Avaya One-x mobile Remote Worker for IP Office with SBCE 7.1

Prepared by: Ruel Alagao and Guangyu Hao

Topic Overview

❑ Simulation Deployment Diagram

❑ IP Office Related Configuration

❑ One-x Portal Related Configuration

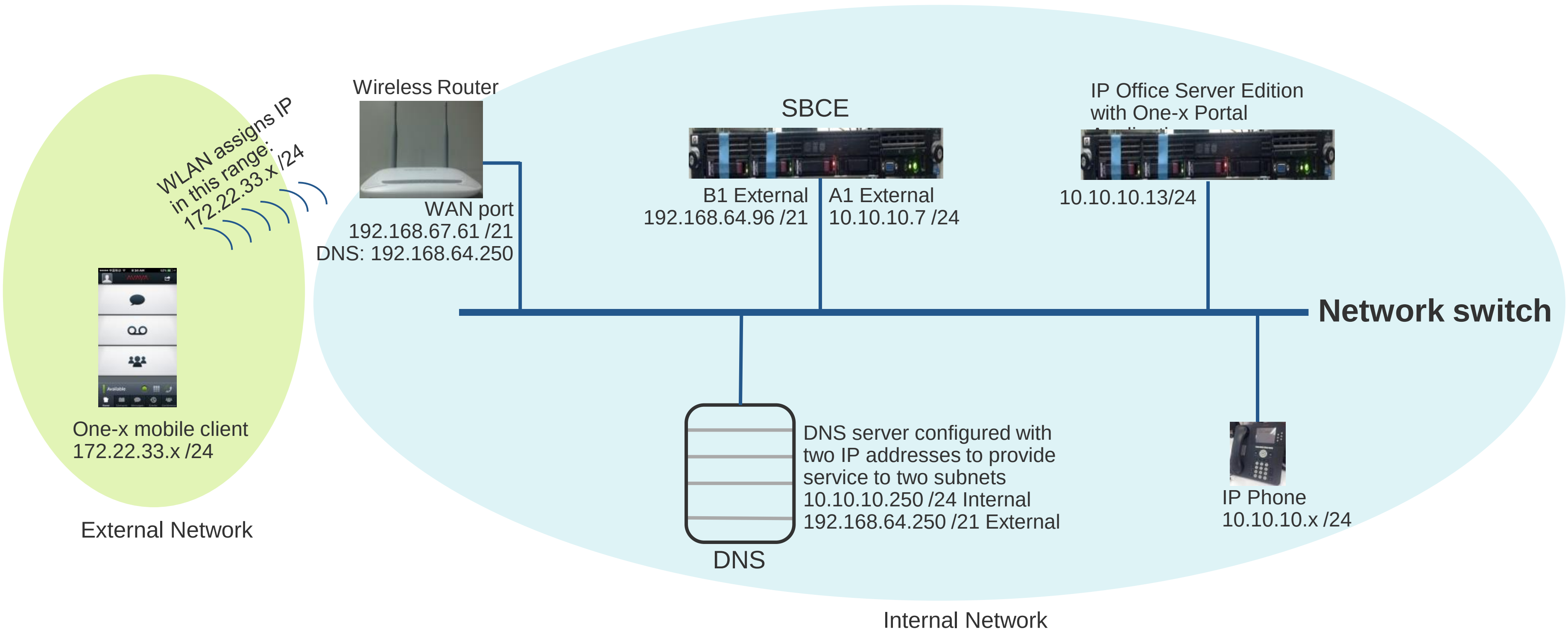
❑ SBCE Related Configuration

❑ Expected Flow of Messages

❑ Important Notes

Simulation Deployment Diagram

Simulation Deployment Diagram



Note: *This document simulates the actual setup the customer may have. We simulated the "External" network by using a Wireless Router device - The WAN port of the Wireless Router is interfaced to the SBCE B1 interface and the wireless side simulates the external/public network interfaced the One-x mobile clients. The WAN port has the same IP subnet as the SBCE and the wireless has different subnet which assigns IP address to the One-x mobile client device.*

Simulation Components

❑ IP Office Server Edition and One-x Portal Server on the same machine
Release: 9.1.7
IP Address: 10.10.10.13 /24
Gateway: 10.10.10.1
FQDN: ipo1xp.ipolab.com

❑ Session Border Controller for Enterprise 7.1
EMS: 192.168.64.90 /21
B1 Interface: 192.168.64.96 /21 External Interface
A1 Interface: 10.10.10.7 /24 Internal Interface

❑ DNS servers on internal and external network
IP Address: 10.10.10.250 /24 for internal network
IP Address: 192.168.64.250 /21 for external network

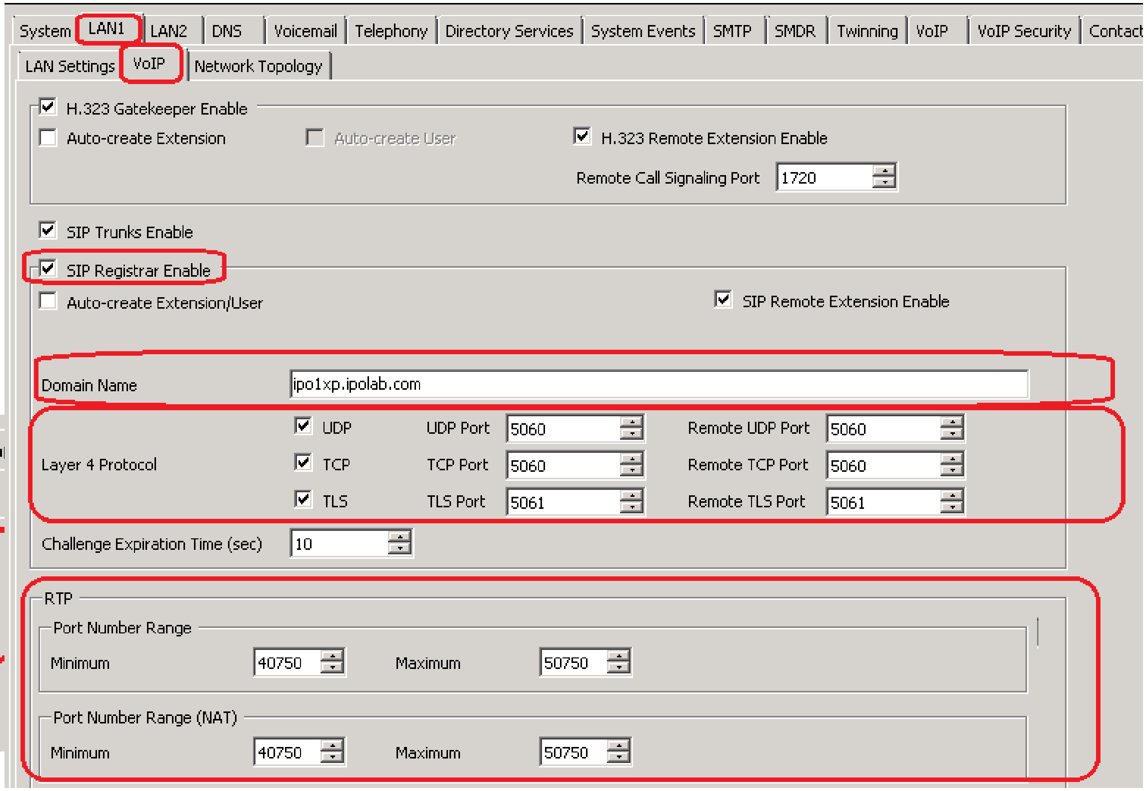
❑ Wireless Router – is utilized to simulate external network
WAN port: 192.168.67.61 /21 (Same subnet as the SBCE B1 interface)
Wireless network: 172.22.33.x /24. Utilized to assign IP subnet to the One-x mobile client. It simulates the 3G/4G/Public Wifi network.

IP Office Related Configuration

IP Office Related Configuration

It is assumed that the IP Office Server Edition has already been installed and configured basic information. The points shown here are the details we needed to setup the One-x mobile client user and be able to register to the One-x Portal and IP Office.

- Verify LAN1 IP Address
- SIP Registrar Enable for One-x mobile client registration
- Domain Name
- Layer 4 Protocols
- RTP ports



☑ H.323 Gatekeeper Enable

□ Auto-create Extension □ Auto-create User ☑ H.323 Remote Extension Enable

Remote Call Signaling Port 1720

☑ SIP Trunks Enable

☑ SIP Registrar Enable

□ Auto-create Extension/User ☑ SIP Remote Extension Enable

Domain Name ipo1xp.ipolab.com

Layer 4 Protocol	☑ UDP	UDP Port	5060	Remote UDP Port	5060
	☑ TCP	TCP Port	5060	Remote TCP Port	5060
	☑ TLS	TLS Port	5061	Remote TLS Port	5061

Challenge Expiration Time (sec) 10

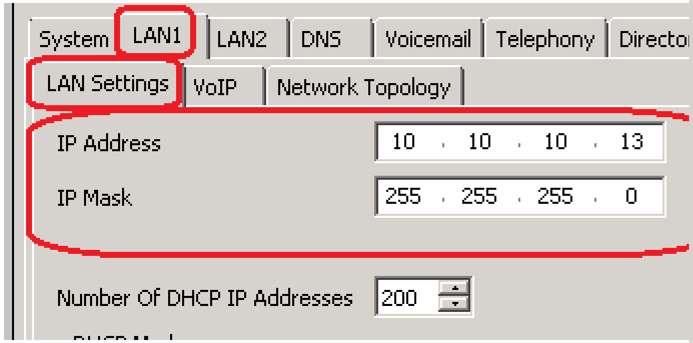
RTP

Port Number Range

Minimum 40750 Maximum 50750

Port Number Range (NAT)

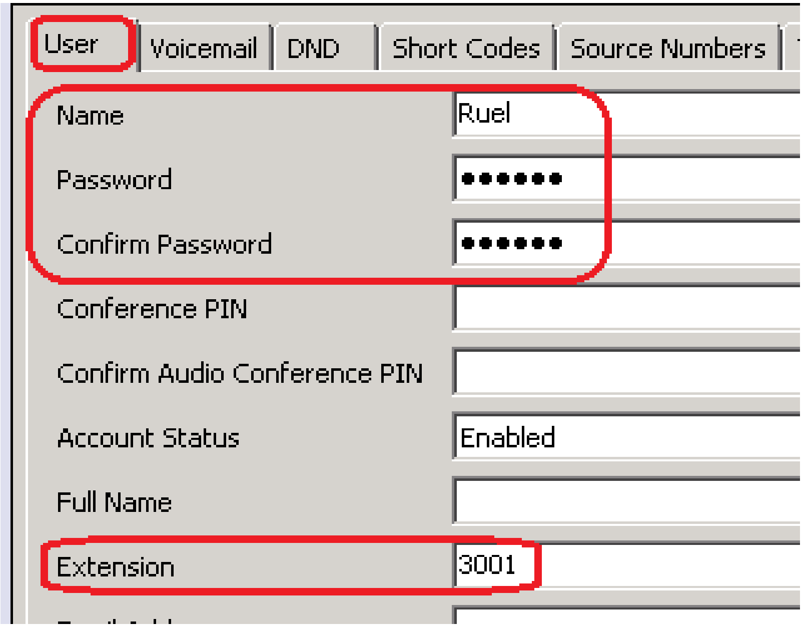
Minimum 40750 Maximum 50750



IP Address 10 . 10 . 10 . 13

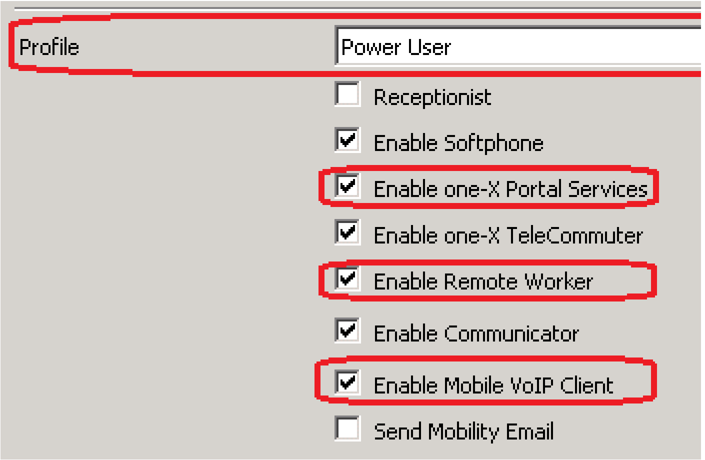
IP Mask 255 . 255 . 255 . 0

Number Of DHCP IP Addresses 200



Name	Ruel
Password	••••••
Confirm Password	••••••
Conference PIN	
Confirm Audio Conference PIN	
Account Status	Enabled
Full Name	
Extension	3001

User settings:
- User name and password
- Assigned extension
- Power User Profile
- Enable one-X Portal Services
- Enable Mobile VoIP Client



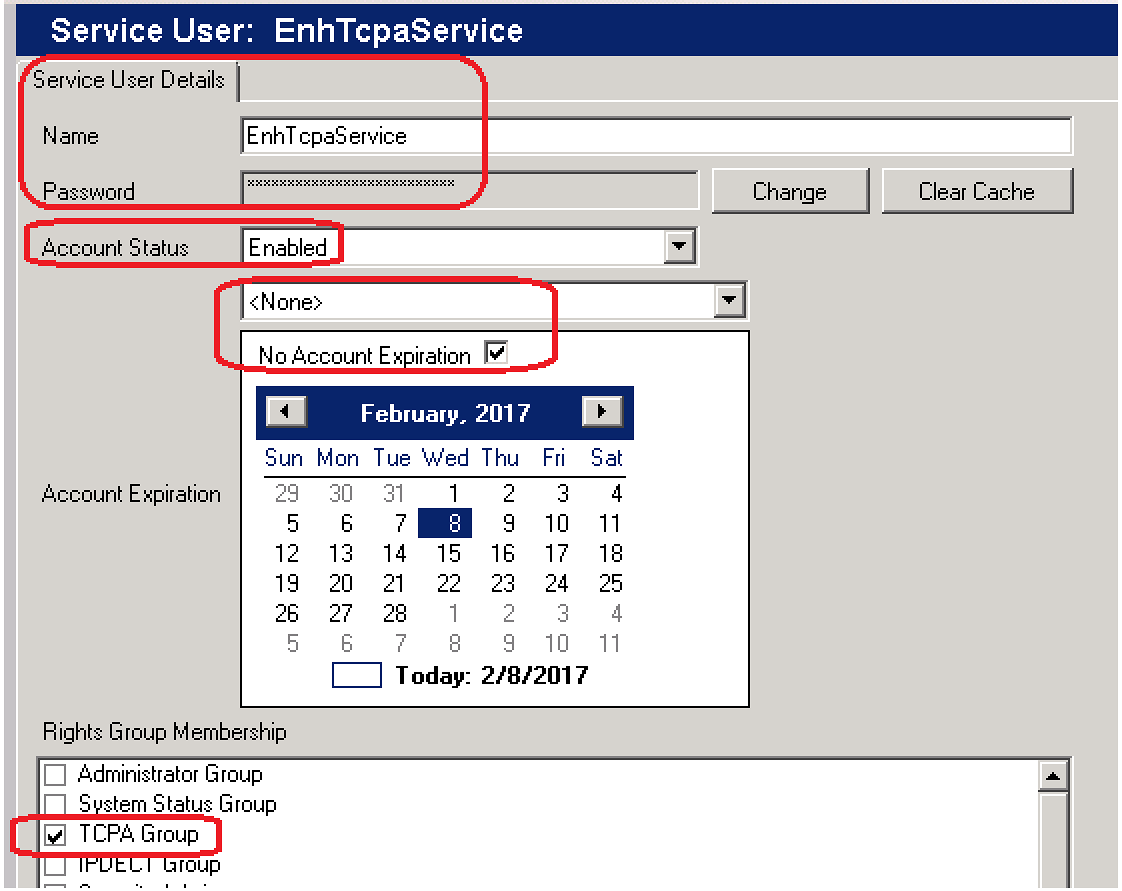
Profile	Power User

□ Receptionist
☑ Enable Softphone
☑ Enable one-X Portal Services
☑ Enable one-X TeleCommuter
☑ Enable Remote Worker
☑ Enable Communicator
☑ Enable Mobile VoIP Client
□ Send Mobility Email

IP Office Security settings: When you add IP Office in the One-x Portal, the credentials here are the ones to be used for connection.

If you changed the default password, it has to be set in the One-x Portal CSTA Telephony Provider as well.

Default password is EnhTcpaPwd1



Service User: EnhTcpaService

Service User Details

Name: EnhTcpaService

Password: ****************************

Account Status: Enabled

<None>

No Account Expiration ☑

Account Expiration

February, 2017

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	1	2	3	4
5	6	7	8	9	10	11

Today: 2/8/2017

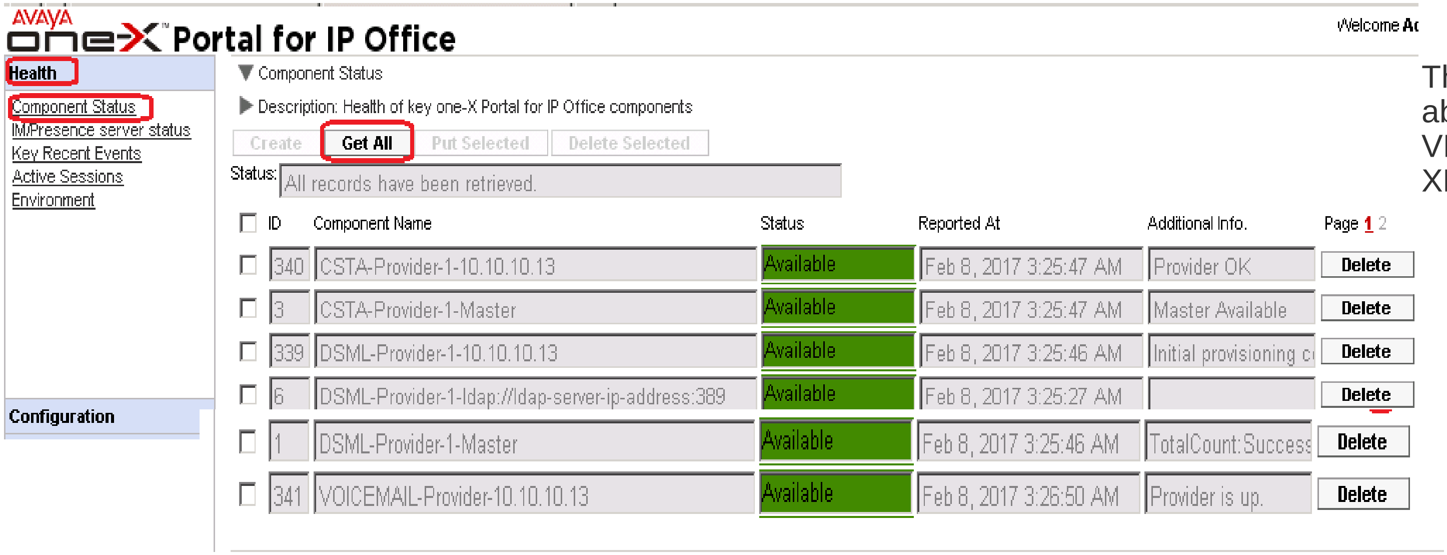
Rights Group Membership

- □ Administrator Group
- □ System Status Group
- ☑ TCPA Group
- □ IPDECT Group

One-x Portal Related Configuration

One-x Portal Related Configuration

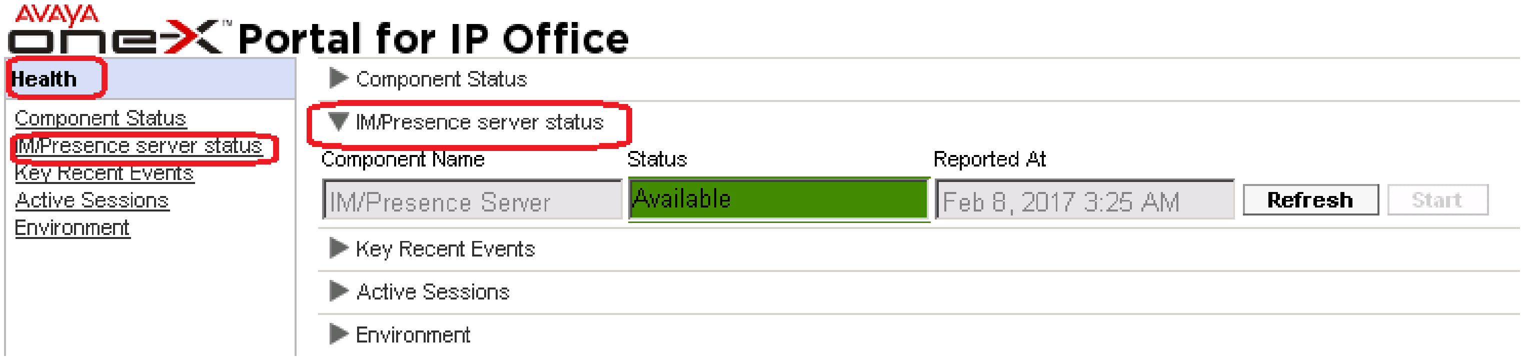
One-x Portal Providers
- CSTA Provider: IP Office Telephony connection
- DSML-IPO Provider: IP Office user synchronization
- DSML-LDAP Provider: Corporate LDAP integration
- VMPro Provider: One-x portal voicemail connection



Status: All records have been retrieved.

□	ID	Component Name	Status	Reported At	Additional Info.	Page 1 2
□	340	CSTA-Provider-1-10.10.10.13	Available	Feb 8, 2017 3:25:47 AM	Provider OK	Delete
□	3	CSTA-Provider-1-Master	Available	Feb 8, 2017 3:25:47 AM	Master Available	Delete
□	339	DSML-Provider-1-10.10.10.13	Available	Feb 8, 2017 3:25:46 AM	Initial provisioning c	Delete
□	6	DSML-Provider-1-ldap://ldap-server-ip-address:389	Available	Feb 8, 2017 3:25:27 AM		Delete
□	1	DSML-Provider-1-Master	Available	Feb 8, 2017 3:25:46 AM	TotalCount:Success	Delete
□	341	VOICEMAIL-Provider-10.10.10.13	Available	Feb 8, 2017 3:26:50 AM	Provider is up.	Delete

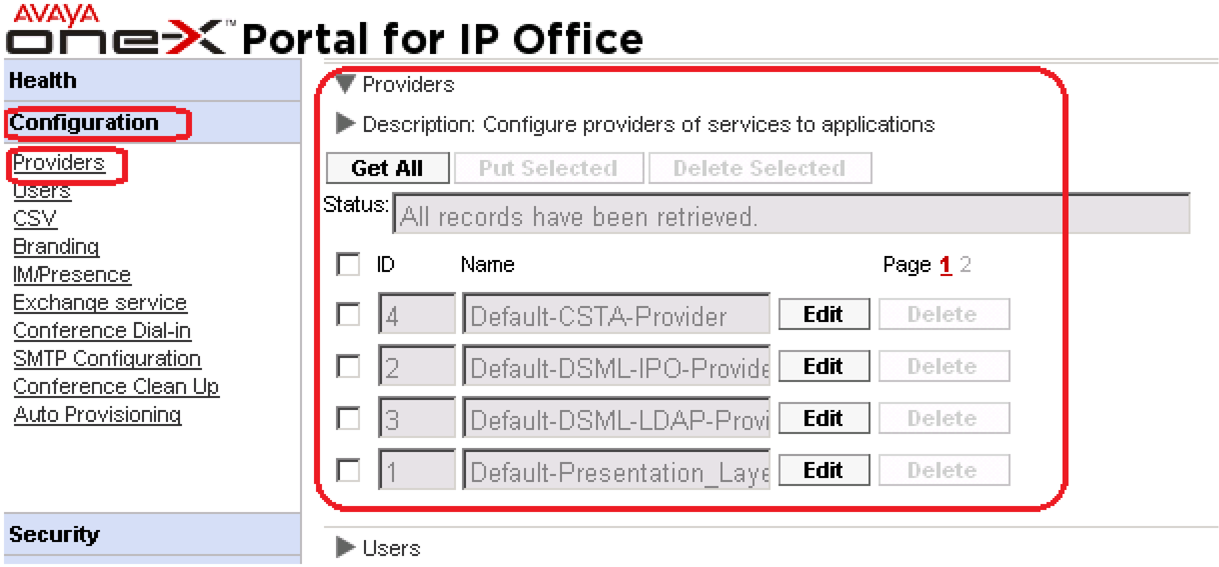
This page provides status about IP Office connection, VMPro, LDAP integration and XMPP.



AVAYA one-X Portal for IP Office
Health
Component Status
IM/Presence server status
Key Recent Events
Active Sessions
Environment
▶ Component Status
▼ IM/Presence server status

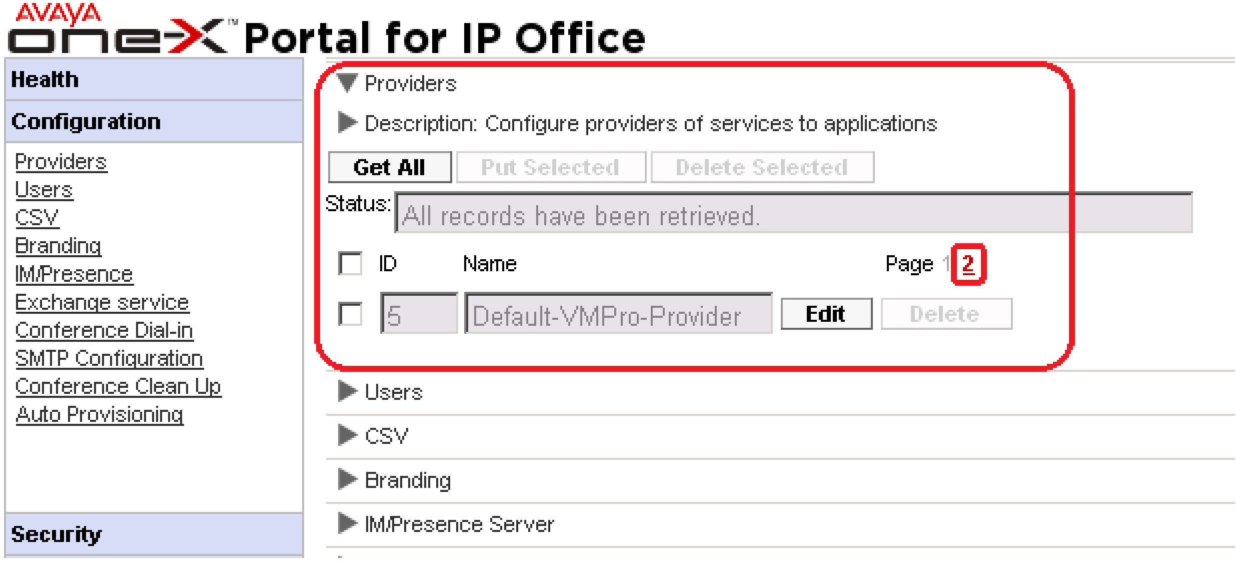
Component Name	Status	Reported At		
IM/Presence Server	Available	Feb 8, 2017 3:25 AM	Refresh	Start

Configuration > Providers allow you to modify each Providers.



Status: All records have been retrieved.

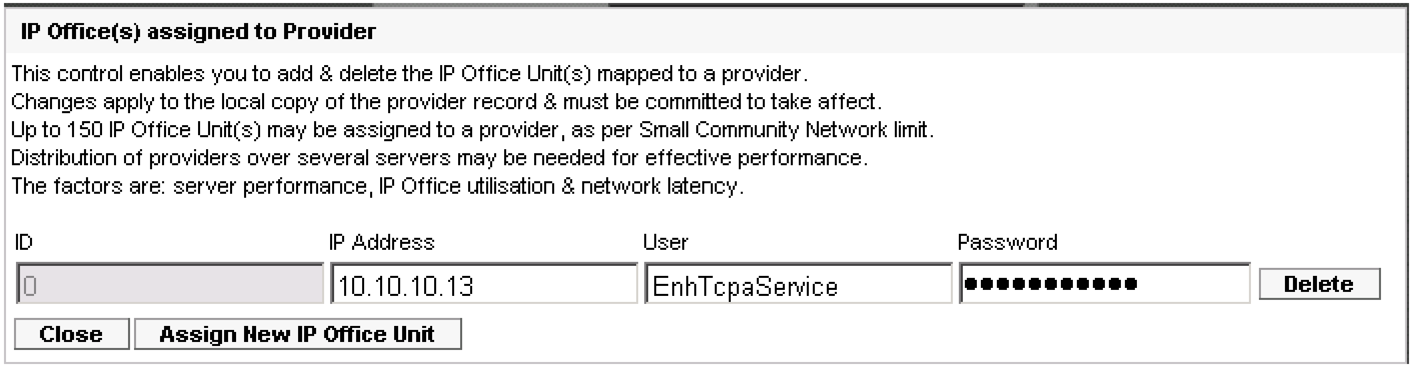
	ID	Name	Page **1** 2	
□	4	Default-CSTA-Provider	Edit	Delete
□	2	Default-DSML-IPO-Provide	Edit	Delete
□	3	Default-DSML-LDAP-Provi	Edit	Delete
□	1	Default-Presentation_Laye	Edit	Delete



Status: All records have been retrieved.

	ID	Name	Page 1 **2**	
□	5	Default-VMPro-Provider	Edit	Delete

IP Office Provider setting

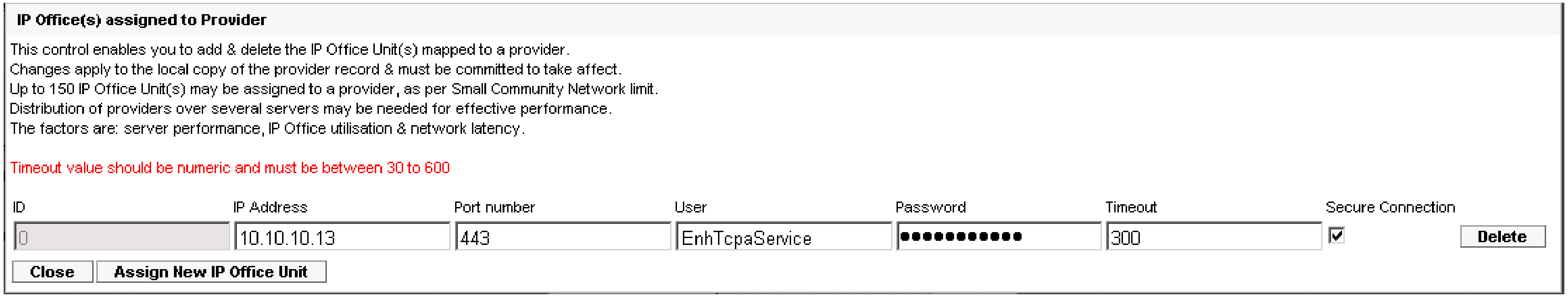


IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 150 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
Distribution of providers over several servers may be needed for effective performance.
The factors are: server performance, IP Office utilisation & network latency.

ID	IP Address	User	Password	
0	10.10.10.13	EnhTcpaService	●●●●●●●●●●●●	Delete

IP Office DSML Provider setting



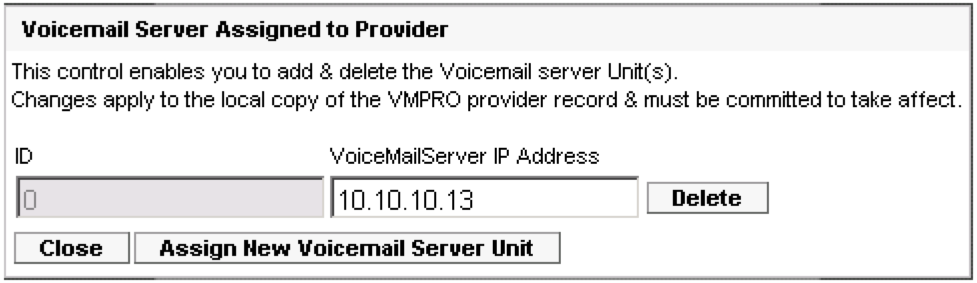
IP Office(s) assigned to Provider

This control enables you to add & delete the IP Office Unit(s) mapped to a provider.
Changes apply to the local copy of the provider record & must be committed to take affect.
Up to 150 IP Office Unit(s) may be assigned to a provider, as per Small Community Network limit.
Distribution of providers over several servers may be needed for effective performance.
The factors are: server performance, IP Office utilisation & network latency.

Timeout value should be numeric and must be between 30 to 600

ID	IP Address	Port number	User	Password	Timeout	Secure Connection	
0	10.10.10.13	443	EnhTcpaService	●●●●●●●●●●●●	300	☑	Delete

Voicemail Provider setting

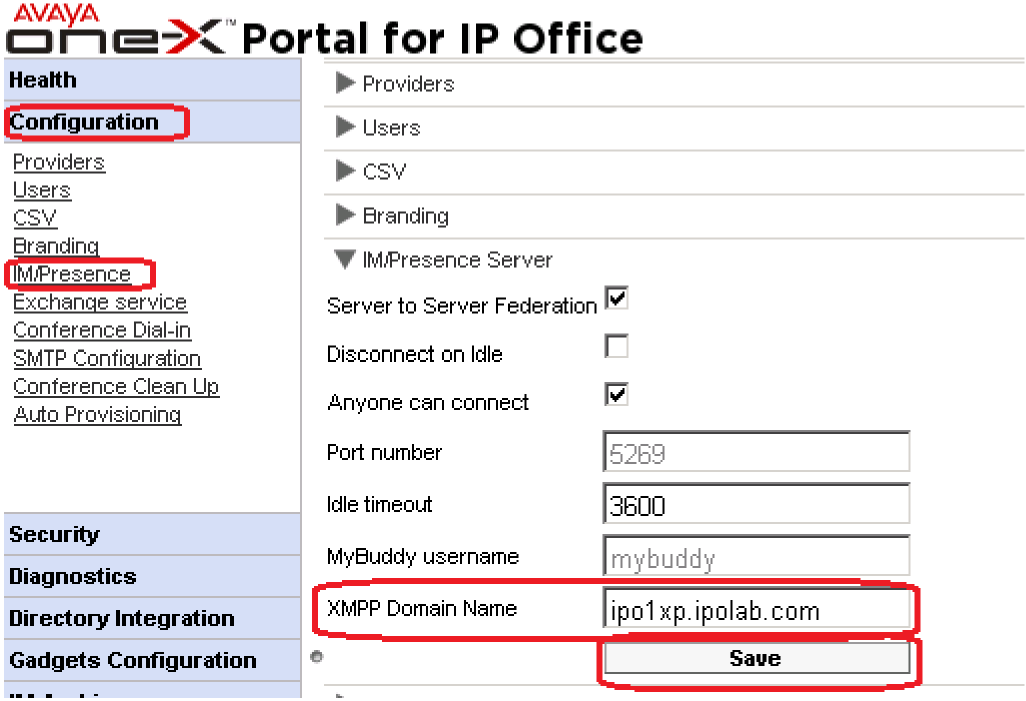


Voicemail Server Assigned to Provider

This control enables you to add & delete the Voicemail server Unit(s).
Changes apply to the local copy of the VMPRO provider record & must be committed to take affect.

ID	VoiceMailServer IP Address	
0	10.10.10.13	Delete

One-x Portal XMPP Domain Name setting
-This should be the FQDN or IP address of the One-x Portal server. In this example, the FQDN is the same with IP Office Server Edition since they are installed on the same machine.
-This setting is for IM/Presence registration of the One-x mobile client.



Server to Server Federation ☑

Disconnect on Idle □

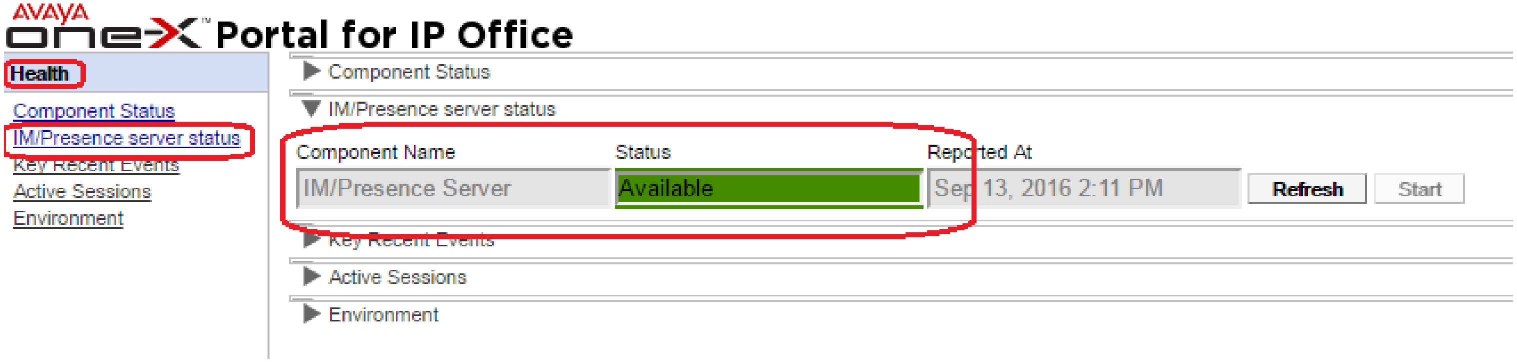
Anyone can connect ☑

Port number: 5269

Idle timeout: 3600

MyBuddy username: mybuddy

XMPP Domain Name: ipo1xp.ipolab.com



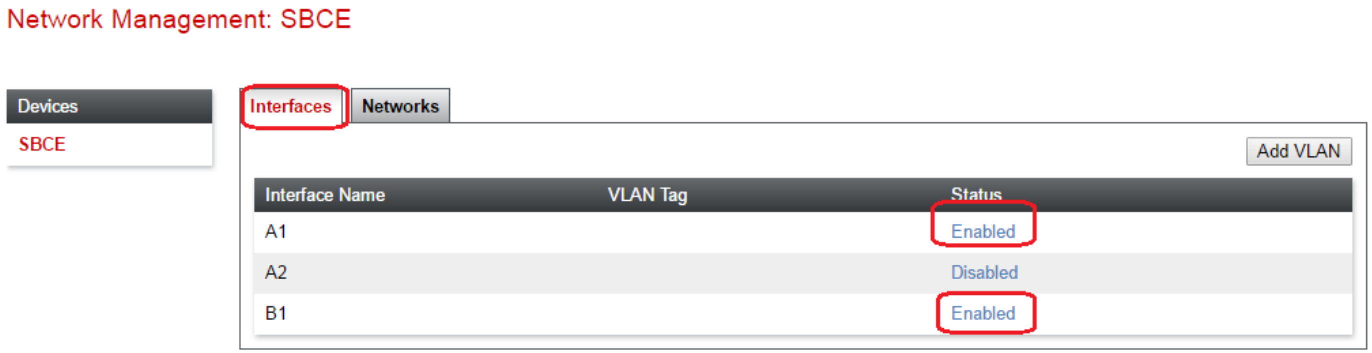
Component Name	Status	Reported At
IM/Presence Server	Available	Sep 13, 2016 2:11 PM

SBCE related configuration

Note: It is assumed that SBCE has already been installed and certificate generation has been done and exported/uploaded accordingly.

SBCE Related Configuration

- ❑ Device Specific Settings > Network Management > Interfaces
Enable A1 and B1 Interfaces



Network Management: SBCE

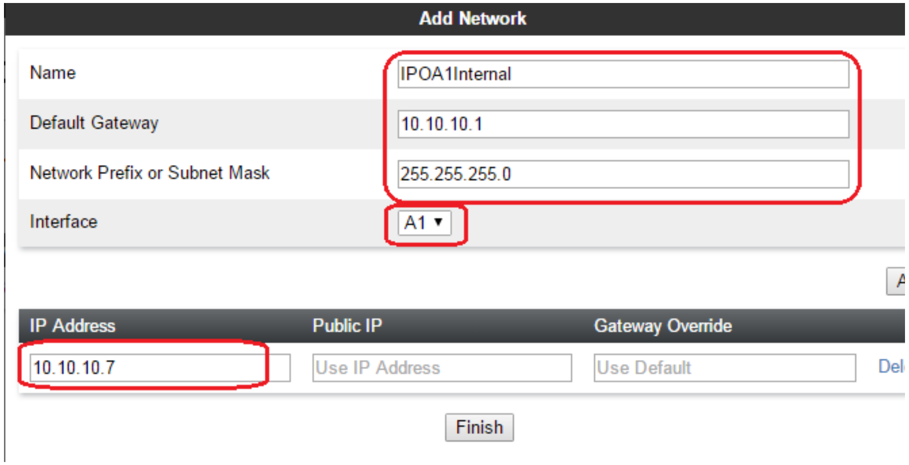
Devices
SBCE

Interfaces | Networks

Add VLAN

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled

- ❑ Device Specific Settings > Network Management > Networks
Add Network entries for A1 (Internal) and B1 (External) interfaces



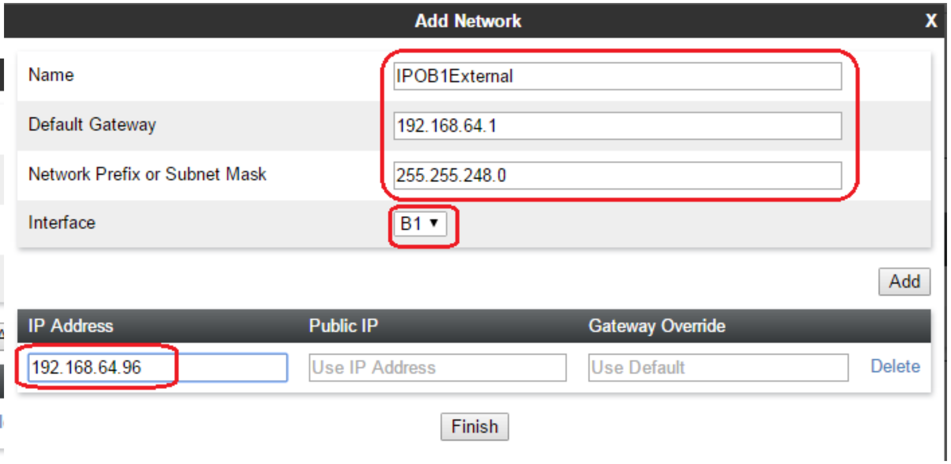
Add Network

Name	IPOA1Internal
Default Gateway	10.10.10.1
Network Prefix or Subnet Mask	255.255.255.0
Interface	A1 ▾

A

IP Address	Public IP	Gateway Override	
10.10.10.7	Use IP Address	Use Default	Del

Finish



Add Network X

Name	IPOB1External
Default Gateway	192.168.64.1
Network Prefix or Subnet Mask	255.255.248.0
Interface	B1 ▾

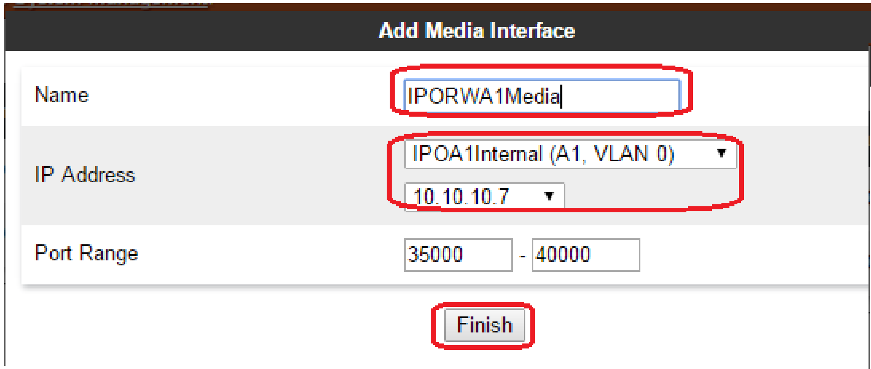
Add

IP Address	Public IP	Gateway Override	
192.168.64.96	Use IP Address	Use Default	Delete

Finish

- ❑ Device Specific Settings > Media Interface

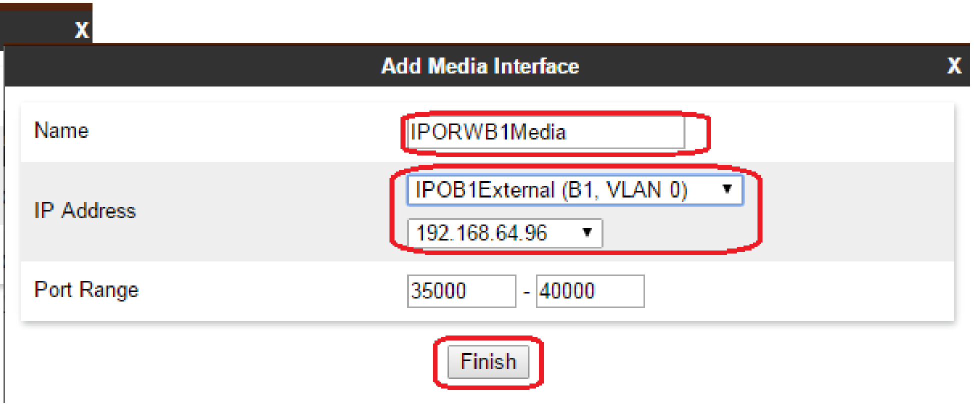
Add Media Interface entries for A1 and B1 interfaces



Add Media Interface X

Name	IPORWA1Media
IP Address	IPOA1Internal (A1, VLAN 0) ▼ 10.10.10.7 ▼
Port Range	35000 - 40000

Finish



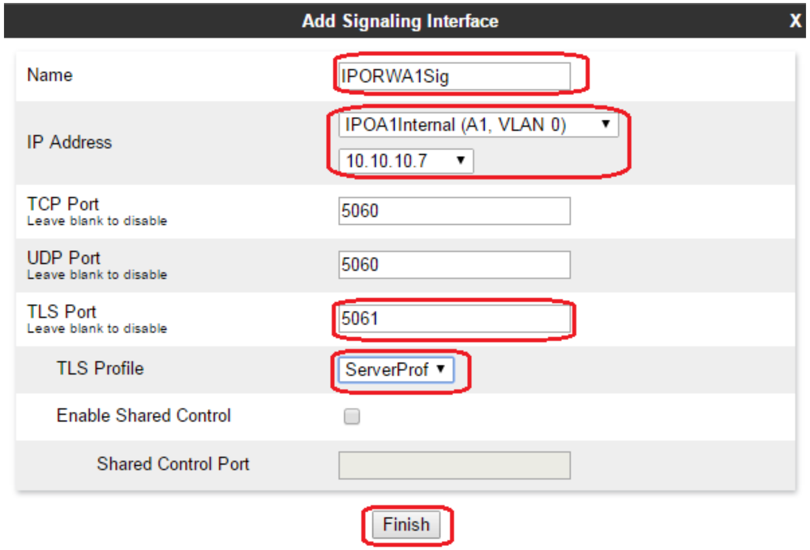
Add Media Interface X

Name	IPORWB1Media
IP Address	IPOB1External (B1, VLAN 0) ▼ 192.168.64.96 ▼
Port Range	35000 - 40000

Finish

- ❑ Device Specific Settings > Signaling Interface

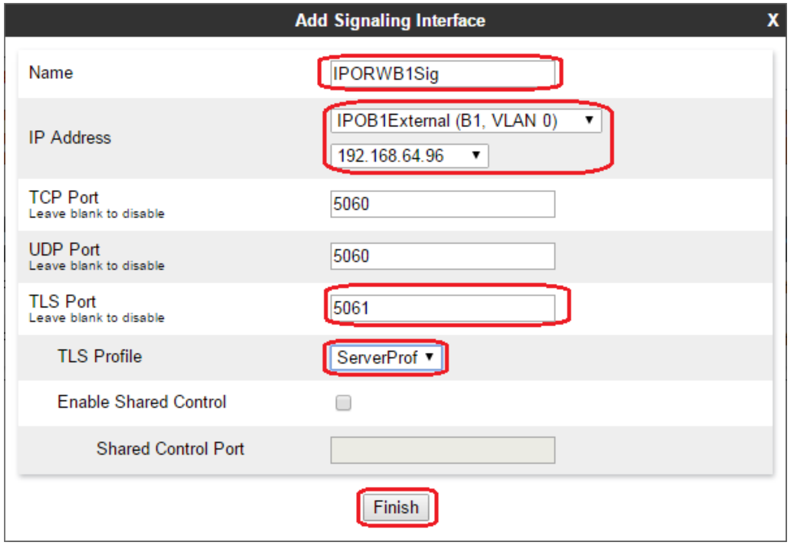
Add Signaling Interface entries for A1 and B1 interfaces
Specify the ports you planned to use.



Add Signaling Interface X

Name	IPORWA1Sig
IP Address	IPOA1Internal (A1, VLAN 0) ▼ 10.10.10.7 ▼
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	5061
TLS Profile	ServerProf ▼
Enable Shared Control	☐
Shared Control Port	

Finish



Add Signaling Interface X

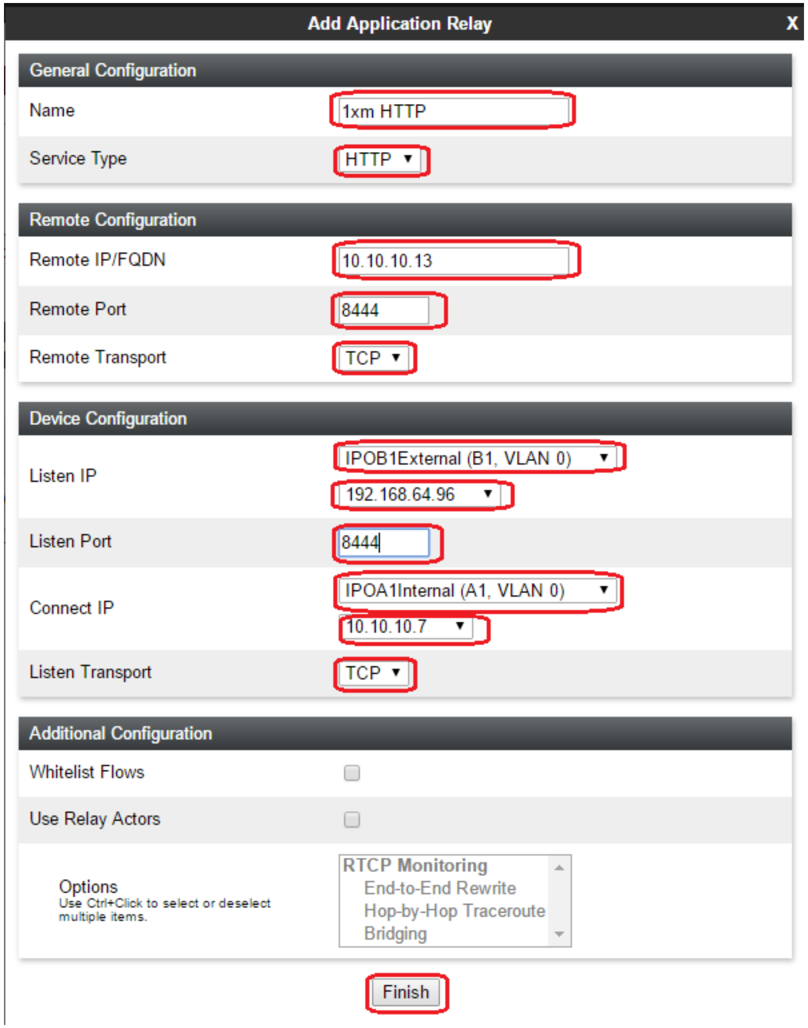
Name	IPORWB1Sig
IP Address	IPOB1External (B1, VLAN 0) ▼ 192.168.64.96 ▼
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	5061
TLS Profile	ServerProf ▼
Enable Shared Control	☐
Shared Control Port	

Finish

- ❑ Device Specific Settings > DMZ Services > Relay Services

Add entry for One-x mobile HTTP request pointing to One-x Portal/IPO IP or FQDN on TCP port 8444. Specify the external interface for Listen IP and Listen port 8444. Connect IP should be the internal interface and Listen transport as TCP.

This entry is for One-x mobile client request on HTTP port 8444. This is to retrieve information about XMPP and SIP information for registration.



Add Application Relay X

General Configuration

Name	1xm HTTP
Service Type	HTTP

Remote Configuration

Remote IP/FQDN	10.10.10.13
Remote Port	8444
Remote Transport	TCP

Device Configuration

Listen IP	IPOB1External (B1, VLAN 0) 192.168.64.96
Listen Port	8444
Connect IP	IPOA1Internal (A1, VLAN 0) 10.10.10.7
Listen Transport	TCP

Additional Configuration

Whitelist Flows	☐
Use Relay Actors	☐
Options Use Ctrl+Click to select or deselect multiple items.	RTCP Monitoring End-to-End Rewrite Hop-by-Hop Traceroute Bridging

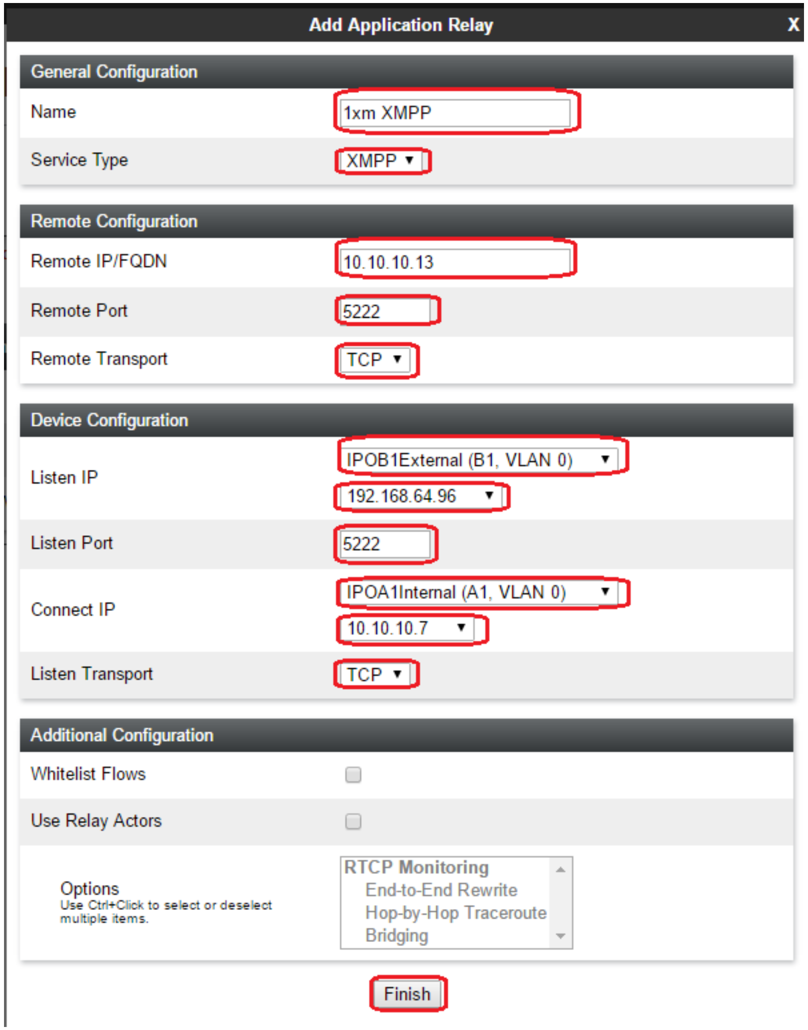
❑ Device Specific Settings > DMZ Services > Relay Services
Add entry for One-x mobile XMPP request pointing to One-x Portal/IPO IP or FQDN on TCP port 5222. Specify the external interface for Listen IP and Listen port 5222. Connect IP should be the internal interface and Listen transport as TCP.

This entry is for One-x mobile client request on XMPP port 5222. This is for IM/Presence registration.

The SIP registration follows right after the XMPP has been registered.

One-x mobile client will not continue with SIP registration until XMPP registered first.

On the side note, if you want Avaya Communicator with Presence service, you need to create similar entry. You just change the port to 9443.



Add Application Relay X

General Configuration

Name	1xm XMPP
Service Type	XMPP ▾

Remote Configuration

Remote IP/FQDN	10.10.10.13
Remote Port	5222
Remote Transport	TCP ▾

Device Configuration

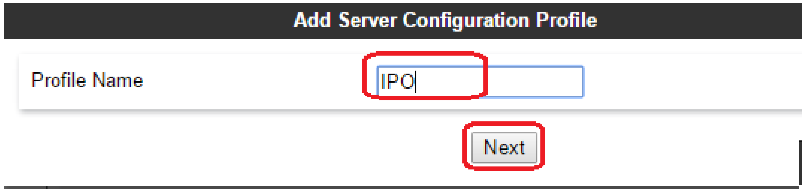
Listen IP	IPOB1External (B1, VLAN 0) ▾ 192.168.64.96 ▾
Listen Port	5222
Connect IP	IPOA1Internal (A1, VLAN 0) ▾ 10.10.10.7 ▾
Listen Transport	TCP ▾

Additional Configuration

Whitelist Flows	□
Use Relay Actors	□
Options Use Ctrl+Click to select or deselect multiple items.	RTCP Monitoring End-to-End Rewrite Hop-by-Hop Traceroute Bridging

Finish

- ❑ Global Policies > Server Configuration
Fill in Profile Name.

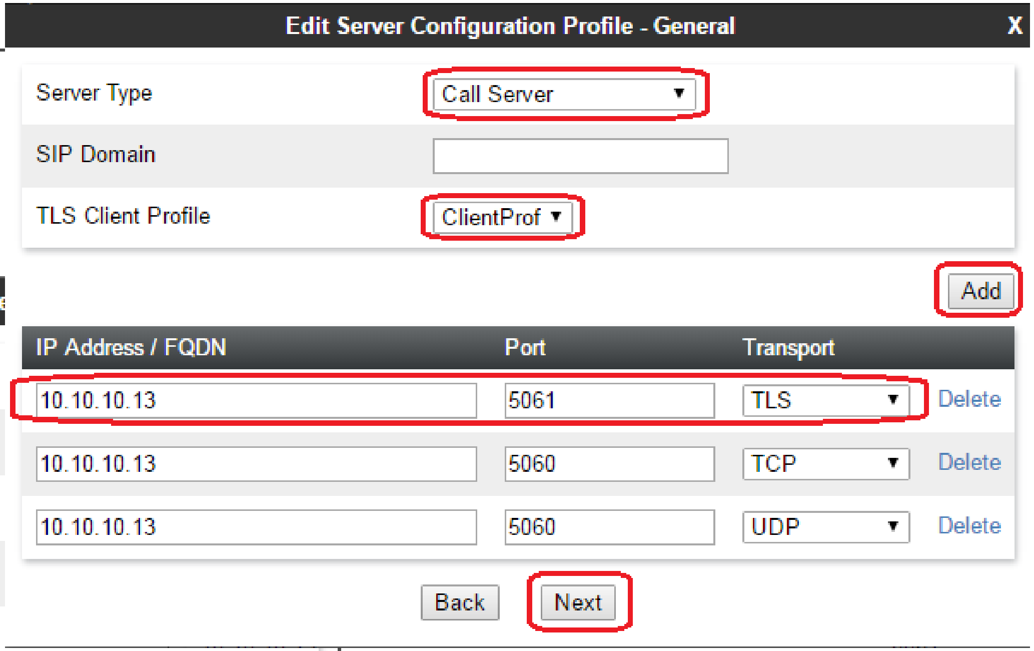


Add Server Configuration Profile X

Profile Name	IPO

Next

- ❑ Set Server Type to Call Server. Select the TLS Client Profile you have created. Add in the IP Address/FQDN of the IPO server, Port and Transport protocol. It should match with the IPO setting. You can also add TCP and UDP as shown. The transport to be used depends on what is set in the Routing Profile.



Edit Server Configuration Profile - General X

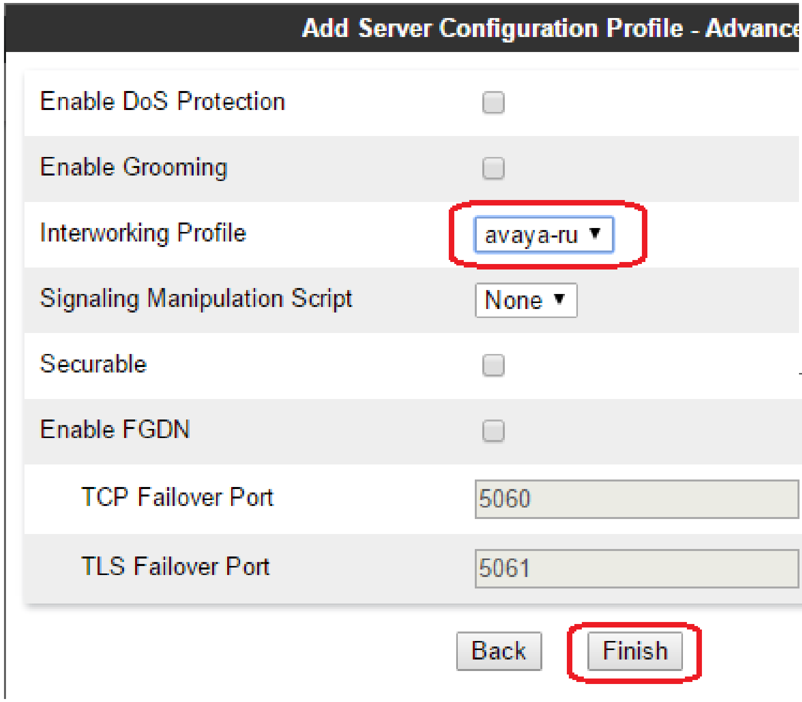
Server Type	Call Server ▼
SIP Domain	
TLS Client Profile	ClientProf ▼

Add

IP Address / FQDN	Port	Transport	
10.10.10.13	5061	TLS ▼	Delete
10.10.10.13	5060	TCP ▼	Delete
10.10.10.13	5060	UDP ▼	Delete

Back Next

- ❑ Enable Grooming should not be enabled. IP Office utilizes different TCP connections to each endpoint.



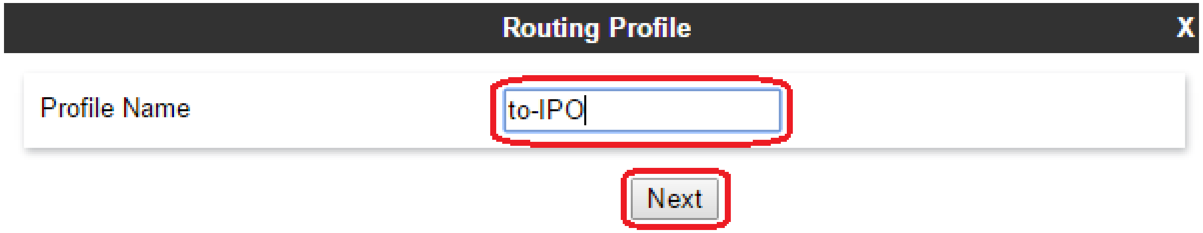
Add Server Configuration Profile - Advance

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	avaya-ru ▼
Signaling Manipulation Script	None ▼
Securable	□
Enable FGDN	□
TCP Failover Port	5060
TLS Failover Port	5061

Back Finish

- ❑ Global Policies > Routing Profile

Fill in Profile Name.

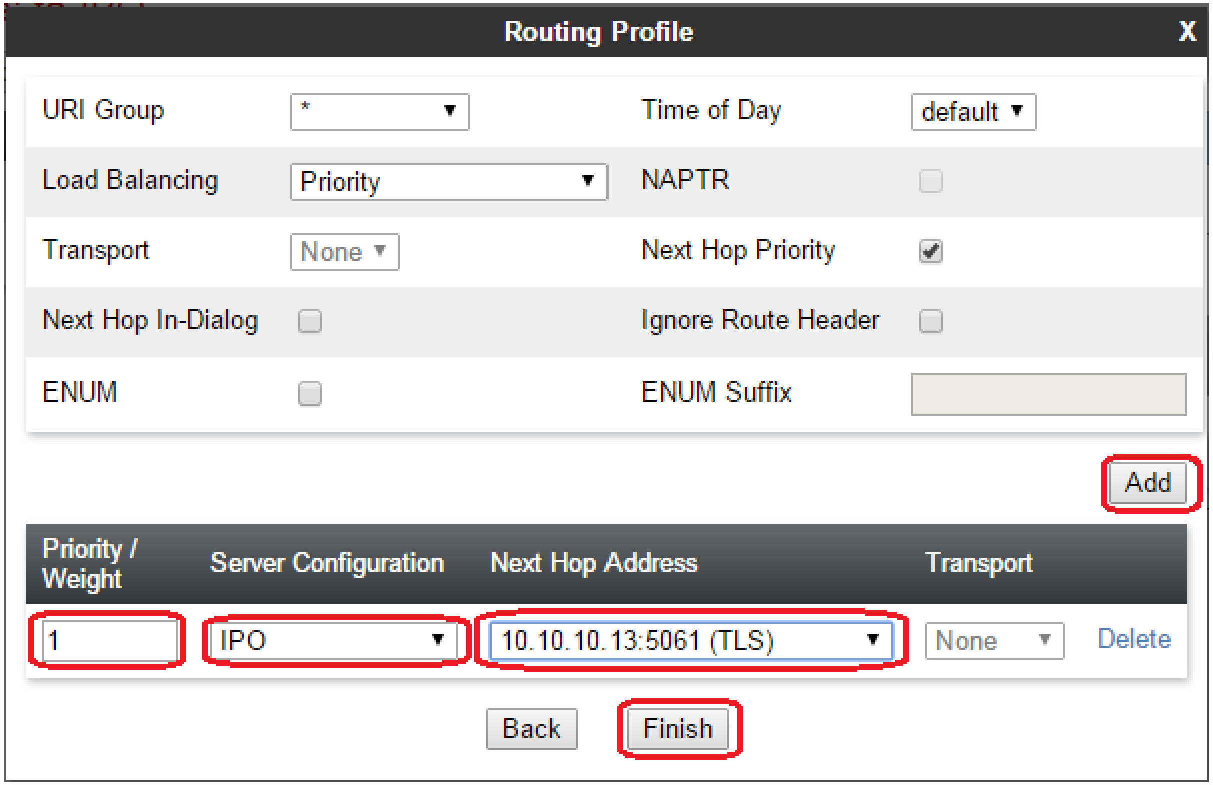


Routing Profile

Profile Name	to-IPO

- ❑ Add an entry. Set Priority/Weight as 1 (This will actually vary when you have multiple entries here). Select the Server Configuration added in the previous step. Then select Next Hop Address accordingly - TLS if TLS is required.

The Next Hop Address selected here will determine at which port (TLS, TCP, UDP) SBCE and IPO would exchange signaling.



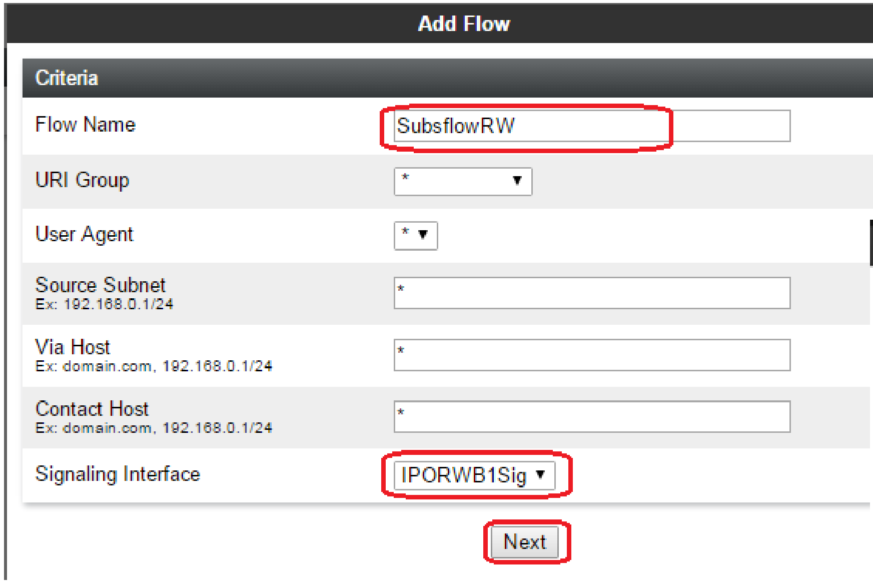
Routing Profile

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	☐	Ignore Route Header	☐
ENUM	☐	ENUM Suffix	

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IPO	10.10.10.13:5061 (TLS)	None	Delete

- Device Specific Settings > End Point Flows > Subscriber Flows

Fill in the Flow Name and set the B1 Signaling Interface.

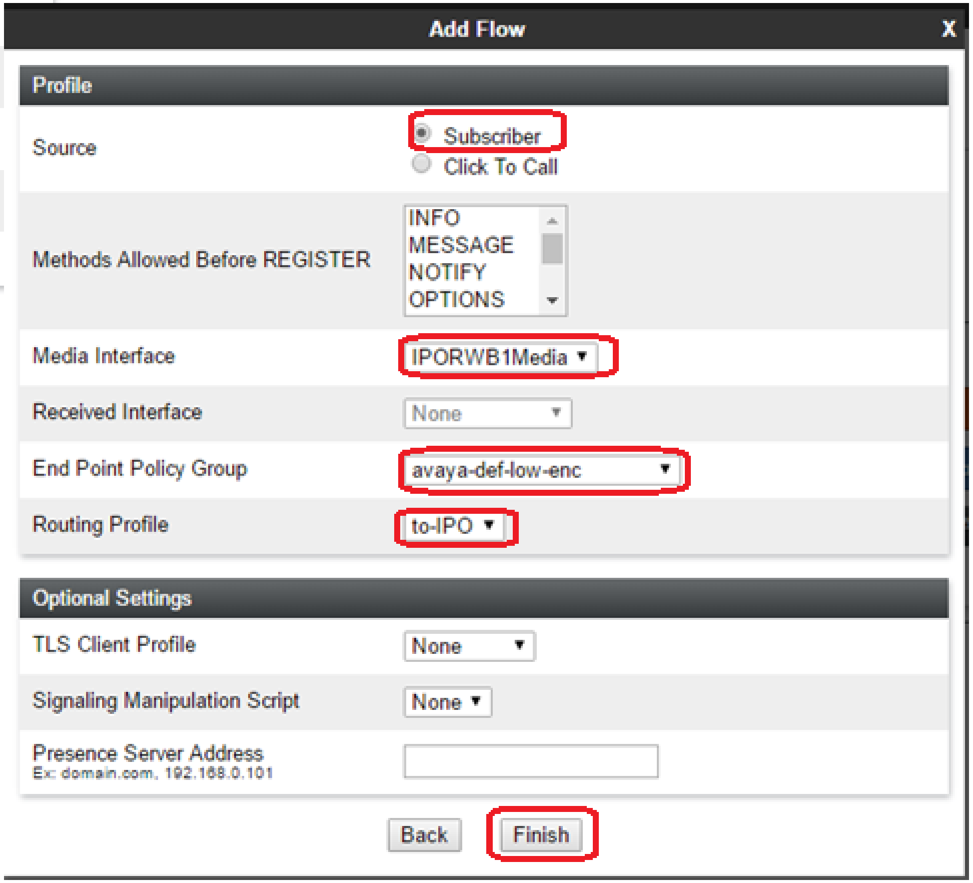


Add Flow

Criteria

Flow Name	SubsflowRW
URI Group	*
User Agent	*
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	IPORWB1Sig

- Select Subscriber as the Source. Set B1 interface in the Media Interface. Select the End Point Policy Group and Routing Profile that you have configured.



Add Flow

Profile

Source	● Subscriber ○ Click To Call
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	IPORWB1Media
Received Interface	None
End Point Policy Group	avaya-def-low-enc
Routing Profile	to-IPO

Optional Settings

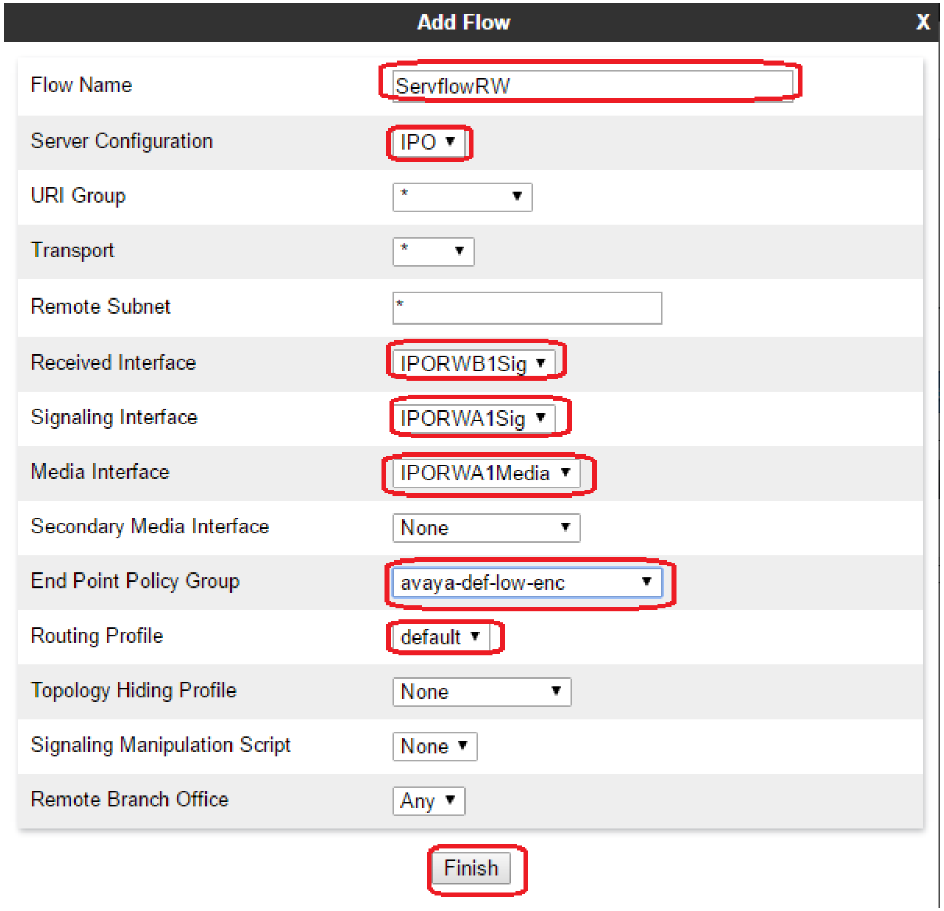
TLS Client Profile	None
Signaling Manipulation Script	None
Presence Server Address Ex: domain.com, 192.168.0.101	

- Subscriber Flow relates to the remote worker side. SBCE listens on the external interface for messages coming from the remote worker. External interface should be selected in Signaling as well as Media Interface. SBCE uses the Policy Group and Routing Profile to determine how to proceed.

❑ Device Specific Settings > End Point Flows > Server Flows

Fill in the Flow Name and set the B1 Signaling Interface in the Received Interface. A1 in the Signaling and Media Interface. Select the End Point Policy Group and Routing Profile default.

❑ Server Flow relates to the communication between SBCE and IP Office. SBCE uses these details to determine a match to proceed with routing the registrations and calls.



Add Flow

Flow Name	ServflowRW
Server Configuration	IPO
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	IPORWB1Sig
Signaling Interface	IPORWA1Sig
Media Interface	IPORWA1Media
Secondary Media Interface	None
End Point Policy Group	avaya-def-low-enc
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Expected Flow of Messages

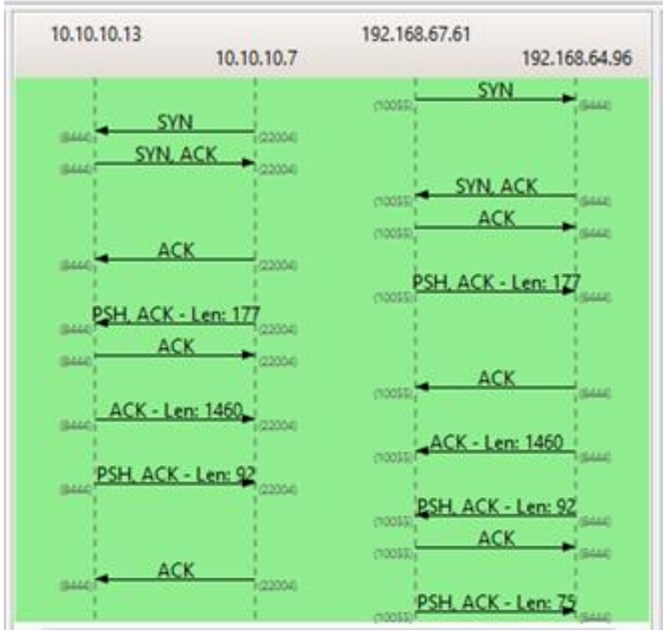
Expected Flow of Messages

- ❑ **One-x Mobile Registration**
  - One-x mobile client initiates the connection. SBCE receives the messages.
  - SBCE then utilizes the Application Relay settings. It will first utilize the entry for HTTP type with port 8444. This is for the One-x mobile client to retrieve the XMPP credentials.
  - When XMPP credentials have been received, One-x mobile client then registers to XMPP and will utilize the Application Relay entry XMPP port 5222.
  - When XMPP registration is successful, One-x mobile client then initiates the request retrieving the SIP registration info in Application Relay HTTP port 8444 entry.
  - Once the SIP registration info have been received, it will then registers to SIP registrar. SBCE will utilize the setting in the Subscriber Flows to route the packet to IP Office.
  - When IP Office respond, SBCE will utilize Server Flows to route the packets back to One-x mobile client.

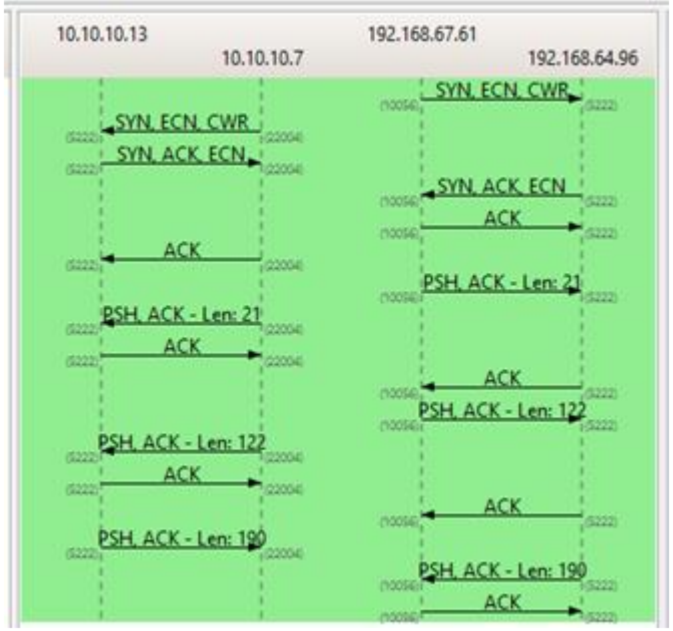
Expected Flow of Messages

- **One-x Mobile Registration**
  - One-x mobile and IP Office/One-x Portal exchanges TCP messages on port 8444 to retrieve XMPP (IM/Presence) and SIP credentials.
  - Once the credentials have been retrieved, IM/Presence registration on port 5222 will follow and then VoIP registration comes next on TCP or UDP or TLS port.

TCP port 8444 messages flow



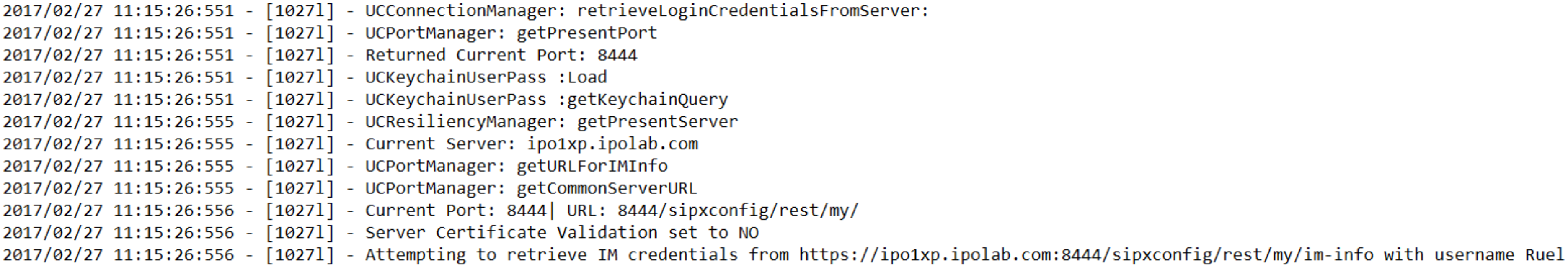
TCP port 5222 messages flow



❑ One-x Mobile Registration

Following are the logs from One-x mobile client.

One-x mobile client attempts to retrieve XMPP credentials.



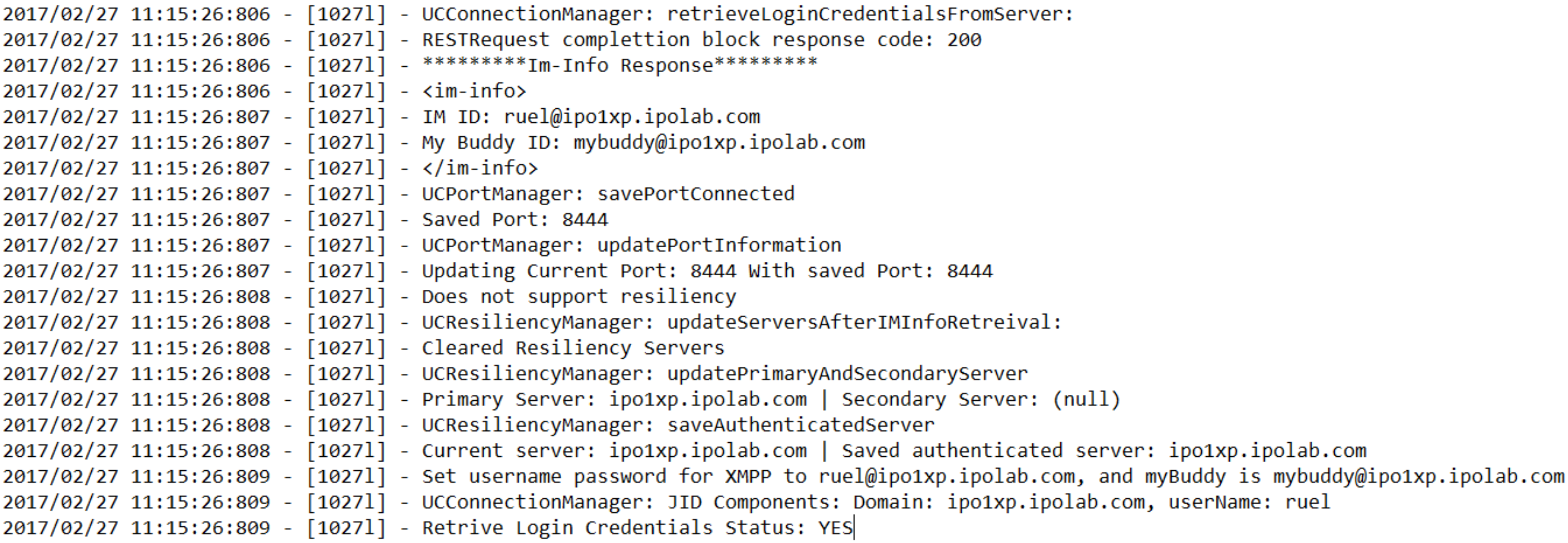
```
2017/02/27 11:15:26:551 - [1027l] - UCConnectionManager: retrieveLoginCredentialsFromServer:
2017/02/27 11:15:26:551 - [1027l] - UCPortManager: getPresentPort
2017/02/27 11:15:26:551 - [1027l] - Returned Current Port: 8444
2017/02/27 11:15:26:551 - [1027l] - UCKeychainUserPass :Load
2017/02/27 11:15:26:551 - [1027l] - UCKeychainUserPass :getKeychainQuery
2017/02/27 11:15:26:555 - [1027l] - UCResiliencyManager: getPresentServer
2017/02/27 11:15:26:555 - [1027l] - Current Server: ipo1xp.ipolab.com
2017/02/27 11:15:26:555 - [1027l] - UCPortManager: getURLForIMInfo
2017/02/27 11:15:26:555 - [1027l] - UCPortManager: getCommonServerURL
2017/02/27 11:15:26:556 - [1027l] - Current Port: 8444| URL: 8444/sipxconfig/rest/my/
2017/02/27 11:15:26:556 - [1027l] - Server Certificate Validation set to NO
2017/02/27 11:15:26:556 - [1027l] - Attempting to retrieve IM credentials from https://ipo1xp.ipolab.com:8444/sipxconfig/rest/my/im-info with username Ruel
```

Where does One-x Mobile client got the information in retrieving the XMPP credentials? - It is from what we set in the One-x mobile client settings.

2017/02/27 11:15:11:963 - [1027l] - IN SETTINGS - Server: ipo1xp.ipolab.com --- Port: 8444 --- Username: Ruel

❑ One-x Mobile Registration

One-x mobile client received XMPP credentials.



```
2017/02/27 11:15:26:806 - [1027l] - UCConnectionManager: retrieveLoginCredentialsFromServer:
2017/02/27 11:15:26:806 - [1027l] - RESTRequest complettion block response code: 200
2017/02/27 11:15:26:806 - [1027l] - *********Im-Info Response*********
2017/02/27 11:15:26:806 - [1027l] - <im-info>
2017/02/27 11:15:26:807 - [1027l] - IM ID: ruel@ipo1xp.ipolab.com
2017/02/27 11:15:26:807 - [1027l] - My Buddy ID: mybuddy@ipo1xp.ipolab.com
2017/02/27 11:15:26:807 - [1027l] - </im-info>
2017/02/27 11:15:26:807 - [1027l] - UCPortManager: savePortConnected
2017/02/27 11:15:26:807 - [1027l] - Saved Port: 8444
2017/02/27 11:15:26:807 - [1027l] - UCPortManager: updatePortInformation
2017/02/27 11:15:26:807 - [1027l] - Updating Current Port: 8444 With saved Port: 8444
2017/02/27 11:15:26:808 - [1027l] - Does not support resiliency
2017/02/27 11:15:26:808 - [1027l] - UCResiliencyManager: updateServersAfterIMInfoRetreival:
2017/02/27 11:15:26:808 - [1027l] - Cleared Resiliency Servers
2017/02/27 11:15:26:808 - [1027l] - UCResiliencyManager: updatePrimaryAndSecondaryServer
2017/02/27 11:15:26:808 - [1027l] - Primary Server: ipo1xp.ipolab.com | Secondary Server: (null)
2017/02/27 11:15:26:808 - [1027l] - UCResiliencyManager: saveAuthenticatedServer
2017/02/27 11:15:26:808 - [1027l] - Current server: ipo1xp.ipolab.com | Saved authenticated server: ipo1xp.ipolab.com
2017/02/27 11:15:26:809 - [1027l] - Set username password for XMPP to ruel@ipo1xp.ipolab.com, and myBuddy is mybuddy@ipo1xp.ipolab.com
2017/02/27 11:15:26:809 - [1027l] - UCConnectionManager: JID Components: Domain: ipo1xp.ipolab.com, userName: ruel
2017/02/27 11:15:26:809 - [1027l] - Retrive Login Credentials Status: YES
```

Once the XMPP credentials have been retrieved, One-x Mobile attempts to connect to XMPP.

2017/02/27 11:15:26:811 - [1027l] - Attempting to connect to XMPP at ipo1xp.ipolab.com:5222 with username ruel@ipo1xp.ipolab.com/pauc-1.2-FE2B8713A0764FEA-#-18535

There will be a lot of XMPP related messages during the connection establishment but at the end of it, you should see the My Buddy is connected. This is an indication that the XMPP is now connected..

2017/02/27 11:15:27:711 - [1027l] - ********* My Buddy connected *********

One-x Mobile Registration

One-x mobile client fetching SIP credentials.

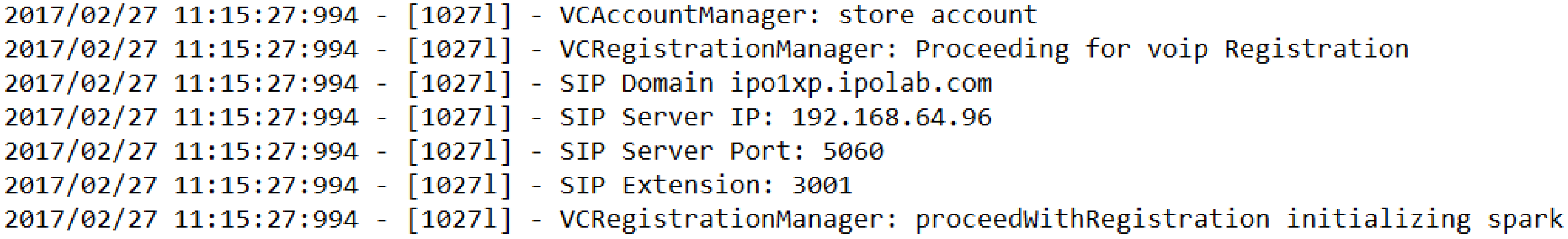
```
2017/02/27 11:15:27:714 - [19735l] - VCRegistrationManager: fetchLoginCredentials
2017/02/27 11:15:27:714 - [19735l] - UCRestClient: fetchSipCredentialsFromOneXServer
2017/02/27 11:15:27:714 - [19735l] - UCRestClient: isReachable for Url: ipo1xp.ipolab.com
2017/02/27 11:15:27:715 - [19735l] - UCRestClient: RestClient server is reachable
2017/02/27 11:15:27:715 - [19735l] - UCPortManager: getURLForSIPInfo
2017/02/27 11:15:27:715 - [19735l] - UCPortManager: getCommonServerURL
2017/02/27 11:15:27:715 - [19735l] - Current Port: 8444| URL: 8444/sipxconfig/rest/my/
2017/02/27 11:15:27:715 - [19735l] - SIPInfo serverURL Format: https://%@:8444/sipxconfig/rest/my/sip-info
2017/02/27 11:15:27:715 - [19735l] - UCRestClient: fetchSipCredentialsFromOneXServer for URL:
https://ipo1xp.ipolab.com:8444/sipxconfig/rest/my/sip-info
```

SIP credentials have been fetched.

```
2017/02/27 11:15:27:989 - [1027l] - RestClient on HttpRequest completed
2017/02/27 11:15:27:990 - [1027l] - VCRegistrationManager: onRestCallComplete
2017/02/27 11:15:27:990 - [1027l] - VCRegistrationManager: checkVoipFeatureStatus
2017/02/27 11:15:27:990 - [1027l] - VCRegistrationManager: checkVoipFeatureStatus: Voip mode is Always. Voip
feature is active
2017/02/27 11:15:27:990 - [1027l] - VCRegistrationManager parseRestQueryResult: entry
2017/02/27 11:15:27:991 - [1027l] - SIP Settings obtained from 1X
2017/02/27 11:15:27:991 - [1027l] - Identity: 3001@ipo1xp.ipolab.com
2017/02/27 11:15:27:991 - [1027l] - Private Address: 10.10.10.13
2017/02/27 11:15:27:991 - [1027l] - Private TCP Port: 5060
2017/02/27 11:15:27:991 - [1027l] - Private UDP Port: 5060
2017/02/27 11:15:27:991 - [1027l] - Private TLS Port: 5061
2017/02/27 11:15:27:991 - [1027l] - Public Address: 0.0.0.0
2017/02/27 11:15:27:991 - [1027l] - Public TCP Port: 5060
2017/02/27 11:15:27:991 - [1027l] - Public UDP Port: 5060
2017/02/27 11:15:27:991 - [1027l] - Public TLS Port: 5061
2017/02/27 11:15:27:991 - [1027l] - Signalling Qos: 136
2017/02/27 11:15:27:991 - [1027l] - Voice Qos: 184
2017/02/27 11:15:27:991 - [1027l] - Video Qos: 184
```

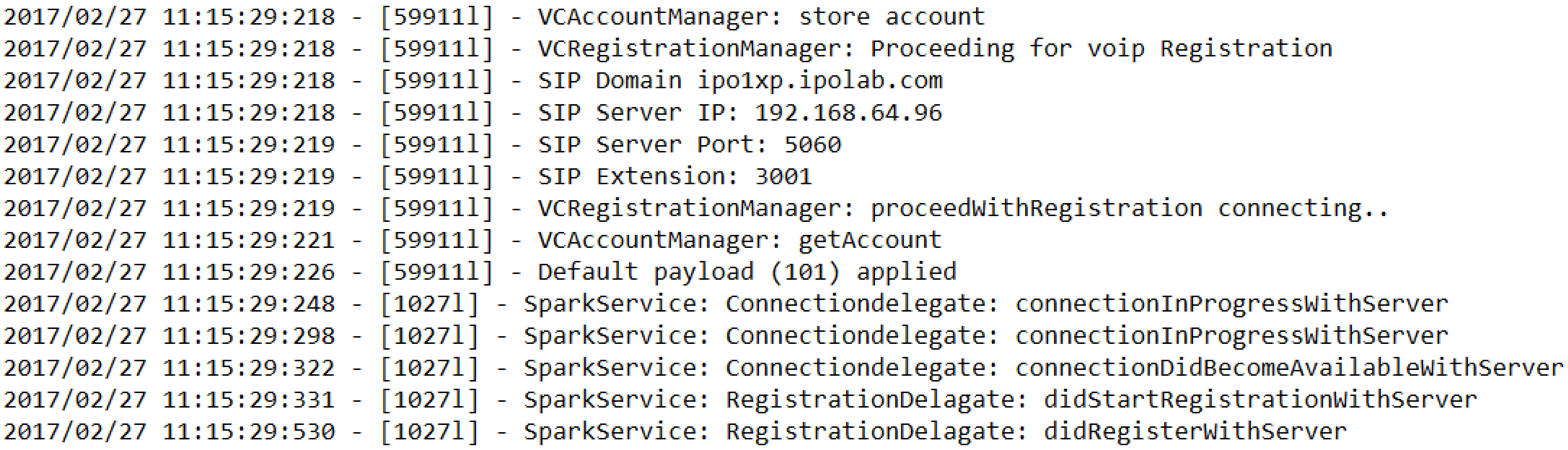
❑ One-x Mobile Registration

One-x mobile client initiating voip registration.



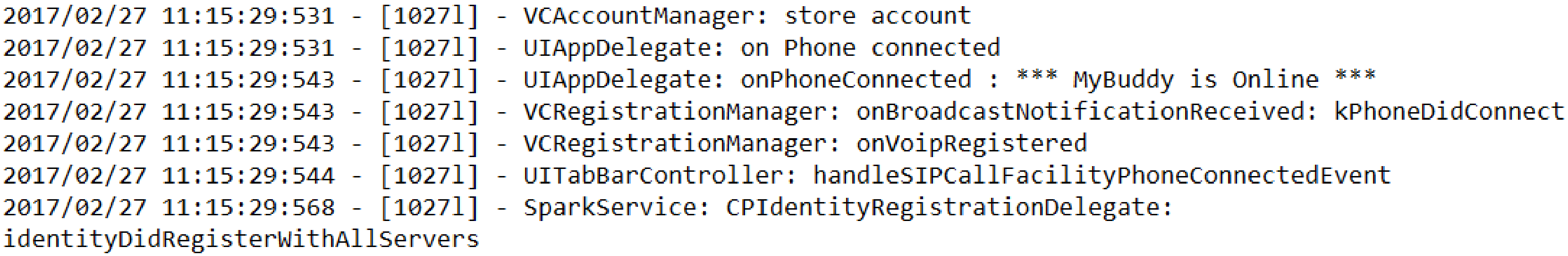
```
2017/02/27 11:15:27:994 - [1027l] - VCAccountManager: store account
2017/02/27 11:15:27:994 - [1027l] - VCRegistrationManager: Proceeding for voip Registration
2017/02/27 11:15:27:994 - [1027l] - SIP Domain ipo1xp.ipolab.com
2017/02/27 11:15:27:994 - [1027l] - SIP Server IP: 192.168.64.96
2017/02/27 11:15:27:994 - [1027l] - SIP Server Port: 5060
2017/02/27 11:15:27:994 - [1027l] - SIP Extension: 3001
2017/02/27 11:15:27:994 - [1027l] - VCRegistrationManager: proceedWithRegistration initializing spark
```

One-x mobile client voip registration in progress.



```
2017/02/27 11:15:29:218 - [59911l] - VCAccountManager: store account
2017/02/27 11:15:29:218 - [59911l] - VCRegistrationManager: Proceeding for voip Registration
2017/02/27 11:15:29:218 - [59911l] - SIP Domain ipo1xp.ipolab.com
2017/02/27 11:15:29:218 - [59911l] - SIP Server IP: 192.168.64.96
2017/02/27 11:15:29:219 - [59911l] - SIP Server Port: 5060
2017/02/27 11:15:29:219 - [59911l] - SIP Extension: 3001
2017/02/27 11:15:29:219 - [59911l] - VCRegistrationManager: proceedWithRegistration connecting..
2017/02/27 11:15:29:221 - [59911l] - VCAccountManager: getAccount
2017/02/27 11:15:29:226 - [59911l] - Default payload (101) applied
2017/02/27 11:15:29:248 - [1027l] - SparkService: Connectiondelegate: connectionInProgressWithServer
2017/02/27 11:15:29:298 - [1027l] - SparkService: Connectiondelegate: connectionInProgressWithServer
2017/02/27 11:15:29:322 - [1027l] - SparkService: Connectiondelegate: connectionDidBecomeAvailableWithServer
2017/02/27 11:15:29:331 - [1027l] - SparkService: RegistrationDelagate: didStartRegistrationWithServer
2017/02/27 11:15:29:530 - [1027l] - SparkService: RegistrationDelagate: didRegisterWithServer
```

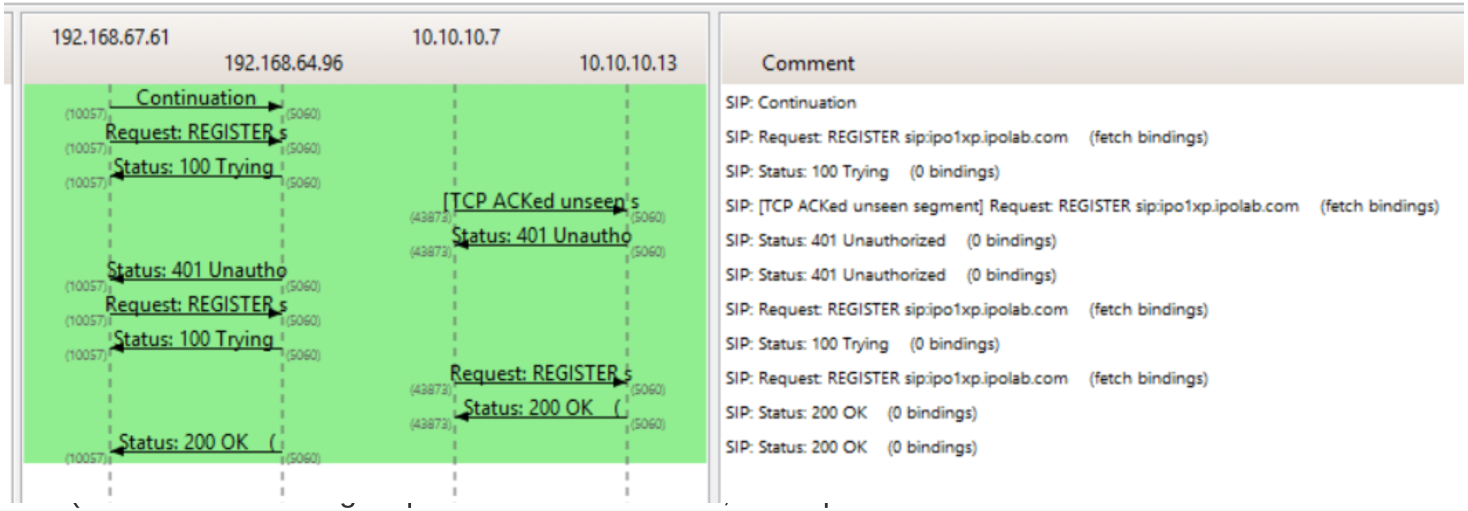
One-x mobile client is now registered.



```
2017/02/27 11:15:29:531 - [1027l] - VCAccountManager: store account
2017/02/27 11:15:29:531 - [1027l] - UIAppDelegate: on Phone connected
2017/02/27 11:15:29:543 - [1027l] - UIAppDelegate: onPhoneConnected : *** MyBuddy is Online ***
2017/02/27 11:15:29:543 - [1027l] - VCRegistrationManager: onBroadcastNotificationReceived: kPhoneDidConnect
2017/02/27 11:15:29:543 - [1027l] - VCRegistrationManager: onVoipRegistered
2017/02/27 11:15:29:544 - [1027l] - UITabBarController: handleSIPCallFacilityPhoneConnectedEvent
2017/02/27 11:15:29:568 - [1027l] - SparkService: CPIdentityRegistrationDelegate:
identityDidRegisterWithAllServers
```

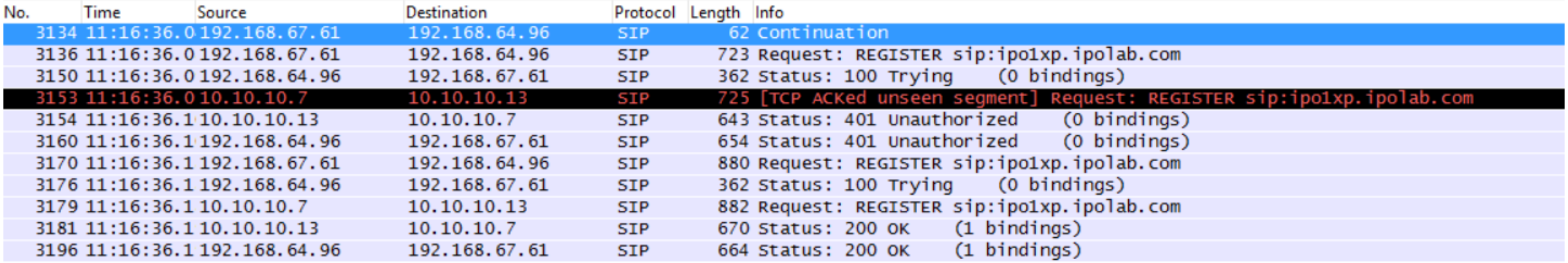
❑ One-x Mobile VOIP Registration

- One-x Mobile <> wireless LAN (Router) WAN port <> B1 (SBCE) A1 <> IP Office
  (Wireless LAN assigns ip address 172.22.33.x; WAN port is 192.168.67.61 – same subnet as SBCE B1 interface; SBCE B1 interface is 192.168.64.96; A1 interface is 10.10.10.7 – same subnet as IP Office; IP Office is 10.10.10.13



Comment

SIP: Continuation
SIP: Request: REGISTER sip:ipo1xp.ipolab.com (fetch bindings)
SIP: Status: 100 Trying (0 bindings)
SIP: [TCP ACKed unseen segment] Request: REGISTER sip:ipo1xp.ipolab.com (fetch bindings)
SIP: Status: 401 Unauthorized (0 bindings)
SIP: Status: 401 Unauthorized (0 bindings)
SIP: Request: REGISTER sip:ipo1xp.ipolab.com (fetch bindings)
SIP: Status: 100 Trying (0 bindings)
SIP: Request: REGISTER sip:ipo1xp.ipolab.com (fetch bindings)
SIP: Status: 200 OK (0 bindings)
SIP: Status: 200 OK (0 bindings)



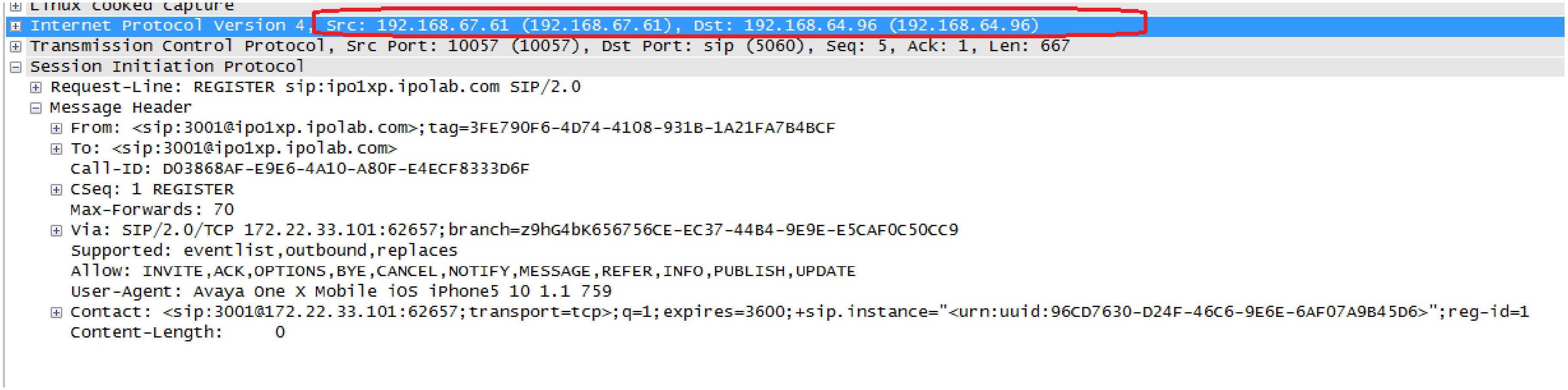
No.	Time	Source	Destination	Protocol	Length	Info
3134	11:16:36.0	192.168.67.61	192.168.64.96	SIP	62	Continuation
3136	11:16:36.0	192.168.67.61	192.168.64.96	SIP	723	Request: REGISTER sip:ipo1xp.ipolab.com
3150	11:16:36.0	192.168.64.96	192.168.67.61	SIP	362	Status: 100 Trying (0 bindings)
3153	11:16:36.0	10.10.10.7	10.10.10.13	SIP	725	[TCP ACKed unseen segment] Request: REGISTER sip:ipo1xp.ipolab.com
3154	11:16:36.1	10.10.10.13	10.10.10.7	SIP	643	Status: 401 Unauthorized (0 bindings)
3160	11:16:36.1	192.168.64.96	192.168.67.61	SIP	654	Status: 401 Unauthorized (0 bindings)
3170	11:16:36.1	192.168.67.61	192.168.64.96	SIP	880	Request: REGISTER sip:ipo1xp.ipolab.com
3176	11:16:36.1	192.168.64.96	192.168.67.61	SIP	362	Status: 100 Trying (0 bindings)
3179	11:16:36.1	10.10.10.7	10.10.10.13	SIP	882	Request: REGISTER sip:ipo1xp.ipolab.com
3181	11:16:36.1	10.10.10.13	10.10.10.7	SIP	670	Status: 200 OK (1 bindings)
3196	11:16:36.1	192.168.64.96	192.168.67.61	SIP	664	Status: 200 OK (1 bindings)

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile VOIP Registration

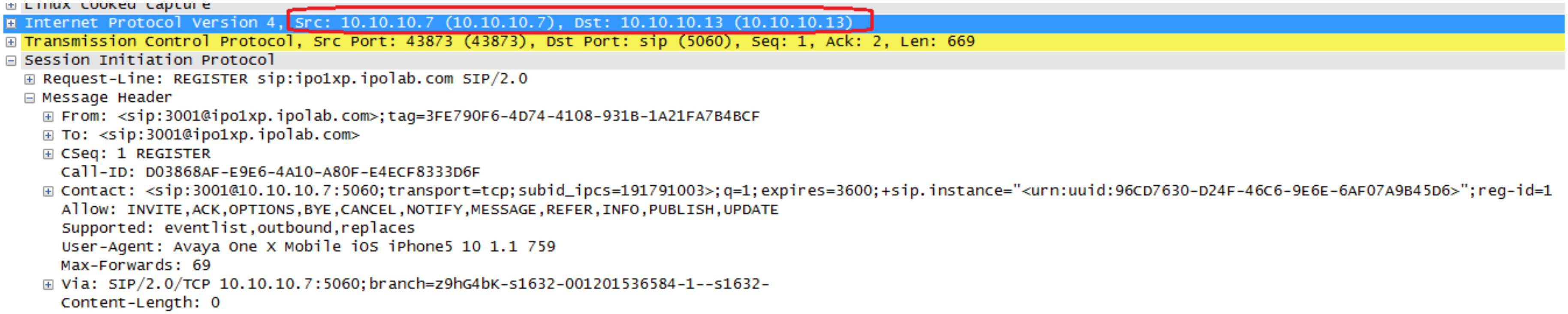
This packet trace was captured from SBCE.

SIP Register from One-x mobile forwarded by Wireless Router to the B1 Interface of the SBCE (Frame #3136 in the previous slide)



```
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 192.168.67.61 (192.168.67.61), Dst: 192.168.64.96 (192.168.64.96)
⊞ Transmission Control Protocol, Src Port: 10057 (10057), Dst Port: sip (5060), Seq: 5, Ack: 1, Len: 667
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:ipo1xp.ipolab.com SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
    ⊞ To: <sip:3001@ipo1xp.ipolab.com>
      Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
    ⊞ CSeq: 1 REGISTER
      Max-Forwards: 70
    ⊞ Via: SIP/2.0/TCP 172.22.33.101:62657;branch=z9hG4bK656756CE-EC37-44B4-9E9E-E5CAF0C50CC9
      Supported: eventlist,outbound,replaces
      Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
      User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
    ⊞ Contact: <sip:3001@172.22.33.101:62657;transport=tcp>;q=1;expires=3600;+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>";reg-id=1
      Content-Length:     0
```

SIP Register forwarded by SBCE A1 interface to IP Office (Frame #3153 in the previous slide)

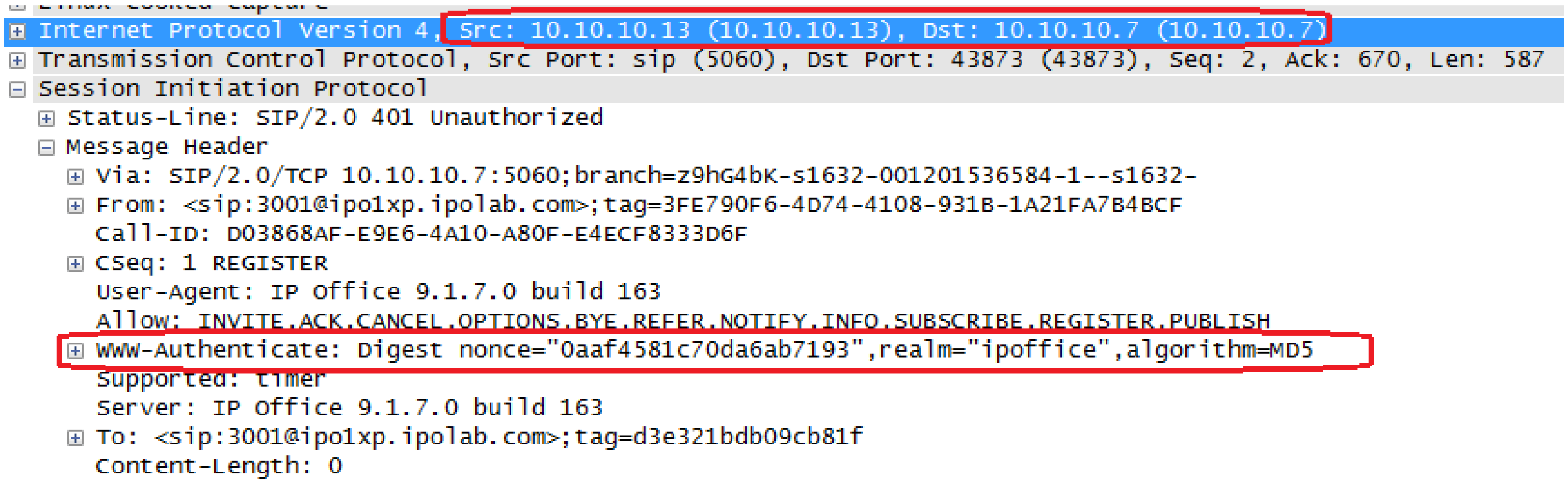


```
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 10.10.10.7 (10.10.10.7), Dst: 10.10.10.13 (10.10.10.13)
⊞ Transmission Control Protocol, Src Port: 43873 (43873), Dst Port: sip (5060), Seq: 1, Ack: 2, Len: 669
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:ipo1xp.ipolab.com SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
    ⊞ To: <sip:3001@ipo1xp.ipolab.com>
    ⊞ CSeq: 1 REGISTER
      Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
    ⊞ Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>;q=1;expires=3600;+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>";reg-id=1
      Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
      Supported: eventlist,outbound,replaces
      User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
      Max-Forwards: 69
    ⊞ Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001201536584-1--s1632-
      Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

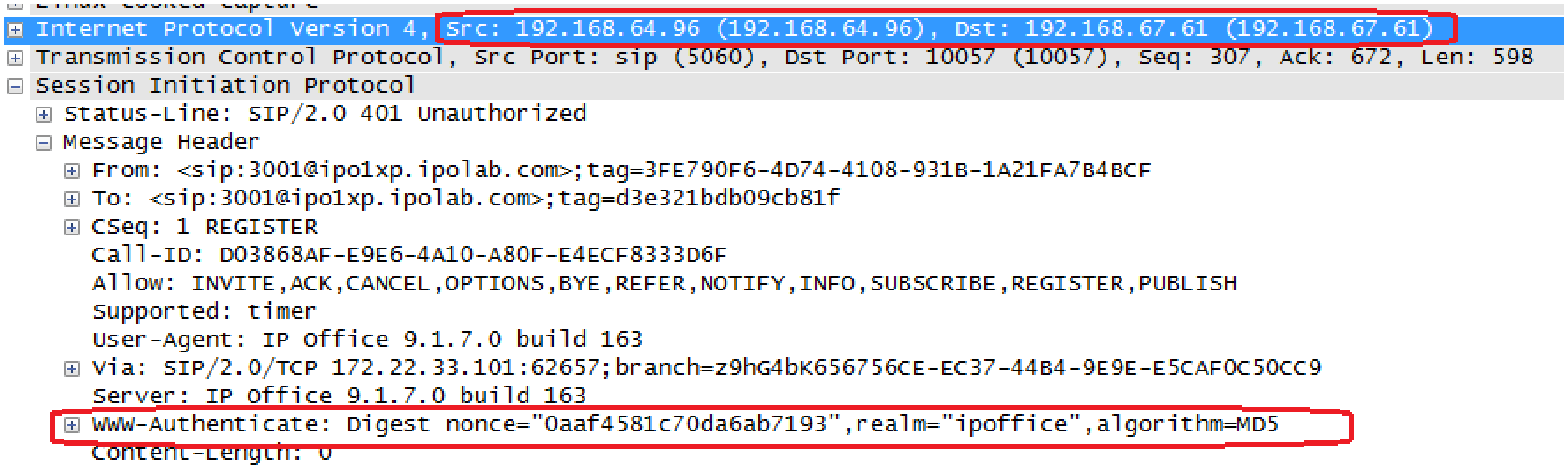
❑ One-x Mobile VOIP Registration

IP Office responded with 401 Unauthorized and provided Authenticate header with nonce value.



```
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 10.10.10.13 (10.10.10.13), Dst: 10.10.10.7 (10.10.10.7)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 43873 (43873), Seq: 2, Ack: 670, Len: 587
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 401 Unauthorized
  ⊟ Message Header
    ⊞ Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001201536584-1--s1632-
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
      Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
    ⊞ CSeq: 1 REGISTER
      User-Agent: IP Office 9.1.7.0 build 163
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
    ⊞ WWW-Authenticate: Digest nonce="0aaf4581c70da6ab7193",realm="ipoffice",algorithm=MD5
      Supported: timer
      Server: IP Office 9.1.7.0 build 163
    ⊞ To: <sip:3001@ipo1xp.ipolab.com>;tag=d3e321bdb09cb81f
      Content-Length: 0
```

SBCE then forwarded the SIP 401 Unauthorized message to One-x mobile client via Wireless Router.

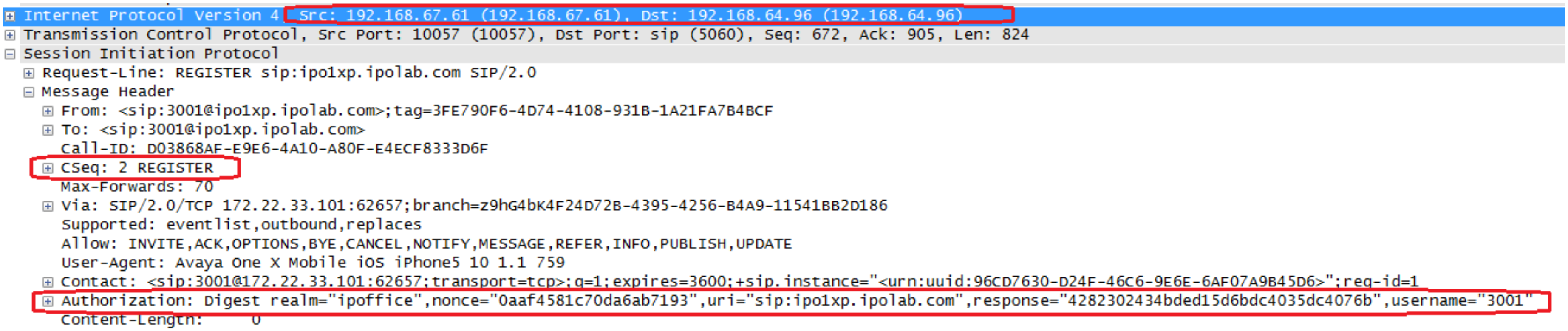


```
⊞ Linux cooked capture
⊞ Internet Protocol Version 4, Src: 192.168.64.96 (192.168.64.96), Dst: 192.168.67.61 (192.168.67.61)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 10057 (10057), Seq: 307, Ack: 672, Len: 598
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 401 Unauthorized
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
    ⊞ To: <sip:3001@ipo1xp.ipolab.com>;tag=d3e321bdb09cb81f
    ⊞ CSeq: 1 REGISTER
      Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
      Supported: timer
      User-Agent: IP Office 9.1.7.0 build 163
    ⊞ Via: SIP/2.0/TCP 172.22.33.101:62657;branch=z9hG4bK656756CE-EC37-44B4-9E9E-E5CAF0C50CC9
      Server: IP Office 9.1.7.0 build 163
    ⊞ WWW-Authenticate: Digest nonce="0aaf4581c70da6ab7193",realm="ipoffice",algorithm=MD5
      Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

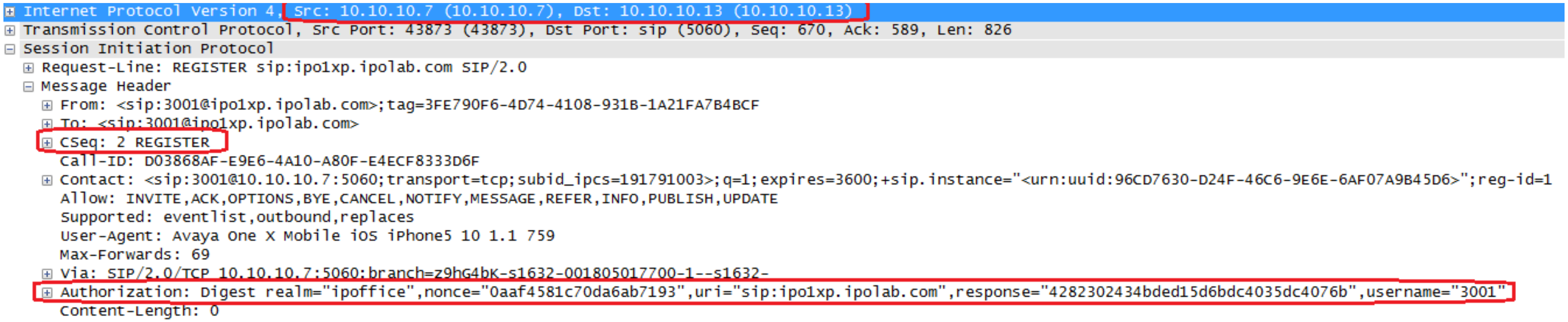
❑ One-x Mobile VOIP Registration

One-x mobile client sent another Register message with Authorization header with calculated “response”.



```
⊞ Internet Protocol Version 4, Src: 192.168.67.61 (192.168.67.61), Dst: 192.168.64.96 (192.168.64.96)
⊞ Transmission Control Protocol, Src Port: 10057 (10057), Dst Port: sip (5060), Seq: 672, Ack: 905, Len: 824
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:ipo1xp.ipolab.com SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
    ⊞ To: <sip:3001@ipo1xp.ipolab.com>
      Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
    ⊞ CSeq: 2 REGISTER
      Max-Forwards: 70
    ⊞ Via: SIP/2.0/TCP 172.22.33.101:62657;branch=z9hG4bK4F24D72B-4395-4256-B4A9-11541BB2D186
      Supported: eventlist,outbound,replaces
      Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
      User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
    ⊞ Contact: <sip:3001@172.22.33.101:62657;transport=tcp>;q=1;expires=3600;+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>";reg-id=1
    ⊞ Authorization: Digest realm="ipoffice",nonce="0aaf4581c70da6ab7193",uri="sip:ipo1xp.ipolab.com",response="4282302434bded15d6bdc4035dc4076b",username="3001"
      Content-Length:     0
```

SBCE forwarded the new Register message to IP Office via A1 interface.

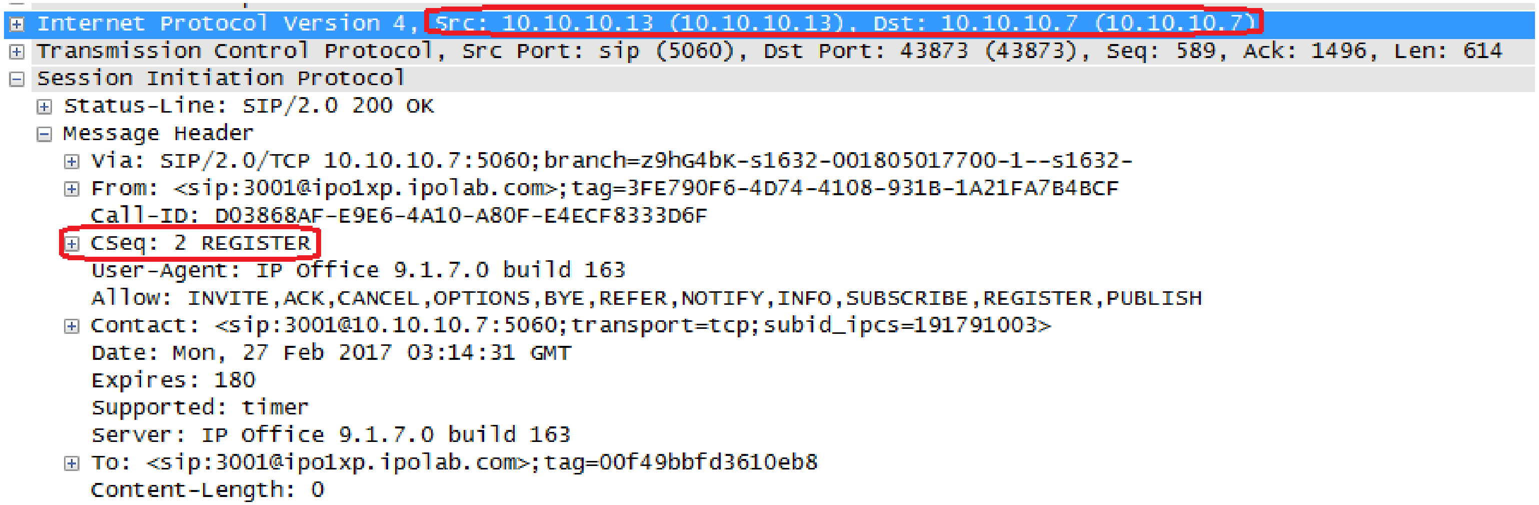


```
⊞ Internet Protocol Version 4, Src: 10.10.10.7 (10.10.10.7), Dst: 10.10.10.13 (10.10.10.13)
⊞ Transmission Control Protocol, Src Port: 43873 (43873), Dst Port: sip (5060), Seq: 670, Ack: 589, Len: 826
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:ipo1xp.ipolab.com SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
    ⊞ To: <sip:3001@ipo1xp.ipolab.com>
    ⊞ CSeq: 2 REGISTER
      Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
    ⊞ Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>;q=1;expires=3600;+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>";reg-id=1
      Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
      Supported: eventlist,outbound,replaces
      User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
      Max-Forwards: 69
    ⊞ Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001805017700-1--s1632-
    ⊞ Authorization: Digest realm="ipoffice",nonce="0aaf4581c70da6ab7193",uri="sip:ipo1xp.ipolab.com",response="4282302434bded15d6bdc4035dc4076b",username="3001"
      Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

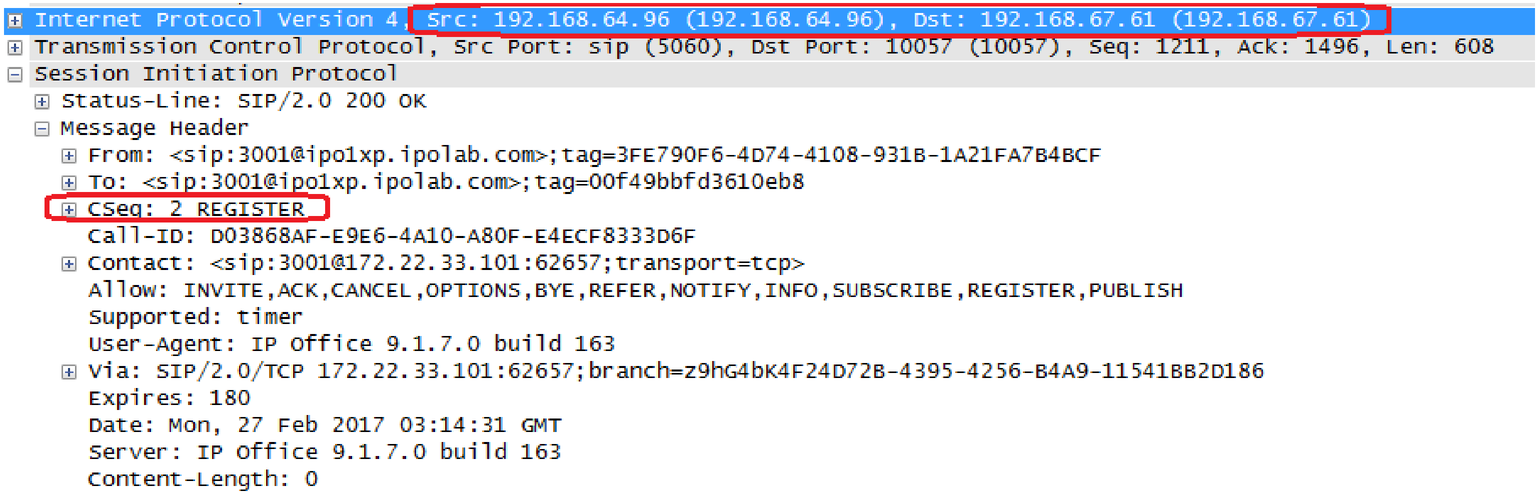
❑ One-x Mobile VOIP Registration

IP Office accepted the registration and responded with 200OK.



```
⊞ Internet Protocol Version 4, Src: 10.10.10.13 (10.10.10.13), Dst: 10.10.10.7 (10.10.10.7)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 43873 (43873), Seq: 589, Ack: 1496, Len: 614
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊟ Message Header
    ⊞ Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001805017700-1--s1632-
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
      Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
    ⊞ CSeq: 2 REGISTER
      User-Agent: IP Office 9.1.7.0 build 163
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
    ⊞ Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>
      Date: Mon, 27 Feb 2017 03:14:31 GMT
      Expires: 180
      Supported: timer
      Server: IP Office 9.1.7.0 build 163
    ⊞ To: <sip:3001@ipo1xp.ipolab.com>;tag=00f49bbfd3610eb8
      Content-Length: 0
```

SBCE then forwarded the 200OK to the One-x mobile client via the Wireless Router.



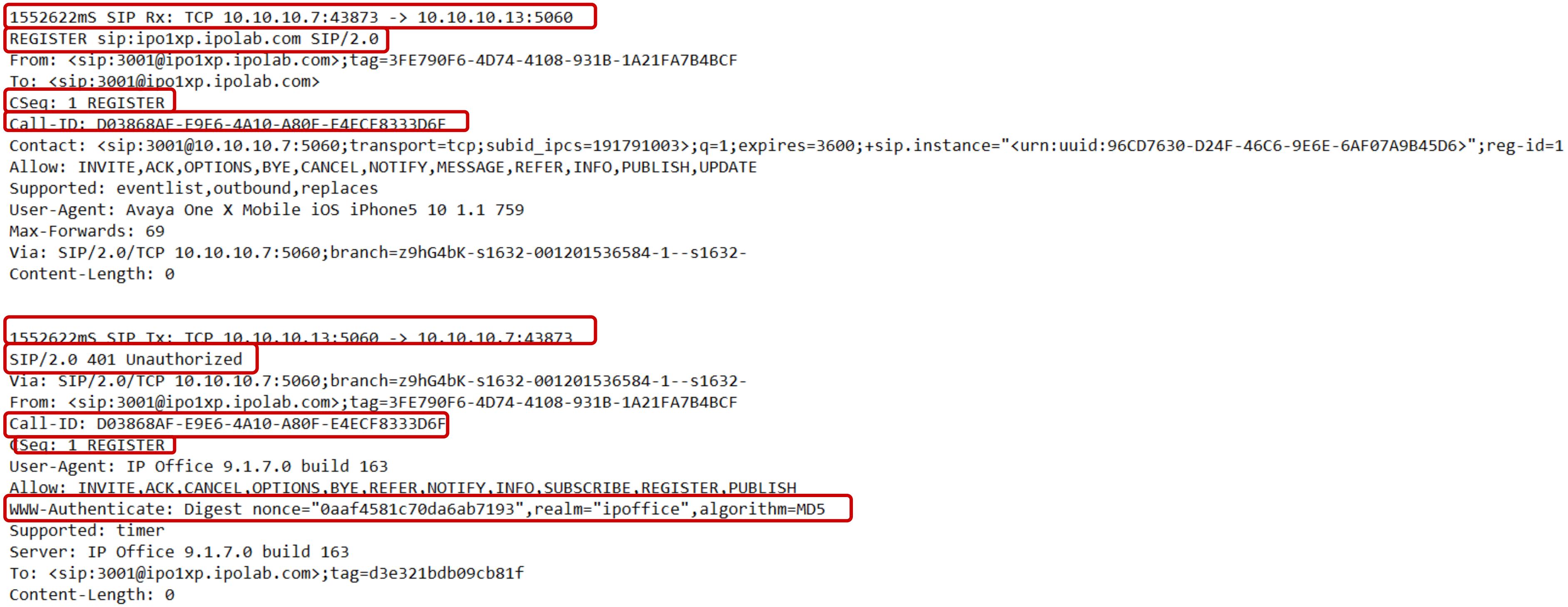
```
⊞ Internet Protocol Version 4, Src: 192.168.64.96 (192.168.64.96), Dst: 192.168.67.61 (192.168.67.61)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 10057 (10057), Seq: 1211, Ack: 1496, Len: 608
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
    ⊞ To: <sip:3001@ipo1xp.ipolab.com>;tag=00f49bbfd3610eb8
    ⊞ CSeq: 2 REGISTER
      Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
    ⊞ Contact: <sip:3001@172.22.33.101:62657;transport=tcp>
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
      Supported: timer
      User-Agent: IP Office 9.1.7.0 build 163
    ⊞ Via: SIP/2.0/TCP 172.22.33.101:62657;branch=z9hG4bK4F24D72B-4395-4256-B4A9-11541BB2D186
      Expires: 180
      Date: Mon, 27 Feb 2017 03:14:31 GMT
      Server: IP Office 9.1.7.0 build 163
      Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile VOIP Registration

Here is the corresponding IPO System Monitor trace.

IP Office received the Register request but needs to be authenticated, hence it sent back 401 Unauthorized with Authenticate header.

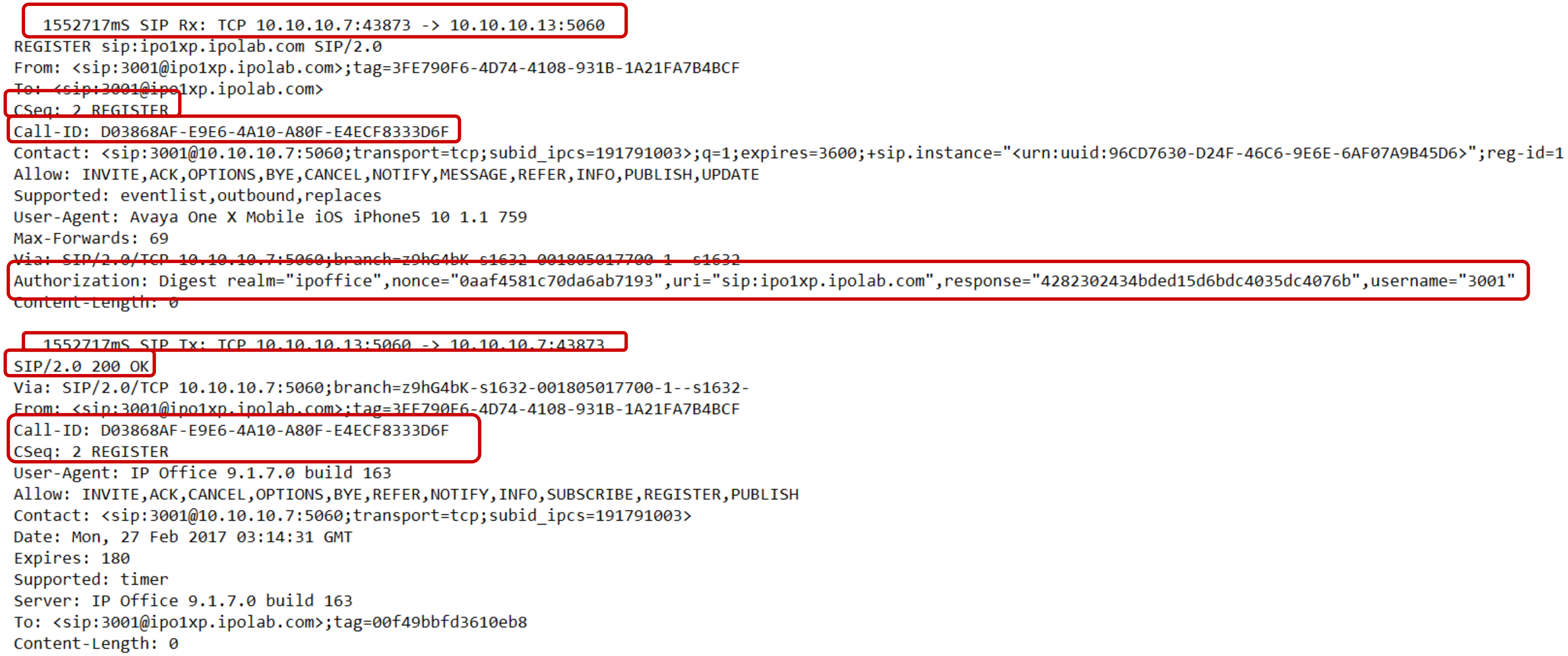


```
1552622mS SIP Rx: TCP 10.10.10.7:43873 -> 10.10.10.13:5060
REGISTER sip:ipo1xp.ipolab.com SIP/2.0
From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
To: <sip:3001@ipo1xp.ipolab.com>
CSeq: 1 REGISTER
Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>;q=1;expires=3600;+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>";reg-id=1
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
Supported: eventlist,outbound,replaces
User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
Max-Forwards: 69
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001201536584-1--s1632-
Content-Length: 0


1552622mS SIP Tx: TCP 10.10.10.13:5060 -> 10.10.10.7:43873
SIP/2.0 401 Unauthorized
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001201536584-1--s1632-
From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
CSeq: 1 REGISTER
User-Agent: IP Office 9.1.7.0 build 163
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
WWW-Authenticate: Digest nonce="0aaf4581c70da6ab7193",realm="ipoffice",algorithm=MD5
Supported: timer
Server: IP Office 9.1.7.0 build 163
To: <sip:3001@ipo1xp.ipolab.com>;tag=d3e321bdb09cb81f
Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile VOIP Registration

Then IP Office received another Register request with Authorization header with calculated response value.
Then IP Office accepted the request and responded with 200OK.

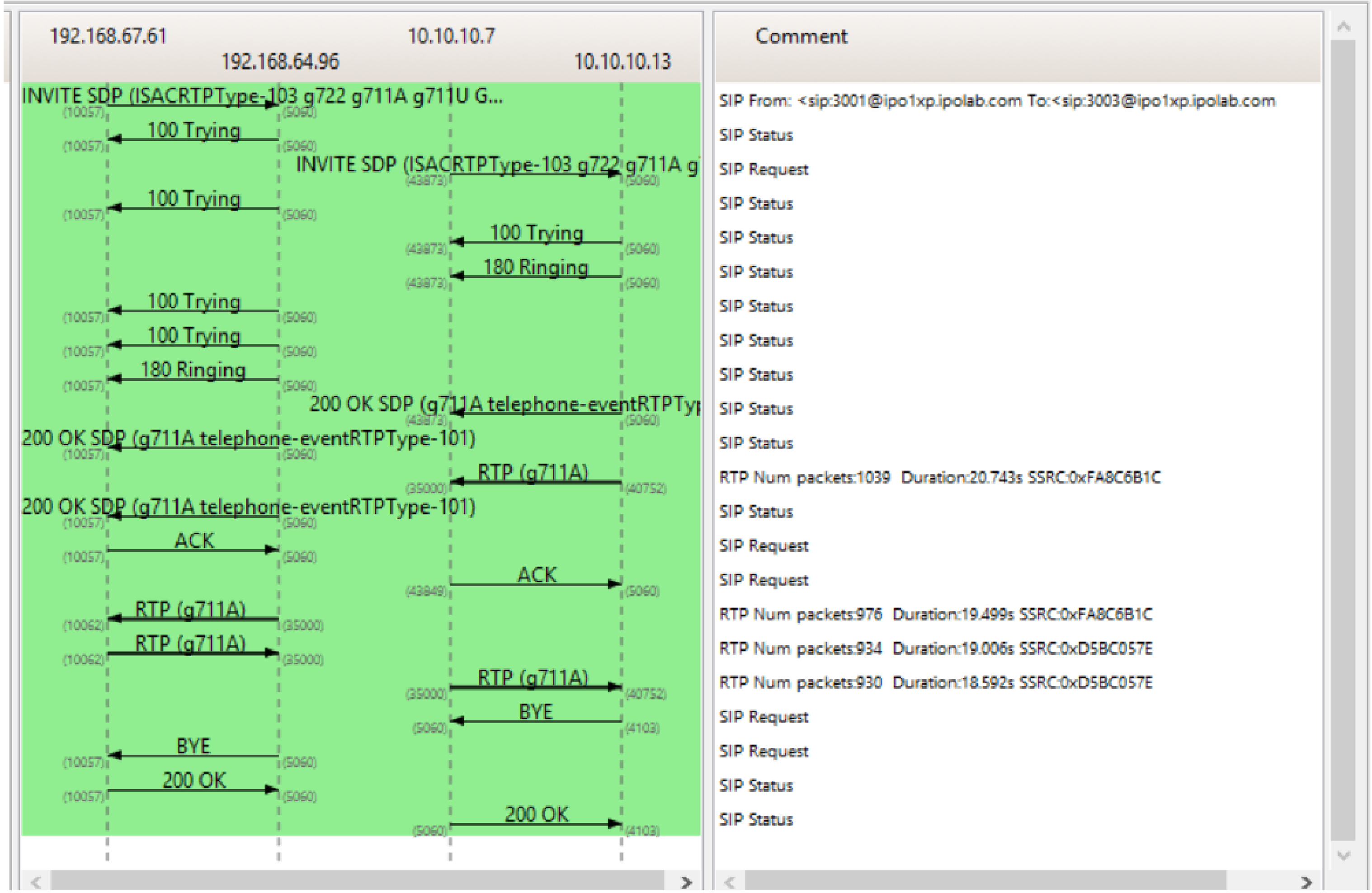


```
   1552717mS SIP Rx: TCP 10.10.10.7:43873 -> 10.10.10.13:5060
REGISTER sip:ipo1xp.ipolab.com SIP/2.0
From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
To: <sip:3001@ipo1xp.ipolab.com>
CSeq: 2 REGISTER
Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>;q=1;expires=3600;+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>";reg-id=1
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
Supported: eventlist,outbound,replaces
User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
Max-Forwards: 69
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001805017700-1--s1632
Authorization: Digest realm="ipoffice",nonce="0aaf4581c70da6ab7193",uri="sip:ipo1xp.ipolab.com",response="4282302434bded15d6bdc4035dc4076b",username="3001"
Content-Length: 0

   1552717mS SIP Tx: TCP 10.10.10.13:5060 -> 10.10.10.7:43873
SIP/2.0 200 OK
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001805017700-1--s1632-
From: <sip:3001@ipo1xp.ipolab.com>;tag=3FE790F6-4D74-4108-931B-1A21FA7B4BCF
Call-ID: D03868AF-E9E6-4A10-A80F-E4ECF8333D6F
CSeq: 2 REGISTER
User-Agent: IP Office 9.1.7.0 build 163
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>
Date: Mon, 27 Feb 2017 03:14:31 GMT
Expires: 180
Supported: timer
Server: IP Office 9.1.7.0 build 163
To: <sip:3001@ipo1xp.ipolab.com>;tag=00f49bbfd3610eb8
Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

Scenario: One-x Mobile user Ruel on extension 3001 calls H323 user Dora on extension 3003



Comment

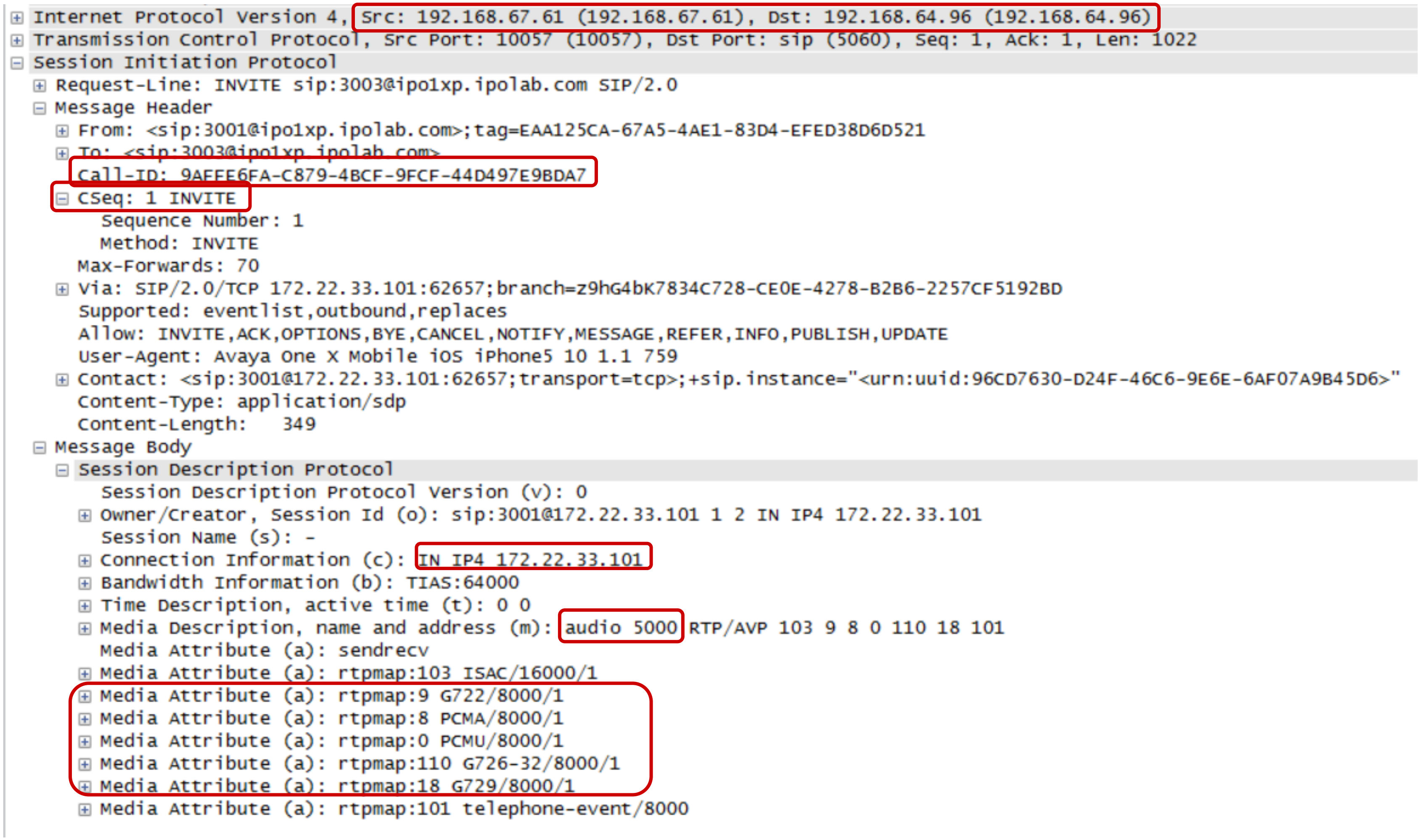
SIP From: <sip:3001@ipo1xp.ipolab.com To:<sip:3003@ipo1xp.ipolab.com
SIP Status
SIP Request
SIP Status
SIP Status
SIP Status
SIP Status
SIP Status
SIP Status
SIP Status
SIP Status
RTP Num packets:1039 Duration:20.743s SSRC:0xFA8C6B1C
SIP Status
SIP Request
SIP Request
RTP Num packets:976 Duration:19.499s SSRC:0xFA8C6B1C
RTP Num packets:934 Duration:19.006s SSRC:0xD5BC057E
RTP Num packets:930 Duration:18.592s SSRC:0xD5BC057E
SIP Request
SIP Request
SIP Status
SIP Status

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

This packet trace was captured from SBCE.

One-x mobile sent INVITE message which was forwarded by Wireless Router to SBCE B1 interface.

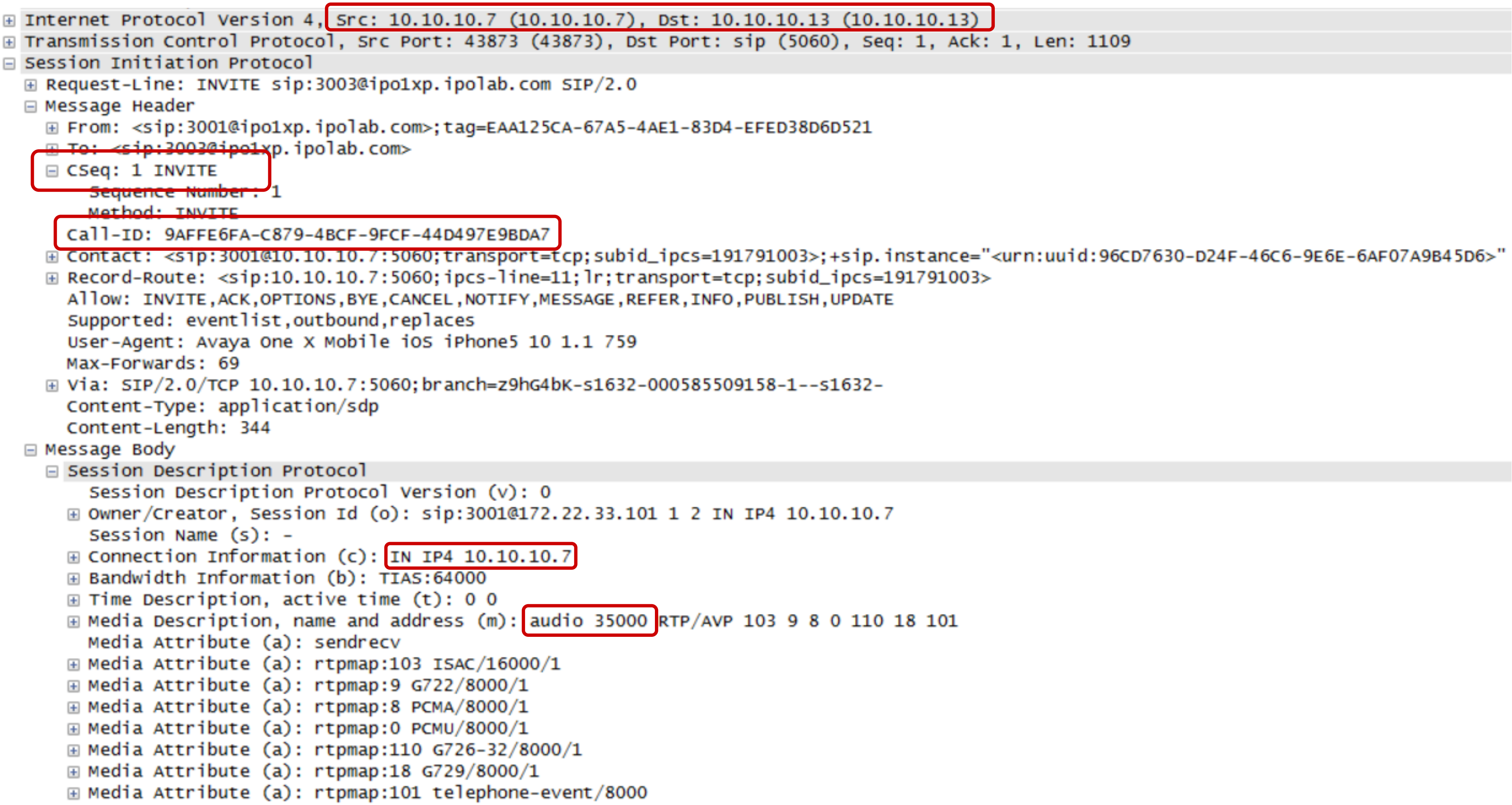


```
⊞ Internet Protocol Version 4, Src: 192.168.67.61 (192.168.67.61), Dst: 192.168.64.96 (192.168.64.96)
⊞ Transmission Control Protocol, Src Port: 10057 (10057), Dst Port: sip (5060), Seq: 1, Ack: 1, Len: 1022
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:3003@ipo1xp.ipolab.com SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
    ⊞ To: <sip:3003@ipo1xp.ipolab.com>
      Call-ID: 9AFEE6FA-C879-4BCF-9FCF-44D497E9BDA7
    ⊟ CSeq: 1 INVITE
        Sequence Number: 1
        Method: INVITE
      Max-Forwards: 70
    ⊞ Via: SIP/2.0/TCP 172.22.33.101:62657;branch=z9hG4bK7834C728-CE0E-4278-B2B6-2257CF5192BD
      Supported: eventlist,outbound,replaces
      Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
      User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
    ⊞ Contact: <sip:3001@172.22.33.101:62657;transport=tcp>;+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>"
      Content-Type: application/sdp
      Content-Length:   349
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): sip:3001@172.22.33.101 1 2 IN IP4 172.22.33.101
        Session Name (s): -
      ⊞ Connection Information (c): IN IP4 172.22.33.101
      ⊞ Bandwidth Information (b): TIAS:64000
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 5000 RTP/AVP 103 9 8 0 110 18 101
        Media Attribute (a): sendrecv
      ⊞ Media Attribute (a): rtpmap:103 ISAC/16000/1
      ⊞ Media Attribute (a): rtpmap:9 G722/8000/1
      ⊞ Media Attribute (a): rtpmap:8 PCMA/8000/1
      ⊞ Media Attribute (a): rtpmap:0 PCMU/8000/1
      ⊞ Media Attribute (a): rtpmap:110 G726-32/8000/1
      ⊞ Media Attribute (a): rtpmap:18 G729/8000/1
      ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

SBCE forwarded the INVITE to IP Office via A1 interface.

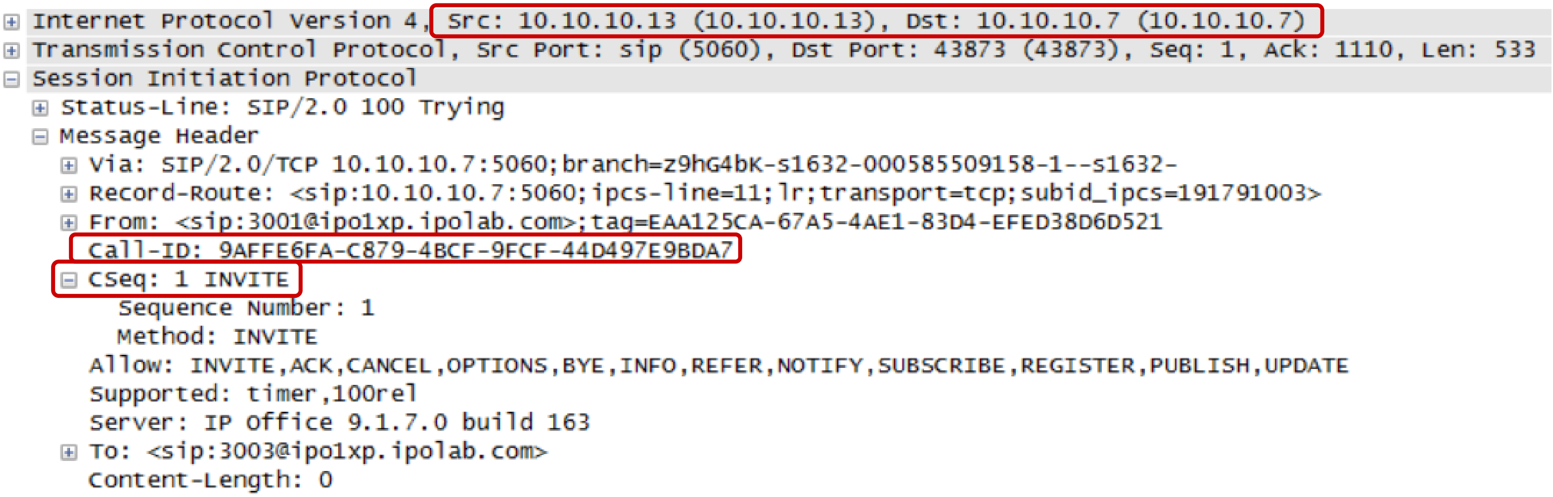


```
⊞ Internet Protocol Version 4, Src: 10.10.10.7 (10.10.10.7), Dst: 10.10.10.13 (10.10.10.13)
⊞ Transmission Control Protocol, Src Port: 43873 (43873), Dst Port: sip (5060), Seq: 1, Ack: 1, Len: 1109
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:3003@ipo1xp.ipolab.com SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
    ⊞ To: <sip:3003@ipo1xp.ipolab.com>
    ⊟ CSeq: 1 INVITE
        Sequence Number: 1
        Method: INVITE
      Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
    ⊞ Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>;+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>"
    ⊞ Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
      Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
      Supported: eventlist,outbound,replaces
      User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
      Max-Forwards: 69
    ⊞ Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-000585509158-1--s1632-
      Content-Type: application/sdp
      Content-Length: 344
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): sip:3001@172.22.33.101 1 2 IN IP4 10.10.10.7
        Session Name (s): -
      ⊞ Connection Information (c): IN IP4 10.10.10.7
      ⊞ Bandwidth Information (b): TIAS:64000
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 35000 RTP/AVP 103 9 8 0 110 18 101
        Media Attribute (a): sendrecv
      ⊞ Media Attribute (a): rtpmap:103 ISAC/16000/1
      ⊞ Media Attribute (a): rtpmap:9 G722/8000/1
      ⊞ Media Attribute (a): rtpmap:8 PCMA/8000/1
      ⊞ Media Attribute (a): rtpmap:0 PCMU/8000/1
      ⊞ Media Attribute (a): rtpmap:110 G726-32/8000/1
      ⊞ Media Attribute (a): rtpmap:18 G729/8000/1
      ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
```

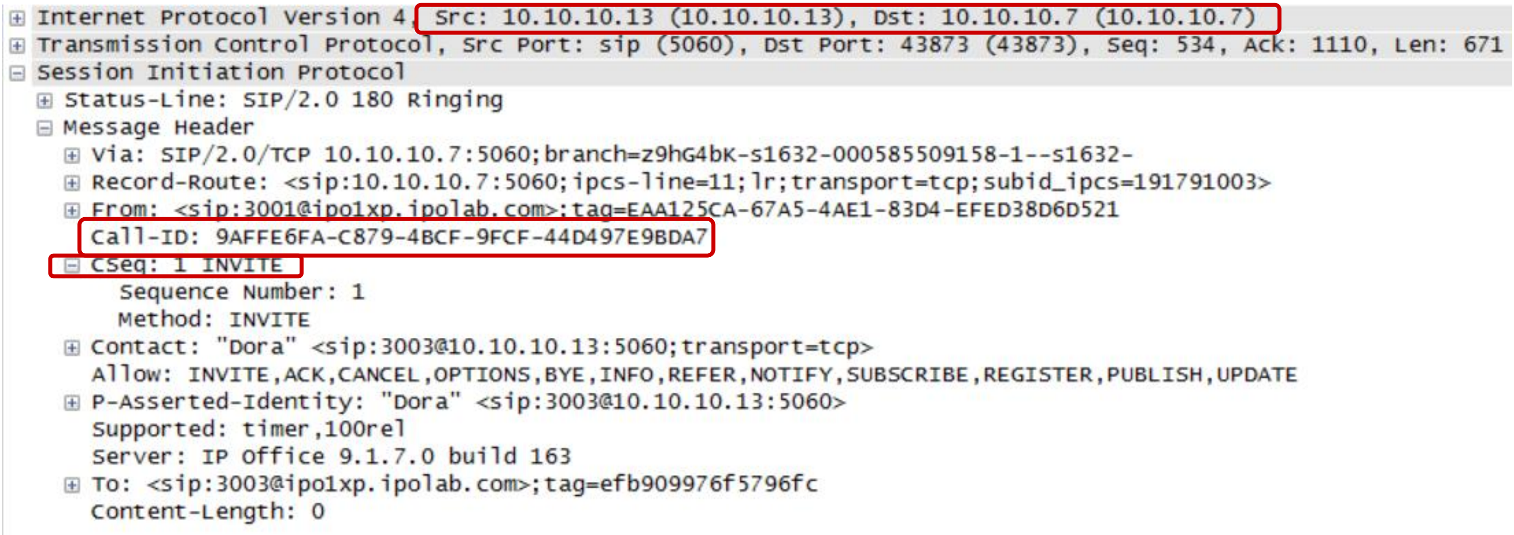
Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

IP Office responded with 100 Trying and 180 Ringing.



```
⊞ Internet Protocol Version 4, Src: 10.10.10.13 (10.10.10.13), Dst: 10.10.10.7 (10.10.10.7)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 43873 (43873), Seq: 1, Ack: 1110, Len: 533
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 100 Trying
  ⊟ Message Header
    ⊞ Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-000585509158-1--s1632-
    ⊞ Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
      Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
    ⊟ CSeq: 1 INVITE
        Sequence Number: 1
        Method: INVITE
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
      Supported: timer,100rel
      Server: IP Office 9.1.7.0 build 163
    ⊞ To: <sip:3003@ipo1xp.ipolab.com>
      Content-Length: 0
```

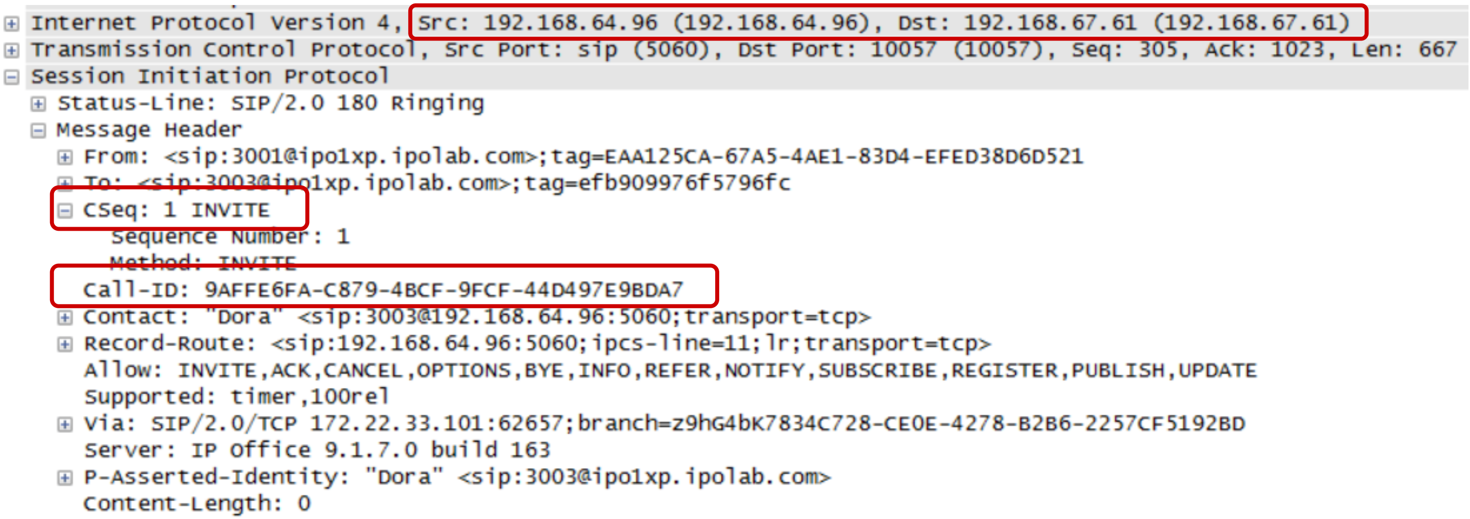


```
⊞ Internet Protocol Version 4, Src: 10.10.10.13 (10.10.10.13), Dst: 10.10.10.7 (10.10.10.7)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 43873 (43873), Seq: 534, Ack: 1110, Len: 671
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 180 Ringing
  ⊟ Message Header
    ⊞ Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-000585509158-1--s1632-
    ⊞ Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
      Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
    ⊟ CSeq: 1 INVITE
        Sequence Number: 1
        Method: INVITE
    ⊞ Contact: "Dora" <sip:3003@10.10.10.13:5060;transport=tcp>
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
    ⊞ P-Asserted-Identity: "Dora" <sip:3003@10.10.10.13:5060>
      Supported: timer,100rel
      Server: IP Office 9.1.7.0 build 163
    ⊞ To: <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
      Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

SBCE relayed the 180 Ringing to One-x Mobile client via the Wireless Router.

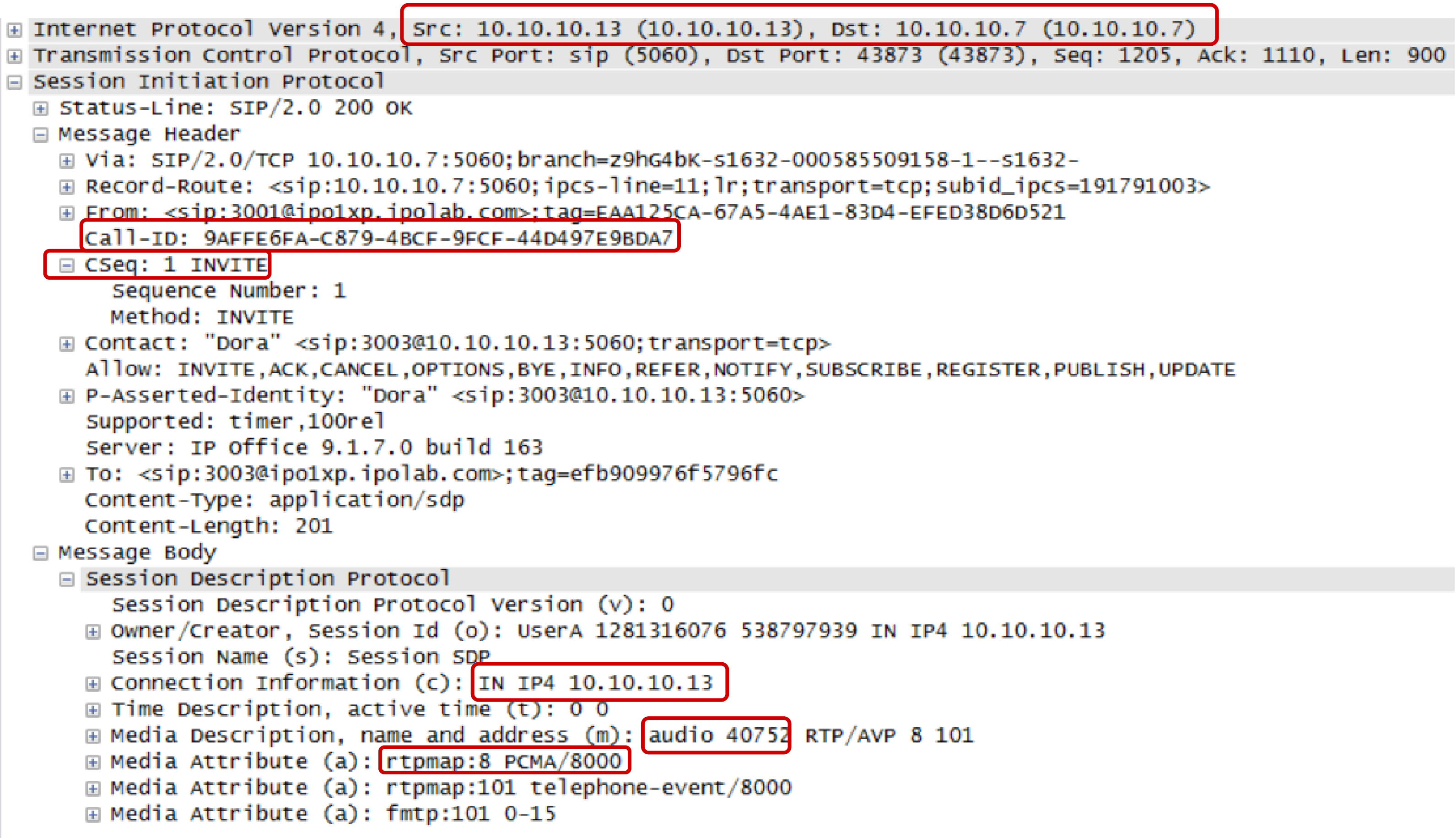


```
⊞ Internet Protocol Version 4, Src: 192.168.64.96 (192.168.64.96), Dst: 192.168.67.61 (192.168.67.61)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 10057 (10057), Seq: 305, Ack: 1023, Len: 667
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 180 Ringing
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
    ⊞ To: <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
    ⊟ CSeq: 1 INVITE
        Sequence Number: 1
        Method: INVITE
      Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
    ⊞ Contact: "Dora" <sip:3003@192.168.64.96:5060;transport=tcp>
    ⊞ Record-Route: <sip:192.168.64.96:5060;ipcs-line=11;lr;transport=tcp>
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
      Supported: timer,100rel
    ⊞ Via: SIP/2.0/TCP 172.22.33.101:62657;branch=z9hG4bK7834C728-CE0E-4278-B2B6-2257CF5192BD
      Server: IP Office 9.1.7.0 build 163
    ⊞ P-Asserted-Identity: "Dora" <sip:3003@ipo1xp.ipolab.com>
      Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

Extension 3003 answers the call. IP Office then sent 200OK to SBCE on A1 interface.

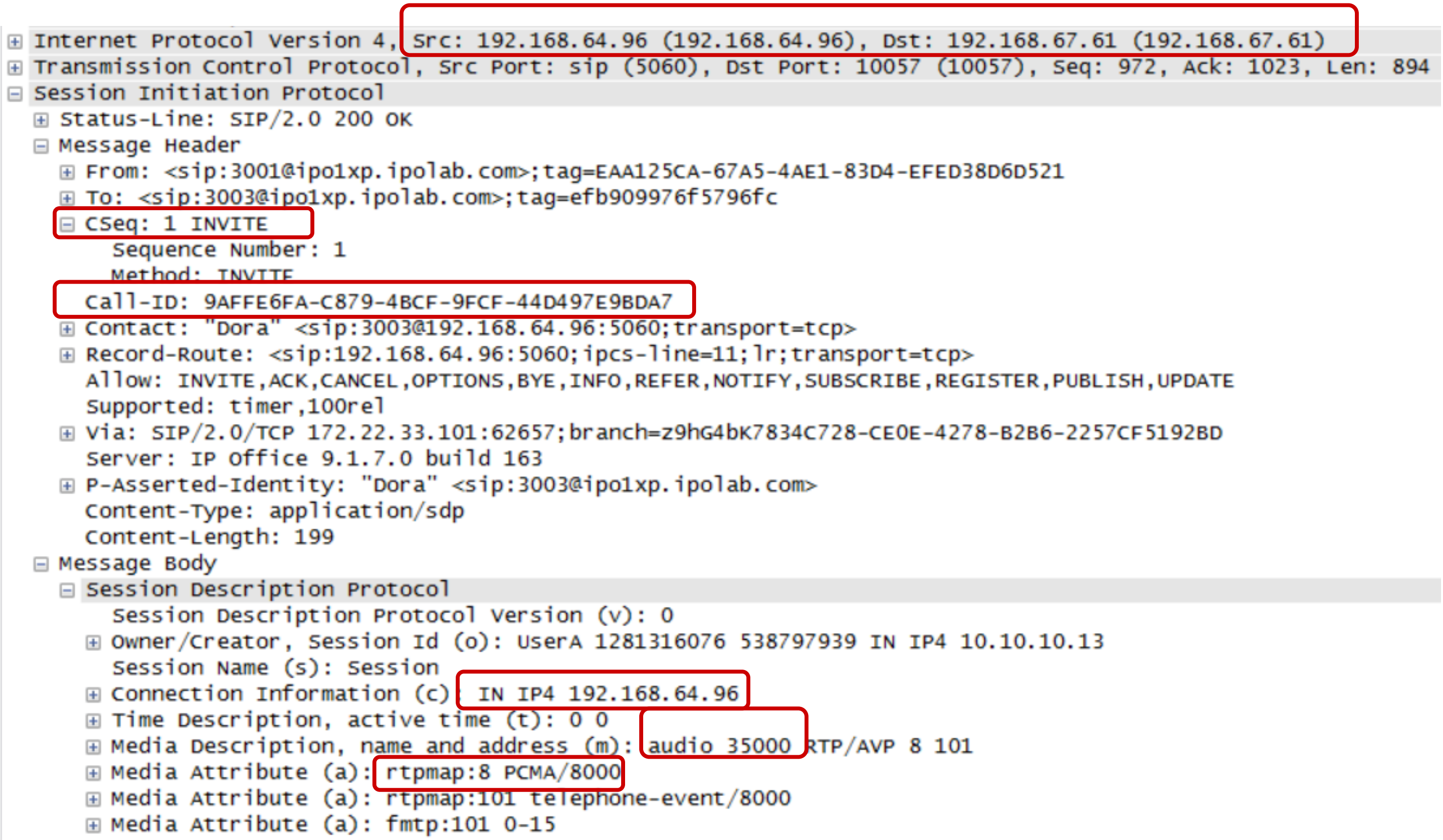


```
⊞ Internet Protocol Version 4, Src: 10.10.10.13 (10.10.10.13), Dst: 10.10.10.7 (10.10.10.7)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 43873 (43873), Seq: 1205, Ack: 1110, Len: 900
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊟ Message Header
    ⊞ Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-000585509158-1--s1632-
    ⊞ Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
      Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
    ⊟ CSeq: 1 INVITE
        Sequence Number: 1
        Method: INVITE
    ⊞ Contact: "Dora" <sip:3003@10.10.10.13:5060;transport=tcp>
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
    ⊞ P-Asserted-Identity: "Dora" <sip:3003@10.10.10.13:5060>
      Supported: timer,100rel
      Server: IP Office 9.1.7.0 build 163
    ⊞ To: <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
      Content-Type: application/sdp
      Content-Length: 201
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): UserA 1281316076 538797939 IN IP4 10.10.10.13
        Session Name (s): Session SDP
      ⊞ Connection Information (c): IN IP4 10.10.10.13
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 40752 RTP/AVP 8 101
      ⊞ Media Attribute (a): rtpmap:8 PCMA/8000
      ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
      ⊞ Media Attribute (a): fmtp:101 0-15
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

SBCE forwarded the 200OK to One-x Mobile client via the Wireless Router. The call is now connected.



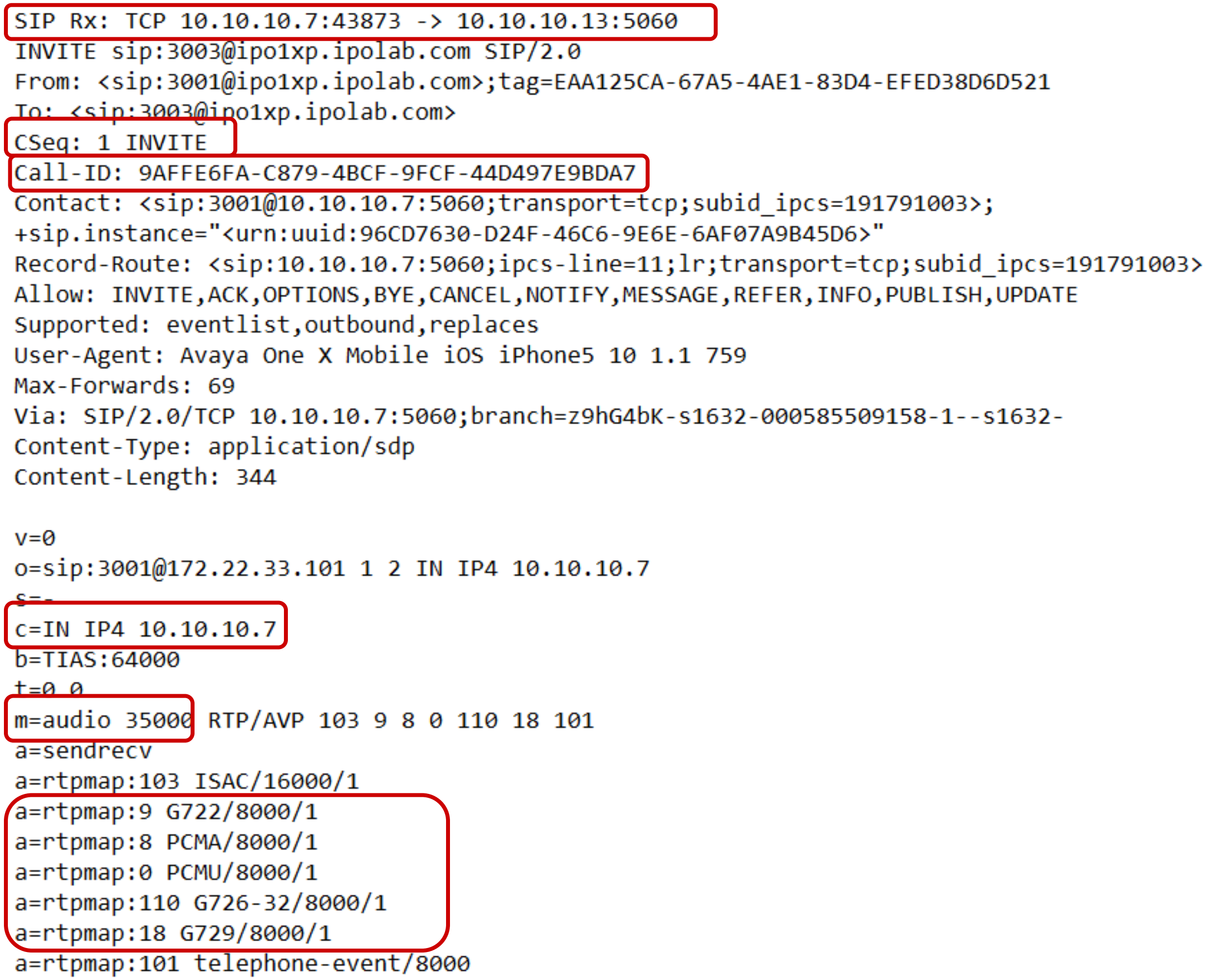
```
⊞ Internet Protocol Version 4, Src: 192.168.64.96 (192.168.64.96), Dst: 192.168.67.61 (192.168.67.61)
⊞ Transmission Control Protocol, Src Port: sip (5060), Dst Port: 10057 (10057), Seq: 972, Ack: 1023, Len: 894
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊟ Message Header
    ⊞ From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
    ⊞ To: <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
    ⊟ CSeq: 1 INVITE
        Sequence Number: 1
        Method: INVITE
      Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
    ⊞ Contact: "Dora" <sip:3003@192.168.64.96:5060;transport=tcp>
    ⊞ Record-Route: <sip:192.168.64.96:5060;ipcs-line=11;lr;transport=tcp>
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
      Supported: timer,100rel
    ⊞ Via: SIP/2.0/TCP 172.22.33.101:62657;branch=z9hG4bK7834C728-CE0E-4278-B2B6-2257CF5192BD
      Server: IP Office 9.1.7.0 build 163
    ⊞ P-Asserted-Identity: "Dora" <sip:3003@ipo1xp.ipolab.com>
      Content-Type: application/sdp
      Content-Length: 199
  ⊟ Message Body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): UserA 1281316076 538797939 IN IP4 10.10.10.13
        Session Name (s): session
      ⊞ Connection Information (c): IN IP4 192.168.64.96
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 35000 RTP/AVP 8 101
      ⊞ Media Attribute (a): rtpmap:8 PCMA/8000
      ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
      ⊞ Media Attribute (a): fmtp:101 0-15
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

Here is the corresponding system monitor trace from IPO.

SIP INVITE request coming from SBCE A1 interface.

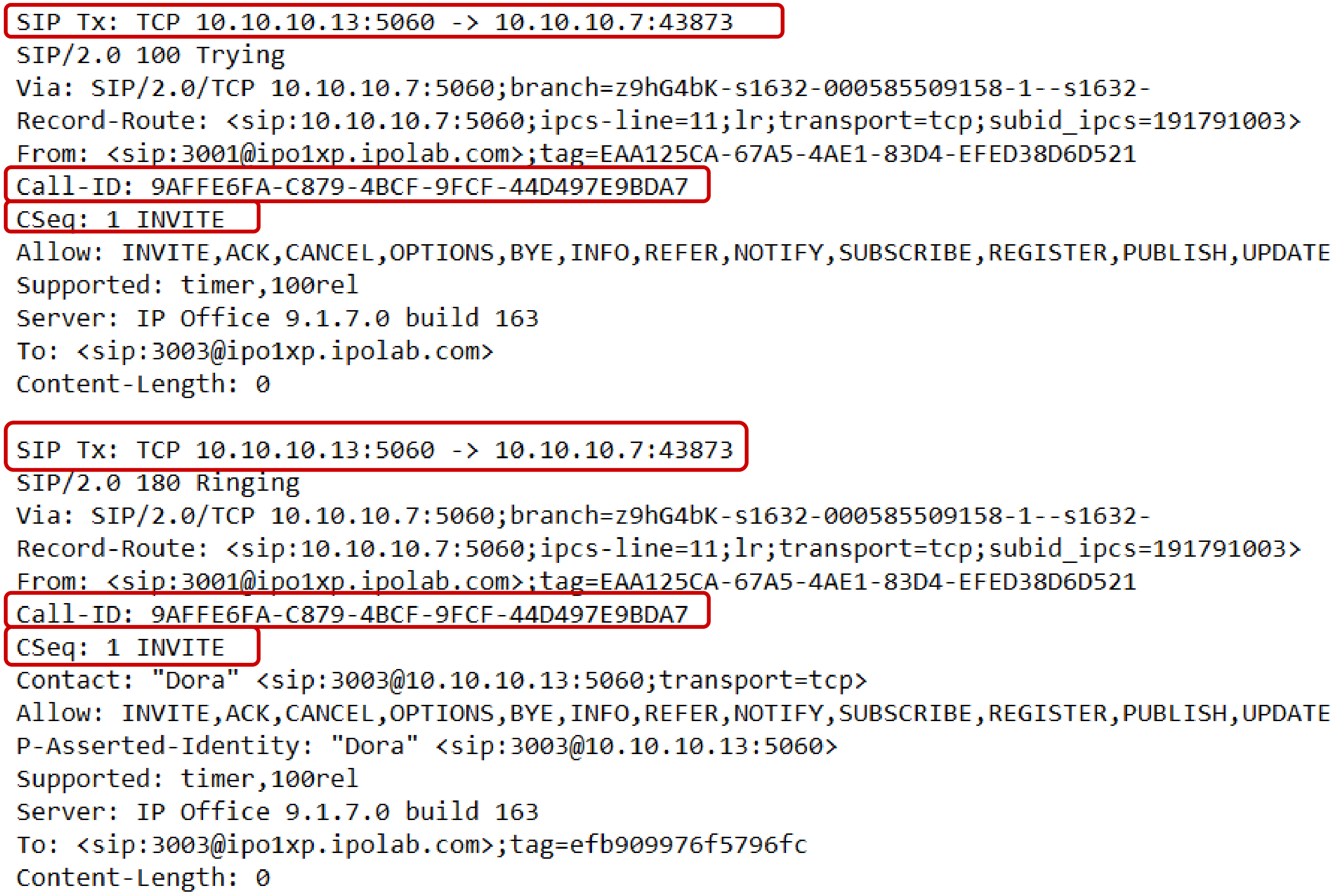


```
SIP Rx: TCP 10.10.10.7:43873 -> 10.10.10.13:5060
INVITE sip:3003@ipo1xp.ipolab.com SIP/2.0
From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
To: <sip:3003@ipo1xp.ipolab.com>
CSeq: 1 INVITE
Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>;
+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>"
Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
Supported: eventlist,outbound,replaces
User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
Max-Forwards: 69
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-000585509158-1--s1632-
Content-Type: application/sdp
Content-Length: 344

v=0
o=sip:3001@172.22.33.101 1 2 IN IP4 10.10.10.7
s=-
c=IN IP4 10.10.10.7
b=TIAS:64000
t=0 0
m=audio 35000 RTP/AVP 103 9 8 0 110 18 101
a=sendrecv
a=rtpmap:103 ISAC/16000/1
a=rtpmap:9 G722/8000/1
a=rtpmap:8 PCMA/8000/1
a=rtpmap:0 PCMU/8000/1
a=rtpmap:110 G726-32/8000/1
a=rtpmap:18 G729/8000/1
a=rtpmap:101 telephone-event/8000
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

SIP 100 Trying and 180 Ringing from IPO to SBCE A1 interface.

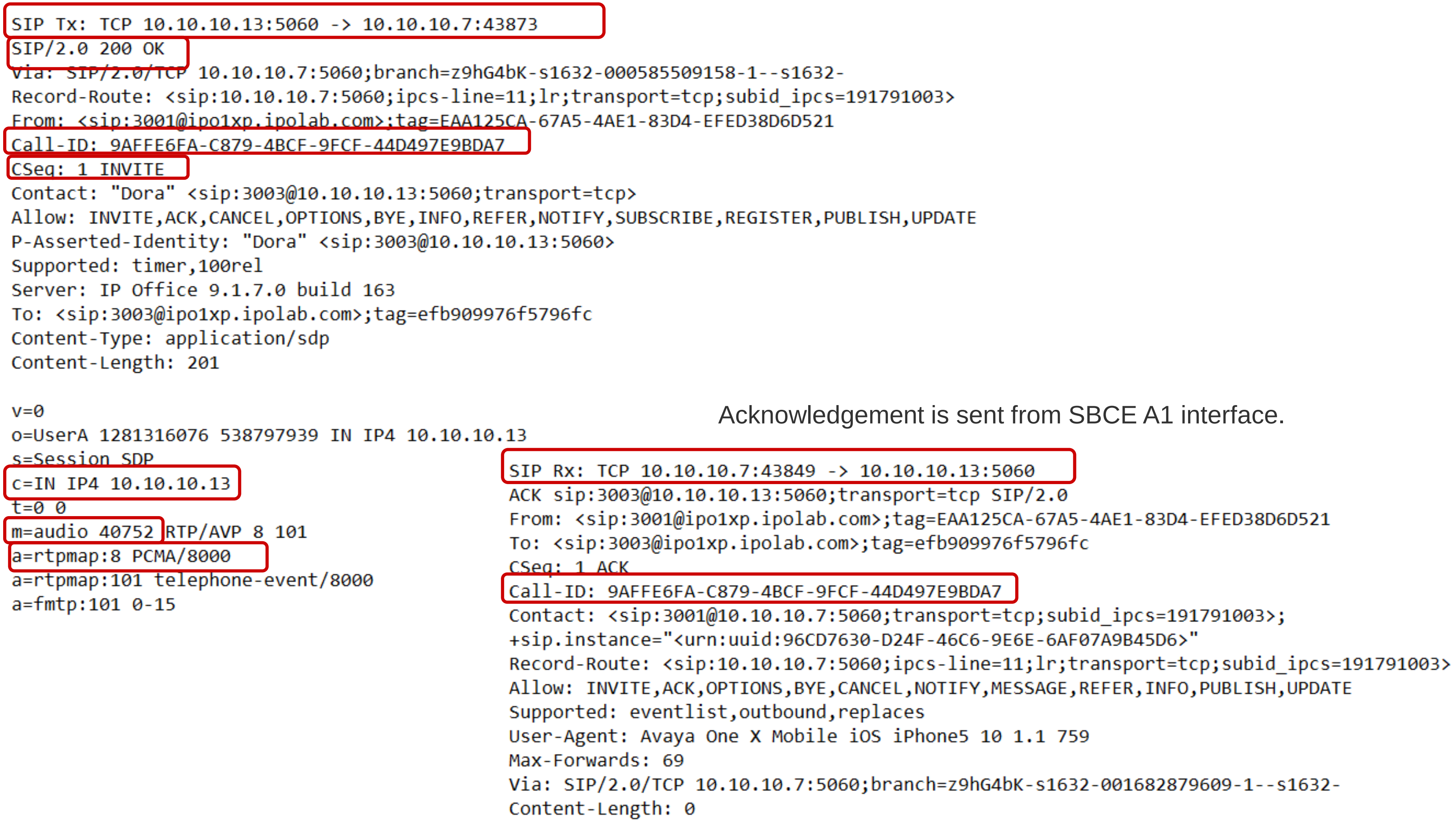


```
SIP Tx: TCP 10.10.10.13:5060 -> 10.10.10.7:43873
SIP/2.0 100 Trying
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-000585509158-1--s1632-
Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
CSeq: 1 INVITE
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
Supported: timer,100rel
Server: IP Office 9.1.7.0 build 163
To: <sip:3003@ipo1xp.ipolab.com>
Content-Length: 0

SIP Tx: TCP 10.10.10.13:5060 -> 10.10.10.7:43873
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-000585509158-1--s1632-
Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
CSeq: 1 INVITE
Contact: "Dora" <sip:3003@10.10.10.13:5060;transport=tcp>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
P-Asserted-Identity: "Dora" <sip:3003@10.10.10.13:5060>
Supported: timer,100rel
Server: IP Office 9.1.7.0 build 163
To: <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

Called party has now answered. Codec negotiated is G711 alaw. RTP port used by IPO is 40752.



```
SIP Tx: TCP 10.10.10.13:5060 -> 10.10.10.7:43873
SIP/2.0 200 OK
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-000585509158-1--s1632-
Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
CSeq: 1 INVITE
Contact: "Dora" <sip:3003@10.10.10.13:5060;transport=tcp>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
P-Asserted-Identity: "Dora" <sip:3003@10.10.10.13:5060>
Supported: timer,100rel
Server: IP Office 9.1.7.0 build 163
To: <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
Content-Type: application/sdp
Content-Length: 201

v=0
o=UserA 1281316076 538797939 IN IP4 10.10.10.13
s=Session SDP
c=IN IP4 10.10.10.13
t=0 0
m=audio 40752 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

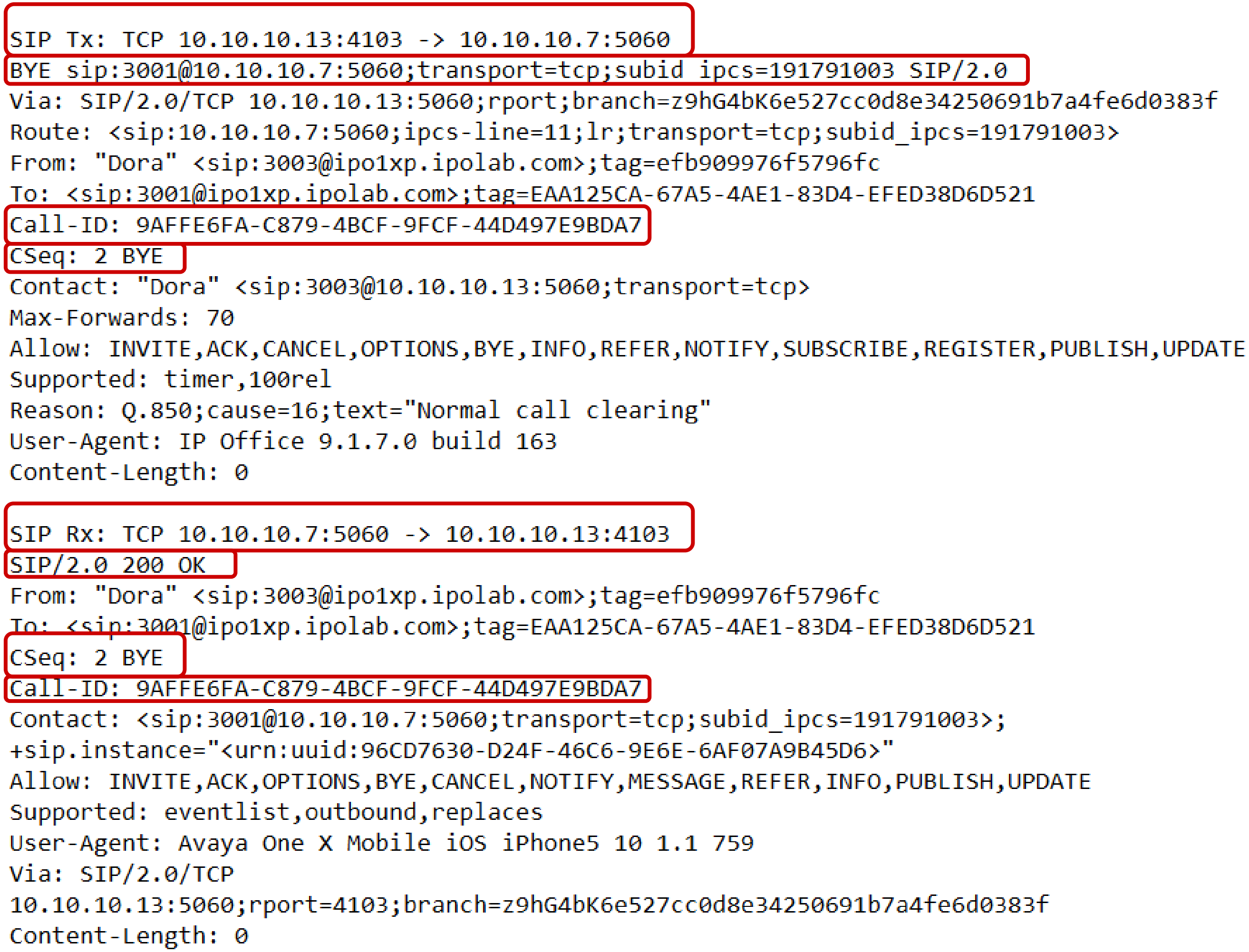
Acknowledgement is sent from SBCE A1 interface.

```
SIP Rx: TCP 10.10.10.7:43849 -> 10.10.10.13:5060
ACK sip:3003@10.10.10.13:5060;transport=tcp SIP/2.0
From: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
To: <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
CSeq: 1 ACK
Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>;
+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>"
Record-Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
Supported: eventlist,outbound,replaces
User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
Max-Forwards: 69
Via: SIP/2.0/TCP 10.10.10.7:5060;branch=z9hG4bK-s1632-001682879609-1--s1632-
Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

❑ One-x Mobile client call to internal extension

Called party dropped the call, IPO sent BYE message to SBCE. SBCE then responded with 200OK.



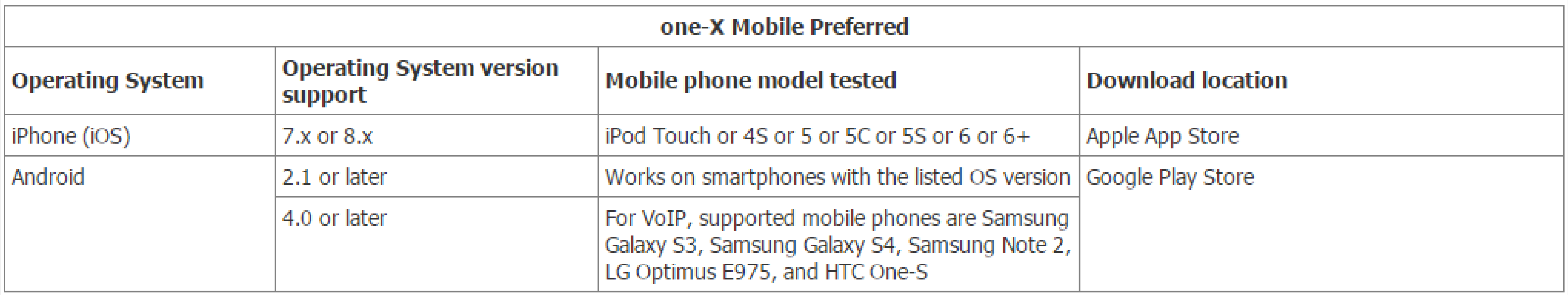
```
SIP Tx: TCP 10.10.10.13:4103 -> 10.10.10.7:5060
BYE sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003 SIP/2.0
Via: SIP/2.0/TCP 10.10.10.13:5060;rport;branch=z9hG4bK6e527cc0d8e34250691b7a4fe6d0383f
Route: <sip:10.10.10.7:5060;ipcs-line=11;lr;transport=tcp;subid_ipcs=191791003>
From: "Dora" <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
To: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
CSeq: 2 BYE
Contact: "Dora" <sip:3003@10.10.10.13:5060;transport=tcp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,REFER,NOTIFY,SUBSCRIBE,REGISTER,PUBLISH,UPDATE
Supported: timer,100rel
Reason: Q.850;cause=16;text="Normal call clearing"
User-Agent: IP Office 9.1.7.0 build 163
Content-Length: 0

SIP Rx: TCP 10.10.10.7:5060 -> 10.10.10.13:4103
SIP/2.0 200 OK
From: "Dora" <sip:3003@ipo1xp.ipolab.com>;tag=efb909976f5796fc
To: <sip:3001@ipo1xp.ipolab.com>;tag=EAA125CA-67A5-4AE1-83D4-EFED38D6D521
CSeq: 2 BYE
Call-ID: 9AFFE6FA-C879-4BCF-9FCF-44D497E9BDA7
Contact: <sip:3001@10.10.10.7:5060;transport=tcp;subid_ipcs=191791003>;
+sip.instance="<urn:uuid:96CD7630-D24F-46C6-9E6E-6AF07A9B45D6>"
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
Supported: eventlist,outbound,replaces
User-Agent: Avaya One X Mobile iOS iPhone5 10 1.1 759
Via: SIP/2.0/TCP
10.10.10.13:5060;rport=4103;branch=z9hG4bK6e527cc0d8e34250691b7a4fe6d0383f
Content-Length: 0
```

Note: In these traces, One-x mobile client was set for Unsecure connection – 5060. In the SBCE Routing Profile, Next Hop Address selected was TCP.

Important Notes

Important Notes

As of release 9.1.x, the following are the supported mobile devices



one-X Mobile Preferred			
Operating System	**Operating System version support**	**Mobile phone model tested**	**Download location**
iPhone (iOS)	7.x or 8.x	iPod Touch or 4S or 5 or 5C or 5S or 6 or 6+	Apple App Store
Android	2.1 or later	Works on smartphones with the listed OS version	Google Play Store
	4.0 or later	For VoIP, supported mobile phones are Samsung Galaxy S3, Samsung Galaxy S4, Samsung Note 2, LG Optimus E975, and HTC One-S	

Ensure the following ports can gain access through the SBCE and Router

❑ Ports 5222 and 8444 must be open for Avaya one-X® Mobile to communicate with the Avaya one-X® Portal server. Port 5222 is for XMPP traffic and Port 8444 is for bootstrap REST API call traffic.

❑ Port 5269 must be open for the Avaya one-X® Portal server to be able to link with another XMPP server outside the company firewall.

❑ Ports 5060 and 5061 for VoIP and the RTP ports.

❑ External/Public DNS as well Internal/Private DNS are required to map FQDN to IP address both in external and internal networks.