of the described. Twilio indicates 2 possible root causes (<https://www.twilio.com/docs/sip-trunking/troubleshooting#problem30>):

1. From Twilio: *“You SIP communications infrastructure is incorrectly Sending an ACK to Twilio using an IP address other than the Contact header's IP address found in Twilio's 200 OK in the Request-URI. This causes Twilio to not process the ACK, so the transaction times out after 30 seconds, and the call is torn down via a BYE sent from Twilio's side to both sides of the call.*

*Your SIP communications infrastructure should use the IP address in the Contact header of Twilio's 200 OK in the Request-URI of the ACK and send the ACK to the IP address in the Record-Route header of the same 200 OK.”*

To understand this cause let’s look at the 2 frames (marked on the sip diagram with numbers and . Here 2 messages – valid example, for clearance SDP header was removed from SIP frame:

Received:

SIP/2.0 200 OK

CSeq: 101 INVITE

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;rport=47202;received=34.XXX.XXX.XXX;branch=z9hG4bK14FB20AB

Record-Route: <sip:172.18.24.78:5060;r2=on;transport=udp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Record-Route: <sip:208.78.112.64:5060;r2=on;transport=tcp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Timestamp: 1549958561

Server: Twilio

Contact: <sip:172.18.49.157:5060>

Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY

Content-Type: application/sdp

X-Twilio-CallSid: CA86709cb205c057544def524f55ccc6dc

Content-Length: 240

Sent:

ACK sip:172.18.49.157:5060 SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK14FC1F6E

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Date: Tue, 12 Feb 2019 08:02:41 GMT

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Route: <sip:208.78.112.64:5060;r2=on;transport=tcp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>,<sip:172.18.24.78:5060;r2=on;transport=udp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Max-Forwards: 70

CSeq: 101 ACK

Allow-Events: telephone-event

Session-ID: d9f4f55c15b558a18306f14451d81b7d;remote=df83546a26525df9a8a6ce497941cb9a

Content-Length: 0

Important part is highlighted with yellow. Information provided in the SIP Contact Header in the frame received from Twilio should appear in the SIP ACK frame send back to Twilio. It may happen that translations that you apply for you SIP Header affect this SIP-URI-Request. Please validate tis in your traces.

1. From Twilio: “*Your SIP communications infrastructure is incorrectly adjusting/replacing the Twilio Private IP addresses in the URI and headers of the ACK they return with their own Public IP addresses. This is causing Twilio to route the ACK back to the SIP communications infrastructure, and as such not process it. Because the ACK is not processed, Twilio (correctly) times out and tears down the call.*

*Your SIP communications infrastructure should never replace any of Twilio's own IP addresses; they should only adjust their own IP addresses.*”

 To understand this let’s look at the SDP Header received from Twilio:

v=0

o=root 1990313469 1990313469 IN IP4 208.78.112.118

s=Twilio Media Gateway

c=IN IP4 208.78.112.118

t=0 0

m=audio 19688 RTP/AVP 0 101

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-16

a=ptime:20

a=sendrecv

Important parts were highlighted in yellow. What Twilio says’ those IP addresses should not be modified and changed as they are set by Twilio’s Media Gateway. If you are observing this type of messages please review your voice class sip-profiles configured on the voice gateway. Translation presented in the [No audio issues](#_No_audio_issues) section work only on the IP addresses assigned to the edge device should not affect media IP ranges received in SIP SDP Header from Twilio.

Those two tips are very helpful but, in our case, they did not resolve 20-30 second call drops. After taking long debug session, Gaman team discovered potential 3 possible cause of the issue:

1. Our primary setup of the test environment was done using UDP SIP Signaling. All messages across all components were using UDP. But as mentioned above – we experienced a call drop. Because we didn’t have any ideas, we switched the SIP Signaling to TCP. And that was the problem solution. If you look at the proposed dial-peer configuration you will see that there is a session transport tcp forced on it.

At the end we didn’t debug the problem deeper. We don’t know if this is something with our environment or Twilio Media Gateway problem.

Our Tip

If experience 20-30 second call drops and use UDP for SIP Signaling between Twilio and your edge device, change the SIP Signaling to TCP but only for this connection. Other parts of infrastructure can be left on UDP.

# Contact information

If presented solution interested you, you have questions or ideas how we can improve this article feel free to contact us using the following email addresses. Our team is always happy to answer your questions and help you with your deployment.

**Email addresses**

General, Sales mailbox **(****info@gaman-gt.com****)**

Support mailbox (**support@gaman-gt.com****)**

To find out more about Gaman Team and our project please visit our **Website:** [**https://gaman-gt.com**](https://gaman-gt.com)

Find us in social networks:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Linked In** | **Twitter** | **Upwork** |

# Appendix 1 - vRouter licensing and pricing models on AWS

Here is a table that presents the available licensing and pricing models including license cost for a vRouter. All costs were calculated at the end of 2018 and they may change in future. To calculate the costs, we assumed that the AWS provisioning will be made via **Reserved Instance** and all will be payed **Upfront**.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Region | Central |   |   |   |
| Term | 1 Year |   |   |   |
| Payment option | All upfront |   |   |   |
| Instance type (Reserved Instance) | t2 medium |  |   |
|  |  |  |  |
| **Cisco License "from AWS"**  | 1 year |  | **Cisco License BYOL (all features)**  | 1 year |
| Cisco license - 1year |  2 233,00$  |  | Cisco license 10MB throughput (L-CSR-10M-AX=) |  2 550,00$  |
| EC2 T2 medium RI standard |  261,00$  |  | Cisco SWSS CON-ECMU-LCSRAX1M - 12 month (EMEA GPL, perpetual license) | 440,45$ |
| Provisioned Storage |  5,28$  |  | EC2 T2 medium RI standard | 261,00$  |
| I/O requests |   |  | Provisioned Storage |  5,28$  |
| Data transfer fees |   |  | I/O requests |   |
| Additional Elastic IP |  43,92$  |  | Data transfer fees |   |
| **TOTAL** |  **2 543,20$**  |  | Additional Elastic IP |  43,92$  |
|  |  |  | **TOTAL** |  **3 300,65$**  |
|  |  |  |  |  |
|  |  |  | **Cisco License BYOL (No TLS/SRTP support)**  | 1 year |
|  |  |  | Cisco license 10MB throughput L-CSR-10M-APP=) |  1 660,00$  |
|  |  |  | Cisco SWSS CON-ECMU-LCS1MAPP - 12 month (EMEA GPL, perpetual license) | 286,35$ |
|  |  |  | EC2 T2 medium RI standard |  261,00$  |
|  |  |  | Provisioned Storage |  5,28$  |
|  |  |  | I/O requests |   |
|  |  |  | Data transfer fees |   |
| BYOL – Buy Your Own Licenses |  |  | Additional Elastic IP |  43,92$  |
|  |  |  | **TOTAL** |  **2 256,55$**  |

# Appendix 2 – Detailed SIP Log Reference

Below you can find a reference SIP communication log between vRouter (acting as a virtual Cube) and Twilio Cloud Connect. All logs were gathered from the vRouter side. Logs are marked with 2 colors:

* Red – all messages send from vRouter to Twilio
* Blue – all messages received by vRouter from Twilio

This log may be used to compare your SIP dumps with the working log to check SIP Headers. All IP’s and ID’s were hidden.

Sent:

INVITE sip:+1647XXXXXXX@gaman.pstn.twilio.com:5060;tnx=TN01011XXXXXXXXXXXXXXXXXXXXXXXXXXX SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK14FB20AB

Remote-Party-ID: <sip:1648XXXXXXX@172.YYY.YYY.YYY>;party=calling;screen=no;privacy=off

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>

Date: Tue, 12 Feb 2019 08:02:41 GMT

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Supported: 100rel,timer,resource-priority,replaces,sdp-anat

Min-SE: 1800

Cisco-Guid: 1426215482-0270341829-1440371967-1355394071

User-Agent: Cisco-SIPGateway/IOS-16.9.1

Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER

CSeq: 101 INVITE

Timestamp: 1549958561

Contact: <sip:1648XXXXXXX@172.YYY.YYY.YYY:5060;transport=tcp>

Expires: 180

Allow-Events: telephone-event

Max-Forwards: 68

Session-ID: d9f4f55c15b558a18306f14451d81b7d;remote=00000000000000000000000000000000

Content-Type: application/sdp

Content-Disposition: session;handling=required

Content-Length: 249

v=0

o=CiscoSystemsSIP-GW-UserAgent 4922 9570 IN IP4 34.XXX.XXX.XXX

s=SIP Call

c=IN IP4 34.XXX.XXX.XXX

t=0 0

m=audio 8130 RTP/AVP 0 101

c=IN IP4 34.XXX.XXX.XXX

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-15

a=ptime:20

Received:

SIP/2.0 100 Giving a try

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;received=34.XXX.XXX.XXX;rport=47202;branch=z9hG4bK14FB20AB

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

CSeq: 101 INVITE

Server: Twilio Gateway

Content-Length: 0

Received:

SIP/2.0 180 Ringing

CSeq: 101 INVITE

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;rport=47202;received=34.XXX.XXX.XXX;branch=z9hG4bK14FB20AB

Record-Route: <sip:172.18.24.78:5060;r2=on;transport=udp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Record-Route: <sip:208.78.112.64:5060;r2=on;transport=tcp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Timestamp: 1549958561

Server: Twilio

Contact: <sip:172.18.49.157:5060>

X-Twilio-CallSid: CA86709cb205c057544def524f55ccc6dc

Content-Length: 0

Received:

SIP/2.0 200 OK

CSeq: 101 INVITE

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;rport=47202;received=34.XXX.XXX.XXX;branch=z9hG4bK14FB20AB

Record-Route: <sip:172.18.24.78:5060;r2=on;transport=udp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Record-Route: <sip:208.78.112.64:5060;r2=on;transport=tcp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Timestamp: 1549958561

Server: Twilio

Contact: <sip:172.18.49.157:5060>

Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY

Content-Type: application/sdp

X-Twilio-CallSid: CA86709cb205c057544def524f55ccc6dc

Content-Length: 240

v=0

o=root 1990313469 1990313469 IN IP4 208.78.112.118

s=Twilio Media Gateway

c=IN IP4 208.78.112.118

t=0 0

m=audio 19688 RTP/AVP 0 101

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-16

a=ptime:20

a=sendrecv

Sent:

ACK sip:172.18.49.157:5060 SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK14FC1F6E

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Date: Tue, 12 Feb 2019 08:02:41 GMT

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Route: <sip:208.78.112.64:5060;r2=on;transport=tcp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>,<sip:172.18.24.78:5060;r2=on;transport=udp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Max-Forwards: 70

CSeq: 101 ACK

Allow-Events: telephone-event

Session-ID: d9f4f55c15b558a18306f14451d81b7d;remote=df83546a26525df9a8a6ce497941cb9a

Content-Length: 0

Sent:

INVITE sip:172.18.49.157:5060 SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK14FD1971

Remote-Party-ID: "TOR-Outbound" <sip:4479@172.YYY.YYY.YYY>;party=calling;screen=no;privacy=off

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Date: Tue, 12 Feb 2019 08:02:49 GMT

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Route: <sip:208.78.112.64:5060;r2=on;transport=tcp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>,<sip:172.18.24.78:5060;r2=on;transport=udp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Supported: 100rel,timer,resource-priority,replaces,sdp-anat

Min-SE: 1800

Cisco-Guid: 1426215482-0270341829-1440371967-1355394071

User-Agent: Cisco-SIPGateway/IOS-16.9.1

Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER

CSeq: 102 INVITE

Max-Forwards: 70

Timestamp: 1549958569

Contact: <sip:1648XXXXXXX@172.YYY.YYY.YYY:5060;transport=tcp>

Expires: 180

Allow-Events: telephone-event

Session-ID: d9f4f55c15b558a18306f14451d81b7d;remote=df83546a26525df9a8a6ce497941cb9a

Content-Type: application/sdp

Content-Length: 249

v=0

o=CiscoSystemsSIP-GW-UserAgent 4922 9570 IN IP4 34.XXX.XXX.XXX

s=SIP Call

c=IN IP4 34.XXX.XXX.XXX

t=0 0

m=audio 8130 RTP/AVP 0 101

c=IN IP4 34.XXX.XXX.XXX

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-15

a=ptime:20

Received:

SIP/2.0 100 Giving a try

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;received=34.XXX.XXX.XXX;rport=47202;branch=z9hG4bK14FD1971

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

CSeq: 102 INVITE

Server: Twilio Gateway

Content-Length: 0

Received:

SIP/2.0 200 OK

CSeq: 102 INVITE

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;rport=47202;received=34.XXX.XXX.XXX;branch=z9hG4bK14FD1971

Timestamp: 1549958569

Server: Twilio

Contact: <sip:172.18.49.157:5060>

Record-Route: <sip:172.18.24.78:5060;r2=on;transport=udp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Record-Route: <sip:208.78.112.64:5060;r2=on;transport=tcp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Content-Type: application/sdp

X-Twilio-CallSid: CA86709cb205c057544def524f55ccc6dc

Content-Length: 240

v=0

o=root 1990313469 1990313470 IN IP4 208.78.112.118

s=Twilio Media Gateway

c=IN IP4 208.78.112.118

t=0 0

m=audio 19688 RTP/AVP 0 101

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-16

a=ptime:20

a=sendrecv

Sent:

ACK sip:172.18.49.157:5060 SIP/2.0

Via: SIP/2.0/TCP 172.YYY.YYY.YYY:5060;branch=z9hG4bK14FE5F1

From: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

To: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

Date: Tue, 12 Feb 2019 08:02:49 GMT

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Route: <sip:208.78.112.64:5060;r2=on;transport=tcp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>,<sip:172.18.24.78:5060;r2=on;transport=udp;ftag=D05DA885-223D;lr;twnat=sip:34.XXX.XXX.XXX:47202>

Max-Forwards: 70

CSeq: 102 ACK

Allow-Events: telephone-event

Session-ID: d9f4f55c15b558a18306f14451d81b7d;remote=df83546a26525df9a8a6ce497941cb9a

Content-Length: 0

Received:

BYE sip:1648XXXXXXX@172.YYY.YYY.YYY:5060;transport=tcp SIP/2.0

CSeq: 1 BYE

From: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

To: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Max-Forwards: 68

Via: SIP/2.0/TCP 208.78.112.64:5060;branch=z9hG4bK7feb.a99b3d03.0

Via: SIP/2.0/UDP 172.18.49.157:5060;rport=5060;received=172.18.49.157;branch=z9hG4bK279ab587-af2f-482b-a83a-d74d0000999e\_6772d868\_352-13226931207023951702

User-Agent: Twilio Gateway

X-Twilio-CallSid: CA86709cb205c057544def524f55ccc6dc

Content-Length: 0

Sent:

SIP/2.0 200 OK

Via: SIP/2.0/TCP 208.78.112.64:5060;branch=z9hG4bK7feb.a99b3d03.0,SIP/2.0/UDP 172.18.49.157:5060;rport=5060;received=172.18.49.157;branch=z9hG4bK279ab587-af2f-482b-a83a-d74d0000999e\_6772d868\_352-13226931207023951702

From: <sip:+1647XXXXXXX@Gaman-Cloud.pstn.us1-ix.twilio.com>;tag=92752060\_6772d868\_279ab587-af2f-482b-a83a-d74d0000999e

To: <sip:1648XXXXXXX@gaman.pstn.twilio.com>;tag=D05DA885-223D

Date: Tue, 12 Feb 2019 08:03:48 GMT

Call-ID: 67B38A52-2DD311E9-9929C3D9-6221335B@172.YYY.YYY.YYY

Server: Cisco-SIPGateway/IOS-16.9.1

CSeq: 1 BYE

Reason: Q.850;cause=16

Session-ID: d9f4f55c15b558a18306f14451d81b7d;remote=df83546a26525df9a8a6ce497941cb9a

Content-Length: 0