

Three Things I Really Like About sipXecs 4.0

By: Tony Graziano

'tgraziano at myitdepartment dot net'

Blog - blog.myitdepartment.net

Date: November 11, 2009

Version: 1.0.2

Ver. History: 1.0

After getting a basic system up and running, there are three things that I really like about sipXecs 4.0. These are things that make it easy to roll out a system to any small/medium business.

These are not the things I'm talking about:

- New voice conferencing solution based on the FreeSWITCH media server. Thanks to Michal Bielicki and Pawel Pierscionek from VoiceWorks and of course the FreeSWITCH team (Anthony Minessale, Michael Jerries and Brian West). Conferencing solution supports HD Voice and offers dynamic Web based conference controls
- sipXecs cluster management now allows creating a fully distributed system that is centrally managed
- Support for 64 bit CPU architectures for both Interl/AMD as well as PPC
- A new integrated reporting solution based on Jasper reports
- Source routing that allows call routing based on where the call originates (i.e. in a branch office)
- Lot's of updated phone and gateway profiles with plug & play management (Linksys, Cisco (thanks to Sen Heng), Grandstream, Aastra, Polycom, Audiocodes, and others)
- Improved operations including certificate management, log and snapshot management, patch and upgrade management, DNS/DHCP configuration assistance, backup/restore to FTP, time and DST management
- Click-to-call from the user portal

Don't get me wrong, they are all great things to add to the project. Below are **my** top three reasons. These are the ones that impact the small businessperson the most when looking at moving into a VoIP system, especially firms that deal with any amount remote staff who generate huge cell phone bills or expense reports that include long-distance costs. These are the three things that I think have the best chance at reducing costs almost immediately and helping to offset the amount of time a system like this pays for itself.

SIP Trunking, Remote Worker Support & Bulk Provisioning of Counterpath Bria Pro

Let's take these one at a time:

1. **SIP Trunking** – No longer do you have to build (or buy) your own separate open source SBC system or proxy to sit between your sipXecs system and your ITSP. Using a compatible firewall,

you can easily spend fifteen minutes and have the system up and running, you can add sip trunking from bandwidth.com and start calling. Realize it takes several days to get an account with bandwidth.com setup, so when you start building your sipXecs system, get service ordered so you'll be ready.

2. Remote Worker Support (far-end and near-end NAT traversal) with support for an optionally redundant media relay for media anchoring. – Most small business won't have a redundant system, meaning two PBX systems running in the even one goes away for one reason or another, so this conversation will take place assuming there is one server. What the Remote worker support function does is allow home based workers, small branch office users, or road warriors with the ability to use either a "hard phone" (regular handset) or "soft phone" (software based handset on the PC or laptop they use) in their location, but use it as though they were in the next room.

3. Bulk provisioning of Counterpath Bria Professional phone – This is a software based phone from Counterpath. This software has a feature that makes setting up a remote user "very painless" for the sipXecs system administrator. When you buy the software, download it and install it, it will ask four questions at first startup.

- a. Username
- b. Password
- c. Provisioning URL
- d. License key

On subsequent startups only A& B are asked. This means your sipXecs administrator can set your account up, give you the necessary information above, and when you login, your phone will be provisioned for you to work on the sipXecs system and you can start making calls right away. It also means if you use another computer with the same software and login to the account, it will be brought to you, like email.

So are you saying "Wow! How do I do all this?" First, I'd recommend installing a system from the ISO installer on the sipXecs download site. Getting the system up and running properly is important before turning on advanced functions like SIP Trunking and Remote workers. So once you've done this, make sure you have the following accomplished:

Your locally connected phones can register, call each other, call the Auto Attendant and deposit and listen to voicemail without any audio issues. This also means your DNS needs to be setup properly. This is perhaps the #1 cause of new user issues, so please understand and grasp this concept first!

Please read the DNS primer:

<http://sipx-wiki.calivia.com/images/0/0b/SipXecsDNSConcepts.pdf>

What you will need:

1. Internet connection with a static IP address.
2. Access to your LAN firewall to “punch through” some ports needed for these new services.

Your firewall "does matter". It needs to support symmetric port nat.

If you have no idea how to do this, I've written a "how-to" that helps you build a firewall from a very basic standalone PC in 30 minutes (VMWare Appliance is available also) with a configuration pre-written for sipxecs, please read this primer and the associated bandwidth shaping wizard I've made available for sipXecs:

<http://blog.myitdepartment.net/?p=37>

3. A bandwidth.com account.
4. At least one copy of Bria Professional (note: xlite or other compatible softphone can be used here)

Before we begin talking about SIP trunking, realize every firewall is not equal. Neither are Internet connections nor ITSP's. The more familiar you are with all of these things will certainly help you achieve a better running system.

So let's start with the Internet connection. First, determine the number of SIP Trunks you will need. Think of a “trunk” as a “line” (I prefer to characterize it as a “call path”). Understand that if you have 15 phone users, you don't need 15 trunks, unless of course your employees are on the phone all the time making or receiving calls from the outside. Remember if the calls your office staff are fielding are from Remote workers, this is not a “call path” with the ITSP, it's an internal call now. So let's take an example of an office with the need for “5” trunks. You need to make sure your Internet connection has the ability to provide enough bandwidth for 5 simultaneous calls. On average 80k of bandwidth need to be reserved per call, in each direction (upload/download), so this means 400k upload (talking/400k download (listening). It's really helpful if your firewall has the ability to prioritize this traffic if you use the Internet for anything else (email, web surfing, etc.), but this is a function of the firewall, which we'll specify later.

Your firewall can be “anything” that supports symmetric NAT (not 1:1 NAT, but symmetric port NAT), since the sipXbridge and Media Relay components (the additional software modules that does all this magic stuff) is able to traverse this more basic type of firewall without using one that is “SIP aware”, which costs much more than your standard firewall. I have a basic "how-to" on setting up and configuring a pfSense firewall (PC Based Linux firewall) already posted at:

<http://blog.myitdepartment.net>.

First, you'll want the firewall to know that it has a static ip address and can get to the Internet. Then you'll want to use the following map to alter what it is allowing both in, and out.

Port Number	Direction	Protocol	Description
5060	Inbound	UDP	Inbound for remote worker signaling. Outbound for call setup and signaling to bandwidth.com.
5060	Inbound	TCP	Inbound for remote worker signaling. Outbound for call setup and signaling to bandwidth.com.
5080	Inbound	UDP	Bandwidth.com needs to be sending inbound calls to your static IP address on this port to avoid conflicts with remote users.
80	Inbound	TCP	This is for the sipXecs User Interface, which redirects to port 8443
8443	Inbound	TCP	This is for the sipXecs User Interface.
12000	Inbound	TCP	This allows the Bria Professional software to auto provision.
30000-31000	Inbound	UDP	These are the ports used by sipXbridge to allow the “audio” portion of the call to go through.

So now that you have allowed your firewall to use the system, a remote user can be setup, even if you don't have a bandwidth.com account yet. So let's enable that basic function from sipXconfig:

System>Servers>(choose yours)>NAT. Choose “Specify IP Address”. This is where you put in the IP address from your ISP, the port number should be 5060. Under Advanced Settings, you will see RTP information Start RTP Port is 30000 and End RTP Port is 31000. Unless that interferes with another service you should leave it at default. Click OK, you will get a message about some services that need to be restarted, so go ahead and do that. It’s also a good idea to go to System>Servers>(Choose yours)>Services and make sure there are no error messages related to this and that everything that is needed has indeed restarted. If there was an error, it would be visually apparent.

Now enable NAT Traversal. System>Internet Calling>NAT Traversal>Enable NAT Traversal. Check the box next to NAT Traversal and click OK. You will again get a message about some services that need to be restarted, so go ahead and do that just like before.

I will not include instructions for a “hard phone” configuration right now, but will provide one later. This will come later. Today we’ll concentrate For now we’ll concentrate on creating the Bria phone in sipxconfig, adding the line, and generating the profile. Once that is done, we’ll go through the first login.

Software phones for sipXconfig also require a MAC address, which you can attribute to the PC network card address, but in reality you can make something up as long as you don’t duplicate another phone on the system. Since software phones are not always local, your DHCP server will not be involved or care. At the same time, it is possible for the remote user to use a regular network card or a wireless card, both of which have different mac addresses. Use your own judgement how you want to do this. In this example we’ll use 000100010001 (remember MAC addresses are 12 characters in length, valid characters are 0-9 and A-F).

So do it: In sipXconfig, go to Devices>Phones>Add new phone>choose Bria Professional. Serial number (the mac address) 000100010001, Description Mel the Road Warrior. Click OK, and then assuming you already created a “line” for Mel, assign it. Go to Devices>Phones>000100010001<choose>. Click LINES, then ADD LINE, and find Mel’s extension (example: 201). Select it and click OK. Now at the Phone devices list, select 000100010001 and click “Send Profile”. This generates the configuration file for the phone Mel has installed on his remote PC. If Mel is a remote worker, we want to do something a little different, by creating a Device Group called "RemoteBriaWorker", choose the Bria Professional and go to the Lines>Network and enable port range 30000-31000. When we create Mel's device, we want to also include this device group to get this special setting for every line we include for Mel’s Bria pro phone used remotely.

Mel needs the four pieces of information:

- a. Username – 201
- b. Password – This is the SIP password shown in advanced settings of the LINE 201 in sipXconfig.
- c. Provisioning URL – This is your sipx hostname (fqdn), see below:
<http://sipx.yourdomain.com:12000/cmcpov/login>
- d. License key – This is sent by email from the Counterpath store.

If you set the port 12000 to be forwarded to your sipx server ip address, and have all your private/public DNS records set properly, this will work. Now Mel can be dialed like any other user, over the Internet and without need a SIP Trunk to bypass the traditional telephone company or even having phone lines hooked up to the sipXecs system at all.

Now the last thing to do is configure our SIP Trunk account. This will involve making several changes, so we'll work through them one at a time. Before we do that, we'll outline the steps here:

Patch It: IF running a version less than 4.0.4, please patch first. The wiki has the latest information on this, so visiting the wiki would be a good idea before performing this step. The wiki has the patch, I've provided the steps here for you as they seem to work for me. Paste this from your ssh session with the server:

```
mkdir /bridgepatch
cd /bridgepatch
wget http://track.sipfoundry.org/secure/attachment/22556/patch20.zip
unzip patch20.zip
cd patch
chmod +x runme.sh
./runme.sh
```

Then go into sipxconfig, pick your server, choose SIP Trunking and Configuration and choose to restart them.

Also, if you are using Polycom phones, please be using Bootrom 4.2 and Firware 3.1.3RevC (nothing later as there are Polycom issues and a new version from them is forthcoming).

Enable Trunking: Enable the role in the Server>Configure>Siptrunking
Turn on "server behind NAT"
Enable SBC, gateway, Dial Plan, Configure Gateway

Configure NAT: In System>Server>(pick your server)>NAT
Address Type: Specify IP Address
Public IP Address: x.x.x.x
Port: 5060

Configure SBC: In Devices>SBC
Choose default SBC the system creates for you.
Public Port: (should be empty)
External Port: 5080 (your ITSP should send calls to this port)
Music on Hold: <checked>

Incoming Calls Destination: Optional. **(If you have DID's going directly to users, this should be blank. If all calls should hit an Operator or AA, please input "operator" here, the default is "operator".)**

If you do not have ALL calls hitting your operator, specify the DID number in your DialPlan>AutoAttendant for call that are supposed to hit the AA. Numbers that route to users directly should be entered as an "alias" in the user account in this format "+1xxxxyyzzzz..

Configure ITSP Account/Gateway: Devices>Gateway>Add new SIP TRUNK

Name it and choose bandwidth.com as the template and choose "sipXbridge-1" as the route in the drop down box at the bottom. Click OK.

Now go to your gateway and define a few extra things. Since we haven't defined a dialplan yet, we just want to make sure the Prefix has a value of "+1", I change this to "+". Now go to the ITSP account and make sure the "default callerid" is used here as the username. It must be in the format of 1xxxxxxxxx, like 12025551212. A password is not needed, and the default settings should work OK. You should ONLY use a number assigned to your organization here. It's not cool to spoof numbers, and some ITSP's charge you international rates for outgoing calls that show a number that is illegal, invalid or does not belong to your organization.

Now it is time to do some work on your dialplans. If you have your bandwidth.com account setup and are sure they are sending calls to port 5080, and your firewall is setup properly, you should be able to receive calls. You might want to test this first before modifying dialplans and placing calls. Make sure you can login to your bandwidth.com portal and CHECK that your test number is provisioned for port 5080.

Now go to your System>Server>(choose yours) and send all profiles, restarting any services that are prompted to restart.

Configure DialPlans: Dial Plans in sipx are a "filter" and the first rule matched on a dialed number uses the appropriate permissions and gateway(s). I prefer to leave the default dial plans in place and disabled. Since I also use Polycom phones, and the missed calls/received calls have the "+1" character already in them, I do a simple thing to make sure the dial plan removes this before sending the call out. I also prefer to make it easy so local (7 digit) calls are automatically adding the area code so the caller doesn't have to dial the area code.

custom_local (required permissions, local dialing)

Dialed Number

Prefix (blank) and (7 digits)

Resulting Call

Dial +xxx (xxx is your local area code) and append "Matched Suffix"

Gateway (choose your new bandwidth.com gateway)

return_call (required permissions, long distance)

Dialed Number

Prefix (+) and (11 digits)

Resulting Call

Dial (blank) and append "Matched Suffix"

Gateway (choose your new bandwidth.com gateway)

custom_ld (required permissions, long distance)

Dialed Number

Prefix (blank) and (10 digits)

Resulting Call

Dial 1 and append "Matched Suffix"

Gateway (choose your new bandwidth.com gateway)

(Optional, if needed)custom_international (required permissions, long distance)

Dialed Number

Prefix (011) and (any number of digits)

Resulting Call

Dial (blank) and append "Matched Suffix"

Gateway (choose your new bandwidth.com gateway)

Now, here is the important part, ordering the dial plan rules.

From top to bottom, arrange them so "EMERGENCY" is at the top. Then only the following rules should be enabled.

Emergency

custom_local

return_call

custom_ld

(OPTIONAL) custom_international

AutoAttendant

Voicemail

The default or other rules can be in here and disabled.

This is "just" the way I do it so I can revert to an analog or other gateway as needed and pick from different rules.

I also prefer to change the "+1" to a "+" at the gateway because when I have a customer who needs full international calling, stripping the "011" from the call makes the call look like any other and even local calls can match international rules, so people might not be able to make local calls if they don't have international permissions. Also note, toll free calls match the normal dial plans here so there is no need for another enabled rule. The nice thing about dialplans is that you can have another analog gateway (fxo, pri, etc.) to handle just "local" or "toll free" calls or

whatever makes the best business sense for your location. You would alter this in the bandth.com gateway setting at the top.

Now restart any services prompted for to "activate" the dial plan changes.

This dialplan works for me, but there are certainly ways to simplify it. I intentionally don't address "911" here. Emergency rules should be enabled on every phone system, and testing should be done to make sure that dialing 911 works and that the proper address comes up for the dispatcher.

First you need to determine how you are going to dial 911. Using an ITSP trunk OR via a locally connected circuit or line. If you dial through your ITSP trunk, you will most likely get the national 911 center. If you are using a locally connected line or circuit, you will get the local PSAP. The FCC has a PSAP Registry. Here is their link to it:

<http://www.fcc.gov/pshs/docs/services/911-services/MasterPSAPRegistryV2.xls>

It's always a good idea to call the local PSAP by dialing 911, the first words you utter should be "I don't have an emergency, we are installing a new phone system and want to confirm the address you have for this number." The PSAP operator will be able to read it back to you if your callerid is configured properly, since the number is linked to the address.