From Technologies to Solutions

Building Enterprise Ready Telephony Systems with sipXecs 4.0

Leveraging open source VOIP for a rock-solid communications system

Michael W. Picher

PACKT PUBLISHING

Building Enterprise-Ready Telephony Systems with sipXecs 4.0

Leveraging open source VoIP for a rock-solid communications system

Michael W. Picher

BIRMINGHAM - MUMBAI

Building Enterprise-Ready Telephony Systems with sipXecs 4.0

First published: June 2009

Production Reference: 1170709

Published by Packt Publishing Ltd.
32 Lincoln Road
Olton
Birmingham, B27 6PA, UK.

ISBN 978-1-847196-80-4

`www.packtpub.com`

Cover Image by Parag Kadam (`paragvkadam@gmail.com`)

Credits

Author
Michael W. Picher

Reviewer
Anthony Graziano
Scott Lawrence

Acquisition Editor
Sarah Cullington

Development Editor
Dilip Venkatesh

Technical Editor
Aditi Srivastava

Indexer
Hemangini Bari

Editorial Team Leader
Abhijeet Deobhakta

Project Team Leader
Priya Mukherji

Project Coordinator
Lata Basantani
Zainab Bagasrawala

Proofreader
Chris Smith

Production Coordinator
Dolly Dasilva

Cover Work
Dolly Dasilva

About the Author

Michael W. Picher is an industry veteran with over 20 years of experience in Information Technology consulting. Michael brings a network engineer's perspective to the Telephony business. After receiving a Bachelor of Science degree in Computer Engineering from the University of Maine, Michael worked hard to build up a computer manufacturing business, which he left in the mid-90s. Following the manufacturing endeavor, Michael worked with two close friends to build what became one of Maine's largest home-grown technology consulting and software development firms. After successfully selling the consulting business to a large out-of-state firm, Michael turned his attention to the growing IP Telephony space. Michael has helped successfully deploy some of the region's largest IP-based communications systems and the infrastructure required to support those systems.

Away from technology, Michael enjoys life with his wife Debra and son Matthew on their large, wild blueberry farm in rural Maine. Snowmobiling and hunting are the family choices for fun, and Michael is also a longtime Autocross fanatic with multiple class wins in his beloved Mini Cooper S.

I'd like to thank my wife Debra for her support while writing this book, my son Matthew for bringing joy to our lives, and my parents who have always been there to keep me pointed in the right direction. I'd also like to thank Tony Graziano and Scott Lawrence, for their contributions and technical review, and the sipXecs development team and community without whom we wouldn't have this wonderful product. A thank you is also due to the team at Packt Publishing for keeping things moving forward and helping to create an excellent final product.

About the Reviewer

Anthony Graziano has spent the last 25 years working in Information Technology and telecommunications. Recruited by a national carrier from his position at a multistate financial services firm concentrating on IBM mainframes and communications, he worked as a data specialist for one of the largest US facilities-based carriers. After deciding to focus on microcomputing technology, he worked for a Virginia-based consulting and services firm, which he helped to grow before it was purchased by a national firm.

Today he operates a CLEC in Virginia (Cavalier Broadband) with a dedicated focus on data services. His growing consulting practice, myITdepartment, helps commercial clients to identify emerging technologies such as VoIP and SaaS, so they can more easily adapt to changing business trends.

He lives in Charlottesville, Virginia, with his wife Lisa and their three daughters. He enjoys saltwater fishing, especially on the Northern Neck of the Cheaspeake Bay, with friends and family as often as he can.

Table of Contents

Preface

Open source telephony systems are making big waves in the communications industry. Moving your organization from a lab environment to production system can seem like a daunting and inherently risky proposition. *Building Enterprise Ready Telephony Systems with sipXecs* delivers proven techniques for deploying reliable and robust communications systems.

Building Enterprise Ready Telephony Systems with sipXecs provides a guiding hand in planning, building, and migrating a corporate communications system to the open source sipXecs SIP PBX platform. Following this step-by-step guide makes normally complex tasks, such as migrating your existing communication system to VoIP and deploying phones, easy. Imagine how good you'll feel when you have a complete, enterprise-ready telephony system at work in your business.

Planning a communications system for any size of network can seem an overwhelmingly complicated task. Deploying a robust and reliable communications system may seem even harder. This book will start by helping you understand the nuts and bolts of a Voice over IP Telephony system. The base knowledge gained is then built upon with system design and product selection. Soon you will be able to implement, utilize, and maintain a communication system with sipXecs. Many screenshots and diagrams help to illustrate and make simple what can otherwise be a complex undertaking. It's easy to build an enterprise-ready telephony system when you follow this helpful, straightforward guide.

What this book covers

Chapter 1 introduces some important telephony concepts to establish some necessary background information and an overview of sipX **Enterprise Communications Server** (sipXecs), its features, and its functionality.

Chapter 2 covers data collection about the existing systems, equipment selection, and the planning for phone system programming.

Chapter 3 covers steps involved in completing the cabling requirements, network infrastructure requirements, and installing sipXecs. In this chapter we learn to install the base PBX operating system and software. We also learn some important testing steps for verifying DNS and DHCP functionalities.

Chapter 4 covers creating and managing user accounts, managing the extension pool, utilizing user groups, and importing users. We also explore how to use phantom users for voicemail-only mailboxes and for some advanced call routing needs.

Chapter 5 covers the typical day-to-day functions that a communications systems manager needs to perform. The reader gets a good basic knowledge of adding users and phones to the system in this chapter.

Chapter 6 covers adding managed and unmanaged gateways, setting up the Session Border Controller, and working with Dial Plans.

Chapter 7 covers the configuration of sipXces server features. sipXecs has several server-side features that provide additional functionality. These functionalities are not otherwise available in the phones themselves. Many of the basic features will be covered in this chapter while some of the more advanced features will be described in Chapter 9.

Chapter 8 covers all of the information needed as an administrator to help the users acclimatize to their new communications system.

Chapter 9 explores the built-in conference services provided by sipXecs and then explores some more advanced sipXecs call routing features. It also covers some call routing tricks that will find use with the sipXecs installation.

Chapter 10 covers the configuration of ACD services. It also covers how to enable and monitor their operation.

Chapter 11 explores various system maintenance tasks and steps that can be taken to keep the phone system secure.

A glossary is also included at the end of the book. This appendix includes all the important words and terms used throughout the book.

What you need for this book

sipXecs can be installed from a single CD installer. The recommended system should have the following components:

- Two or four (or dual/quad-core) processors operating at 1.8 GHz or better
- 2 gigabytes of system memory (RAM)
- 32 gigabytes or larger SCSI hard drive
- Single Ethernet adapter (100 Mbps or 1000 Mbps)

Who this book is for

This book is written for network engineers who have been asked to deploy and maintain communications systems for their organizations.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text are shown as follows: "The `nslookup` tests are combined."

A block of code is set as follows:

```
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 27 07:00:37 2008
;; MSG SIZE  rcvd: 103
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
> set q=srv
> _sip._tcp.xyzcompany.com
Server:  sipx.xyzcompany.com
Address:  172.16.1.2
```

Any command-line input or output is written as follows:

```
nslookup
 >set q=srv
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Under **Quick Links** on the right side of the page is an **Add Line** hyperlink."

> Warnings or important notes appear in a box like this.

> Tips and tricks appear like this.

Reader feedback

Feedback from our readers is always welcome. Let us know what you think about this book—what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an email to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a book that you need and would like to see us publish, please send us a note in the **SUGGEST A TITLE** form on `www.packtpub.com` or email `suggest@packtpub.com`.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book on it, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration, and help us to improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/support`, selecting your book, clicking on the **let us know** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata added to any list of existing errata. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or web site name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

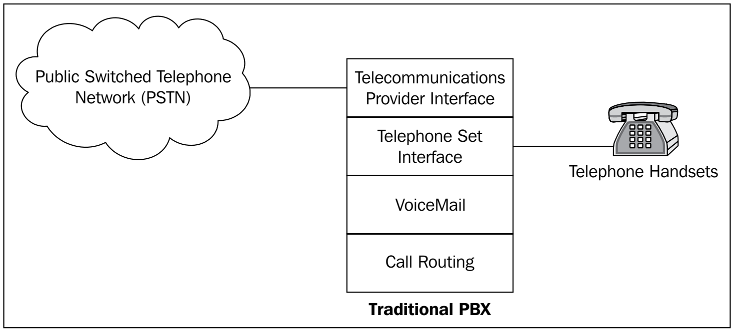
1

Introduction to Telephony Concepts and sipXecs

In this chapter we'll introduce some important telephony concepts to establish some necessary background information. Then we'll move on to an overview of sipX **Enterprise Communications Server** (sipXecs), its features, and its functionality.

Traditional phone system concepts

There are two types of traditional phone systems, PBXs and Key Systems. A **Private Branch Exchange** (**PBX**) is typically found in larger organizations. Key telephone systems that allow users to directly select outside lines via keys on the handsets were designed with smaller organizations in mind. Both types of systems typically consist of interfaces to a telecommunications provider, interfaces to telephone handsets, a voicemail system for auto attendant and leaving messages, and call-routing logic.



The traditional PBX is usually thought of as being housed in a cabinet with various interfaces and logic boards inserted as cards into a backplane across which all of the cards can communicate. These backplanes are vendor specific, so you are typically locked in to purchase all cards and phones from a single vendor. Additionally, many first-generation IP-based phone systems may also be thought of as traditional systems. These early IP systems use proprietary signaling over IP or protocols that have fallen out of favor (MGCP/H.323).

The PBX communicates with the outside world from the interface to a telecommunications provider. In a traditional PBX, this interface is typically some sort of analog circuit (loop-start or ground-start) or digital circuit (E1/T1, ISDN, or **Primary Rate Interface** [**PRI**]).

The telephone set interface is how the PBX connects with the various user devices that it is in direct control of. This is traditionally an analog interface to a limited-feature phone (like a typical home telephone) or a digital interface to a more feature-rich phone.

Voicemail systems in the traditional PBX are designed to handle recording and playback of messages to users of the system, notifying the users they have messages via a **Message Waiting Indicator** (**MWI**), and also automated attendant duties. The automated attendant's function is to answer inbound phone calls, play a message, and wait for a caller to enter an option or extension.

The call-routing logic in a phone system determines where calls route to, based on a number that was dialed (be that an extension on the system or an external phone number). Other factors may also come in to play with call routing such as permissions, time of day, what line a call came from, and so on.

Telecommunications provider interface

The interface to a traditional telecommunications provider (a phone company) can take different forms depending on how your calls are being delivered. If your calls are being delivered by a traditional provider over E1, T1, PRI, BRI, or analog line, this interface device is a hardware-based gateway.

E1s, T1s, and PRIs are all digital circuits that can carry multiple conversations. E1 is a physical layer protocol, much like Ethernet, that defines a 2Mbps pipe. This pipe can be used for data—split into 32 64Kbps communications channels—or a mixture. If the pipe is used for communications channels, 30 of the channels can carry telephone conversations and the remaining 2 carry signaling and timing information.

A T1 is similar to an E1, and it is common in North America. T1s are 1.544Mbps pipes that can carry 24 telephone channels. There are no signaling channels on a T1. Also, like an E1, T1s can be channelized and utilized to deliver voice and data.

E1 and T1 circuits have some problems associated with them. They are limited in what information they can carry and the circuits are relatively slow to set up. ISDN signaling is a more modern protocol that was designed to overcome these problems. On E1s, EuroISDN signaling is standard. On T1s, different providers utilize different standards. NI1, NI2, DMS100, and DMS250 are all examples of ISDN signaling protocols, each delivering different levels of functionality.

A **PRI** (**Primary Rate ISDN**) is an E1 or T1 with ISDN signaling running on top of it. ISDN signaling provides reliable call setup and tear-down detection, as well as detailed information about each call. In the UK, a PRI is also referred to as ISDN30. Voice channels on a PRI are referred to as B channels and the signaling channels are referred to as D channels. On an E1, a PRI will provide 30 B channels of voice and utilize one of the signaling channels as the D channel. Since T1s have no signaling channels, a PRI on a T1 will utilize one of the channels as a D channel and have 23 B channels for voice.

As a cheaper alternative to PRI, **BRI** (**Basic Rate ISDN**) may be offered in some areas. A BRI has 2 64Kbps B channels and a single 16Kbps D channel for signaling. In the UK, a BRI may also be called ISDN2e.

Analog lines from local telephone companies come in a couple of different flavors, both delivered over a pair of copper wires. They will be referred to as **Ground Start Trunks** (**GST**) or loop start circuits. Ground start circuits provide disconnect notification by actually grounding the circuit (when a caller hangs up the phone), which is also called answer and disconnect supervision. Loop start analog circuits are the more typical home and key system phone lines. Loop start lines use either a polarity reversal (called battery reversal), or removal of the line voltage (battery drop) for answer and disconnect supervision.

Telephones on a traditional phone system

Telephone sets on a traditional phone system will interface to the system by using one of the one of three methods: analog, digital, or via IP.

Analog phones are usually the same sort of phones you might find in a residence. They can provide signaling to the PBX for special functionality by flashing the hook switch and utilizing different **DTMF** codes. **Dial Tone Multi Frequency** is the sounds you hear when you push the dial pad buttons of a phone. Analog phones need to be manually configured as there is no means for passing codes down to phones and programming any special keys that may be on the phones.

Digital phone sets provide higher functionality and programmability for phone systems. They are proprietary to each vendor and type of phone system. Digital sets can be programmed centrally. They provide excellent call quality and usually have many buttons that can be programmed to provide different functionality to the user. The majority of phones shipped with phone systems were digital until 2005/2006 when IP phone sets surpassed them in total numbers shipped.

Many traditional phone systems vendors have seen the advantages of an IP-based system and have adapted their phone systems to support IP-based phones. A traditional phone system that has been adapted to support a mix of phones is referred to as a hybrid system. What we'll refer to as first-generation IP-based phone systems utilize a proprietary protocol for communications, or one of the older voice standards. Examples of proprietary protocols are SCCP (Cisco), UNIStim (Nortel), and MiNet (Mitel). As with digital phones, proprietary protocols require vendor-specific phones. **Session Initiated Protocol** (**SIP**), H.323, and MGCP are examples of standards-based protocols. Phones that conform to standards are designed to work on many different phone systems.

Voicemail systems

Voicemail systems are an important part of any business phone system. These systems provide auto attendant functions, and the playing and recording of messages. The voicemail system can be thought of as the voice of the phone system.

When calling into a phone system, the caller will hear the main auto attendant, which provides the caller with a menu of choices. The auto attendant plays a recorded message and waits for the caller to enter DTMF tones selecting a menu option or dialing an extension. Newer advanced auto attendant systems have grown to include voice recognition for menu items or extension selection.

The voicemail system also handles the recording and playback of user greetings and voicemail messages. Many modern voicemail systems allow multiple greetings to be selected by the user for out-of-office or extended-leave situations so that the user doesn't need to keep re-recording his or her notifications.

Unified messaging systems are an extension of voicemail systems that allow users to have a single inbox combining voicemail, email, and faxes. A true unified system will integrate these systems at the server level such that when you open or delete voicemail on a computer, it is marked as read or deleted in the voicemail system. A simple version of unified communications involves SMTP forwarding of voicemail to an email, or requires a setup of client software that handles email integration on the user's computer.

Traditional voicemail systems are usually sold to customers with support for a certain number of ports. The ports control how many simultaneous voice sessions can occur between the phone system and the voicemail system. The system may be contained on a card in the system or on a separate server outside the phone system cabinet.

An important but seemingly simple responsibility of the voicemail system is to signify to users that they have messages waiting. This notification usually takes the form of a **Message Waiting Indicator** (**MWI**) light that is lit on handsets.

Call routing logic

The "brains of the operation" in the traditional phone system is the call routing logic. The routing logic is called different things by different vendors, but may be referred to as the call controller or call manager. Its job is to evaluate calls and direct them (referred to as switching) to where they need to go based on many different factors. These factors include, but are not limited to, what number was dialed, who dialed it, and what time of day it is.

Calling functions and features

There are hundreds of call routing functions and phone system features that have been developed over the years. The following are some of the more common call functions and features.

Call hold

With call hold, the user presses a button on his or her phone that places a caller into a mode such that neither party can hear each other. Often, music or an announcement is played while the party is on hold (**Music on Hold**, or **MoH**). In small key systems, users on other phones can pick up on a line that has been placed on hold. With PBXs, the call is usually retrieved on the same phone that the call was put on hold with.

Call park orbits

Call park orbits were designed for PBX systems where the concepts of phone lines to users don't exist. Putting a call into a park orbit is accomplished by transferring a call to a holding queue (orbit). That call can be retrieved on any phone by dialing a retrieval (also referred to as a pickup) code and the park orbit number.

Call pickup

Call pickup is the ability of one user to pick up another user's ringing phone. Often, permissions are required to do this function. This feature is typically accomplished by dialing a pickup code and the extension of the ringing phone.

Call transfer

Call transfer is the ability of a user to send a phone call to another extension on the phone system. There are two types of transfer: consultative and blind. In a consultative (also referred to as attended or supervised) transfer, the calling party confers with the party that it will transfer the call to before the call is transferred. In a blind (also referred to as unattended) transfer, the call is simply transferred to the selected extension.

Call forwarding

Call forwarding is a service that allows a user (or the phone system) to have a call redirected to another extension or number. The forwarding decision can be a strict choice to always forward, or it could be based on certain criteria such as whether the called party is busy, who is calling, time of day, and so on. Time of day forwarding is also referred to as "Time-based Follow-me/Find-me".

Speed dial

Speed dials in a traditional PBX are phone numbers that can be dialed in order to dial a more complicated number. For example, a user would dial 752 and the phone system would actually dial 18005555555. Most systems allow user-specified as well as system-wide speed dials.

Direct Station Selection/Busy Lamp Field

Direct Station Selection (**DSS**) can be thought of as a one-touch speed dial assigned to a key on a user's telephone. The user presses the button and the number assigned to the button is automatically dialed. When combined with information about an extension on the receiving end of the DSS, the feature is referred to as a **Busy Lamp Field** (**BLF**, DSS/BLF or Presence). If the remote party is on the phone, a BLF will usually have a solid light on or near the button. If the remote party's phone is in a "Do Not Disturb" mode, (the phone rejects all calls) the light may blink.

Hunt groups

A hunt group is a collection of extensions that ring in a particular order when the hunt group number is dialed. The hunt group number is often referred to as the pilot number of the hunt group. Linear hunt groups always start ringing the first extension in the list and end ringing the last extension in the list. With a circular hunt group, the phone system remembers the last number that answered ringing and begins ringing on the next number in the list and when the end of the list is reached, it wraps around to the first number in the list again.

Automatic Call Distribution

Automatic Call Distribution (**ACD**) can be thought of as intelligent hunt groups. They allow phone system users (agents) to sign in and out of calling queues. Calls then ring agents based on different factors such as who is the first person in the ACD list, or which agent has been idle the longest. The ACD systems also allow other niceties such as wrap up time for agents after a call is completed.

Dial plans

The system dial plans provide the routing logic for inbound calls and outbound calls from the system. The dial plans evaluate the dialed numbers by looking for patterns of digits and directing calls to different destinations. It is up to the phone system designer to set up their dial plans based on their phone providers and the phone numbers they know their users will need to dial.

Intercom

The intercom function in a phone system allows a single user to dial another user's extension, makes the receiving user's phone automatically go "off-hook" in speaker phone mode, and allows the two parties to converse.

Paging

Paging is similar to intercom functionality, but it differs in one way. It is designed to allow a single user to broadcast a message to a group of other phones without the ability of the receiving phones to talk back to the caller.

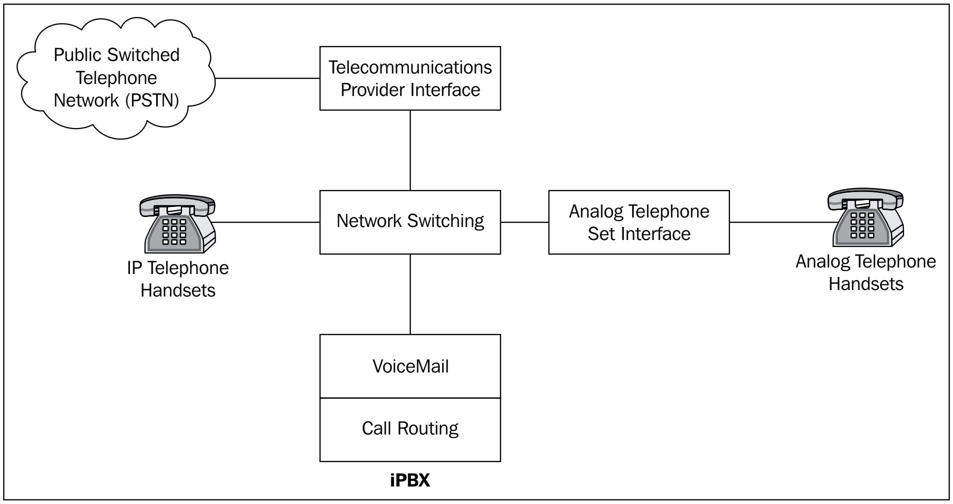
Conferencing

A conference is a call between three or more parties. A conference may be a simple phone-based multi-party conversation, or may be hosted by a full-featured conference server. A simple phone-based conference requires a phone user to call multiple parties and establish the conference call. A conference server allows more parties, achieves finer-grained control by a conference moderator, and allows participants to come and go as they choose. A conference server will host many "rooms" where participants can meet. These conference rooms are often referred to as "Meet-Me" conferences.

sipX Enterprise Communications System overview

sipX Enterprise Communications System (sipXecs) is a highly scalable, enterprise-grade communications solution. It is a product of the independent, not for-profit, open source organization known as SIPFoundry. Leveraging standards and built in an open source environment, sipXecs offers dramatic cost savings, ease of use, and a degree of interoperability, functionality, and scalability that is not found in other systems.

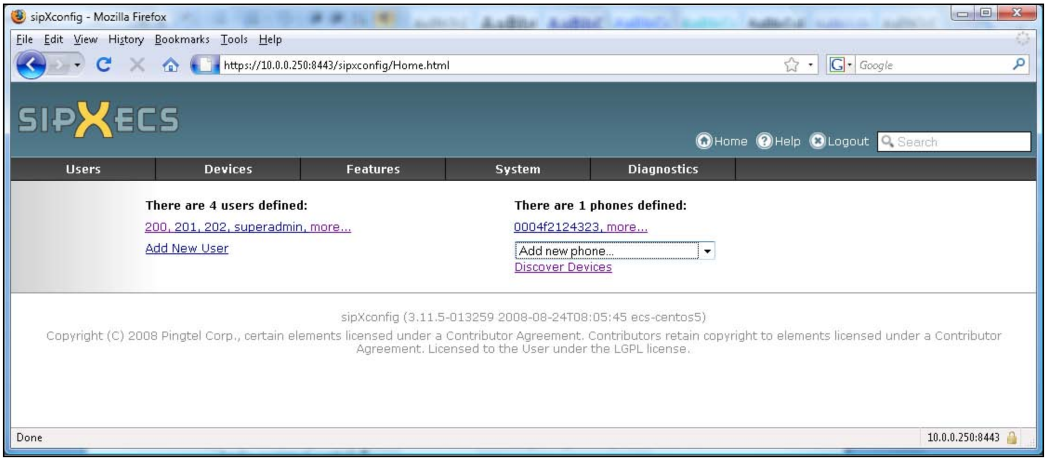
It is without surprise that the sipXecs features mimic much of the well-defined functionality of a traditional phone system that users expect. The usual phone system cabinet is gone, and components of the system are separated and held together by network switching equipment.



The iPBX

The core of the phone system has always been the PBX and this is no different with sipXecs. The traditional PBX is now referred to as an iPBX or a Softswitch. This name is derived from the fact that the PBX functionality is accomplished in software running on a standard server. Since the software can run on a standard type of server, this computer can be as reliable as a customer demands and as fast as required for the number of users the system will support.

Ease of use and installation have been a fundamental founding principal of the sipXecs project. System administration and configuration is done using a web interface provided by a system service called the *configuration server*. The configuration server is a core component of the system, which ensures that data consistency is always maintained across all elements of the iPBX.



Technically, at the heart of the sipXecs iPBX is a **Session Initiated Protocol** (**SIP**) proxy. SIP is an **Internet Engineering Task Force** (**IETF**) standard protocol user for conducting interactive communications. SIP can be utilized for many forms of communications sessions, including voice, video, and chat. The SIP call signaling is independent from the media sessions it controls.

The sipXecs proxy can be thought of as a call router. Its job is to direct SIP calls through the system. The proxy itself does not handle any voice traffic (media). This is one of the reasons why sipXecs systems are so scalable as opposed to other IP phone systems that must process voice traffic within the iPBX.

The iPBX, as a whole, is a collection of 14 separate services running on a single or multiple Linux-based servers. These services are: sipxsupervisor, freeswitch, sipregistrar, sipstatus, sipxacd, sipxbridge, sipxcallresolver, sipxconfig-agent, sipxconfig, sipxivr, sipxpage, sipxpark, sipxpresence, sipXproxy, sipxrelay, sipxrls, and sipXvxml. These services interoperate to deliver all of the system functionality.

Gateways

The gateway provides communications system connectivity to the telecommunications providers. A gateway may be a physical device connecting a traditional type of phone circuit, as discussed earlier, or a software-based gateway providing connectivity to **Internet Telephony Service Providers** (**ITSP**). The quality of the gateway and the type of connectivity will determine the quality of the audio conversation with phones outside the phone system.

Telephones

One of the great advantages of a communications platform built on open standards is the incredible flexibility and the breadth of user peripherals available to customers. Hard phones (standard desk phones), softphones (software-based phones that run on desktop, laptop, or handheld computers), WiFi phones (run over a company's wireless network), SIP DECT phones (run over a DECT wireless network), and interfaces to traditional analog and digital phones are all available.

sipXecs features

sipXecs provides the features that businesses have grown to expect from their communications systems along with some additional functionality that's not possible in traditional PBXs. The feature list is constantly being refined and expanded as developers in the open source community keep adding new functionality.

Voicemail

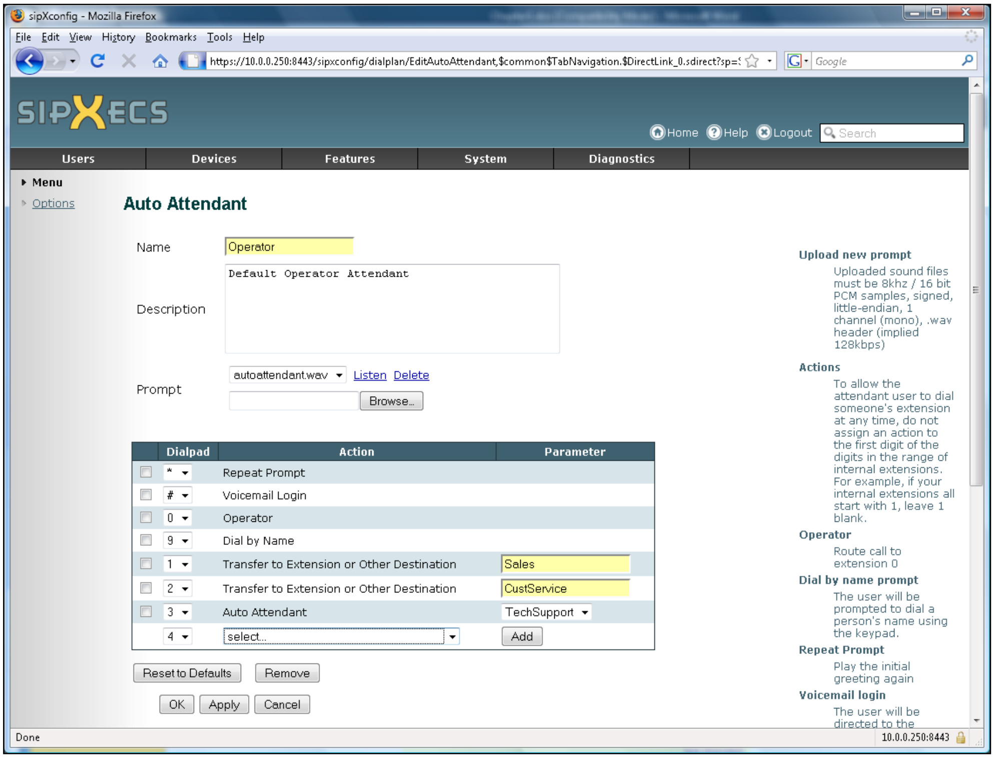
sipXecs includes a simple yet complete voicemail system. Users can access voicemail through their phone, via a web browser, or receive their voicemail as email. Voicemail to email is a simple unified communications type with a twist. Included as part of the email are hyperlinks that allow the user to erase his or her voicemail from the voicemail server.

For the number of minutes of voicemail, administrators are only limited by the capacity of the storage in their servers. Additionally, there is no hard set limit for how many voice paths (ports) can be active to the voicemail server at one time. System speed is the only limiting factor.

sipXecs can optionally integrate with a Microsoft Exchange 2007 Unified Messaging Server for a fully unified messaging experience. The system administrator can also mix and match with some users on the internal voicemail system and some on Exchange.

Auto Attendant

The multilevel **Auto Attendant** service provides system-wide answering of incoming calls, dial by name abilities, automated transfer to local extensions, access to remote voicemail retrieval, and transfer to other auto attendants. The following screenshot shows the sipXconfig interface for modifying system **Auto Attendants**:



The number of auto attendants is limited only by the administrator's creativity and the callers' patience.

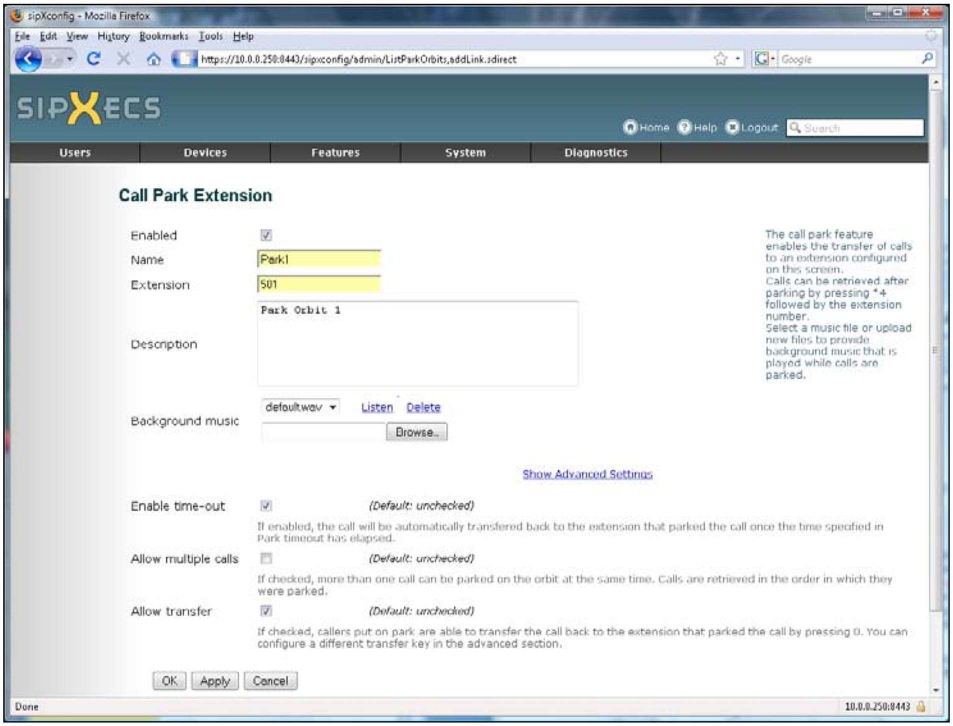
Music on Hold

There are multiple methods of supporting **Music on Hold** (**MoH**) on SIP-based phone systems. For SIP phones that can use it, sipXecs supports a standard as defined in an IETF draft written by Dale R. Worley of Nortel (`http://svn.resiprocate.org/rep/ietf-drafts/worley/draft-worley-service-example-01.html`). This standard is dependent on the phone to transfer the call to a service that is playing the MoH, and then recall the caller when the caller is taken off hold. Presently, this method is known to be supported by Nortel, Polycom, and Snom phones.

For calls from an ITSP, the sipXbridge service can provide MoH, which allows any phone to have MoH capabilities without having to support the IETF draft.

Call park orbits

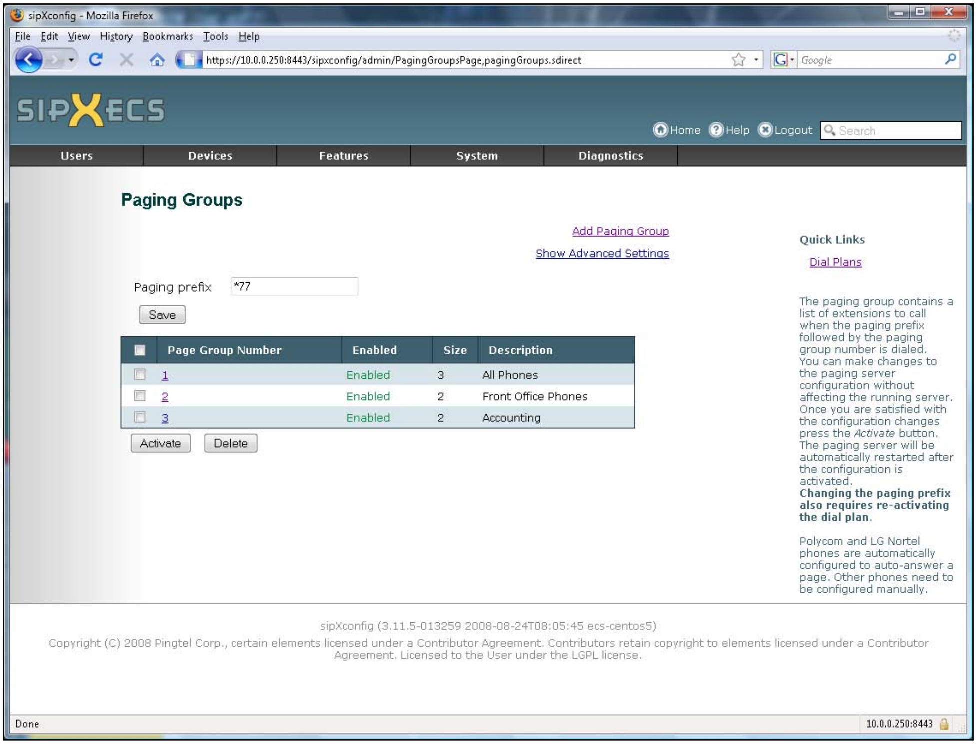
The sipXpark service allows users to park an active call to a park extension, and then later pick up that call from any phone by dialing a retrieve code and the park extension. While the call is parked, the caller will hear call park audio, which can be uploaded by the administrator. This following screenshot shows a typical **Call Park Extension** and its basic configuration elements:



Park orbits can be configured to allow single or multiple callers to be parked. If multiple callers are parked, they are retrieved in a first-in first-out (FIFO) order. An unlimited number of park orbits can be created.

Page groups

The sipXecs paging service (sipxpage) allows the system administrator to define multiple paging groups of phones to contact for paging. When a user dials the paging code followed by the paging group number, all the phones in the paging group go off-hook on speaker phone, a tone (which can be uploaded) is played, and then the user may broadcast their message. The following **Paging Groups** configuration screen allows the administrator to configure the paging dial prefix and define a group of phones that will go off-hook to play the pages:



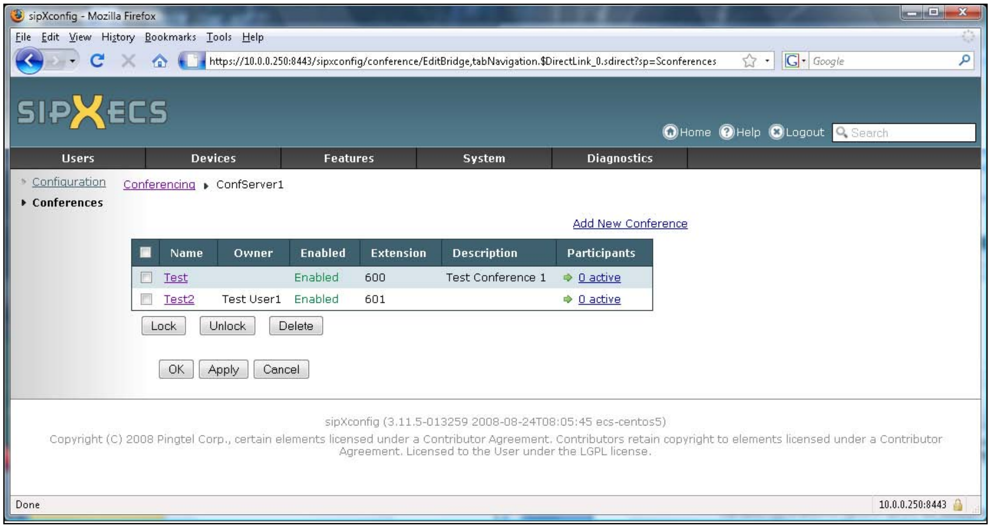
At present, Polycom and LG Nortel phones will be automatically configured to support paging when added to a paging group. Other phones may be configured manually.

Intercom

The intercom feature of sipXecs allows the administrator to configure phones to automatically answer calls. A user dials a feature code and extension, the receiving phone goes off-hook on speaker phone, and the two users can have a conversation. Polycom, LG Nortel, and Snom phones can be automatically configured to support this feature.

Conference server

The conferencing service allows Meet-Me voice conferencing capabilities. Administrators can create as many conferences as they would like with the ability to have separate conferencing servers if the conference demand is high. Conference controls are also integrated into the user portal so that every user can have a personal conference bridge that can be easily administered. The following sipXconfig screenshot shows the system administrator all of the conferences defined in the system, who owns them, and how many participants are in each:

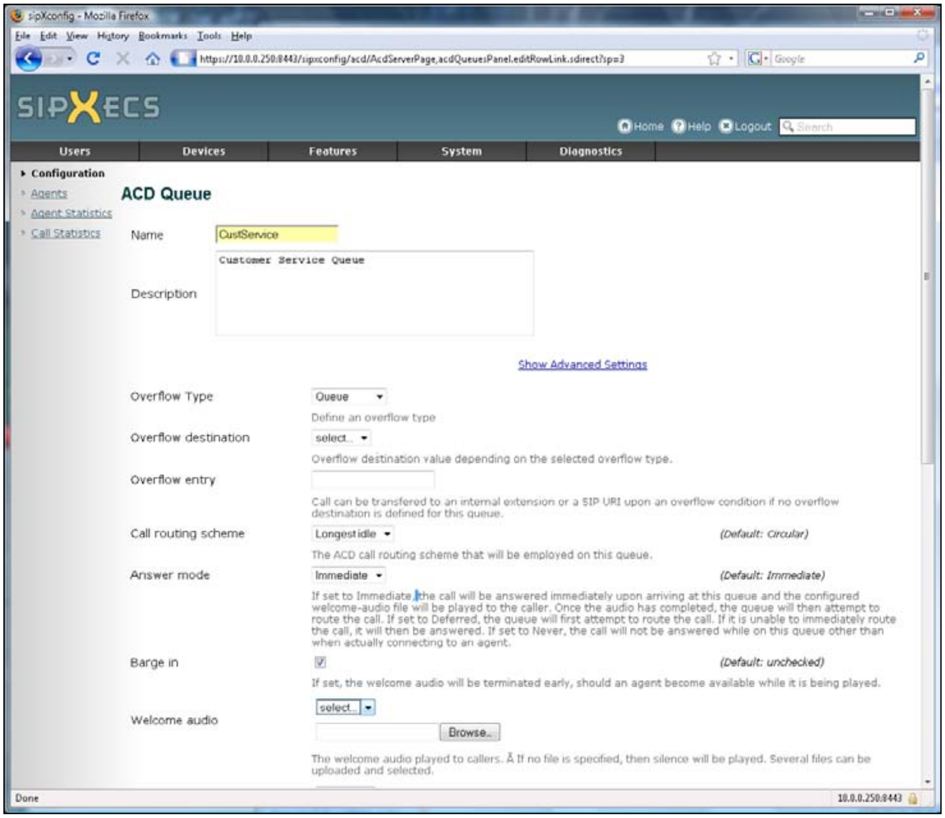


Automatic call distribution

The sipXecs call center solution (sipxacd) integrates into the configuration server where call center lines, queues, agent behavior, and features are configured. The configuration server also provides real-time statistics about call volume and agent activities.

Like other services, the sipxacd service can be configured to run on the same host as the rest of the sipXecs, or it can be installed on a separate host still managed by the configuration server. It is possible to define and configure several ACD servers for the same system and manage them all through the configuration server from a central location.

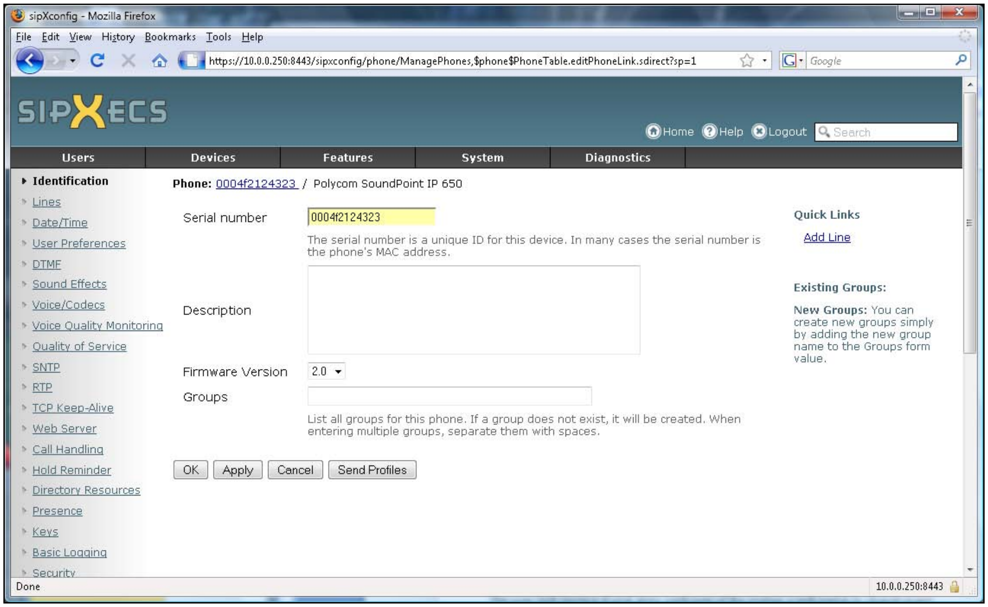
The **ACD Queue** configuration screen is shown as follows. As with most sipXconfig pages, the **ACD Queue** configuration screen is well documented, explaining each of the settings.



Device management

Over 75 different types of phones and gateways can be managed directly in the sipXecs configuration server. The sipXecs configuration server provides default profiles for every managed device. Configuring a phone to register with sipXecs is very easy and will be explained further in Chapter 5.

The following screenshot is the sipXconfig phone configuration screen. As can be seen by the possible configuration options on the leftside of the screen, almost every configurable option for a phone can be modified for each phone:

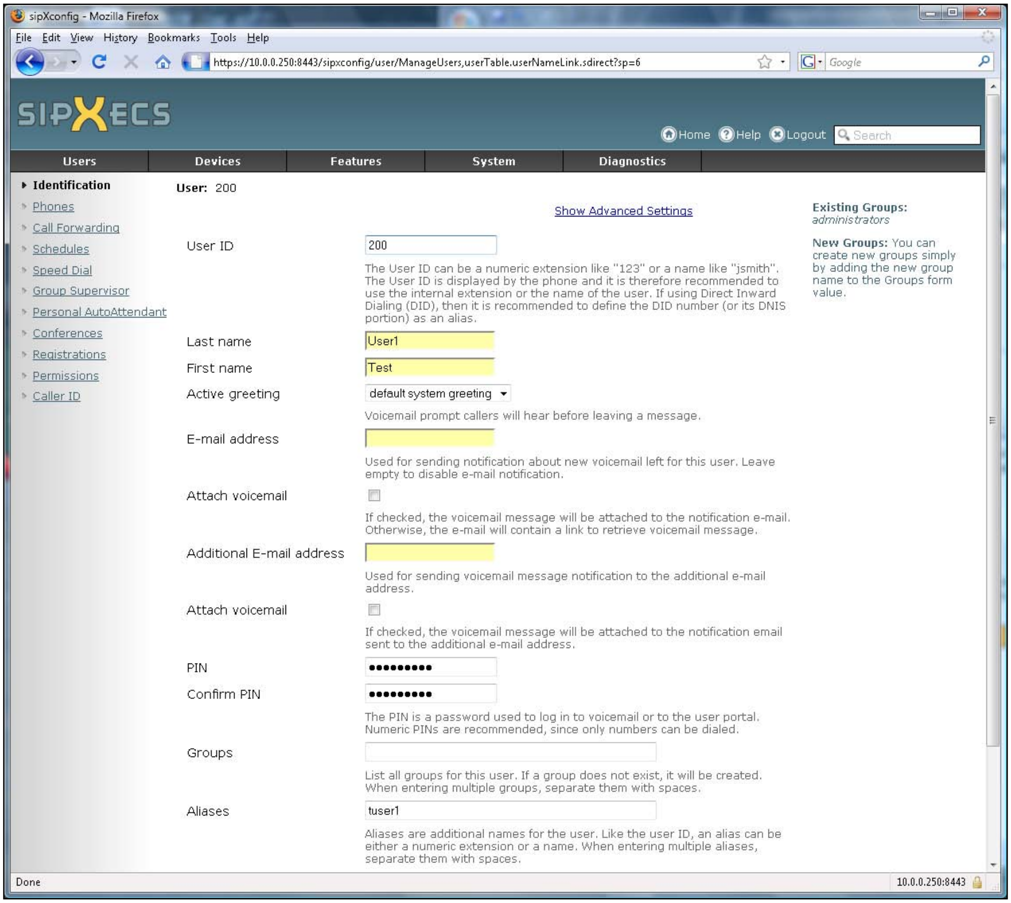


There is an additional service available that will automatically discover unassigned phones on the network and allow the administrator to add them into the system.

User management

Working with SIP provides a great flexibility for different addressing schemes based both on usernames and telephone extension numbers. As a standard SIP-based solution, sipXecs allows an organization to derive its naming scheme from its domain name. This allows the same addressing already used for email to be extended to real-time multimedia communications.

The following sipXconfig user configuration screen allows the administrator to quickly change names or email addresses for the user:

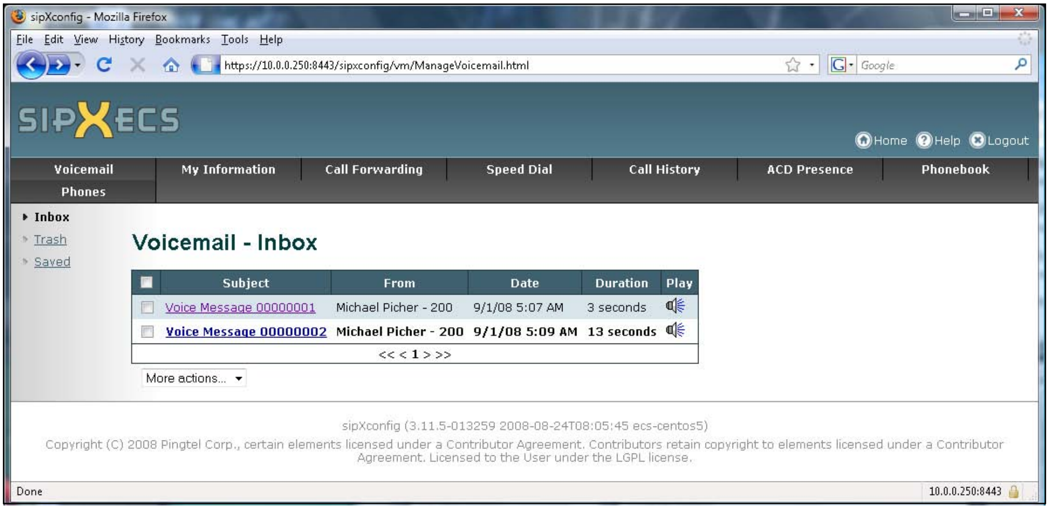


Users can be created one at a time in the sipXecs configuration server, imported from a **Comma Separated Values** (**CSV**) file, synchronized with LDAP, or Microsoft Active Directory, or added programmatically via the SOAP interface provided by the configuration server.

User self-service portal

The User self-service portal gives each user of the system a web portal to change many configuration items that the system administrator may need to have done for them before.

The following screenshot shows what users are greeted with after they log in to the PBX with their web browser:

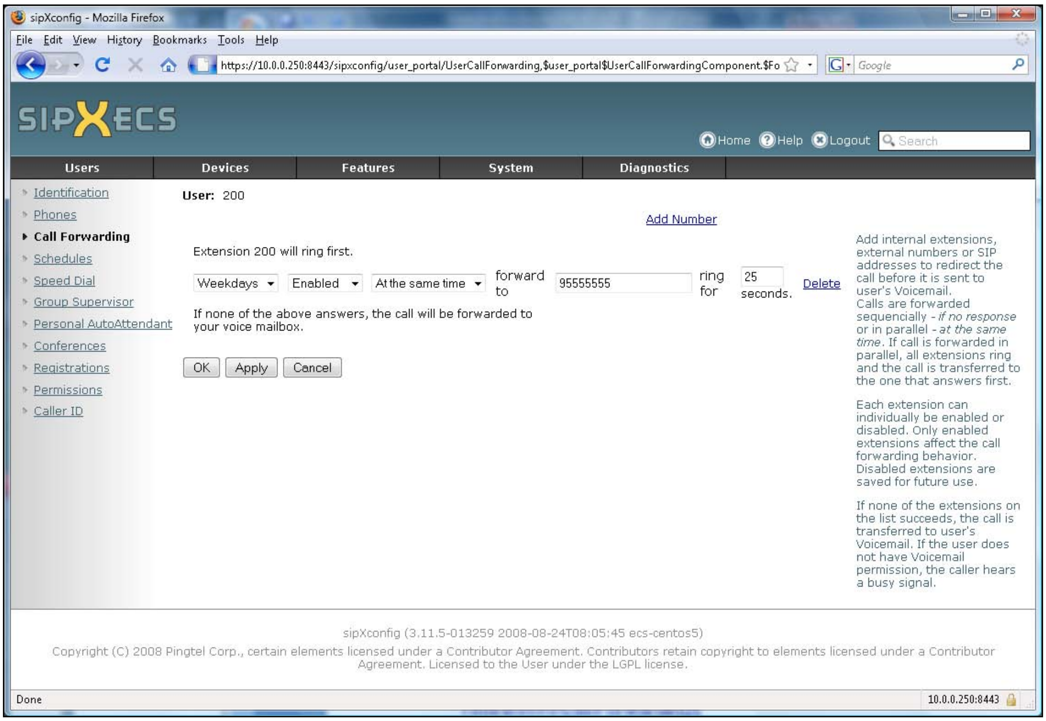


Users can manage their voicemail messages, change their active voicemail greeting, set up to two email addresses to forward their voicemail to, change their **Personal Identification Number** (**PIN**), set up call forwarding with schedules, create a personal auto attendant, set up to 9 Voice Mail distribution lists, manage their conferences, add or remove speed dials from their phones, view call history, sign in and out of ACD queues, maintain a phonebook, and see what phones they may be registered on.

Time-based call forwarding

Users have the ability to set up call forwarding options based on any schedule they would like. For instance, a user may choose to have calls forwarded to his or her cell phone and desk phone to ring at the same time during normal working hours.

The following screenshot shows an administrator's view of a user's call forwarding configuration:



Localization

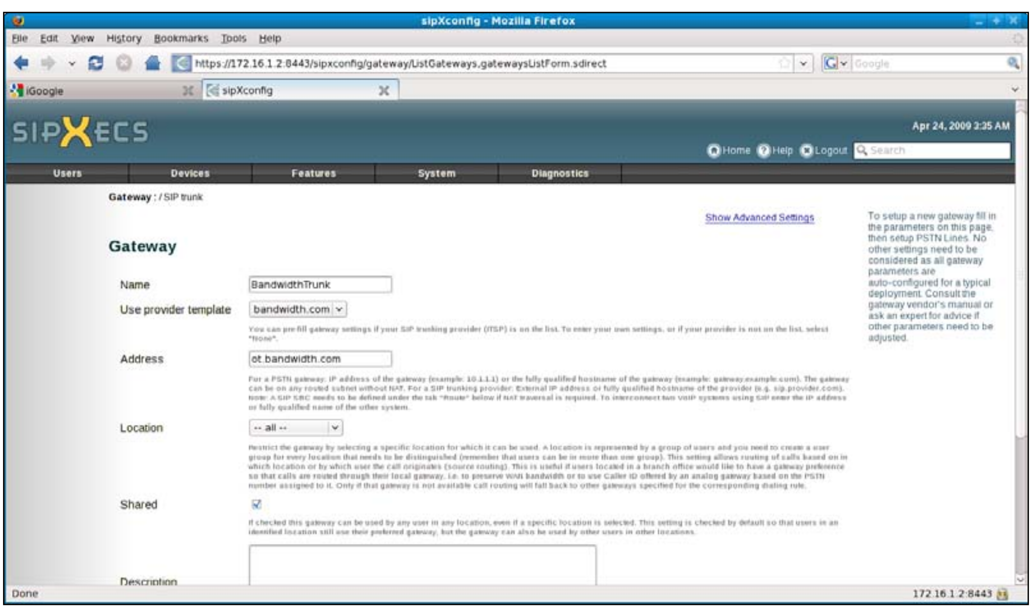
sipXecs was designed with the ability to localize the entire system for different regions of the world. Localization (language) packages provide the ability to change voice prompts, user interface prompts, regionally specific dial plans, and localization files for third-party components.

There are currently nine localization packages available for sipXecs; US English, German, French, UK English, Spanish, Mexican Spanish, Canadian French, Dutch (Netherlands), and Brazilian Portuguese.

Localization packs can also be developed by system administrators if the settings in the available packages don't really meet your regional needs. These packages need to be updated for every future release of sipXecs because of user interface screen changes and new features being added.

Internet calling and NAT traversal

Increasingly, telecommunications services are being provided across the Internet by companies referred to as **Internet Telephony Service Providers** (**ITSP**). Rather than relying on physical phone lines, ITSPs utilize SIP to provide phone service to almost any location. One of the hurdles that are typically faced by SIP phone systems is dealing with company firewalls and **Network Address Translation** (**NAT**).
The sipxbridge service handles the ITSP interface requirements and NAT traversal for the PBX.



The Internet calling configuration screenshot shown above allows the system administrator to configure calling routes to Internet Telephony Service Providers.

Call detail records

sipXecs supports near real-time reporting of **Call Detai**l **Records** (**CDR**) in the configuration server. The sipxcallresolver service is polled by a SOAP web interface to get access to information about the ongoing calls. Historic information is also maintained in the system regarding all calls. Administrators can filter CDR information based on time, date, caller, and called party. Additionally, CDR information can be downloaded in CSV format, or accessed directly from the SQL database that houses it.

Clustering

A cluster is a collection of servers working together to act like a single system to provide high availability and load balancing. sipXecs provides the ability to create a cluster of systems to form an iPBX that allows administrators to build a redundant communications system. This configuration also allows sipXecs to be deployed as a multi-branch office solution that is centrally managed. It acts as a single large system with a cohesive dial plan and number portability between branch offices. In a clustered configuration, the sipXecs scalability can extend into several thousands of users distributed over different locations or offices.

Summary

The sipX Enterprise Communication Server is a robust and easy-to-use iPBX built in an open source environment. It has been developed to meet the communication needs of organizations from 5 to 5,000 users.

2

System Planning and Equipment Selection

Any system that has such a profound impact on an organization as the communications system demands proper planning.

System planning

System planning consists of first understanding what your organization has for a communication system, and how communications flows through the organization. Once information about what is in place is gathered, a new system can be planned based on the existing needs, desired changes to call handling, new system capabilities, and selected equipment features.

Information gathering

Focusing on what exists now will help to define what needs to be changed to meet the final design. Throughout the information gathering phase, identify where call handling can be modified to better support the organization's goals.

Existing telecommunications connectivity

Gathering information about what kind of phone lines the organization has at each site will help with gateway selection and inbound programming. Gather information about every line coming into the building and how it rings in. Gathering special information about who the provider is and any information needed to contact them will come in useful in the future.

The following table shows the type of information that needs to be gathered. It includes the type of line, phone numbers associated with that line if the line rings in some sort of hunt group, and special notes about the line (what vendor provides it, the vendor's support number, and circuit information).

Site A			
Type of Line	**Phone Number**	**Ringing**	**Notes**
PRI	DID 555-5100 – 5199	Main Inbound DID is 555-5100 DID 555-5101 Sales DID 555-5110 -5150 Users	Provider xyz Support: 1-800-222-2222 Circuit ID 34xyz34234xd8293 Line Encoding: B8Zs ISDN Signaling: DMS-100 DID Digits: 7
Analog	555-5203		Provider zzz Support #: 1-800-333-3333 Main Fax
Analog	555-5204		Provider zzz Fire / Security
Analog	555-1215		Provider zzz DSL / Support Fax

Site B			
Type of Line	**Phone Number**	**Ringing Order**	**Notes**
Analog	555-1212	Inbound Hunt 1	
Analog	555-1213	Inbound Hunt 2	
Analog	555-1214	Inbound Hunt 3	
Analog	555-1215		DSL / Fax

Demarcation point

The demarcation point (demarc) is the location in a facility at which communications facilities owned by the telecommunications provider interface with your organization's communications systems. The box that the telecommunications provider utilizes to breakout its lines to interfaces that the customer can utilize, is referred to as the **Network Interface Device** (**NID**). Determine where the demarc is and ensure that all lines are clearly identified. Note any connectivity from the demarc to where the current phone system resides.

Identify if lightning protection is on each phone line. Establishing lightning protection on each line will save both phone system and network equipment from an early demise.

Existing users and phones

Gathering information about existing users and phones will help in planning about what type and how many new phones will be required in the installation. Also make sure to gather additional information and any special notes that may be required for programming the new system, or if cabling is required.

A table, such as the following, can be used to collect all of the pertinent information for each system user. First name, last name, current extension, what type of phone they may have now, if they have voicemail or not, their email address, and any special notes about the phone or user. These special notes might be information such as which extensions the user needs to monitor, if they have a headset (and what make/model), or if they have any special call forwarding in use.

First Name	Last Name	Extension	Phone Model	Voicemail	Email Address	Notes
Joe	User	201	16 Button	Yes	juser@comp.com	Monitor Extension 202, 205
Jane	Doe	202	16 Button	Yes	jdoe@comp.com	Monitors Extensions 201, 202, 203, 204
Joe	Boss	205	16 Button	No	jboss@comp.com	Forwards to ext. 201 after 15 seconds
Conf	Room	210	Analog Conf Phone	No		No network drop available

Existing call flow

Collect information about how communications flow through the organization now. It is important to understand all aspects of what is in place at present before it can be built or redesigned in the new communications system.

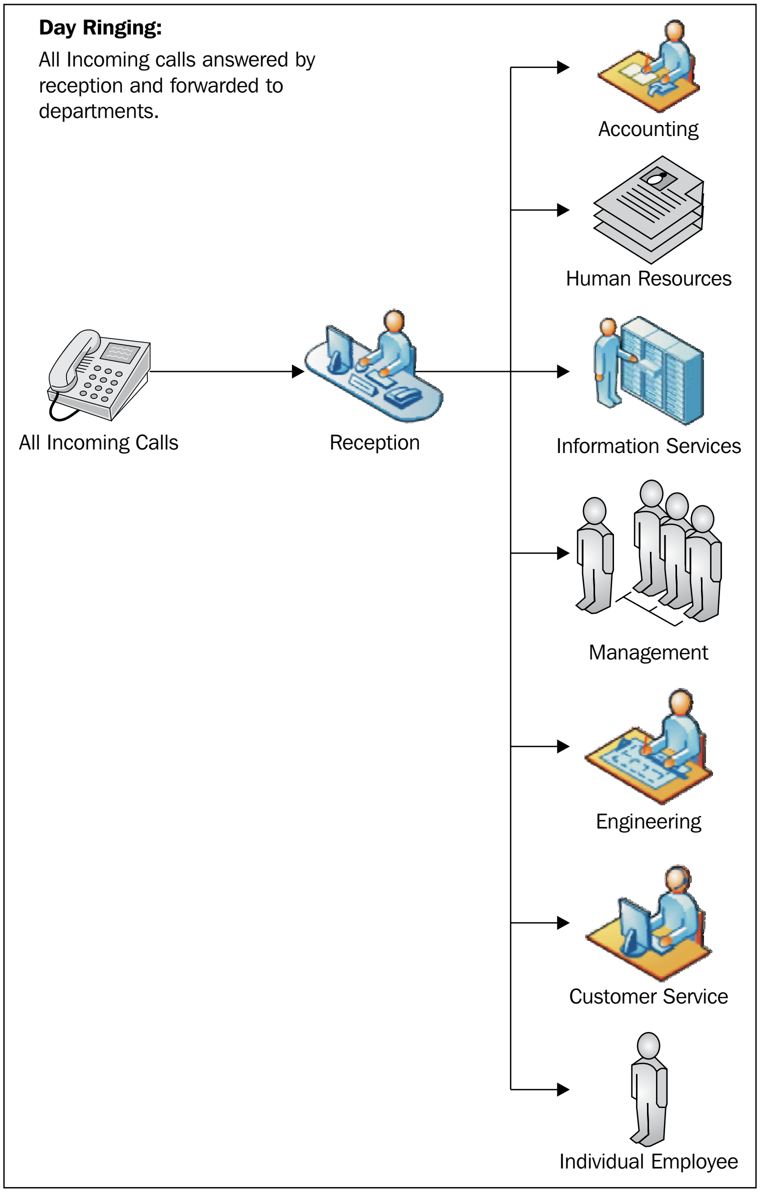
At a minimum, all of the following calling patterns should be identified:

- Where do inbound calls ring during the day for each phone number?
- Where do inbound calls ring after hours for each phone number?
- What are the 'daytime' hours?
- What happens on holidays?
- What happens when the office is unexpectedly closed?
- How does each call destination ring (auto attendant, hunt group, ACD queue, and individual)?

Each call flow will have one of the four types of destinations: an auto attendant, a hunt group, an ACD queue, or an individual user/mailbox. Attempt to identify what each of these call destinations is. There are tables in the following sections to help collect as much information as possible. Gathering the 'big picture' information is more important than gathering minute details. If full details are not available, specifics can be decided during planning.

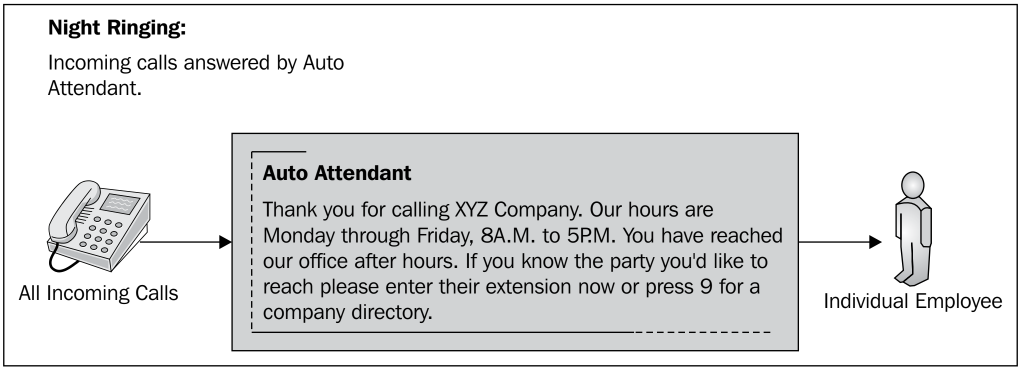
Day call flow example

The following call flow example illustrates how calls arrive at the company during the day and how they should be handled. Diagramming this information helps define how the iPBX will operate.


Day Ringing:
All Incoming calls answered by reception and forwarded to departments.
All Incoming Calls
Reception
Accounting
Human Resources
Information Services
Management
Engineering
Customer Service
Individual Employee

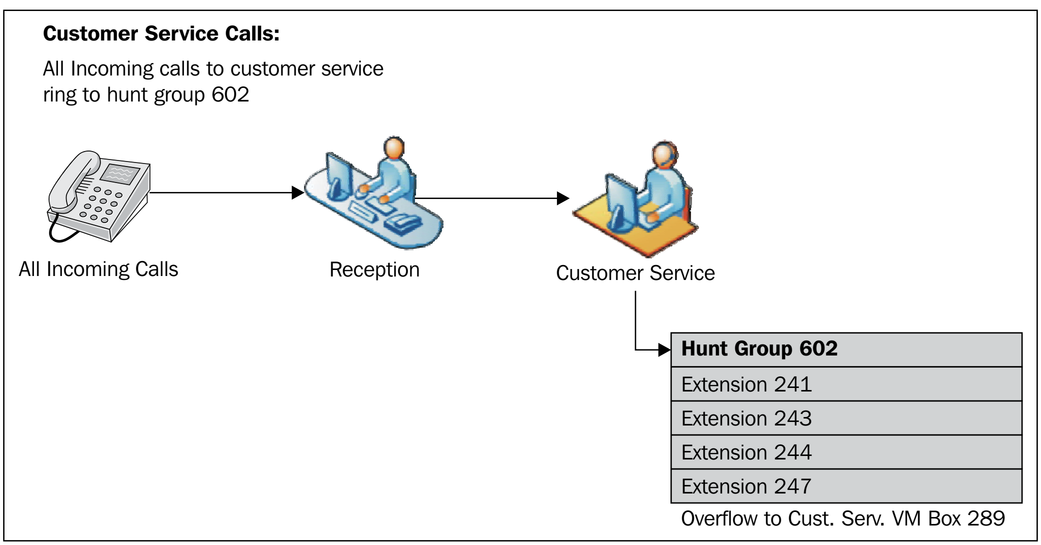
Night call flow example

The following night time call flow diagram illustrates how calls into the company will be handled when nobody is available to answer the call:



Departmental call flow example

The following call flow diagram illustrates how calls transferred to the **Customer Service** department will be handled:



Existing auto attendants

Document any existing auto attendants that may be in use in the system. Auto attendants will have an announcement message that is played to callers. It describes which dial pad buttons to press to get to the destination they are trying to reach. The existing destination information should also be collected.

Auto attendant information can be captured in a spreadsheet like the following:

Auto Attendant Name	Day Auto Attendant	
Description	This is the auto attendant that callers hear if all receptionists are busy.	
Pilot Number	580	
DID	(DID stands for Direct Inward Dial, explained in Chapter 1.)	
Attendant Audio	"Thank you for calling XYZ Company. We're sorry nobody can take your call personally. If you know your party's extension, please feel free to dial it at any time or dial 9 for the directory. For Sales, press 1; for Customer Service, press 2; and for Technical Support, press 3."	
Dialpad	**Action**	**Extension**
1	Transfer to Extension	590 (Sales ACD Queue)
2	Transfer to Extension	591 (Cust Serv. ACD Queue)
3	Transfer to Extension	571 (Tech Suppt Hunt)
9	Dial by Name Directory	
0	Dial Operator	
Failure Action	15 Seconds	
Repeat Menu	3 times	
Failure Action	Hang up / Transfer to Extension	
Transfer Extension	500	

In the example above, the day auto attendant for our fictional XYZ Company is at the extension 580. There is no **Direct Inward Dial** (**DID**) number assigned. Users have menu options from 1 to 3, with 9 being the Dial-by-Name Directory and 0 being the Operator. If nothing is entered for 15 seconds, or the wrong entries are entered for three times, the call is transferred to the extension 500.

Existing hunt groups

Identify any hunt groups that are in use on the existing system. Hunt groups usually have a phone number associated with them, which is referred to as the pilot number. The pilot number is the extension that is dialed to initiate the hunt group call.

Hunt groups in a traditional PBX are either linear or circular. Linear hunt groups start at the first extension in a list of extensions and progress one at a time through the hunt group. Linear hunt groups also need to take some sort of action (fallback) when the end of the list is reached and the call is not answered. They can return a busy, deposit voicemail for the last user, or transfer to another hunt group or extension. Circular hunt groups start back at the first extension when the last extension is reached.

The following table details the "Tech Support" hunt group, which has a pilot number of 550 and operates linearly. The initial call is to the extension 204. After 15 seconds, the extensions 207 and 208 ring for 15 seconds. If the call is still not answered, the call is sent to the extension 203 for 30 seconds after which the call is sent to the Tech Support receptionist at the extension 210.

Capture as much information as possible about any existing hunt groups. If it is not possible to fill in all of the fields, decisions can be made later in the planning section.

Hunt Group Name	Tech Support		
Pilot Number	550		
Type of Hunt Group	Linear / Circular		
Sequence	**Extension**	**Name**	**Timer**
1	204	User Name 1	15 seconds
2	207	User Name 2	15 seconds
2	208	User Name 3	15 seconds
3	203	User Name 4	30 seconds
Fallback Action	Busy /Voicemail of Last / Transfer to Extension: __210__		

In the example above, the Tech Support hunt group is at the extension 550. This is a linear hunt group, so the extension 204 rings for 15 seconds, then 207 rings for 15 seconds, and then 208 rings for 15 seconds, and finally the extension 203 rings for 30 seconds. If the call is not answered, it is transferred to the extension 210.

If details such as the pilot number or type of hunt group are not known, some decisions can be made during the planning phase.

Currently, sipXecs does not support the circular hunt group functionality. As the deployment is planned, this will need to be considered and the call flow adapted.

Existing ACD queues

Automatic Call Distribution (**ACD**) queues are basically fancy hunt groups. They allow the system administrator to design a method for handling larger call volumes than can be dealt with by simple hunt groups. Agents sign in and out of the queues as they become available.

If the existing communications system utilizes ACD queues, that information should be captured in a table such as the one given next. The queue name, pilot extension number, the external DID if applicable, how the calls are routed in the queue, description of the audio heard while in the queue, the list of agents in the queue, and how overflow (call has been queued for too long) is handled.

Gather as much information as is available about how the existing ACD queues work at present. Identify any problems with how calls are handled in the queues and if there is room for improvement.

ACD Queue Name	Sales	
Pilot Number	560	
DID	555-555-5555	
Type of Routing	Ring All / Circular / Linear / Longest Idle	
Queue Audio	"Thank you for calling XYZ Company. All of our Sales Associates are assisting other customers at this time. Please hold and an associate will be on the line momentarily." Music recording of some guitar player for 45 seconds. Message repeated.	
Agent	Extension	Name
1	212	ACD Agent 1
2	215	ACD Agent 2
3	213	ACD Agent 3
4	217	ACD Agent 4
Overflow Timer	120 seconds	
Overflow Action	Hang Up / Overflow Queue: __Inside Sales__ / Transfer to Extension: _______	
Notes about queue		

The preceding table documents an ACD queue for sales with a pilot number of 560. This queue also rings when the phone number 555-555-5555 is dialed directly. Calls are routed to the longest idle agent that is signed into the queue. The agents available to be in this queue are the extensions 212, 215, 213, and 217. If a call is in the queue for more than 120 seconds, the call is transferred to another ACD queue called 'Inside Sales'.

Special considerations

Each organization is different. It is important to consider all of the special functionality in place that may need to be considered in planning for the new system. Facility-wide paging and cordless phones are just two examples of special considerations that may be encountered.

Paging

Consider how staff are paged in the facilities. Is there a paging system in place that needs to be interfaced to? Gather all information about the paging system in place, how to interface to it, and how to page all and page to different paging zones.

Cordless phones

Many organizations will utilize cordless phone technology for employees who are mobile within the facilities. It is important to understand where these users need to operate from and any special features they may require.

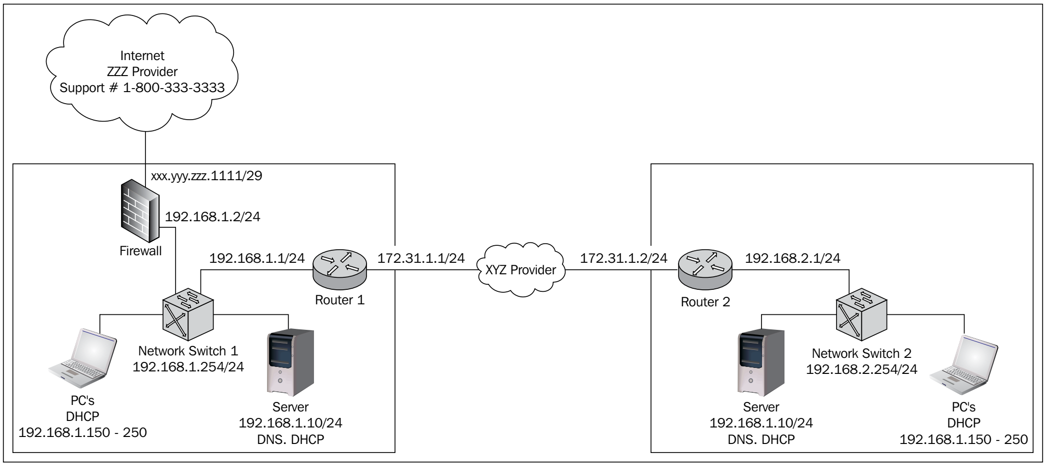
Existing computer network

The network is the foundation upon which the new communications system will be built. A voice over IP application on the network will quickly point out the weak links in any network with poor call quality. Understanding what the current network design is, what equipment is in place, and what its capabilities are is critically important; but is often overlooked.

Gather some basic information about each site first such as IP addressing, **Internet Service Provider** (**ISP**), and DNS hosting information. The following table, completed for each site, will capture the required information:

Site Name	Site1
Internet Service Provider	Really Fast ISP
Support Contact #	1-800-555-5555
External DNS Domain	xyzcompany.com
External DNS Hosting Provider	Super Hosting Provider
DNS Provider support SRV Records?	Yes
External IP Addresses/Subnet Mask	xxx.xxx.xxx.xxx/255.255.255.248
External IP Address of Firewall	xxx.xxx.xxx.zzz
External Default Gateway	xxx.xxx.xxx.yyy
External DNS Servers	yyy.yyy.yyy.yyy, zzz.zzz.zzz.zzz
Internal IP Address Ranges/Subnet Mask	192.168.1.0/255.255.255.0
Internal Default Gateway	192.168.1.1
Internal DNS Server	192.168.1.5
Internal DNS Domain	corp.xyzcopany.com
Internal DHCP Server / type	192.168.1.5/Microsoft
Internal DHCP Range	192.168.1.50 – 192.168.1.200
Notes	

Spend time creating a network diagram that shows all existing network equipment, including network switches, routers, and servers. Also, gather IP addressing information for each site and all devices. For each site, also document the existing VLANs, subnets, gateways, DHCP servers, DNS servers, and WINS servers.



The previous network diagram details the critical components and addressing information for two sites interconnected by a leased line.

Once all of the network equipment has been diagrammed, the switches and routers should be listed out with manufacturer, model, firmware revision, management IP, quality of service (QoS) capabilities, Virtual Local Area Network (VLAN) capabilities, and any notes you might have about them.

Some research will need to be done around the capabilities of each of the pieces of network equipment to determine whether they support QoS if you are expecting to utilize any of it later.

The following table illustrates the type of information that will be required to make decisions about network equipment:

Name	**Mfg**	**Model**	**Firmware**	**IP**	**QoS**	**VlAN**	**Notes**
Switch1	Cisco	2950-48 Port	4.2.4	192.168.1.254	Yes	Yes	Purchased 08/08/2004
Switch2	Cisco	2950-24 Port	4.2.2	192.168.2.254	Yes	Yes	Purchased 04/02/2004 2 spare ports
Router1	Adtran	3205	2.2.3	192.168.1.1	Yes	Yes	Purchased 09/01/2004
Router2	Adtran	3205	2.1.2	192.168.2.1	No	Yes	Purchased 07/03/2003
Firewall1	Cisco	Pix 515	6.2.3	192.168.1.2	No	No	Purchased 8/14/2004 SIP Capable

Equipment selection

Selecting the proper equipment can make or break your project. Phones and network equipment are usually the two largest-ticket items. However, cutting corners too much on either of these components can result in a poor user experience.

Network equipment

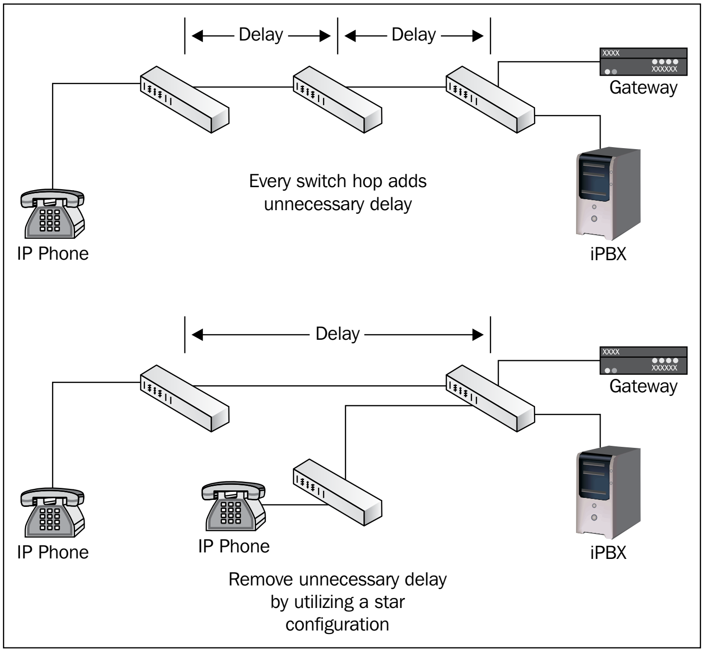
The network equipment selection and configuration is critically important. The network is the foundation on which the entire system will be built. It must be reliable, fast, and robust if the voice system is to follow suit. Several important design considerations drive equipment selection, such as network switch connectivity, Quality of Service support, Virtual Local Area Network support, how to power the phones, whether Gigabit network connectivity is required to each desk, and whether any existing network equipment be utilized.

Network switch connectivity

Some good rules of thumb to follow when determining where and how many network switches may be required for the project are:

- Minimize network closets: By minimizing network equipment locations, fewer UPSs and network switches will be required, and less time will be wasted in locating cables.
- Simplify network connections: Connect network equipment in a 'star' type layout. Avoid connecting switch to switch.

The following diagram illustrates how simplifying the network connectivity can reduce delay in the network:



Quality of service

Many network administrators wrongly assume that because a network doesn't have much network traffic, or because they are running Gigabit switches, they don't need to worry about the small amount of network traffic generated by a phone conversation.

If voice packets do not leave one device and arrive at the second device as quickly as possible and in the same order, system users will experience a poor-quality call. This poor quality will take the form of delay or jitter. Delay is the amount of time it takes the person listening to begin or end hearing what the talking party is saying. Jitter is broken or jumbled parts of a conversation such as typically experienced in a poor quality cell phone call. Echo and static are examples of other quality problems, but these are not created by poor network design.

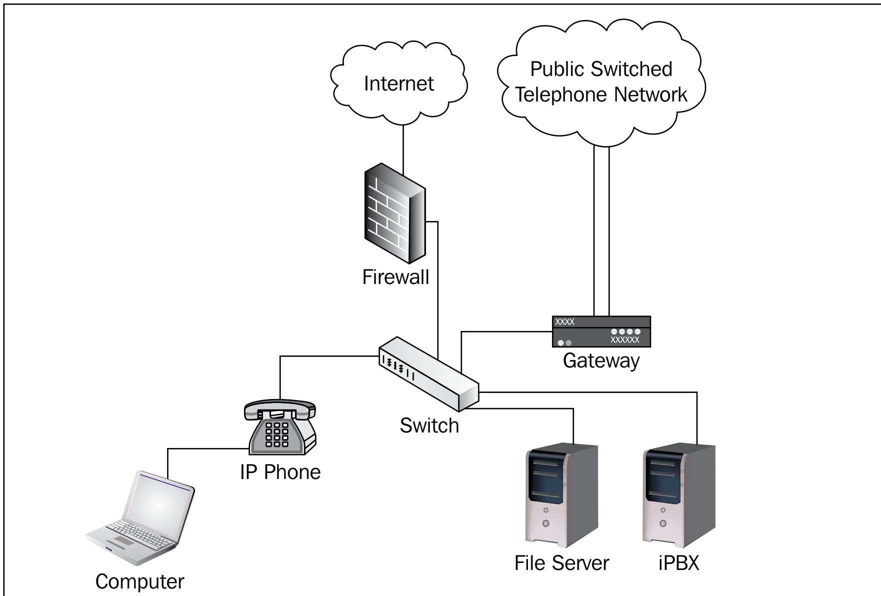
The ability to identify certain traffic on the network as being of higher importance is referred to as **Quality of Service** (**QoS**). Network traffic can be flagged with a priority value, which is in turn honored by network switches. QoS helps to ensure that packets traverse the network and arrive at their destination in an orderly and timely fashion.

There are two types of QoS that are most common across switching products: **Differentiated Services Code Point** (DiffServ or **DSCP**) and **Class of Servic**e (**CoS**). DSCP operates at the IP protocol level (Layer 3 of the **Open Systems Interconnection** or **OSI** model—`http://www.itu.int/rec/T-REC-X.200-199407-I/en`) and utilizes a field in the header of each IP packet to identify the priority of the IP packet. DSCP is defined in IETF's RFC 2474 (`http://tools.ietf.org/html/rfc2474`).

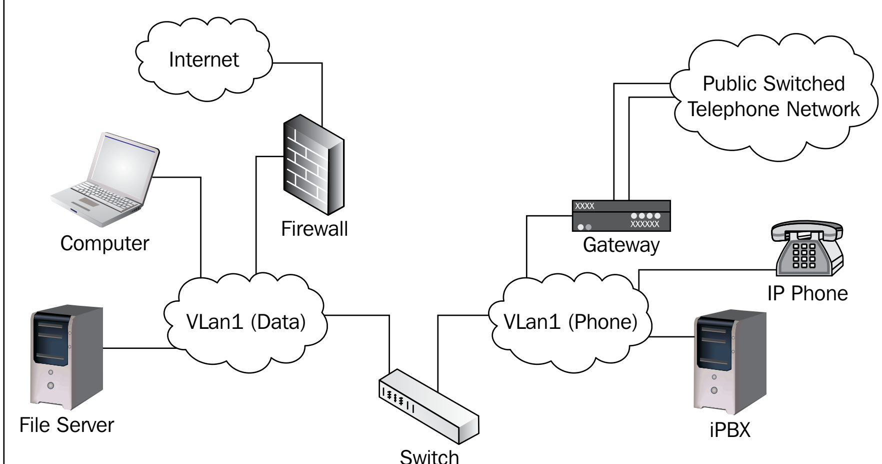
CoS uses a 3-bit field in the Ethernet frame header to identify the priority of the packet. This standard is referred to as the IEEE 802.1p standard (`http://ieee802.org/1/`). Since CoS operates at the Ethernet frame level, it is considered to operate at OSI Layer 2 and is not routable as such. DSCP is routable because it operates within the IP packet.

Virtual Local Area Network support

Virtual Local Area Networks (**VLANs**) allow network administrators to segment their networks into separate logical pieces. By segmenting the phone network from the data network, the system designer is able to separate IP addressing, DHCP, and DNS services. Separating services can make integration easier than attempting to integrate with existing services. This segmentation can also make the phone system more reliable because it is not dependent on anything on the data network in order to operate.



Physical Network Connectivity Diagram



Virtual Network Connectivity Diagram

The preceding network diagram illustrates the difference between how network elements might be physically and virtually connected.

Additionally, if the phone network is segmented from the data network by a VlAN, it is possible to firewall the two networks from each other. This is advantageous if there are applications on the data network that cause problems with the communications systems, or if there is some sort of denial of service attack that originates from the data network.

VLANs operate at the Ethernet frame layer (Layer 2) and their interoperability is defined in the standard referred to as IEEE 802.1Q (`http://ieee802.org/1/`). To ensure interoperability between switches if different vendor products are selected, make sure that all of them support the IEEE 802.1Q standard.

Powering the phones

How to power the IP phones is one of the most important factors while selecting network equipment. Convenience, cost, and reliability are all factors that need to be considered.

The most convenient way to power the phones is with **Power over Ethernet** (**PoE**). PoE is a network standard that detects if a device that is plugged into the network can accept power, and then provides DC power across the network cable.

Power injectors (also referred to as midspans) also can inject power in the network closet. They are inserted between the network switch and a PoE-capable phone. If the existing network equipment can support your network properly and handle Quality of Service, power injectors may make financial sense. However, power injectors introduce extra cables and extra equipment into the network closet. This may reduce reliability and is certainly not as convenient as knowing that every network port has power available on it.

Both PoE switches and power injectors allow the network administrator to power all phones from the convenience of the network closet. In a power outage situation, phones can stay operational for as long as uninterruptable power or generators allow. The most widely accepted standard for PoE is IEEE 802.3af (`http://www.ieee802.org/3/`). Some older Cisco equipment utilized a proprietary PoE standard that has been largely abandoned. Additionally, not all PoE switches are created equal. Some may not be able to supply enough power for all of the devices needed to connect to the switch. Verify the power consumption of the phones to be used and make sure the switch can provide enough power.

Optionally, AC to DC power adapters can be utilized at each phone to plug them into a wall outlet (or a small local UPS). Not all phones come with power adapters, so it is important to consider this potentially added cost at the time of purchase.

Gigabit switches

If Gigabit Ethernet and single network cable are requirements, network switch and IP phone choices become more limited and expensive. IP Phones typically have a two-port network switch built into them. The switch in the phone allows the phone to sit between a user's PC and the network switch. If the switch in the phone is only rated at 100 Mbps, the PC that connects to it will connect to the network at a maximum of 100 Mbps.

If Gigabit Ethernet to the desktop is required and a single network drop is to be utilized, phones with in-built Gigabit Ethernet switches must be utilized. If Gigabit Ethernet needs are limited and network equipment costs are a factor, consider running separate runs to those computers and using 100 Mbps switches for phones.

Utilizing existing network equipment

Most network administrators prefer to have homogeneous network equipment—not because network equipment won't interoperate, but simply for ease of management of the equipment. Consider what equipment you have in place and if any of it will meet the later needs of the communications system. Either DSCP or CoS is a "must have" for a quality deployment.

Servers

To build a highly reliable and enterprise-ready communications system, the iPBX software needs to run on a highly reliable server. Server-class hardware is designed with proper system cooling and reliability to operate 24 hours a day and 365 days a year. The recommended system would have the following components:

- Two or four (or dual/quad-core) processors operating at 1.8 GHz or better
- 2 gigabytes of system memory (RAM)
- 32 gigabytes or larger SCSI hard drive
- Single Ethernet adapter (100 Mbps or 1000 Mbps)

For best compatibility with the single CD installation of sipXecs, ensure all components are Red Hat or CentOS Linux compatible.

Just as with any file server, reliability may be increased by utilizing redundant hard drives (mirrored / RAID-1 or RAID-5) and power supplies.

Since sipXecs supports an unlimited number of voicemail boxes, the total number of hours of recorded messages is determined by the size of the system hard drive. To estimate storage requirements, allow 1 MB of storage space for every minute of recorded messages.

Gateways

If the communications system being built does not need to connect to a traditional telecommunications provider, or analog phones, you may not require gateways.

Unlike some other open source PBXs that utilize cards in the server (Asterisk and FreePBX), sipXecs utilizes external hardware devices to connect to traditional telecommunications providers and analog telephones. The advantages of an external gateway are that the server does not have to process audio and calls can continue if the phone system goes offline. The disadvantage is that external gateways may cost a little more than their internal counterparts.

For port capacity, planning a low phone-to-line ratio (referred to as the subscription rate) would be four users to every phone line. A more reasonable subscription rate is six to eight users to every phone line. Consider the needs of the organization and how many users may need to be on external calls at once.

If there are more than eight lines required at a single physical location, then consider moving to a digital PRI/T1/E1 circuit to reduce monthly costs, get better call quality, and have the additional calling features.

Analog gateways

Analog gateways provide **Foreign Exchange Office** (**FXO**) and/or **Foreign Exchange Station** (**FXS**) interfaces. The FXO lines connect to **Plain Old Telephone Service** (**POTS**) lines provided by the telecommunications provider, whereas the FXS lines connect to analog stations (phones or fax machines).

Analog gateways come in many different port configurations from one to thirty-two ports. Some analog gateways will have a mix of FXO and FXS ports, and some may even allow ports to be configured as either FXO or FXS.

Most analog gateways will support caller ID service from the telecommunications provider if enabled on the phone line. The caller ID will be passed directly to the receiving telephone for display (if it is equipped with a display).

The most popular analog gateways are from AudioCodes and Patton Electronics. The AudioCodes gateways have the ability to be automatically configured in sipxconfig, whereas the Patton Electronics gateways are more configurable.

Digital gateways

Digital gateways will provide interfaces to PRI, T1, E1, or BRI digital phone lines. Because the audio is sent in a digital form to the gateway, the call quality is much better than that of the typical analog phone line.

Additionally, the added feature of DID (which may be referred to as Direct Dial In or DDI in Europe) numbers is that the telecommunications provider will provide a block of phone numbers that are assigned to the circuit. The number of DIDs allocated to a circuit does not correspond to the number of channels on a circuit (for example, a 23-channel PRI may have 200 DIDs assigned to it). As a call begins, the number that was dialed is passed into the gateway before the ringing begins. This dialed number can then be used to route the call to a chosen extension on the phone system.

When selecting a digital gateway, it is important to verify what your telecommunications provider will be supplying for the digital circuit encoding and ISDN signaling on the digital circuit. Then make sure that the gateways you select can accommodate the provider.

For T1/PRI circuits, the line encoding is typically **B8ZS** (**Bipolar with 8 Zeros Substitution**) or **ESF** (**Extended Super Frame**). For E1 circuits, line encoding is typically **HDB3** (**High Density Bipolar three** coding). For the signaling to the provider's phone switch, the provider will typically specify what signaling it will be utilizing. In North America, **DMS**-100 (**Digital Multiplex System**-100, a Nortel standard) or NI2 (US National ISDN Phase 2) signaling standards are the most prevalent.

Like the analog gateways, the most popular digital gateways are from AudioCodes and Patton Electronics. If you are going to have a mix of analog and digital gateways, consider staying with the same brand to ease management.

Phones

There is an abundance of phones available for SIP-based phone systems. Hard phones are the standard sort of desk phone found in business. Softphones are phones that are designed to run on a computer. Wireless phones are meant for portability throughout a facility.

When selecting phones, it is important to understand the functionality that is important to the users of the system. Not all phones support the same Music on Hold standards, or handle attended transfers the same way.

Hard phones

Hard phones are available from many different vendors. They come in many different shapes, sizes, and costs. Almost any SIP phone can be made to work with sipXecs by manually configuring it. However, manually configuring phones would become burdensome in all but the smallest system deployments.

To ease system administration, there is an ever-expanding list of phones and FXS gateways that can be automatically configured by sipXecs' sipxconfig server.
The current list is as follows:

- Aastra: SIP IP 53i, 55i, 57i, 57iCT, 560m
- AudioCodes: MP112FXS, MP114FXS, MP118FXS, MP124FXS
- Cisco: ATA186/188, 7905, 7912, 7940, 7960, 7911G, 7941G, 7945G, 7961G, 7965G, 7970G, 7975G
- Grandstream: Handytone 286/386/486/488/496, BudgeTone 10x/200, GXP 1200, 2000, 2010, 2020, GXV 3000
- Hitatchi: Wireless IP 3000, 5000, 500A
- ipDialog: SipToneV
- Linksys: ATA 2102/3102, SPA 8000, 901, 921, 922, 941, 942, 962
- LG Nortel: IP phone 6804, 6812, 6830
- Mitel: 5224 Dual Mode
- Nortel: IP phone 1120/40, 1535
- Polycom: SoundPoint IP 300, 301, 320, 330, 4000, 430, 500, 501, 550, 560, 600, 601, 650, 670
- Snom: 300, 320, 360

Not all of the above-listed phones support all of the phone system features. The most commonly utilized and most compatible phones with sipXecs are:

- Nortel and LG-Nortel (`www.nortel.com`)
- Polycom SoundPoint IP (`www.polycom.com`)
- Snom (`www.snom.com`)

Spend some time researching the different phone vendors and the different models they offer. Take into consideration the information gathered earlier in the chapter about how the phones are used in the organization and what features are important for individual users.

If there is any question about whether a phone will be compatible with the sipXecs system, free interoperability testing is available at `http://interop.pingtel.com/`.

Softphones

With as many hard phones that are available, it seems like there are twice the number of software-based phones available. Their functionality seems to vary across the board. The great advantage of software-based phones is their low cost. The disadvantage is that it is an interface that users are not used to. Consider the users of the system and how they may adapt to this change.

The most popular softphones are from Counterpath (`http://www.counterpath.com`). Their free X-Lite softphone is used by many. If more integration with desktop applications (such as Microsoft Outlook) is required, consider Counterpath's eyeBeam or Bria products.

An important consideration when using softphones is whether the existing computers in the organization can utilize them. Since all of the voice traffic travels through the PC, the PC needs to be fast enough to process that traffic as well as run any applications the user may be using when on the phone. If the computer is too slow, the quality of the call can suffer.

For sound input and output from the softphone, a headset is utilized. The best option for this is a headset that uses USB and has its own sound processing based in the headset instead of trying to utilize system-integrated sound cards. Poor quality audio may be experienced when utilizing the sound card integrated into the user's PC.

There are many different types of headsets available in the market. Long known for their phone system headsets, Plantronics and GN-Netcom have a wide selection of products for computers. The administrator should verify compatibility of any headset with the softphone that is being utilized.

Wireless phones

There are two types of SIP cordless phones available for use in the market. The phones either use a standard Wi-Fi network (802.11b/g), or they rely on a separate wireless **Digital Enhanced Cordless Telecommunications** (**DECT**) network. It may seem like a no-brainer to use the same Wi-Fi network deployed for mobile computing use in the organization. However, Wi-Fi phones suffer from poor battery performance. Additionally, the **Access Points** (**AP**) deployed may not support QoS and the phones may not roam from AP to AP smoothly.

DECT wireless handsets will cost more to implement because a separate wireless infrastructure will be required to support the phones. The payoff, however, will be with better voice quality and noticeably longer battery life in the handset.

SIP firewalls

If the phone system is going to interact with the Internet in any fashion (connect to an ITSP or support remote phone users), it is important to protect the PBX. A firewall that understands the SIP protocol will be required to allow the traffic to flow between the organization's network and the Internet.

The SIP protocol is quite different from many other IP-based protocols. What is unique about it that causes problems with traditional firewalls is that the signaling part of the protocol is separate from the voice traffic. By default, SIP signaling occurs over port 5060 TCP or UDP. However, the **Real Time Protocol** (**RTP**) used for the voice traffic occurs on a random UDP port between 10000 and 20000. This port is agreed to in the SIP signaling.

In addition to supporting SIP, it is advantageous for the firewall to be able to prioritize SIP traffic over general Internet traffic. This prioritization can help reduce the effects of large downloads on call quality.

Because of the popularity of VoIP, many commercial firewalls now support both SIP and prioritization of voice traffic.

Uninterruptable power supplies

When the power goes out, most users expect their phones to continue operating. This requires that every device utilized by the phone system be on an **Uninterruptable Power Supply** (**UPS**). This includes all network switches, gateways, phones, servers, and firewalls. UPSs will need to be sized for the equipment that they are supporting.

Plan the installation

Begin the planning phase of the installation by utilizing the data collected. Fill this data into spreadsheets, which can be used during the installation. The call flow will be designed and then the network configuration will be diagrammed.

Extension planning

Extensions are required for most devices on the system. To avoid re-numbering user extensions, it is important to think about the organization and plan for the future. If a single site is all that is required, a three-digit dial plan can be utilized. If multiple sites are required, at least a four-digit plan will be needed.

The only new concept that will be added here is that of a phantom extension. A phantom extension is a typical user extension that does not have a phone registered to it. Phantom extensions can be utilized for general delivery mailboxes and call routing.

The following table can be utilized for planning extension use:

Site Name	
User Extensions	
Hunt Groups	
Call Park Orbits	
ACD Queues	
Auto Attendants	
Phantom Extensions	

For an organization with two sites, with one hundred or so users at each, the extensions might be planned out as follows:

Site Name	Example Site 1
User Extensions	2000 – 2199 (leave 100 additional extensions)
Hunt Groups	2300 – 2339
Call Park Orbits	2350 – 2369
ACD Queues	2380 – 2399
Auto Attendants	2410 – 2429
Phantom Extensions	2450 – 2499

Site Name	Example Site 2
User Extensions	2500 – 2699 (leave 100 additional extensions)
Hunt Groups	2800 – 2839
Call Park Orbits	2850 – 2869
ACD Queues	2880 – 2899
Auto Attendants	2910 – 2929
Phantom Extensions	2950 – 2999

In the preceding extension plan, each site uses five hundred extensions. Two hundred extensions are utilized for telephone extensions (one hundred more than needed with yet another one hundred between users and phone system services). Forty extensions are reserved for hunt groups, twenty extensions are reserved for park orbits, ACD queues have twenty reserved, auto attendants have another 20 extensions, and finally, phantom extensions have fifty extensions reserved. Enough buffer has been left on each side of each extension range to allow for unplanned growth.

Users and phones

The sipxconfig service has the ability to import user and phone information to speed up deployment. If you have a small number of users, you may just want to add them one by one. For large numbers, however, importing is the way to go and if the following table is saved as a **Comma Separated Values** (**CSV**) file, it can be directly imported. Either way, organize your collected data and utilize a spreadsheet with the following rows to speed up deployment:

- User name: This is extension the user will use. Extensions typically start at 200 and go up from there.
- Voice-mail PIN: This is the password for the user to go into his or her voicemail. It also is the password for entry into the user portal.
- SIP password: The SIP password is the password the phone will use to register. It should be complex and must consist of at least eight letters (upper and lower case) and numbers.
- First name: This is the user's first name.
- Last name: This is the user's last name.
- User alias: The user alias is something other than a number that can be used to dial the user. Consider adding their email alias here (if the user's email address is `tuser@company.com`, his or her alias would be `tuser`). This will allow the user to be dialed across the Internet from a softphone.
- Email Address: The user's email address can be used to forward his or her voicemail.
- User group: Define groups of users to better manage settings for multiple users. This field can be left blank if you are not sure about what groups you might use. User groups define permissions for users such as Superadmin Access, Change PIN from IVR, Configure Personal Auto Attendant, 900 Dialing, International Dialing, Local Dialing, Long Distance Dialing, Toll Free Dialing, Voicemail, Record System Prompts, and Internal Voicemail Server, or Microsoft Exchange UM Voicemail Server.

- Phone serial number: This will be the Ethernet MAC address of the physical phone that the user will have. If the user has a softphone, this will be left blank.
- Phone model: This will be the model of the managed IP phone that the user will have. If this phone will not be managed (that is, a softphone or not in the list of supported managed phones), this field should be left blank. If you know the web interface has support for the phone model you need, try to extrapolate the phone model from this list (for example, polycom9000). These are some of the phones that are managed as of this writing: polycom300, polycom430, polycom500, polycom550, polycom650, polycom600, polycom4000, cisco7960, cisco7940, cisco18x, cisco7905, cisco7912, gsPhoneBt, gsPhoneGxp, gsPhoneGxv3000, gsHt286, gsHt386, gsHt486, gsHt488, gsHt496, snom300, snom320, and snom360.
- Phone group: Just as with users, phones can be grouped and managed more easily. Consider groups of phones by department or by type of phone (for example, Poly330 or FrontOffice).
- Phone description: A description of the phone may be added. It may be convenient to put the name of the user assigned to the phone here.

Populate the table with information gathered during the information gathering phase. The only field that allows spaces in the data is the "Phone description" field. If you haven't ordered or received phones, fill in this information just before deployment.

Define permissions for user groups

A table with the following rows will help with defining the groups of user privileges:

- Group Name: Name of the group.
- Superadmin Access: User can log into administration interface.
- Change PIN from IVR: User can change PIN value from the voicemail system. PIN is used to log into voicemail system and web interface. PIN does not affect the password that phones use to authenticate with registration server.
- Configure Personal Auto Attendant: User can configure personal auto attendant.
- 900 Dialing: User can dial 900 numbers.
- Attendant Directory: List user in auto attendant.
- International Dialing: User can dial international numbers.
- Local Dialing: User can dial local numbers.

- Long Distance Dialing: User can dial long distance numbers.
- Mobile Dialing: User can dial mobile numbers.
- Toll Free: User can dial toll free numbers.
- Voice Mail: User has a voicemail inbox.
- Record System Prompts: User can record system prompts.
- Internal Voicemail Server: User has permissions for Internal Voicemail Server.
- Microsoft Exchange UM Voicemail Server: User has permissions for Microsoft Exchange UM Voicemail Server.

Groups and users can only have either Internal Voicemail Server or Microsoft Exchange UM Voicemail Server selected.

Call flow

Plan out how calls flow through the organization. Utilize any call flow information gathered previously and modify the call flow if it does not meet the current needs of the organization. Of interest here is developing how the system should work for the organization without worrying about the specifics of how to make the system work.

In the planning phase, the call flow needs to be detailed out to simplify the programming of the phone system. For example, if the call flow defines that inbound calls to telephone number 555-555-5555 during the day ring 'Reception', then 'Reception' needs to be defined. Is it a hunt group of three users, or an ACD group that handles inbound calls, or just a single user at the front desk phone? What happens if that call does not get answered? Does the call go to an auto attendant, or does it go to voice mail? Planning out this call flow is important to how the organization is viewed by its callers.

If the call flows identified in the information gathering phase are complete and function properly for the organization, the job is simpler. Review the following sections and develop the detail behind each of the call destinations by utilizing the previously gathered information as a base.

If a phone system doesn't presently exist for the organization, the call flow needs to be clearly defined. Build flowcharts detailing work-day call flows and after hours/weekend call flows. All call flows should have some sort of destination. These destinations will be one of these four things: an auto attendant, a hunt group, an ACD queue, or an individual user/mailbox.

The two most important call flows to identify are the inbound calls during the day and the inbound calls after hours. All other call flows should build from these.

Auto attendants

If the organization utilized auto attendants previously, much of the information from the information gathering phase can be utilized. Typically, for a good auto attendant design, do not go more than two auto attendants deep. Callers become annoyed if they have to go down through too many layers.

For each auto attendant envisioned, the following table should be completed:

Auto Attendant Name	Day Auto Attendant	
Description	This is the auto attendant that the callers hear if all receptionists are busy.	
Pilot Number	580	
DID	555-555-5555	
Attendant Audio	"Thank you for calling XYZ Company. We're sorry nobody can take your call personally. If you know your party's extension please feel free to dial it at any time, or dial 9 for the directory. For Sales, press 1; for Customer Service, press 2; for Technical Support, press 3."	
Dialpad	**Action**	**Extension**
1	Transfer to Extension	590 (Sales ACD Queue)
2	Transfer to Extension	591 (Cust Serv. ACD Queue)
3	Transfer to Extension	571 (Tech Suppt Hunt)
9	Dial by Name Directory	
0	Dial Operator	
DTMF Timeout	3 seconds	
Overall DTMF Timeout	7 seconds	
Maximum DTMF Digits	10	
Replay Count	2 times	
Invalid Response Count	2 times	
Transfer on Failure	Yes / No	
Prompt to play when transferring on failure	"I am sorry I was not able to handle your call. Please wait while your call is transferred to an operator."	

The columns of the table can be explained as follows:

- DTMF Timeout: The time to wait between each dial pad key before interpreting the user's request (cannot be greater than Overall DTMF Timeout).
- Overall DTMF Timeout: The total time to wait before interpreting a user's request.
- Maximum DTMF Digits: The maximum number of dial pad keys to accept before interpreting the user's request.
- Replay Count: The number of times the auto attendant will repeat the prompt after the initial announcement due to no input being received from the user before giving up and transferring the call or disconnecting.
- Invalid Response Count: The number of times the user can input an invalid response before transferring the call or disconnecting.
- Transfer on Failures: If enabled, the auto attendant will transfer the call to a designated extension if no valid response is received. If disabled, the call will be disconnected.
- Transfer Extension: The extension to be used when transfer on failure is enabled.
- Prompt to play when transferring call on failure: The message that a user will hear when being transferred on failure.

Hunt groups

Hunt groups in sipXecs are defined with the following information: name, extension (pilot number), description of the purpose, whether to allow forwarding to extensions users may have their phone forwarded to, sequencing of the hung group entries, their timeout values, and what to do on failure to reach any user (a fallback extension or go to the voicemail box of the last user in the list). The following table will assist with planning hunt groups:

Hunt Group	Engineering	
Hunt Group Extension	2301	
Hunt Group Description	General call to engineering department	
Allow Forwarding	Yes / No	
Sequence	**Extension**	**Expiration**
Initially Call	2010	30s
At Same Time	2012	30s
If No Response	2014	30s
Fallback / Voicemail	Yes	No

In the preceding example, the engineering hunt group has a pilot number of 2301. When a call is made to 2301, the extensions 2010 and 2012 ring for 30 seconds. After 30 seconds, the extension 2014 rings for 30 seconds. If the call is not answered, the user is directed to voicemail for the extension 2014.

Notice that no circular or linear hunt group is defined as we may have when data was collected. sipXecs does not support the concept of circular hunt groups. Additionally, extensions cannot be utilized in the above hunt group list more than once. If some sort of circular ringing is required, consider utilizing an ACD queue instead.

ACD queues

If ACD Queues are required in the new system, their detail needs to be thought out beforehand. The following table will help capture all of the information required for each ACD Queue:

ACD Queue Name	Sales	
Description	The sales ACD queue handle new sales requests from customers.	
Extension	2380	
Agent	**Extension**	**Name**
1	2012	ACD Agent 1
2	2015	ACD Agent 2
3	2013	ACD Agent 3
4	2017	ACD Agent 4
Overflow Type	Hunt Group / ACD Queue	
Overflow Destination	InsideSales	
Overflow Entry		
Call Routing Scheme	Ring All / Circular / Linear / Longest Idle	
Max Ring Delay	15 seconds	
Max Queue Length	10 callers	
Max Wait Time	180 seconds	
FIFO Overflow	Yes / No	
Answer Mode	Immediate	
Barge In	Yes	
Welcome Audio	"Thank you for calling XYZ Company. All of our Sales Associates are assisting other customers at this time. Please hold and an associate will be on the line momentarily."	

ACD Queue Name	Sales
Queue Audio	Music recording of some guitar player for 45 seconds followed by, "Please continue to hold and an agent will be with you shortly."
Audio Interval	50 seconds
Call Term Audio	"Due to high call volume, one of our external sales associates cannot take your call. We are transferring your call to the Inside Sales staff."
Term Tone Duration	
Agent Wrap Up Time	20 seconds
Agent Non-Resp Time	60 seconds
Max Bounce Count	3

The columns of the table can be explained as follows:

- Overflow type: Calls will either overflow to a hunt group or another ACD queue.
- Overflow destination: The destination will be a hunt group pilot number or the name of the overflow ACD queue.
- Overflow entry: If no hunt group or overflow queue is defined, the call can be transferred to this extension or SIP URI.
- Call routing scheme: The ACD call routing scheme that will be employed on this queue. The options are Ring All, Circular, Linear, and Longest Idle Agent.
- Maximum ring delay: This is the maximum time in seconds that the queue will allow an agent station to ring before a ring-no-answer condition is declared and the call is re-routed to a different agent.
- Maximum queue length: This is the maximum number of calls that are allowed to wait in this queue. If a call arrives at this queue and the resulting call count exceeds this number, then an overflow condition for this queue will be triggered. A value of "-1" disables this limit check.
- Maximum wait time: The maximum time in seconds that a call can reside in a queue. When a waiting call exceeds this time limit, an overflow condition for this queue will be triggered. A value of zero disables timeouts.
- FIFO overflow: If "Yes", then an overflow condition occurs and a First-In, First-Out (FIFO) scheme will be employed in order to determine which call will be moved to the configured overflow queue. If not set, then a Last-In, First-Out (LIFO) scheme will be employed.

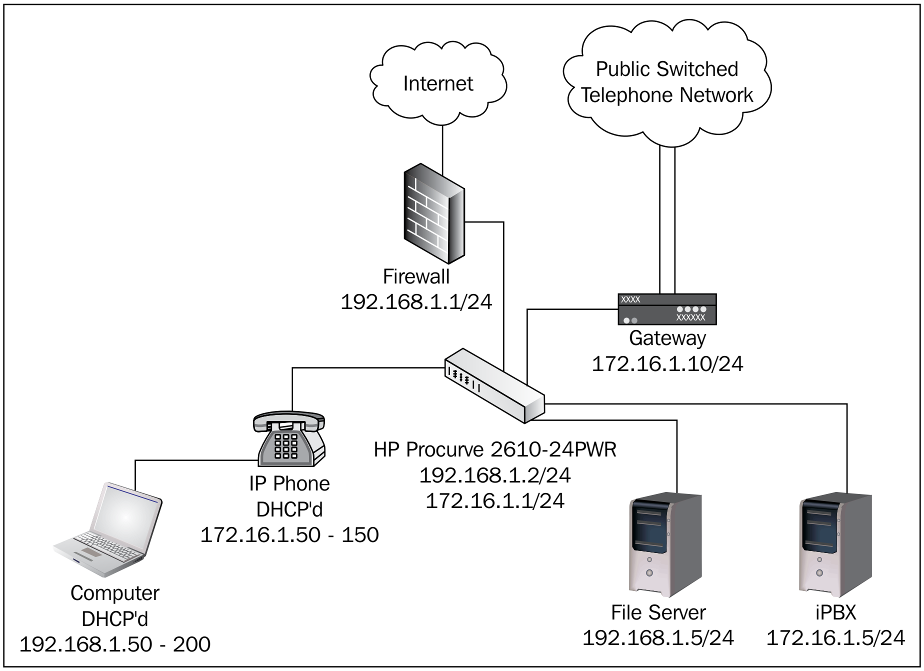
- Answer mode: If set to "Immediate", the call will be answered immediately upon arriving at this queue and the configured welcome-audio file will be played to the caller. Once the audio has completed, the queue will then attempt to route the call. If set to "Deferred", the queue will first attempt to route the call and if it is unable to immediately route the call, it will then be answered. If set to "Never", the call will not be answered while on this queue; but will be answered when actually connecting to an agent.
- Barge in: If set, the welcome audio will be terminated early should an agent become available while it is being played.
- Welcome audio: The welcome audio is a WAV file that is played to callers. If no file is specified, there will be silence.
- Queue audio: The queue audio is a WAV file that is played repeatedly to the caller until the queue either routes the call to an agent or to another queue.
- Audio interval: This is the interval in seconds before repeating the play of the specified queue audio. If the queue audio is actually longer than this time, it will be terminated and restarted from the beginning.
- Call termination audio: This is the WAV file message that is played to the caller when it has been determined that the call must be terminated. Once the audio has completed, the call will be dropped. If no audio is specified, then a busy tone will be played prior to terminating the call. The duration of the busy tone is specified by the termination-tone-duration attribute.
- Termination tone duration: This is the duration in seconds that the termination tone (busy tone) is to be played if no call-termination audio is specified and the call is to be dropped by the queue. A value of zero indicates that no tone is to be played prior to dropping the call.
- Agent wrap-up time: The period of time in seconds that has to pass before the ACD transfers a new call to an agent after a previous call has been completed. If set to 0, it will be disabled.
- Agent non-responsive time: The period of time in seconds that has to pass before the ACD transfers a new call to an agent after a previous call was not answered.
- Maximum bounce count: The number of rejected or non-answered calls an agent may have before being "bounced" (automatically signed out of the ACD queue). If set to 0, it will be disabled.

Network planning

Plan out the network changes required. Start with making some decisions about virtual networks and IP addressing. VLANs are strongly encouraged, though not required, for all of the reasons stated in the *Equipment selection* section of this chapter.

Physical network

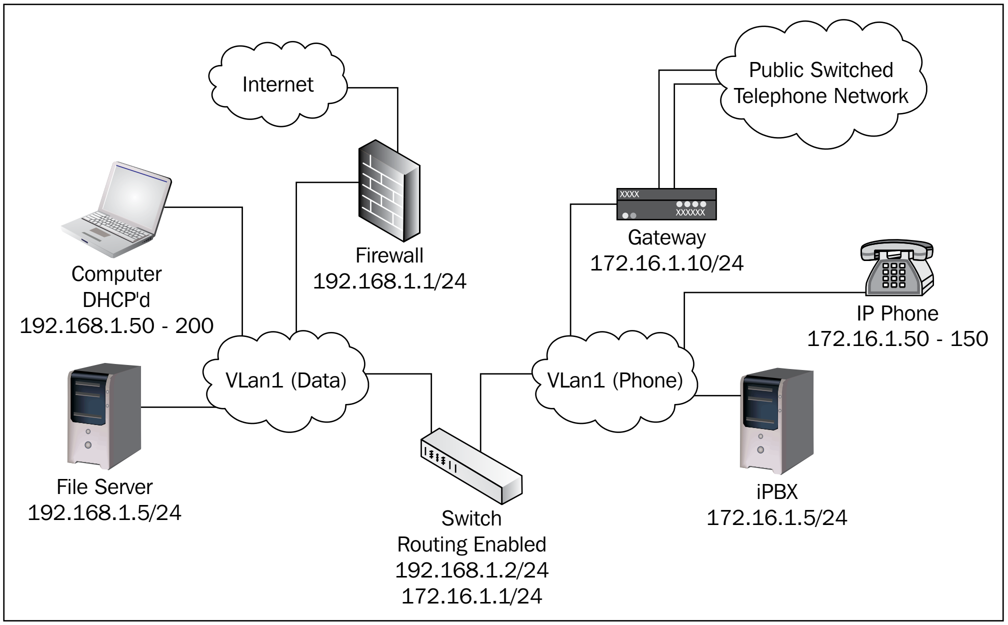
Plan the physical network connectivity by starting with a network diagram.
The following network diagram details the physical network's critical components and IP addressing information:



Virtual network

The virtual network diagram should look decidedly different from the physical network diagram. In planning the virtual network, pay particular attention to how routing between the data VLANs and phone VLANs will be handled. Not all firewalls are not able to route internal traffic. If this is the case with the firewall in use at the organization, the default gateway may need to be relocated to the Layer 3 switch (assuming that it can route between VLANs). This routing should be tested as the new network is deployed.

The following network diagram details the virtual network's critical components and IP addressing information:



Site preparations

Once the network diagram is complete, consider where all of the equipment is to be physically located as well as how it is connected. Identify any new network connections required to complete the new network configuration. Identify any services that need to be extended from the demarc to where the gateways will be located.

Verify that ample power supply is in each network closet and that adequately sized UPS equipment has been identified for each closet. Ensure that proper ventilation and/or cooling systems are in place in each closet.

Document additional network information

Some additional information should now be added to the site IP addressing table. One seemingly simple decision that needs to be made is what the SIP domain will be. This decision can have some wide-ranging implications.

One of the goals of a SIP system is to simplify communications. One way to help simplifying communications is by utilizing the same email and SIP phone addresses. For instance, if I want to email Bob Jones at XYZ Company, it would be very convenient if his email address and phone number were both `bjones@xyzcompany.com`.

In order to support this functionality, the external DNS hosting provider needs to support SRV records. Also, the network administrator for the internal network will need to maintain an internal copy of the external domain on the internal DNS server. The internal copy of the external DNS host names should reference internal IP addresses of local network resources instead of any external references that might be pointed at the organization's firewall.

Site Name	Site1
Internet Service Provider	Really Fast ISP
Support Contact #	1-800-555-5555
External DNS Domain	xyzcompany.com
External DNS Hosting Provider	Super Hosting Provider
DNS Provider support SRV Records?	Yes
External IP Addresses/Subnet Mask	xxx.xxx.xxx.xxx/255.255.255.248
External IP Address of Firewall	xxx.xxx.xxx.zzz
External Default Gateway	xxx.xxx.xxx.yyy
External DNS Servers	yyy.yyy.yyy.yyy., zzz.zzz.zzz.zzz
Internal IP Address Ranges/Subnet Mask	192.168.1.0/255.255.255.0
Internal Default Gateway	192.168.1.1
Internal DNS Server	192.168.1.5
Internal DNS Domain	corp.xyzcopany.com
Internal DHCP Server / type	192.168.1.5/Microsoft
Internal DHCP Range	192.168.1.50 – 192.168.1.200
Internal Router to Phone VLAN	192.168.1.2
Data VLAN Number	1
Phone VLAN Number	2
Phone VLAN IP Address / Subnet Mask	172.16.1.0/255.255.255.0
Phone VLAN Default Gateway	172.16.1.1

Site Name	Site1
SIP Domain	xyzcompany.com
sipXecs PBX Host Name	sipx.xyzcompany.com
IP Address of PBX	172.16.1.5/255.255.255.0
IP Addresses of Local Gateway(s)	172.16.1.10/255.255.255.0
Notes	

Summary

A lot of ground was covered in this chapter. Data was collected about the existing systems, equipment selection was covered, and the phone system programming was planned.

3
Installing sipXecs

sipXecs can be installed by compiling for a specific Linux distribution, by RPM to an existing Linux installation or from a single CD ISO installer (an ISO is an image file of a CD that be used to burn a CD). This installation chapter will focus only on the single CD ISO installer. Methods for installing from RPM or compiling sipXecs from source can be found in the sipXecs Wiki (linked at `http://www.sipfoundry.org`). This chapter will cover:

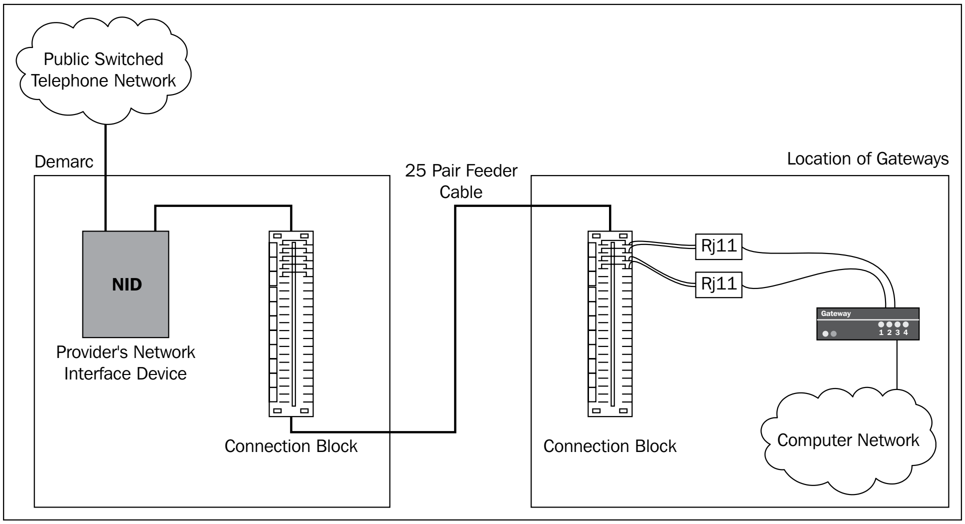
- Completing the cabling requirements
- Completing the network infrastructure requirements
- Installing sipXecs

Complete cabling requirements

Make sure that the network drops are available wherever phones are required. Review the notes collected for each user and phone to make sure that none are missed. By utilizing network drops for standard analog phones as well as IP phones, future cabling may not be required if an IP phone is desired at some point.

In most cases the demarc is in a location that is not particularly well suited for computer equipment. Extend the demarc where the gateways will be located. In the location of the gareway(s), the phone lines are broken out according to the type of connection required by the selected gateways. For example, most analog gateways require RJ-11 plugs, so have the phone lines broken out onto RJ-11 plugs so that typical phone patch cords can be used to connect to the gateway(s).

The following diagram illustrates how connection blocks are utilized along with a 25 pair feeder cable to extend the demarc to where the gateway equipment will be located.



Ensure that lightning protection is inserted on every phone line connecting to the system. Lightning protection can be located between the NID and the connection block, or just before the gateway.

Establish and test any new network connections between the network closets that will be required for any new network equipment.

Complete network requirements

Build out the network infrastructure according to the plan established in Chapter 2. Take care to verify that VLANs are configured properly and the QoS settings that will be required by the phones are set up according to the manufacturer's guidelines.

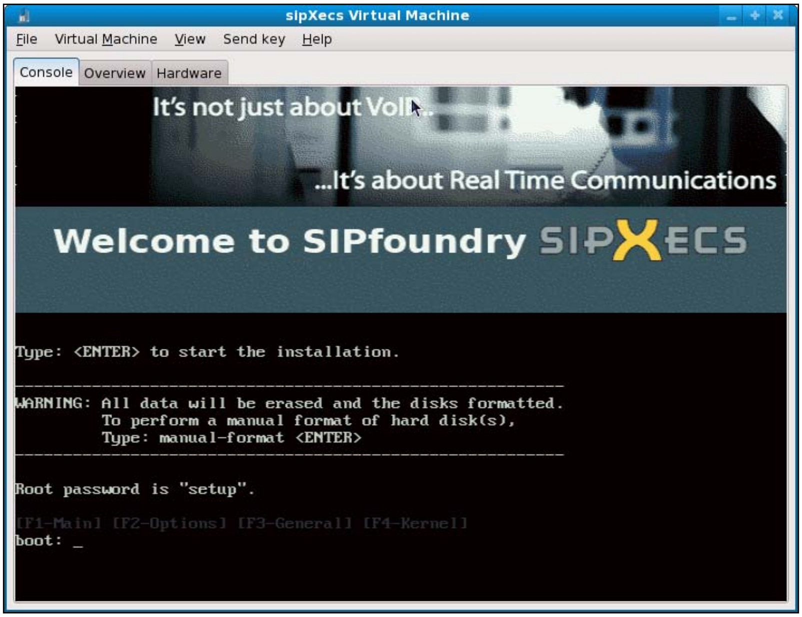
If virtual networks are being established, configure all trunking between switches. The PBX and gateways will not be able to tag their traffic for specific VLANs. Ensure that some ports are available that are natively configured (untagged) to exist in the phone VLAN. It is also a good idea to configure an extra port natively set in the phone VLAN for testing purposes.

If DHCP and DNS services are not going to be configured on the sipXecs server, it is important to have them configured and operational before installing sipXecs.

Installing sipXecs

Installation from the single CD installer is by far the easiest method. The single CD ISO can be obtained from the sipXecs Wiki. The easiest way to locate the Wiki is from the navigation bar at the SIPFoundry web site (`http://www.sipfoundry.org`). Download the latest stable release of the PBX ISO and burn it to a CD-ROM (`http://sipxecs.sipfoundry.org/pub/sipXecs`).

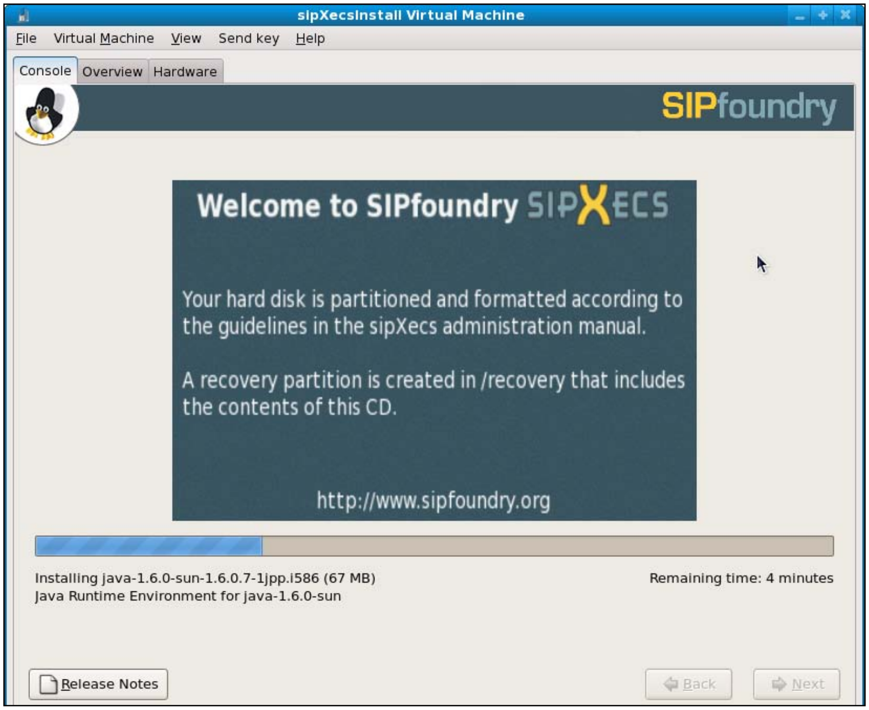
Insert the CD into the PBX computer and boot from it.



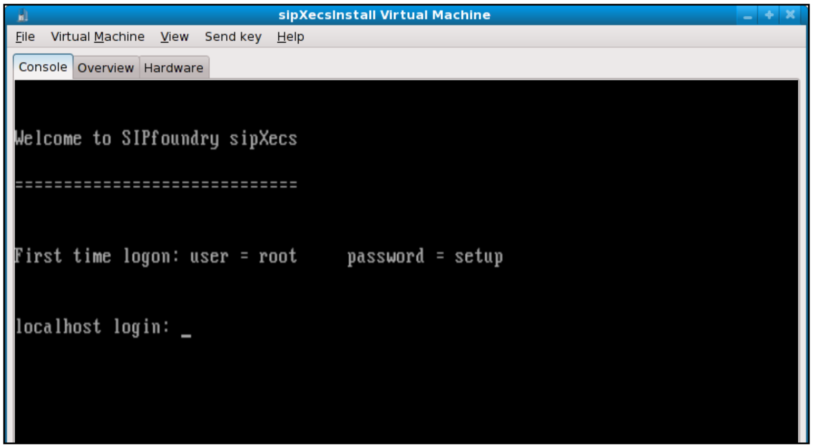
Press the *Enter* key and installation will begin.

> The installation will erase and format the hard drives in the computer. If the server that is being utilized has an IDE drive, instead of pressing *Enter*, enter `manual-format` at the `boot:` prompt.

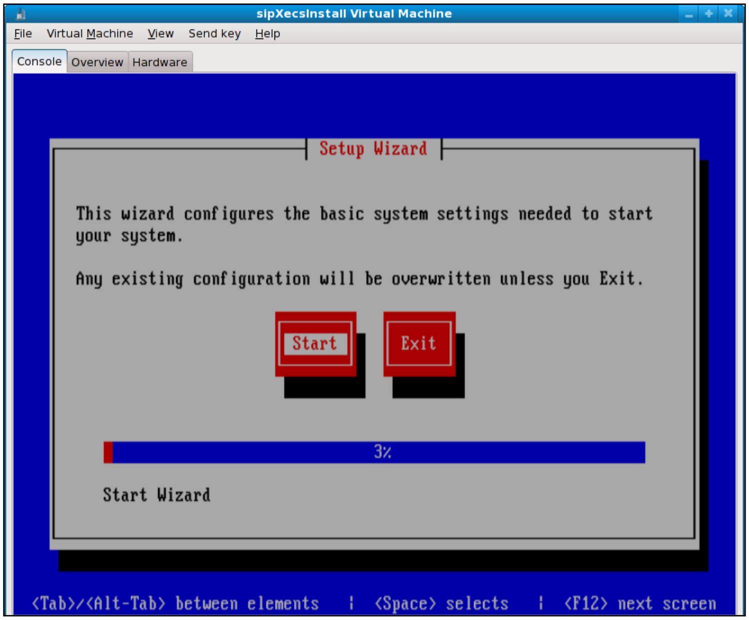
Installation will begin and the preceding screen will be displayed with a progress bar indicating approximately how much of the installation is complete.



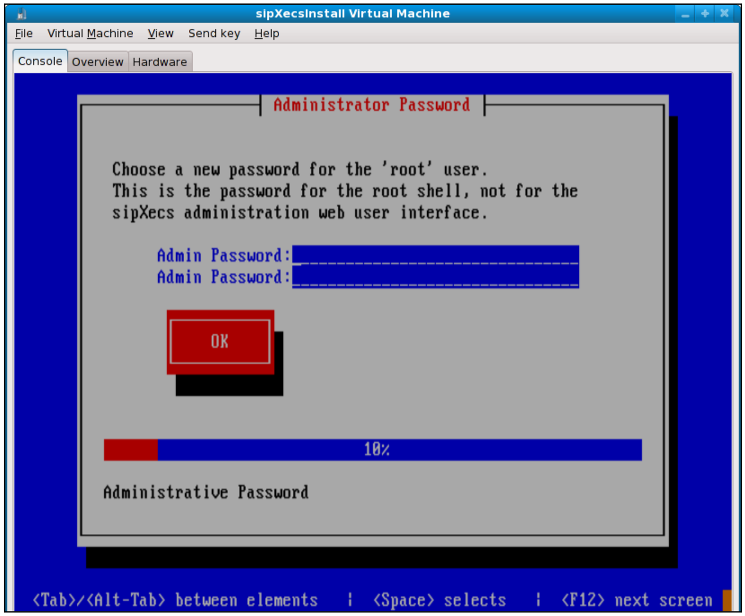
Once the initial part of the installation is complete, the server will reboot and the Linux login screen will appear.



As prompted, for the first time that you **logon**, enter **root** and press the *Enter* key and then enter the **password** as **setup**.

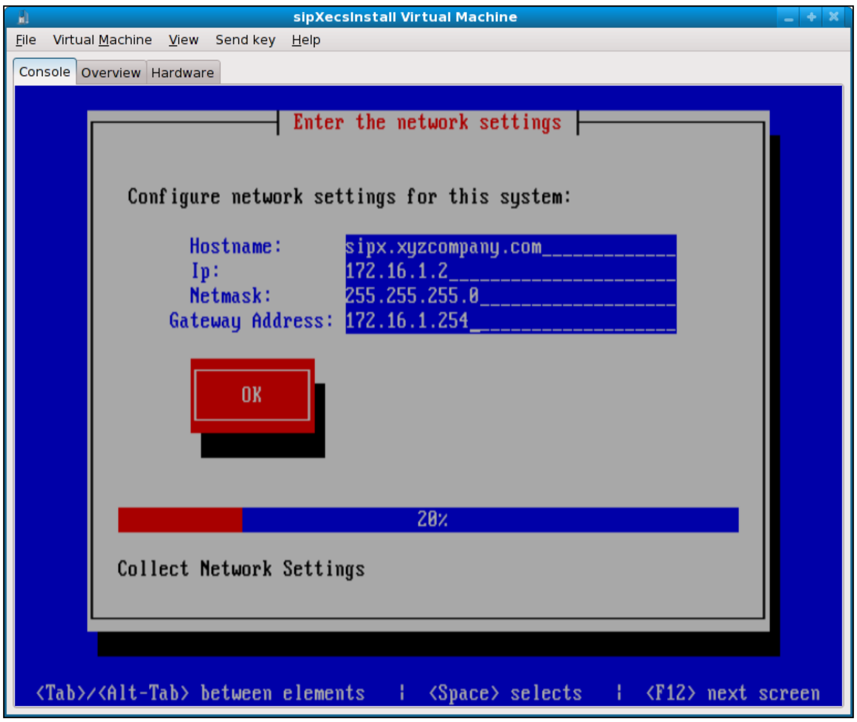


The first screen of the **Setup Wizard** will then appear, prompting you to press *Spacebar* or *Enter* to select **Start**.



The first piece of information entered is the password to be assigned to the system root user. The root user is the Linux system "superuser" account, which is used to administer the system. This account password should be reasonably complex and guarded. Enter the password twice and press the *Tab* key to select the **OK** button and press *Enter*.

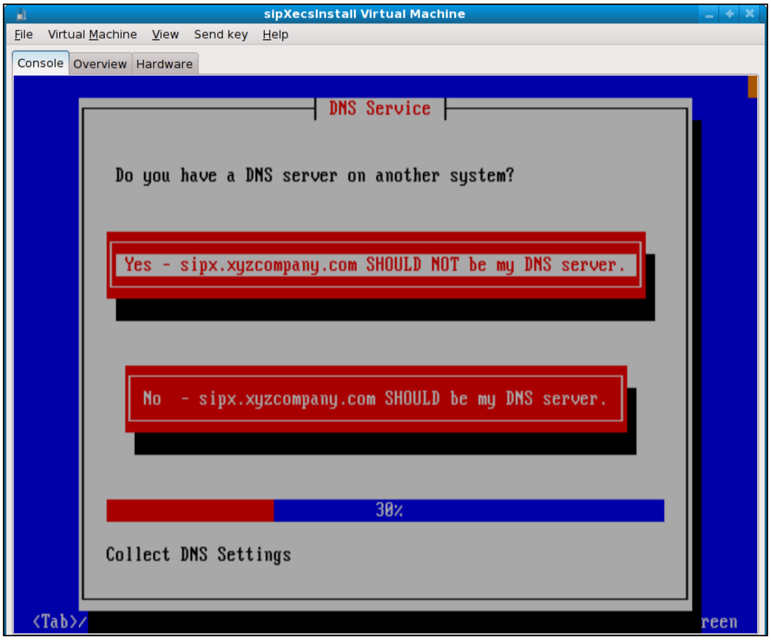
The next screen will require some information from the *Network planning* section of Chapter 2. These are important settings that are required to interoperate with existing network equipment, so revisit Chapter 2 if there are any questions.



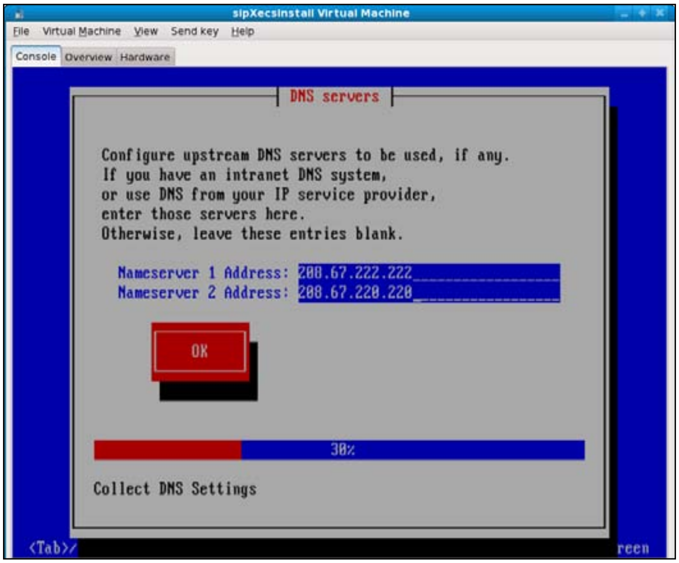
For the **Hostname**, enter the **Fully Qualified Domain Name** (**FQDN**) of the PBX. The FQDN is a concatenation of the hostname and the domain name. Enter the IP address of the PBX, the subnet mask, and the PBX's default gateway address. *Tab* to the **OK** button and press *Enter*.

If you fully understand how to configure DNS, you can elect to configure your own services. If you are unfamiliar with these services, sipXecs can configure and host them for you. If your system is on its own VLAN or operates isolated from an existing data network, it is suggested that you allow sipXecs to provide both DNS and DHCP services for the communications system network.

On the following screen, use the *Tab* key to select **YES** if you will use your own DNS server, or **NO** to have sipXecs as your DNS server (recommended). Use the *Spacebar* or *Enter* to make the selection.

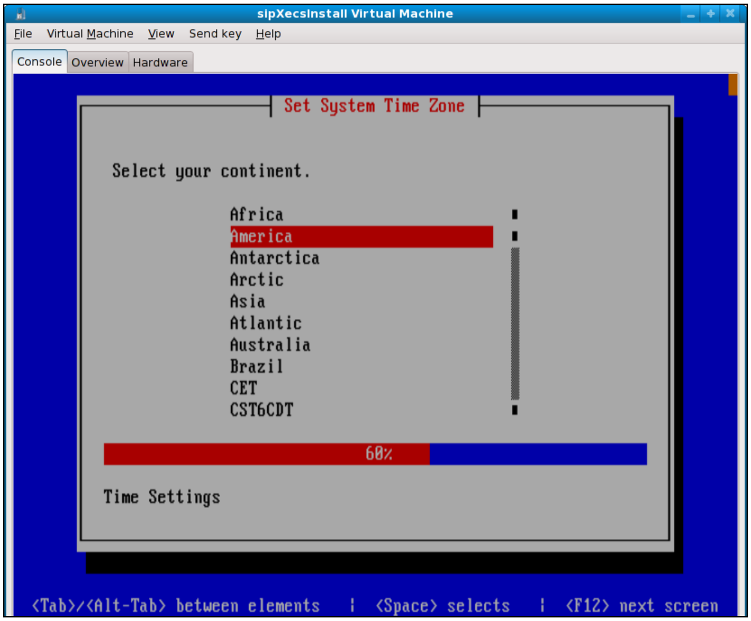


The next screen (shown below) asks for DNS servers for forward lookup. `OpenDNS.com`'s DNS servers were entered as an example.

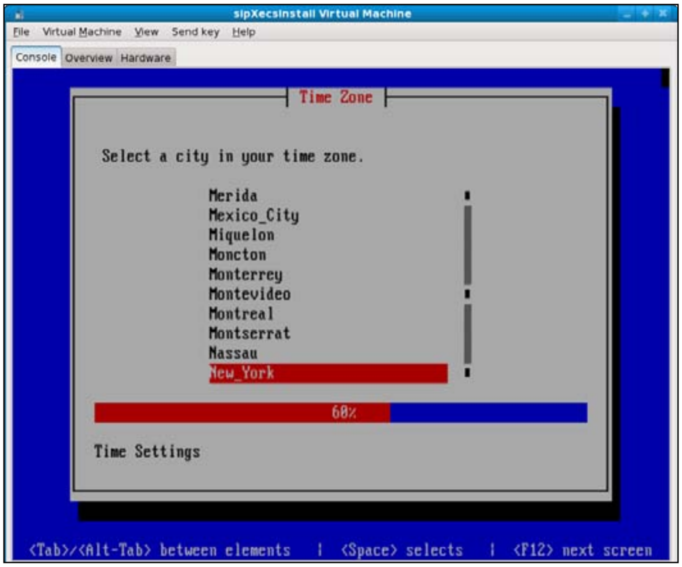


Press the *Tab* key to select the **OK** button and press the *Spacebar* or *Enter*.

To get correct time, proper time zone settings are important for the PBX. Scheduled call forwarding, time stamps on messages, and other system services depend on accurate time.

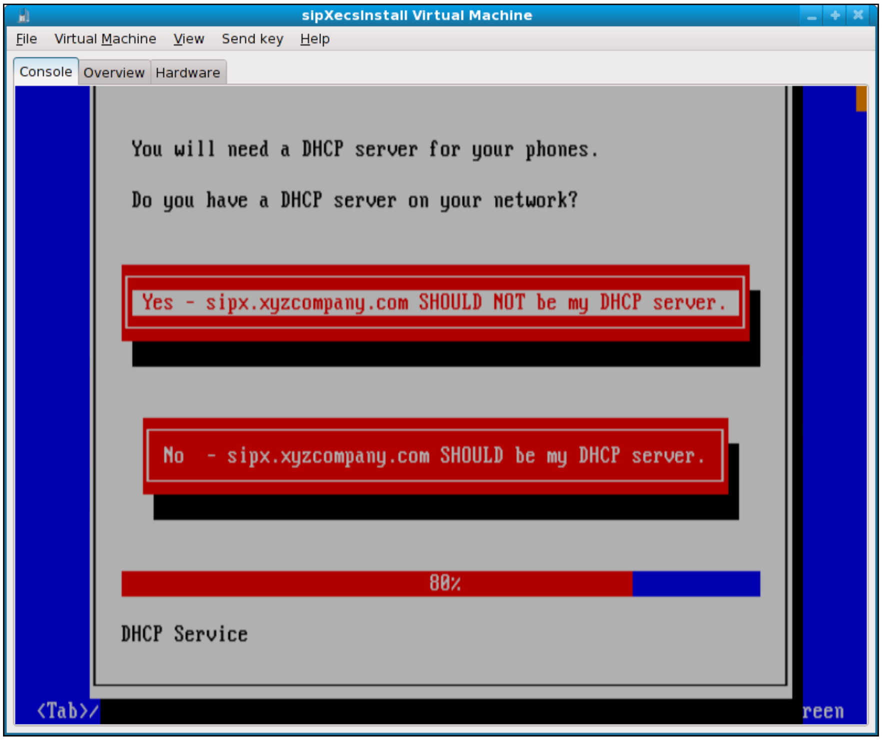


For time purposes, select the continent on which the iPBX will be used.



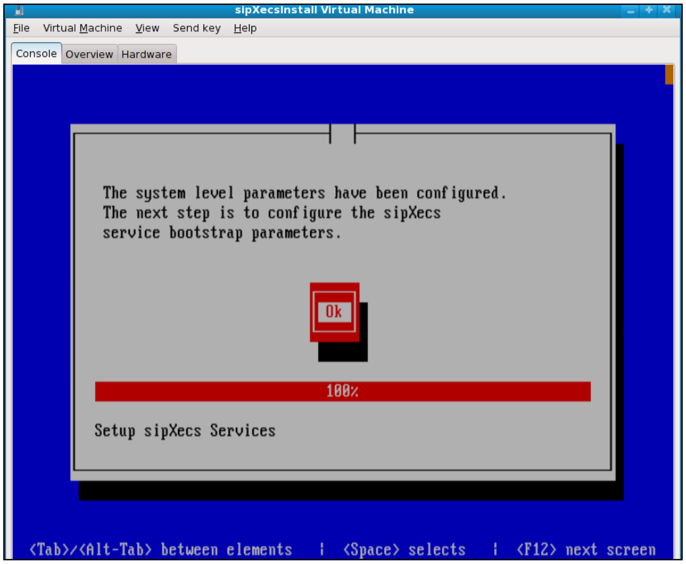
Next, select a city in the same time zone as the sipXecs server and press *Enter*.

The screenshot shown below will allow you to utilize your own DHCP server or have sipXecs as the DHCP server for the network. Again, as with the DNS services, if your system is on its own VLAN or operates isolated from an existing data network, it is suggested that you allow sipXecs to provide both DNS and DHCP services for the communications system network.



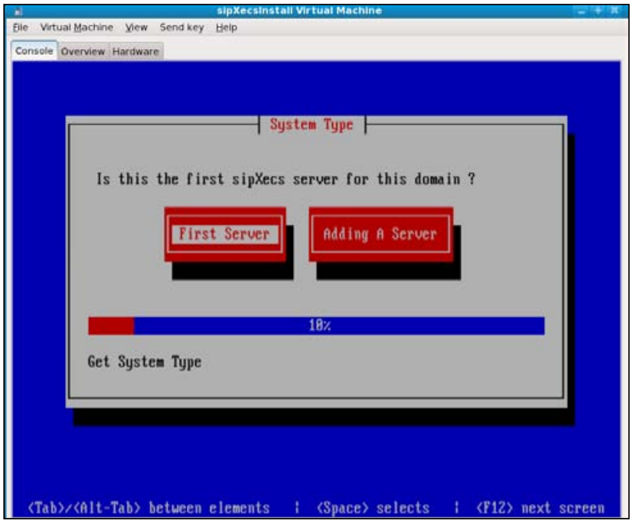
Use the *Tab* key to select **Yes** or **No**, and to continue.

The next screen confirms that system-level settings are configured and we will now begin configuring service bootstrap parameters. Service bootstrap parameters are base settings for the sipXecs system.



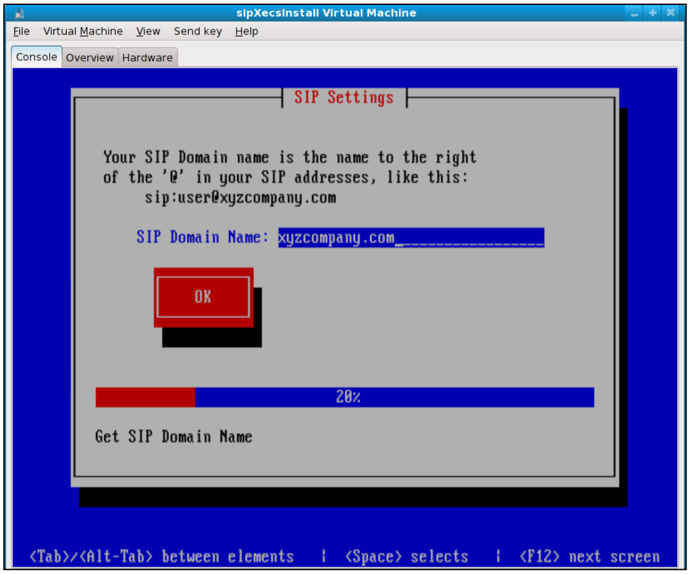
Press the *Enter* key to continue.

The first configuration item identifies if it is the first sipXecs server or if we are adding another clustered system. Clustering allows many sipXecs servers to act as a single system for high availability and load balancing. See *High availability installation* later in this chapter.



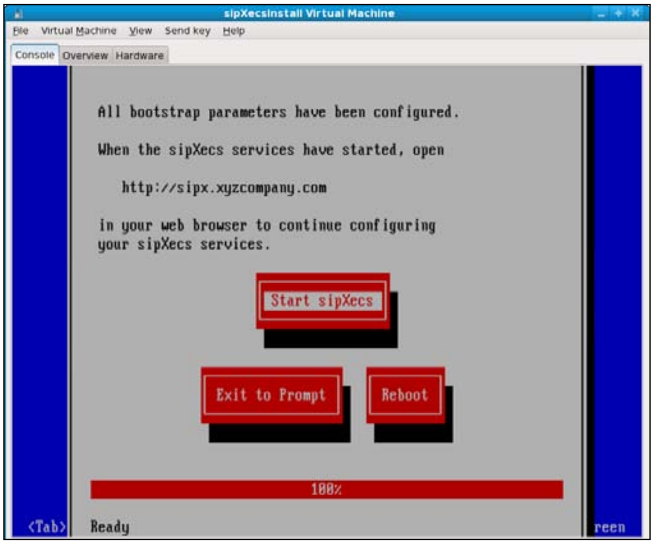
Press the *Enter* key to select the **First Server** option.

Next, enter the **SIP Domain Name**. The setup wizard will attempt to interpret this from the FQDN that was entered earlier.



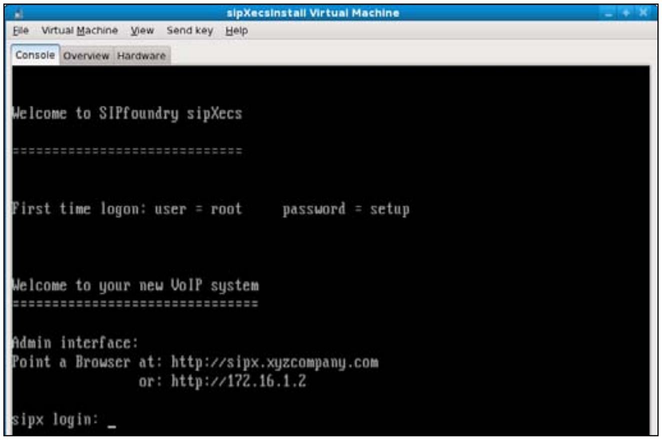
Tab to the **OK** button and press *Enter*.

All services have now been configured. The services can be started or the system rebooted. A reboot is recommended.



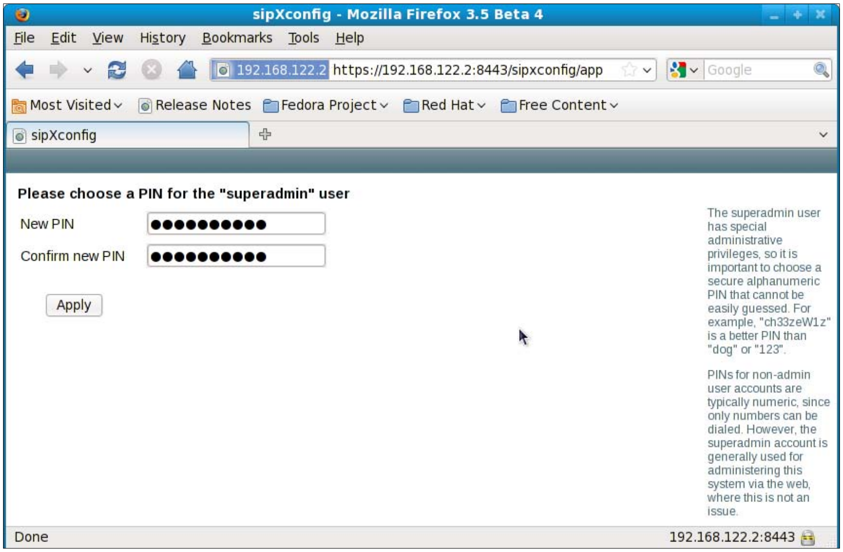
Press the *Tab* to the **Reboot** button and press *Enter*.

Remove the installation CD and wait for the system to reboot to the login screen.

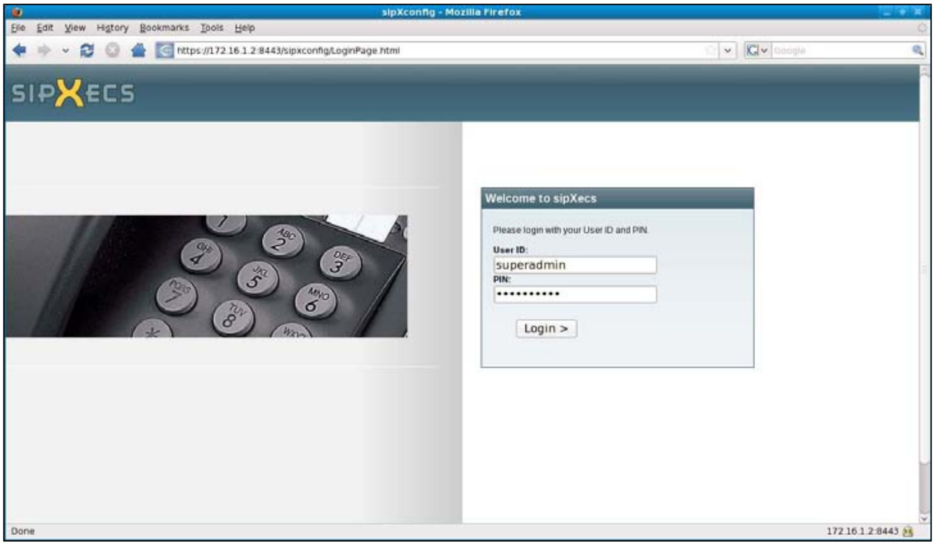


sipXecs is now installed and ready for configuration. To make sure that the sipXecs host system operates as efficiently as possible, a Linux GUI is not installed on the server. All of the administration for sipXecs is handled with a web GUI frontend called *sipXconfig*. Since there is no GUI on the server, (from another computer on the network) start a web browser and in the address bar enter the IP address or hostname of the sipXecs iPBX.

The administrator will be prompted to enter a new PIN (password) for the "superadmin" user when the sipXconfig is accessed for the first time.



Enter a secure alphanumeric PIN (twice) that cannot be easily guessed and click on the **Apply** button.



At this point, sipXconfig is ready for the administrator to begin configuring the system.

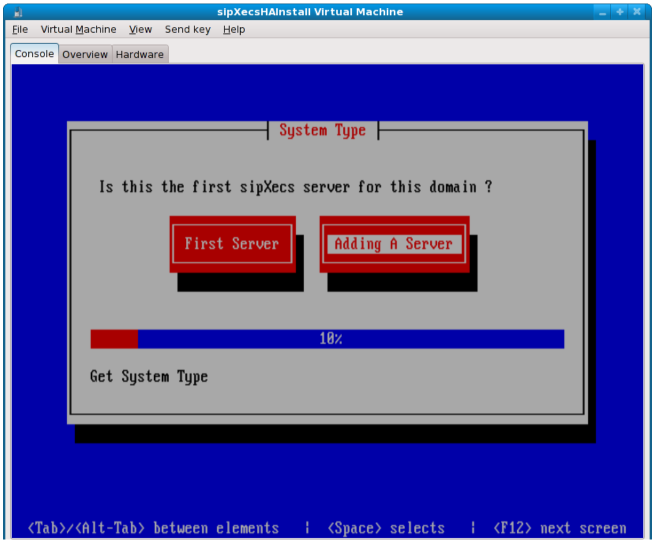
High availability installation

The installation wizard is able to install and configure a highly available system that consists of two physically separate servers. A **High Availability** (**HA**) system consists of a master server and a distributed server. Failover is taken care of by utilizing DNS SRV records that include information about master and distributed servers. The HA system allows redundancy of the call control system and load balancing of traffic. Media services such as voicemail, auto attendant, and other services such as ACD and sipXconfig are not redundant and will only run on one of the master server.

For a high availability installation, the master server must be installed and configured first. The installation procedure is similar to the steps taken in the previous section to install and configure a non-redundant system. Configuring the distributed servers of the cluster begins at the bootstrap portion of the setup. It is required that you run DNS and NTP services both on the master and distributed system unless you have a different setup that provides these services in a reliable way to both systems.

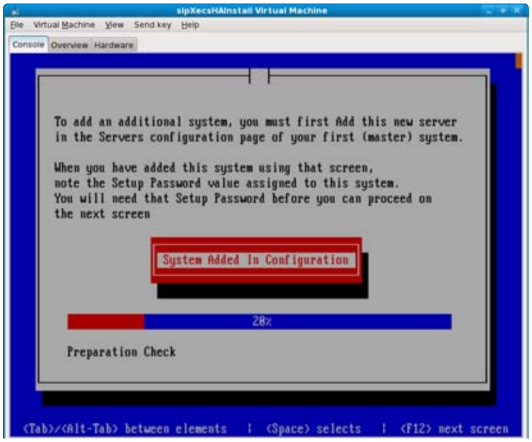
Install and configure the distributed server

The installation of the distributed server begins during the bootstrap portion of the installation. Configure the distributed server with a different IP address, enable DNS services, make sure that the DNS server used for forwarding DNS requests can resolve the name of the master server (use the master server IP if DNS is enabled on that server), and do not enable DHCP services if another server on the same network is handling DHCP requests.

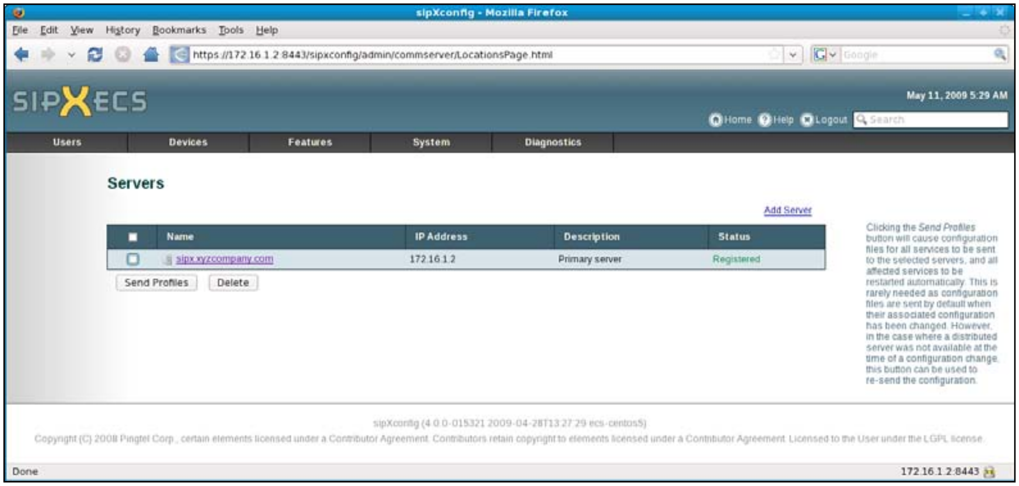


Use the *Tab* key to move to the **Adding A Server** option and press *Spacebar* or *Enter*.

The following screenshot prompts the administrator to first add the new server on the master server (first server installed).

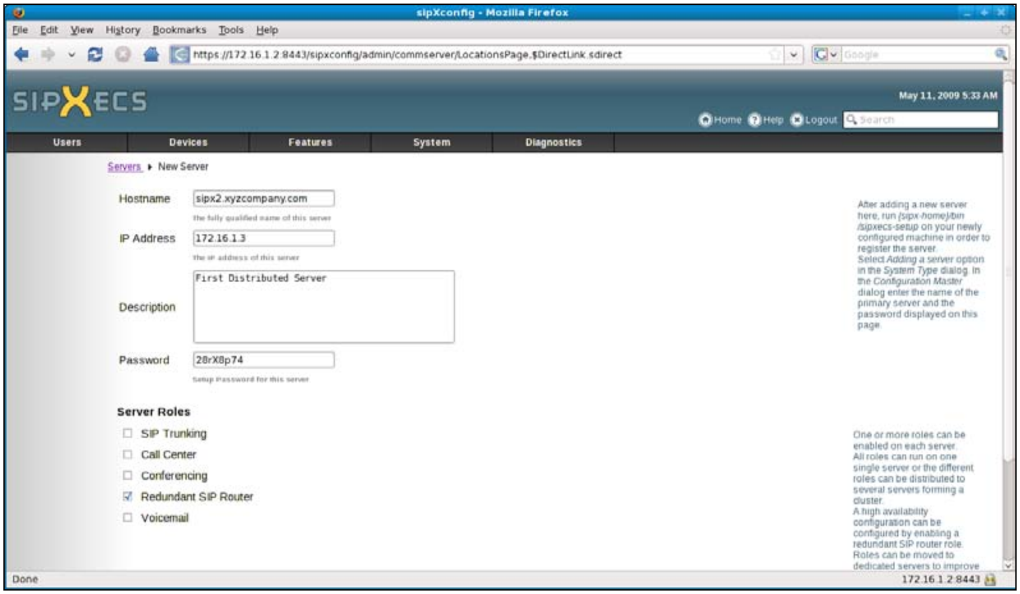


Before pressing any key on the distributed server that is being set up, open a web browser and log in as "superadmin" to the system administration for the master server. Click on the **System** menu and select the **Servers** menu item to display the following page:



Click on the **Add Server** hyperlink above the **Status** column.

The **New Server** page will then be displayed as seen in the following screenshot:



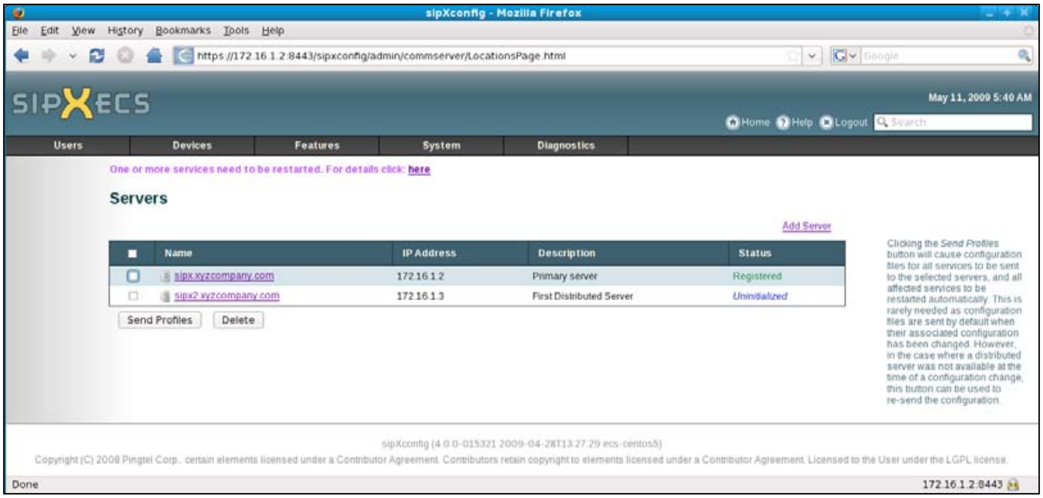
Enter the **Hostname** for the new server (this should be the fully qualified domain name). Next, enter the IP **Address** and a **Description** of the new server. A random password is generated and is displayed in the **Password** field. Write this password down as you will need it on the distributed server.

One or more roles can be enabled on each server. All roles can run on one single server or different roles can be distributed to several servers forming a cluster.

A high availability configuration can be configured by only enabling a redundant SIP router role. Roles can be moved to dedicated servers to improve performance.

Click on the **OK** button to add the new server.

The system administration session will return to the **Servers** page, shown next:

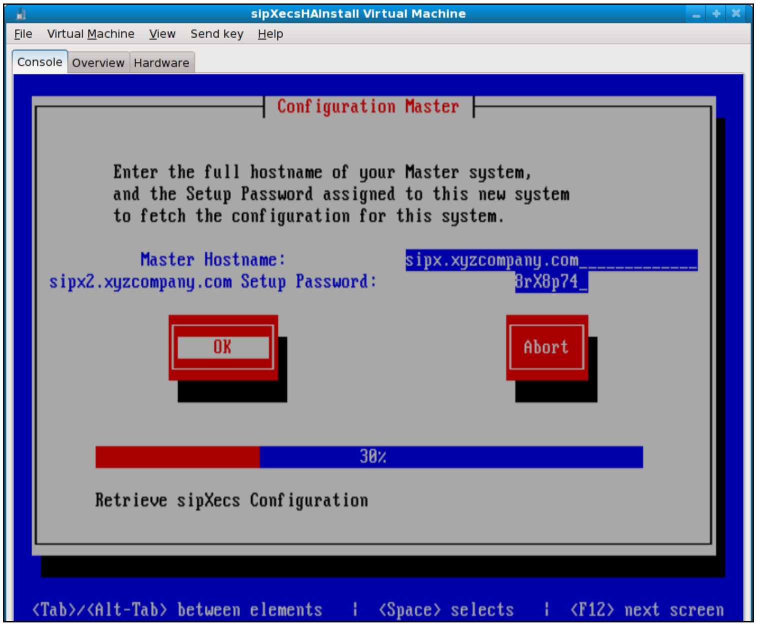


If prompted at the top of the screen, click on the **here** hyperlink to restart the services that need to be restarted.

The **First Distributed Server** will appear in the list of servers and have a **status** of **Uninitialized**.

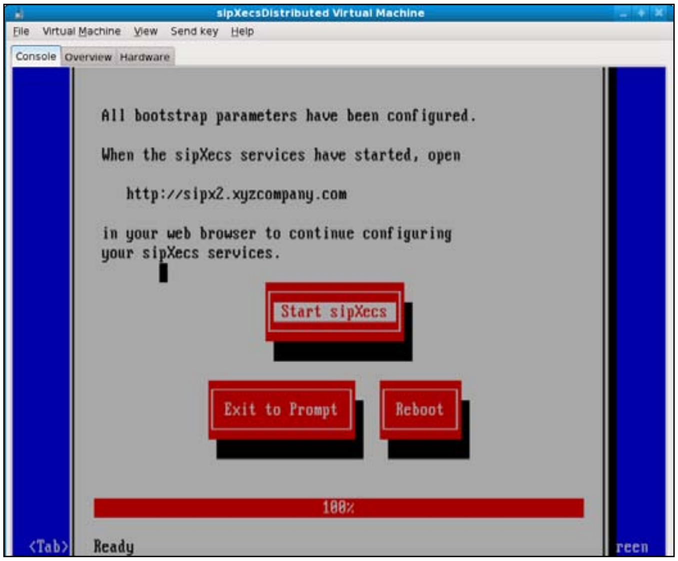
Return to the distributed server's console setup routine and press *Enter*.

The setup will then display the following screen requesting information about the master server:



For the **Master Hostname**, enter the FQDN of the master server and then enter the server setup password that was noted when the server was added on the master system. Press *Tab* to move to **OK**. Press *Space* or *Enter* to select the option.

The installation wizard will now complete the setup and pull required information from the master server.



Press *Tab* to move to the **Reboot** option and press *Enter* to reboot the completed system.

Verify DNS and DHCP operation

Before continuing with the installation process, it is important that DNS and DHCP are both operating properly. sipXecs relies heavily on DNS, especially for HA installation, to function properly.

Single PBX testing

Log in to the PBX as the 'root' user. Verify that all of the following commands return the expected results:

`ping sipx`

`ping sipx.your.domain`

`dig -t A sipx.your.domain`

`dig -t SRV _sip._tcp.your.domain`

`dig -t SRV _sip._udp.your.domain`

The following are the expected results for each of the above PING tests (expect different IP addresses and domain names; press *Ctrl*+*C* to break continuous PING):

```
[root@sipx ~]# ping sipx
PING sipx.xyzcompany.com (172.16.1.2) 56(84) bytes of data.
64 bytes from sipx.xyzcompany.com (172.16.1.2): icmp_seq=1 ttl=64
time=0.043 ms
64 bytes from sipx.xyzcompany.com (172.16.1.2): icmp_seq=2 ttl=64
time=0.031 ms
64 bytes from sipx.xyzcompany.com (172.16.1.2): icmp_seq=3 ttl=64
time=0.029 ms
64 bytes from sipx.xyzcompany.com (172.16.1.2): icmp_seq=4 ttl=64
time=0.033 ms
--- sipx.xyzcompany.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.029/0.034/0.043/0.005 ms
```

Note that the first line returned should return the FQDN of the PBX and not just the host name.

```
[root@sipx ~]# ping sipx.xyzcompany.com
PING sipx.xyzcompany.com (172.16.1.2) 56(84) bytes of data.
64 bytes from sipx.xyzcompany.com (172.16.1.2): icmp_seq=1 ttl=64
time=0.043 ms
```

```
64 bytes from sipx.xyzcompany.com (172.16.1.2): icmp_seq=2 ttl=64
time=0.031 ms
64 bytes from sipx.xyzcompany.com (172.16.1.2): icmp_seq=3 ttl=64
time=0.029 ms
64 bytes from sipx.xyzcompany.com (172.16.1.2): icmp_seq=4 ttl=64
time=0.033 ms

--- sipx.xyzcompany.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.029/0.034/0.043/0.005 ms
```

The first DIG test checks that the FQDN is working properly. The test should return results similar to the following:

```
[root@sipx ~]# dig -t A sipx.xyzcompany.com

; <<>> DiG 9.3.4-P1 <<>> -t A sipx.xyzcompany.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22369
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:
0

;; QUESTION SECTION:
;sipx.xyzcompany.com.                IN      A

;; ANSWER SECTION:
sipx.xyzcompany.com.         86400   IN      A       172.16.1.2

;; AUTHORITY SECTION:
xyzcompany.com.              86400   IN      NS      ns1.xyzcompany.
com.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 27 06:46:23 2008
;; MSG SIZE  rcvd: 65
```

The next DIG test checks the operation of the SIP TCP service record for the SIP domain.

```
[root@sipx ~]# dig -t SRV _sip._tcp.xyzcompany.com

; <<>> DiG 9.3.4-P1 <<>> -t SRV _sip._tcp.xyzcompany.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12430
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:
1

;; QUESTION SECTION:
;_sip._tcp.xyzcompany.com.           IN      SRV
```

```
;; ANSWER SECTION:
_sip._tcp.xyzcompany.com.     86400   IN      SRV     1 0 5060 sipx.
xyzcompany.com.

;; AUTHORITY SECTION:
xyzcompany.com.               86400   IN      NS      ns1.xyzcompany.
com.

;; ADDITIONAL SECTION:
sipx.xyzcompany.com.          86400   IN      A       172.16.1.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 27 06:56:17 2008
;; MSG SIZE  rcvd: 103
```

The last DIG test checks the operation of the SIP UDP service record for the SIP domain.

```
[root@sipx ~]# dig -t SRV _sip._udp.xyzcompany.com
; <<>> DiG 9.3.4-P1 <<>> -t SRV _sip._udp.xyzcompany.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33618
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:
1

;; QUESTION SECTION:
;_sip._udp.xyzcompany.com.            IN      SRV

;; ANSWER SECTION:
_sip._udp.xyzcompany.com.     86400   IN      SRV     1 0 5060 sipx.
xyzcompany.com.

;; AUTHORITY SECTION:
xyzcompany.com.               86400   IN      NS      ns1.xyzcompany.
com.

;; ADDITIONAL SECTION:
sipx.xyzcompany.com.          86400   IN      A       172.16.1.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 27 07:00:37 2008
;; MSG SIZE  rcvd: 103
```

To test DHCP functionality, connect a computer to the same network as the PBX (that is, if the PBX is in a phone VLAN, connect the computer to that VLAN). Verify that the computer gets an appropriate IP address from the DHCP service on the PBX and that the DNS domain name of the computer is the same as the SIP domain name.

If testing from a Linux or Mac-based system, utilize the same commands as just described to test DNS functionality. The same results are expected.

If testing from a Windows based system, use the following command to test DNS functionality from a DOS command line:

```
ping sipx
ping sipx.your.domain
 nslookup
 >set q=srv
 _sip._tcp.your.domain
 _sip._udp.your.domain
quit
```

Following are the expected results for each of the above DOS command-line PING tests (expect different IP addresses and domain names):

```
F:\>ping sipx

Pinging sipx.xyzcompany.com [172.16.1.2] with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time=181ms TTL=62
Reply from 172.16.1.2: bytes=32 time=101ms TTL=62
Reply from 172.16.1.2: bytes=32 time=124ms TTL=62
Reply from 172.16.1.2: bytes=32 time=147ms TTL=62

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 101ms, Maximum = 181ms, Average = 138ms
```

Note that the first line returned should return the FQDN of the PBX and not just the host name.

```
F:\>ping sipx.xyzcompany.com

Pinging sipx.xyzcompany.com [172.16.1.2] with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time=181ms TTL=62
Reply from 172.16.1.2: bytes=32 time=101ms TTL=62
Reply from 172.16.1.2: bytes=32 time=124ms TTL=62
Reply from 172.16.1.2: bytes=32 time=147ms TTL=62

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 101ms, Maximum = 181ms, Average = 138ms
```

The `nslookup` tests are combined as follows:

```
F:\>nslookup
Default Server:  sipx.xyzcompany.com
Address:  192.168.100.10

> set q=srv
> _sip._tcp.xyzcompany.com
Server:  sipx.xyzcompany.com
Address:  172.16.1.2

_sip._tcp.xyzcompany.com      SRV service location:
          priority       = 0
          weight         = 0
          port           = 5060
          svr hostname   = sipx.xyzcompany.com
sipx.xyzcompany.com   internet address = 172.16.1.2
> _sip._udp.xyzcompany.com
Server:  sipx.xyzcompany.com
Address:  172.16.1.2

_sip._udp.xyzcompany.com      SRV service location:
          priority       = 0
          weight         = 0
          port           = 5060
          svr hostname   = sipx.xyzcompany.com
sipx.xyzcompany.com   internet address = 172.16.1.2
> quit
```

The expected results are very similar to the results obtained earlier from the Linux DNS tests.

High availability PBX testing

Testing DNS functionality for an HA installation is similar to the testing for a single PBX. The results for the SRV record tests, however, should return a series of records with their priority and weight with the master server being preferred over the distributed server. Log in to each of the PBXs as the 'root' user. Verify that all of the following commands return results similar to those in the *Single PBX testing* section covered earlier:

```
ping sipx1
ping sipx2
ping sipx1.your.domain
ping sipx2.your.domain

dig -t A sipx1.your.domain
```

```
dig -t A sipx2.your.domain
dig -t SRV _sip._tcp.your.domain
dig -t SRV _sip._udp.your.domain
```

The DIG service record tests (those beginning with `dig -t SRV`) should again return information similar to the DIG tests in the *Single PBX testing* section except that two servers with different IP addresses and priorities will be in the DIG answer.

To test DHCP functionality, connect a computer to the same network as the PBX (that is, if the PBX is in a phone VLAN, connect the computer to that VLAN). Verify that the computer gets an appropriate IP address from the DHCP service on the PBX and that the DNS domain name of the computer is the same as the SIP domain name.

If testing from a Linux or Mac-based system, utilize the same commands as above to test DNS functionality. The same results are expected.

If testing from a Windows-based system, use the following command to test DNS functionality from a DOS command line:

```
ping sipx1
ping sipx2
ping sipx1.your.domain
ping sipx2.your.domain
```

```
 nslookup
 >set q=srv
 _sip._tcp.your.domain
 _sip._udp.your.domain
```

The `nslookup` tests, like the DIG tests, should return information similar to the `nslookup` tests above in the *Single PBX testing* section except that two servers with different IP addresses and priorities will be in the results.

Summary

In this chapter you have learned to install the base PBX operating system and software. You have also learned some important testing steps for verifying DNS and DHCP functionalities. A robust infrastructure should now be in place on which the communication system can be built.

4
Configuring Users

Managing users on any type of system, be it a computer network or phone system, consumes much of an administrators time. Users come and go, get married and change their name, change locations, and come up with needs that we, as administrators, could never dream of. In this chapter we'll get in depth with the following:

- Creating and managing user accounts
- Managing the extension pool
- Utilizing user groups
- Importing users

Creating users

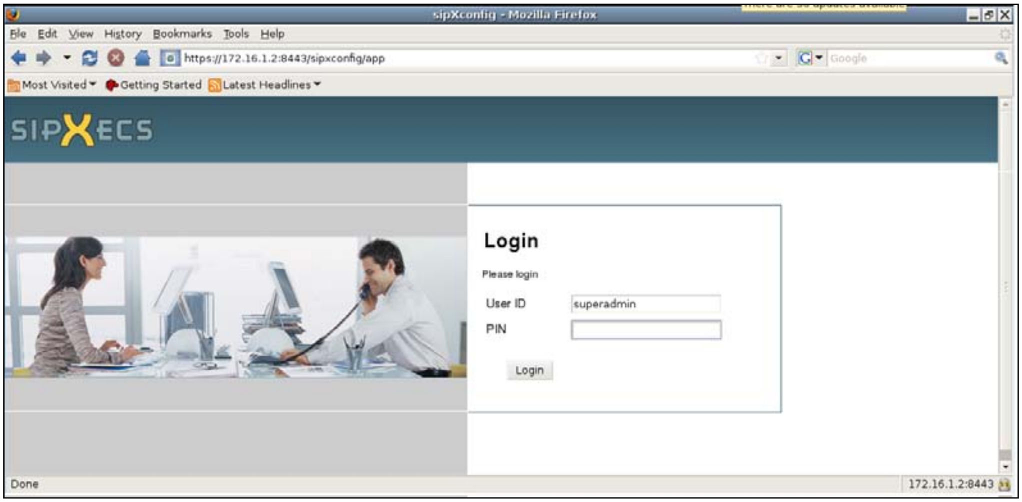
A user ID on a sipXecs system is typically an extension. By default, the system is configured for three digits starting at 200 (100 is the default auto attendant and 101 is the VoiceMail pilot number). Automatic extension numbering is controlled by the extension pool.

User IDs are not limited to numeric values. The administrative account "superadmin" is an example of a user account that is non-numeric.

If four or more digit extensions are required by the organization, there are two changes that should be made before users are added to the system (however, they can be changed later without problems). The extension pool and the internal extension length values should be set.

Extension pool

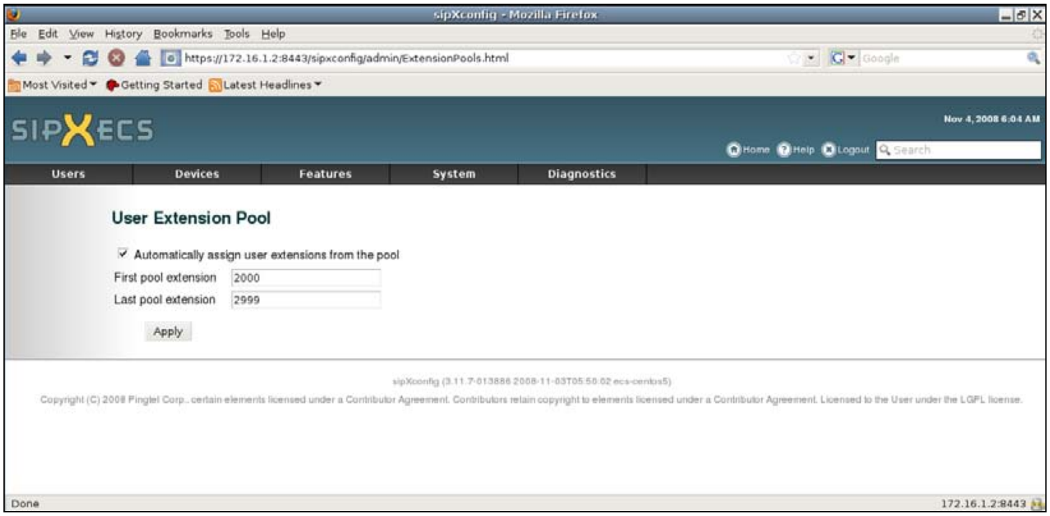
As mentioned earlier, the extension pool controls the automatic numbering of extensions (user accounts). To modify the extension pool, connect to the system with your favorite web browser at the IP address specified for the PBX.



Log in as the **superadmin** user by putting the password chosen earlier in the PIN field and clicking on the **Login** button.

The following screen will appear:

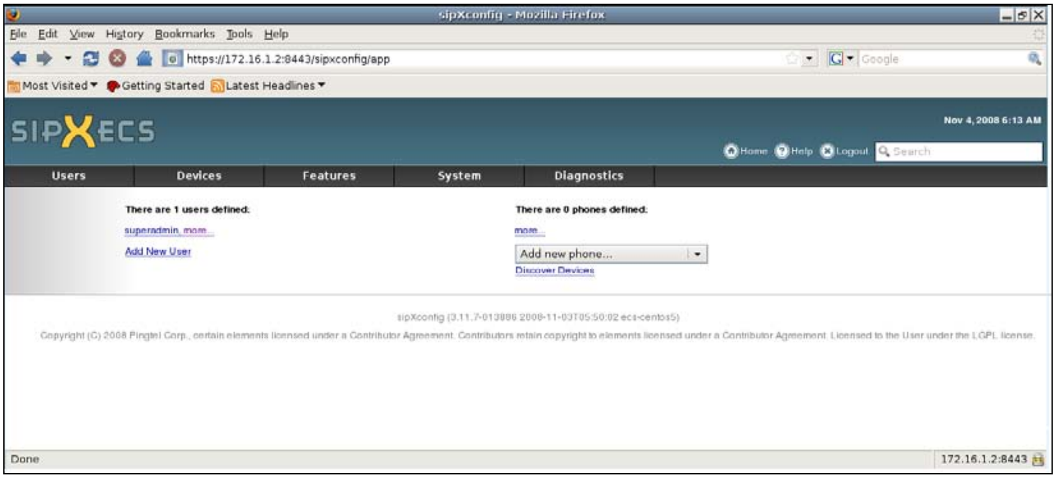
Click on the **Users** drop-down menu in the upper left and select the **Extension Pool** menu item.



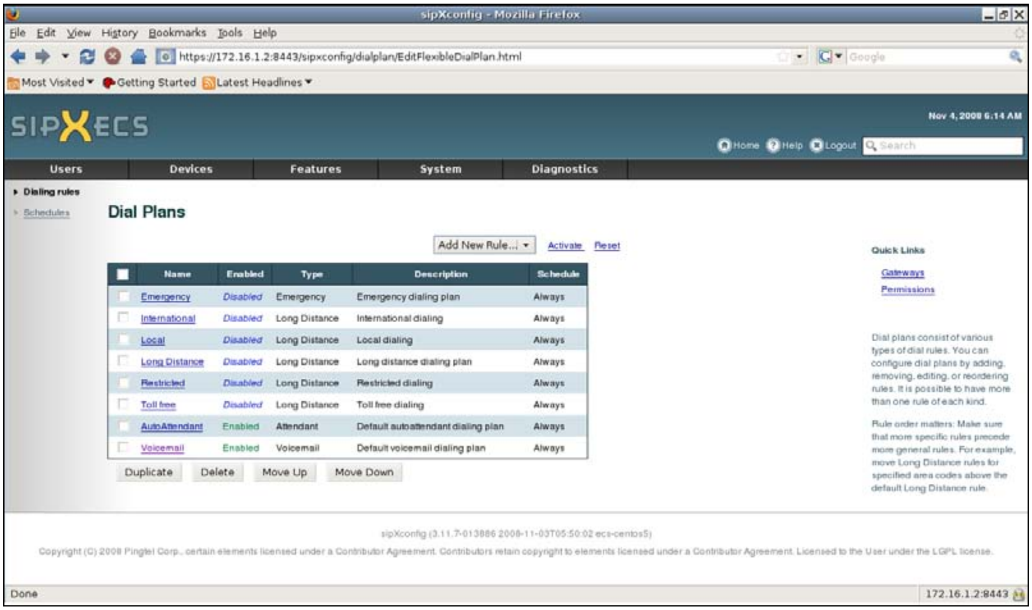
Enter the range of extensions desired for the system and then click on the **Apply** button.

Internal extension length

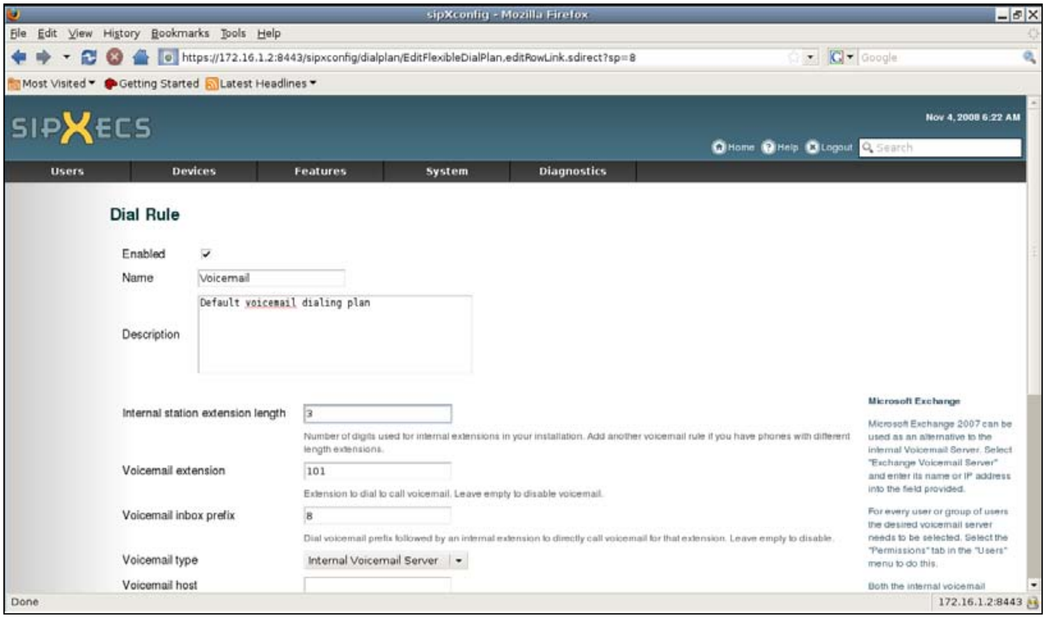
If the internal extension length needs to be different from the default of three digits, it needs to be modified in the Voicemail dial plan. To get to the Voicemail dial plan, get logged into the PBX as **superadmin**.



Click on the **System** drop-down menu and click on the **Dial Plans** menu item. The following screen will be displayed:



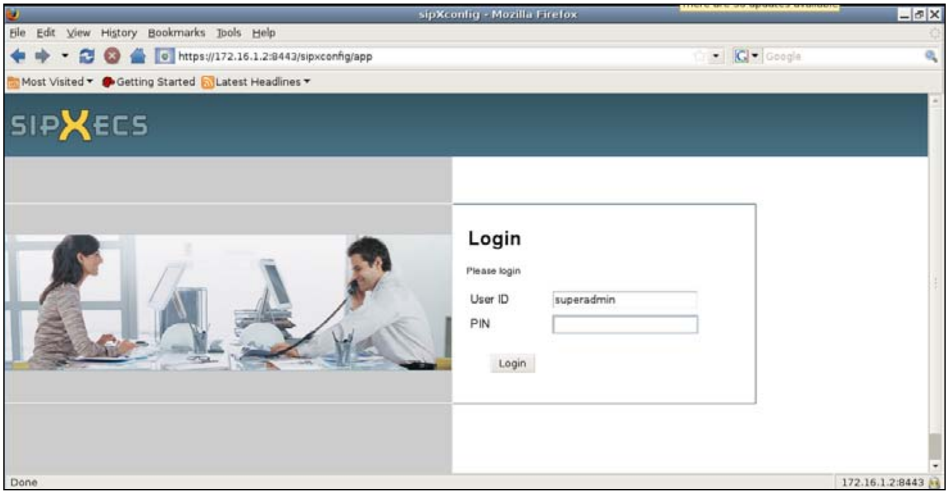
Click on the **Voicemail** dial plan hyperlink and the following screen will be displayed:



Modify the **Internal station extension length** value with the number of digits in the internal extensions, then scroll down the browser page and click the **OK** button. The screen will change back to the dial plan screen and the change will be saved.

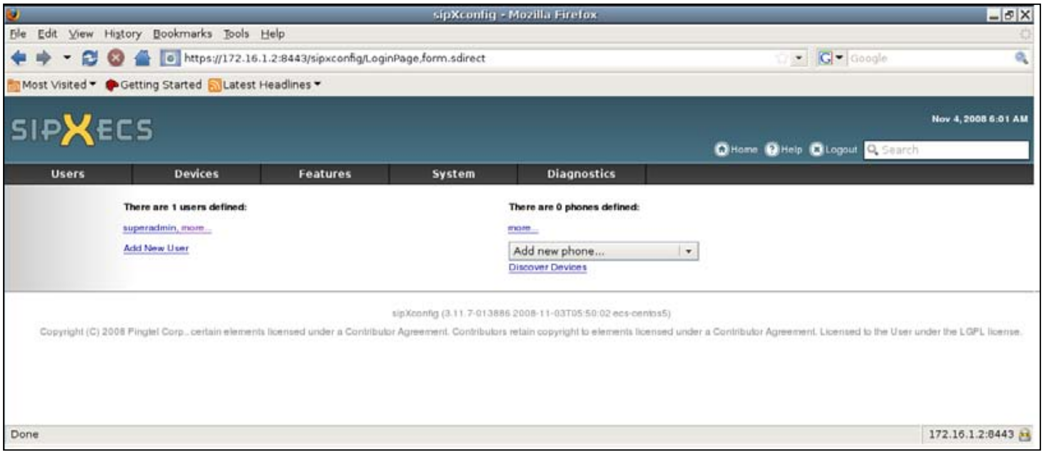
Adding a user

To add a new user, connect to the system with your favorite web browser at the IP address specified for the PBX.

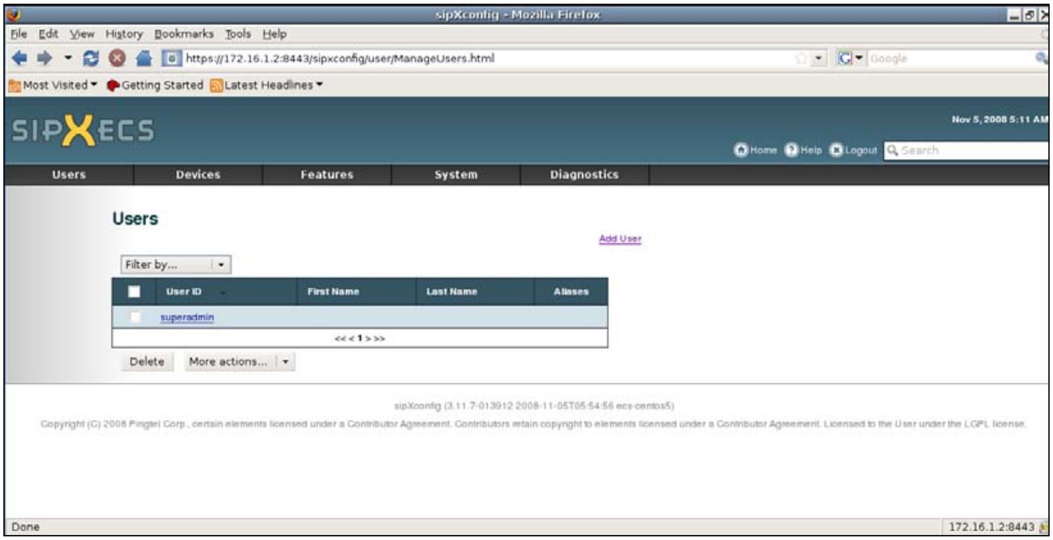


Log in as the **superadmin** user by putting the password chosen earlier in the PIN field and clicking on the **Login** button.

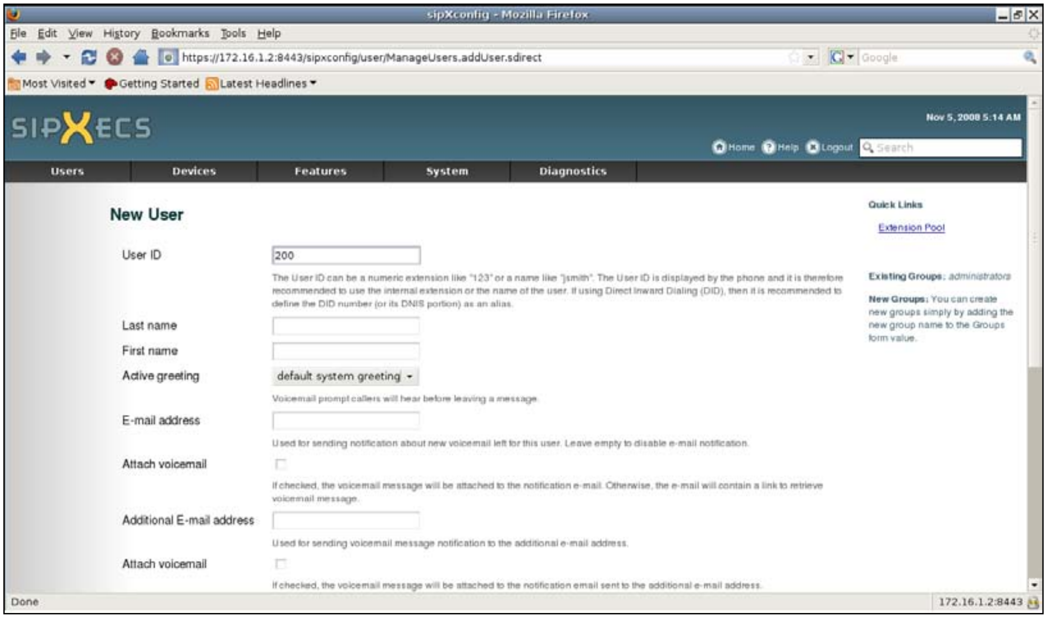
The following screen will appear:



Click on the **Users** drop-down menu and click on the **Users** menu item. The following screen will be displayed:



Click on the **Add User** hyperlink near the middle of the screen. The following screen will be displayed, pre-populated with the first available extension in the extension pool:



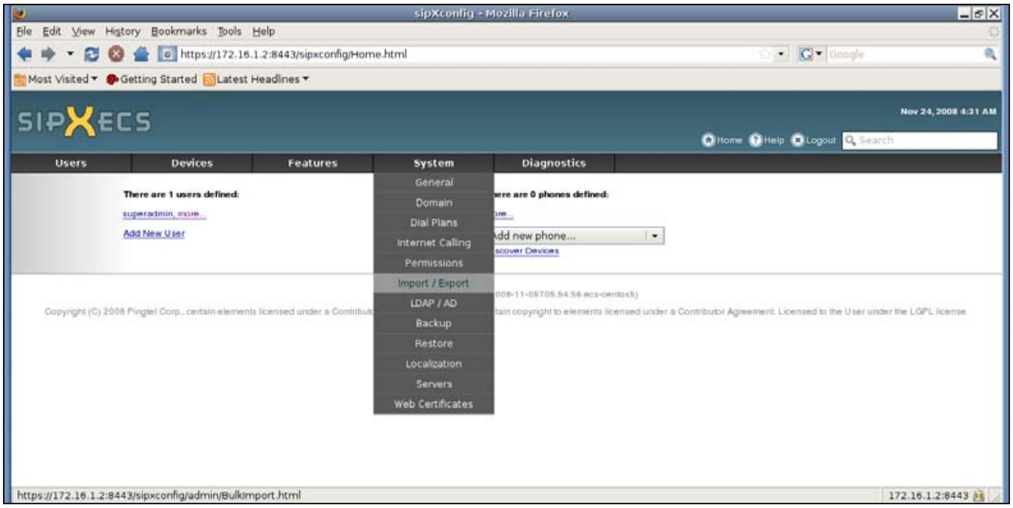
The following fields are available on the **New User** screen:

- **User ID**: This is the user's extension. It can also be alphanumeric for administrative accounts. If a specific number is desired, this field can be changed from the value supplied automatically.
- **Last name**: This is the user's last name.
- **First name**: This is the user's first name.
- **Active greeting**: The administrator can specify the user's active greeting to be played by the voicemail system to be the default system greeting, the user's standard greeting, out of office greeting, or extended absence greeting.
- **Email address**: This is an email address for notifications and/or voicemail messages.
- **Attach voicemail**: If checked, a WAV file containing voicemail messages will be sent along with the notification to the primary email address.
- **Additional E-mail address**: A secondary email address for notifications and/or voicemail messages.
- **Attach voicemail**: If this is checked, a WAV file containing voicemail messages will be sent along with the notification to the additional email address.
- **PIN**: The PIN is a password used to log in to voicemail. Numeric values are recommended for typical users because they need to be dialled from telephones. Alphanumeric values can be utilized for administrative accounts, but those mailboxes will not be accessible from a telephone.
- **Confirm PIN**: Re-enter the same PIN to confirm that the PIN was entered properly.
- **SIP password**: The SIP password is prepopulated with a random value (which may be changed) and is used by the user's **User Agent** (**UA**) or phone to register with the PBX. If this user is assigned to a managed phone, the SIP password will be configured in the phone automatically. It is very important to have a secure password because any device that can register to the PBX can make phone calls.
- **Groups**: User groups can be utilized to assign particular permissions to groups of users. If a group is entered that does not exist, it will be created. To enter multiple groups, separate them with a space.
- **Aliases**: Additional names for the user. An alias can be either another numeric extension or a name (such as an email alias). To enter multiple aliases, separate them with a space. Aliases cannot be used to register with the PBX. If you are using **Direct Inward Dial** (**DID**) numbers, they should be put on a user as an Alias.

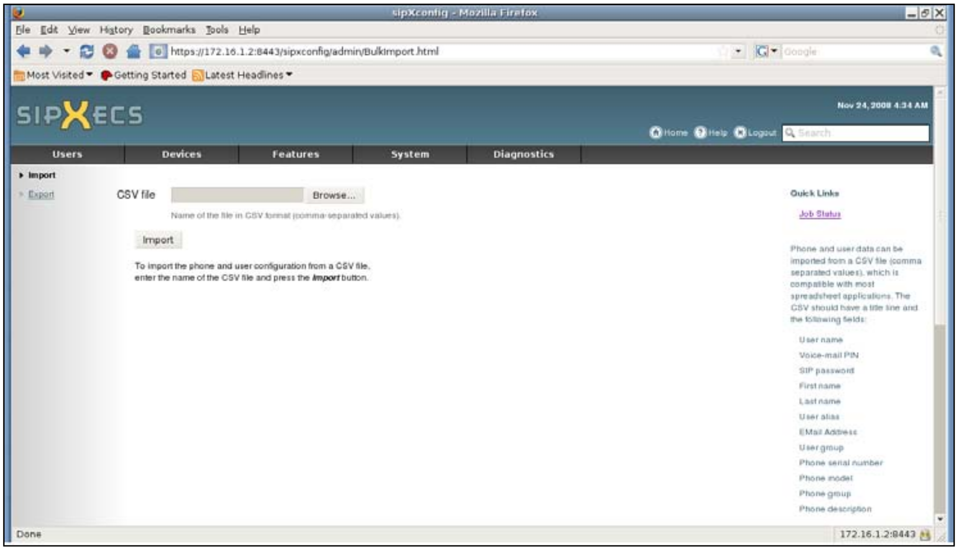
Importing users

As explained in Chapter 2 (under the *Plan the installation* section), the sipxconfig service has the ability to import user and phone information to speed up deployment. If a CSV file has been created in the proper format, importing the users to the system with their phones is easy.

Assuming you already know how to log in to the superadmin account, click on the **System Menu** and then the **Import / Export** menu item shown as follows:



Then the **Import** screen will be displayed, shown as follows:



Click on the **Browse** button and navigate to the CSV file on your local computer. Click on the **Import** button once the local file has been located.

As described in the help section on the righthand side of the screen, each line from the imported file will result in the creation of a phone and the user assigned to that phone. If the user group or phone group fields are not empty, the newly created user and phone will be added to the specified groups. Groups will be created if they do not exist.

If a user with the same username (extension) is already present, the system will update the existing user instead of creating a new user. Likewise, if a phone with the same serial number exists, it will be updated.

The username and phone serial number fields are the only required fields. All other fields may be left blank and the system will not overwrite any existing values in the database.

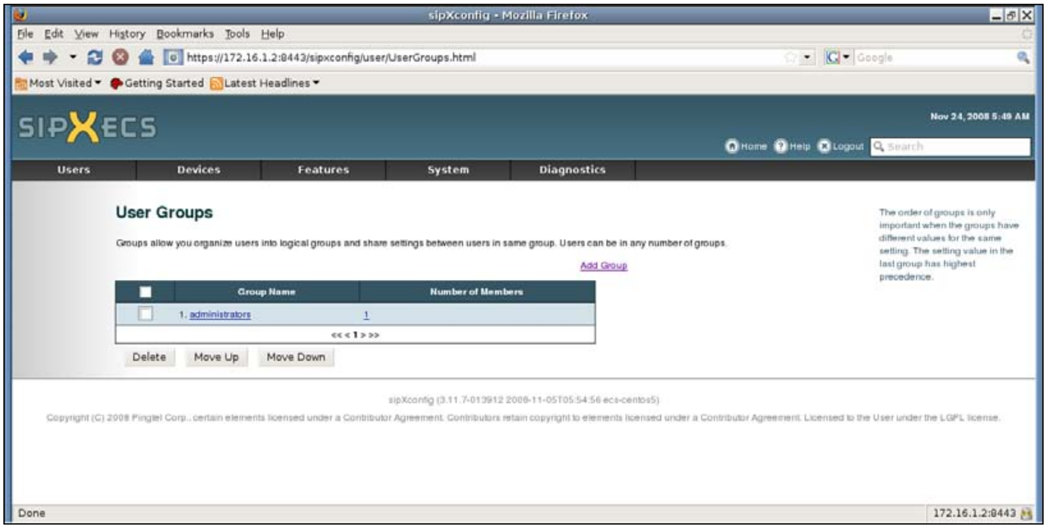
> If a SIP password is not specified, it will be left blank. Users with blank passwords are not permitted to register with the PBX. Make sure to create complex passwords for each user in the import file.

Click on the **Diagnostics** menu and **Job Status** menu item to check the status of the CSV import.

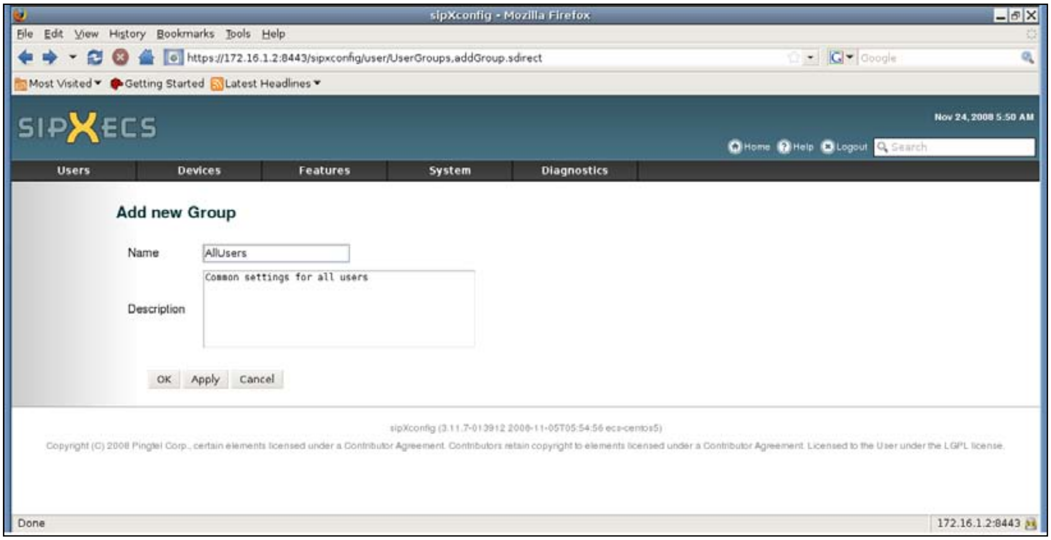
> If you are having trouble getting the format of the CSV file correct, or identifying a particular phone model name, create a user with the information you'd like and perform an export of the information.

User groups

User groups are utilized by administrators to organize users into logical groupings and share settings between the users in the same group. To create a group, click on the **Users** drop-down menu and then select the **User Groups** menu item. The following screen will be displayed:



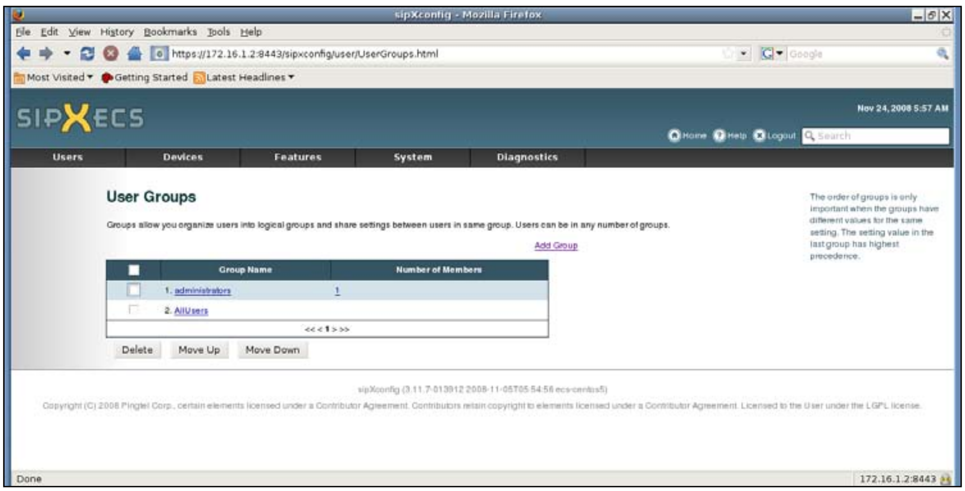
Click on the **Add Group** hyperlink near the middle of the page.



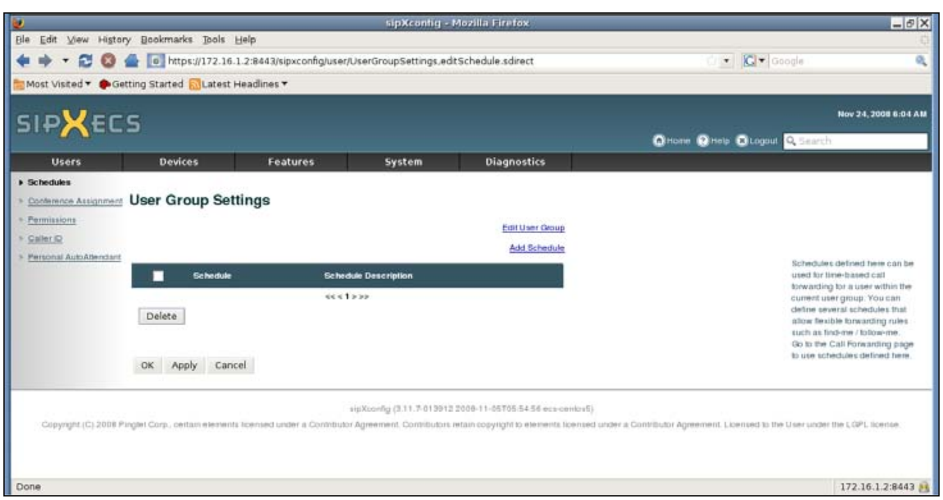
In the **Name** dialog box enter the group name (no spaces are allowed) and the purpose for the group in the **Description** dialog box. Click **OK** when complete.

> Groups can be created on any user account by simply entering a group name. If the group does not exist, it will be created. If you are trying to add to an existing group, make sure that the spelling and capitalization are correct, else a new group will be created.

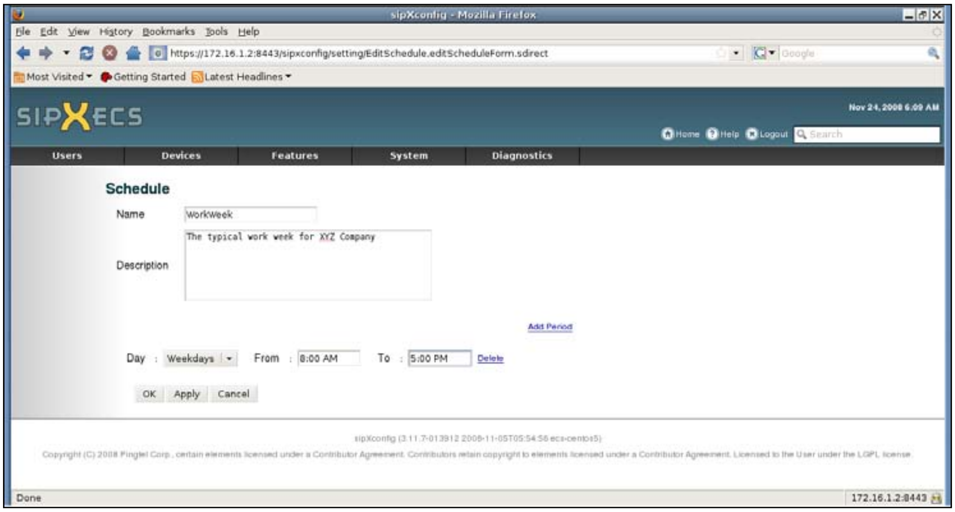
After clicking on **OK,** the list of **User Groups** will be displayed as follows:



Click on the new user group just created to set the common settings for this group of users. The following screen will be displayed:

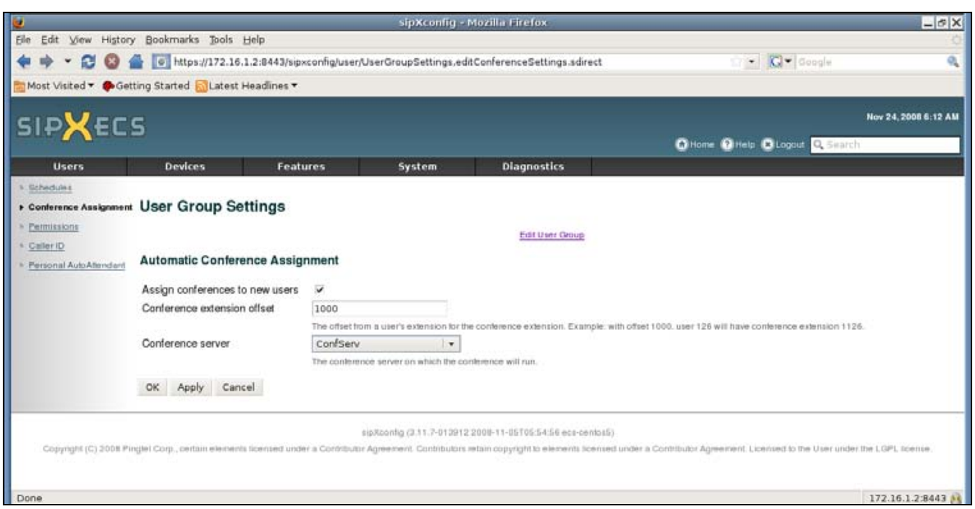


The common settings available are **Schedules**, **Conference Assignment**, **Permissions**, **Caller ID**, and **Personal Auto Attendant**. Click on the **Add Schedule** hyperlink near the middle of the screen. A **Schedule** creation screen will then appear that will allow the administrator to create a schedule that is common across this group of users. For example, a common **WorkWeek** schedule could be created in the following manner:



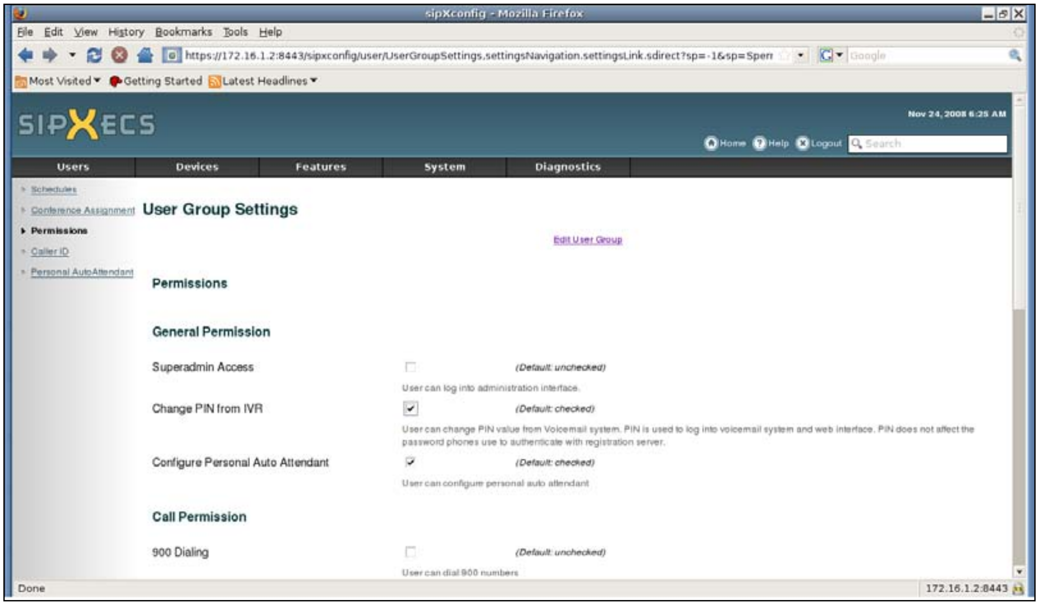
Schedules are utilized by the user's call forwarding settings. Creating schedules for groups simplifies the user's call forwarding setup.

Meet-me conference rooms can be automatically created for all the users in the group by clicking on **Conference Assignment**.



A common extension offset can be utilized for conference room numbers. This offset will be added to each user's extension to determine the conference room number. Take care when assigning the offset to make sure that it incorporates with the extension ranges planned for the system.

Common user permissions can be assigned by clicking on the **Permissions** hyperlink. The following screen will be displayed:



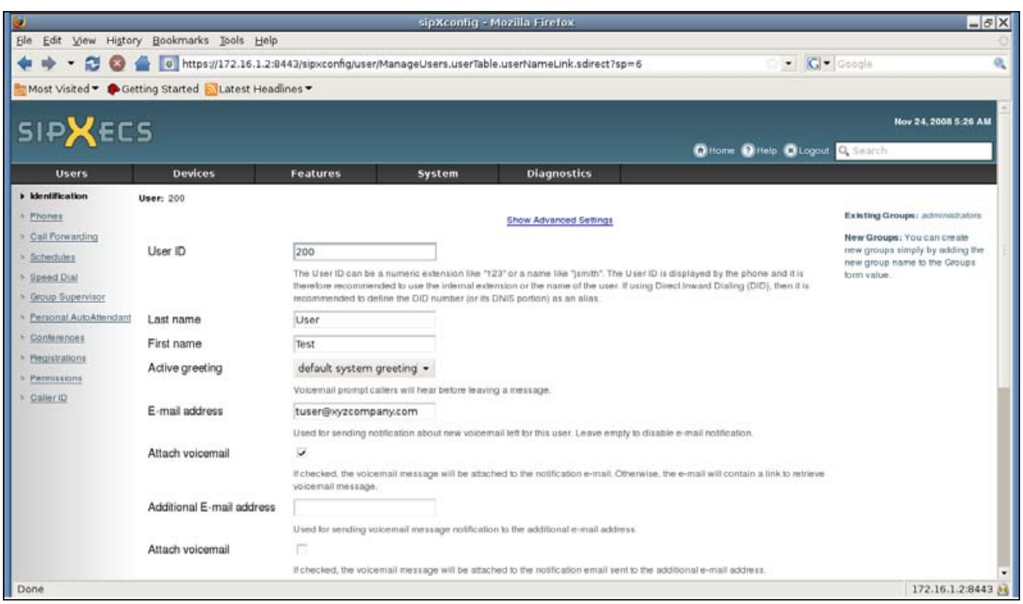
In **User Group Permissions**, the system administrator can allow or deny the following permissions:

- **Superadmin Access**: This user can log into the administration interface.
- **Change PIN from IVR**: The user can change the PIN value from the Voicemail system PIN as used to log into the voicemail system and user portal. **IVR** is the acronym for **Interactive Voice Response** system, the equivalent of an auto attendant receiving input from a touchtone phone. In this case, the user can have the permission to change his/her password from any telephone instead of using a computer.
- **Configure Personal Auto Attendant**: The user can configure his/her own personal auto attendant.
- **900 Dialing**: User can dial 900 numbers. In the United States "900" numbers are phone numbers that begin with the digits 900 and require the calling party to pay for the charges of a call.

- **Attendant Directory**: The user is listed in the Auto Attendant dial by name directory.
- **International Dialing**: The user can dial international numbers.
- **Local Dialing**: The user can dial local numbers.
- **Long Distance Dialing**: The user can dial long distance numbers.
- **Mobile Dialing**: The user can dial mobile numbers.
- **Toll Free**: The user can dial toll free numbers.
- **Voice Mail**: The user has a voicemail inbox.
- **Record System Prompts**: The user can record system prompts in the IVR.
- **Internal Voicemail Server**: The user's voicemail will be on the sipXecs integrated voicemail server. This setting or the next setting may be checked but not both together.
- **Microsoft Exchange UM Voicemail Server**: The user's voicemail will be on a separate Microsoft Exchange UM voicemail server. This setting or the previous setting may be checked but not both together.

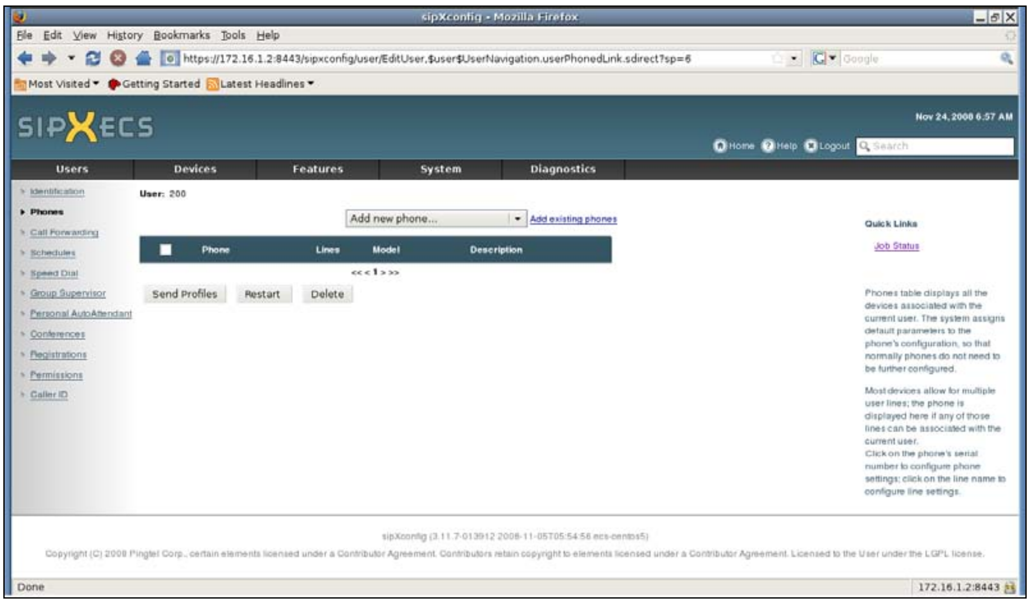
Advanced user configuration

Once a user is created in the system, there are more user configuration options available to the administrator. Click on the **Users** drop-down menu and select the **Users** menu item. Click on a user account and the following screen will be displayed:



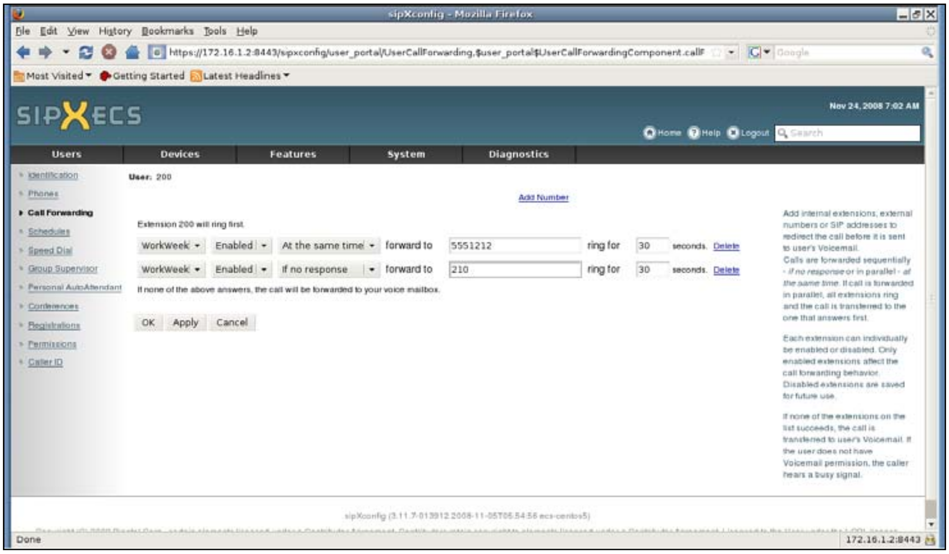
This is the User Identification page. It has all of the information that was entered when the user was created. Notice the **Show Advanced Settings** hyperlink near the top middle of the page. Clicking on this link will display the user's SIP password on the page. This password is used to register user agents (hard phones, softphones, and so on) to the system. An administrator might need the SIP password if he or she is adding an unmanaged phone (such as a softphone) to the phone system. See Chapter 5 for information about managed and unmanaged phones.

On the lefthand side of the screen are the rest of the user configuration options. Clicking on **Phones** reveals the following screen:



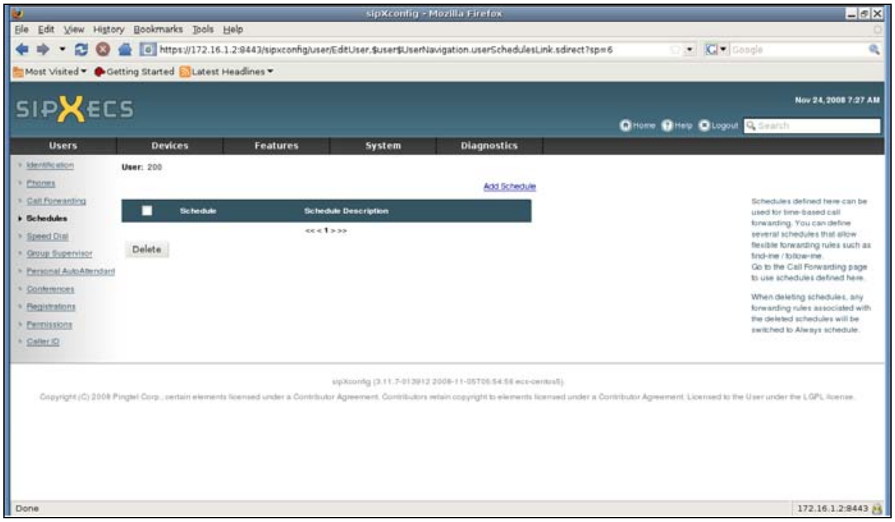
This screen allows administrators to view all of the managed devices associated with the user and add the user to new or existing phones.

The call forwarding screen allows very flexible scheduled call forwarding. As seen on the following screen, the user can add internal extensions, external phone numbers, or SIP addresses to redirect the call before it is sent to the user's voicemail.



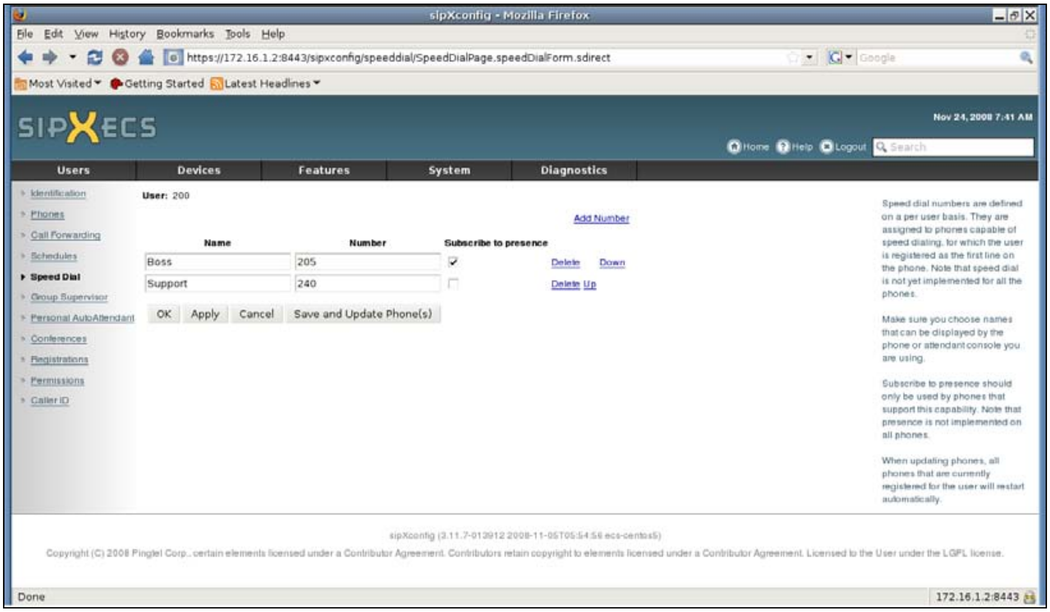
Calls can be forwarded in a sequential manner by selecting **If no response**, or in a parallel fashion by selecting **At the same time** in the dropdown. If calls are forwarded in parallel, all extensions will ring and the call will be connected to the extension that answers the call first.

The **Schedules** page allows the administrator to add schedules specific for this user.



When setting up new call forwarding extensions, user schedules as well as group schedules will be available as options.

The **Speed Dial** screen allows speed dials to be placed on compatible phones. As shown in the following screenshot, any name can be used. The number can be an extension on the system or an external phone number.

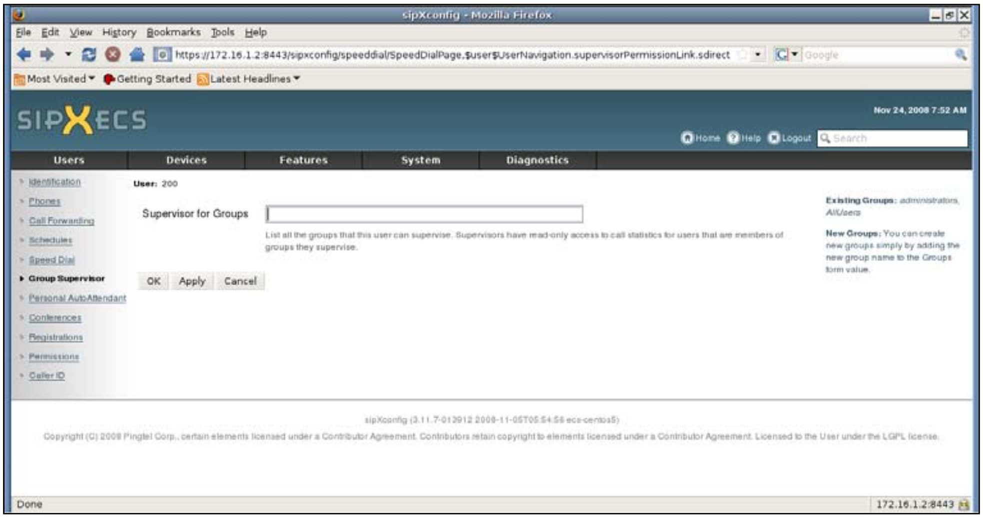


The user can also subscribe to the presence of the selected extension if supported by the phones. Presence allows a phone to see whether another user is on the phone or in **Do Not Disturb** mode. **DND** is a mode the user can put their phone on, to not accept phone calls.

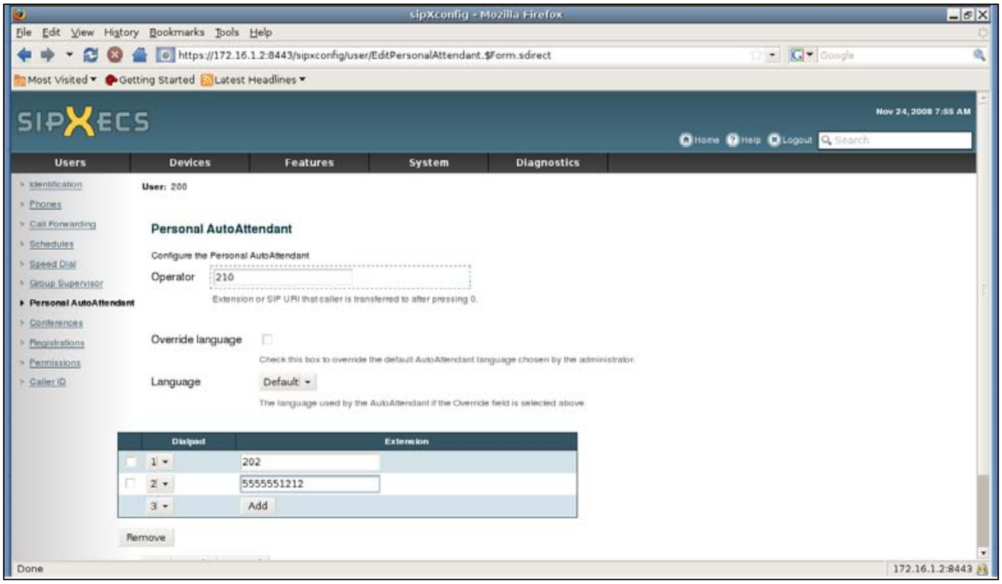
This feature may be referred to as **Direct Station Select** (**DSS**) on other phone systems. If presence is enabled, the feature is referred to as **Direct Station Select** with **Busy Lamp Field** (**DSS/BLF**).

When any speed dials are added, the configuration file for the phone must be recreated and the phone rebooted. This can be done with the **Save and Update Phone(s)** button.

The **Group Supervisor** screen allows the administrator to specify for which groups of users the particular user can see call statistics. Enter an existing or new group name in the **Supervisor for Groups** dialog box and click on **OK** or **Apply**.

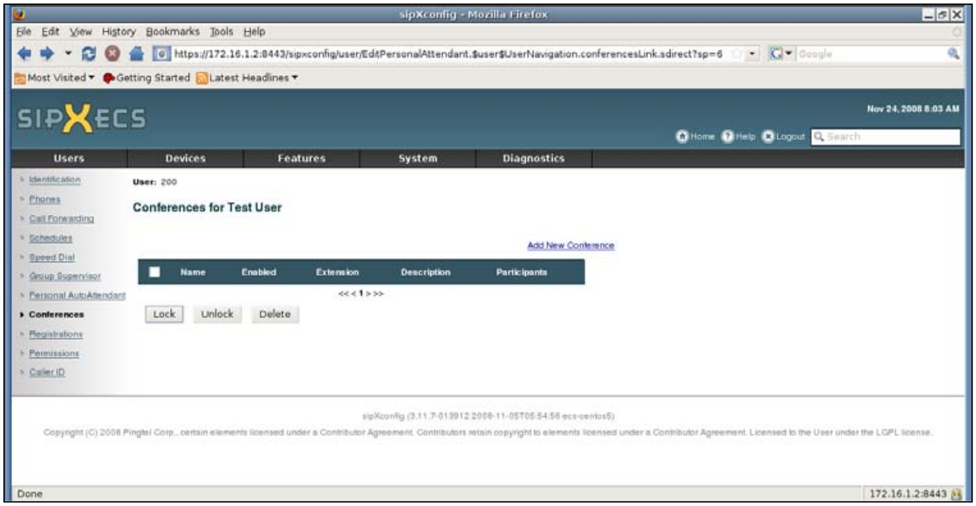


The **Personal AutoAttendant** screen allows the administrator to configure the auto attendant type functionality for each user in the system. As seen in the following screenshot, **Dialpad** entries are added (with extensions or phone numbers) to dial when pressed.

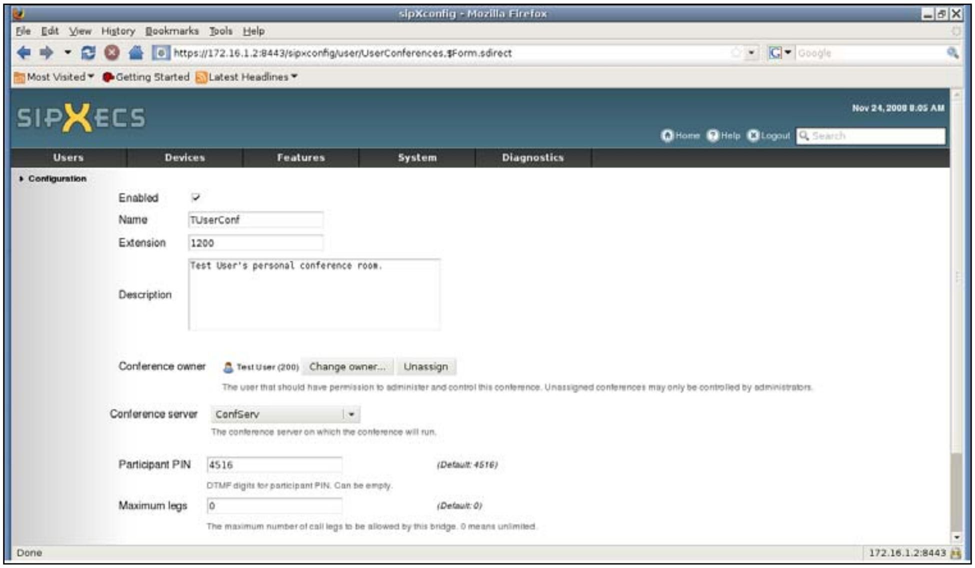


In their voicemail box greeting, the user must record their announcement message to have enough information to let callers know the different options that are available to them. For example, "Hi, this is Mike, sorry I can't take your call, please press 1 to reach my assistant, press 2 to ring my cell phone, or wait for the tone to leave a voicemail message."

The **Conferences** screen allows administrators to create meet-me type conferences that belong to this particular user.

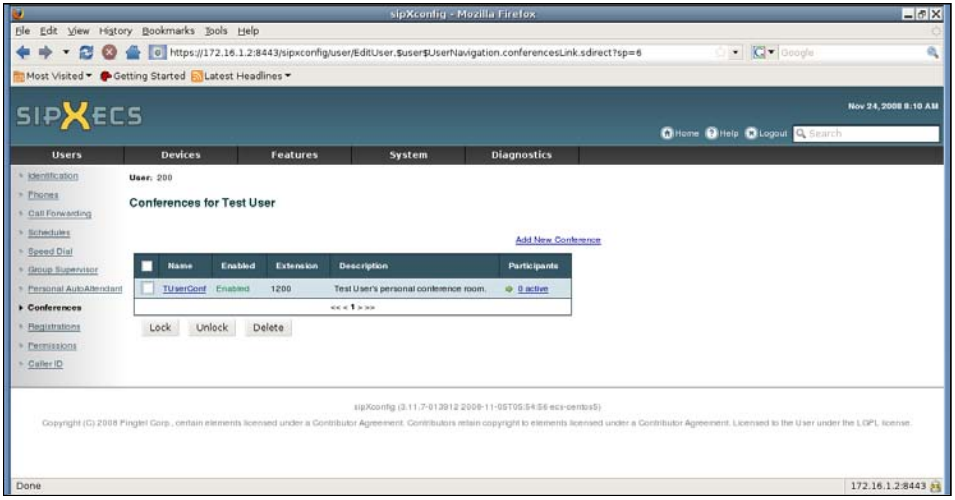


Click on the **Add New Conference** hyperlink to display the following page:



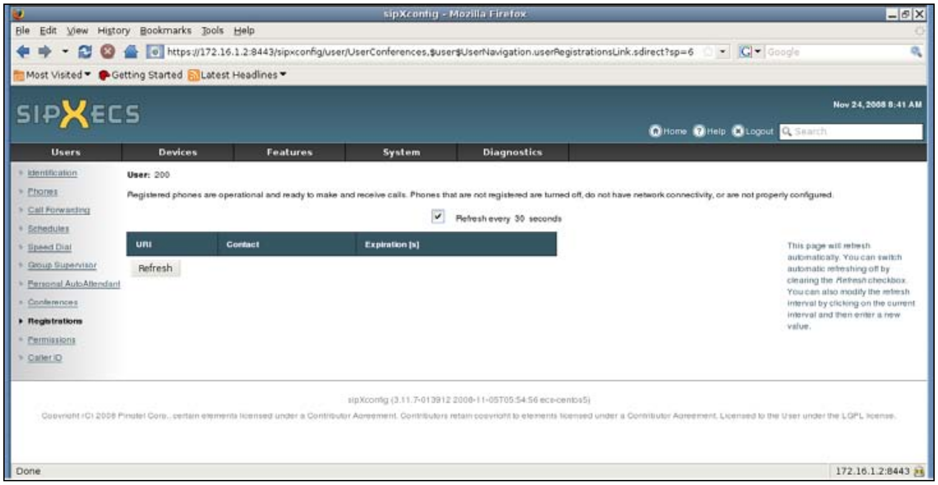
Add a name for the conference, an extension (make sure it works within the overall dialing scheme), a description, the owner defaults to the (owner that is being edited), which conference server is being utilized, the PIN (if desired) for participants to utilize, and how many users are allowed in a conference simultaneously.

Click on **OK** and the **Conferences** screen will be displayed again with the new conference added to the list.

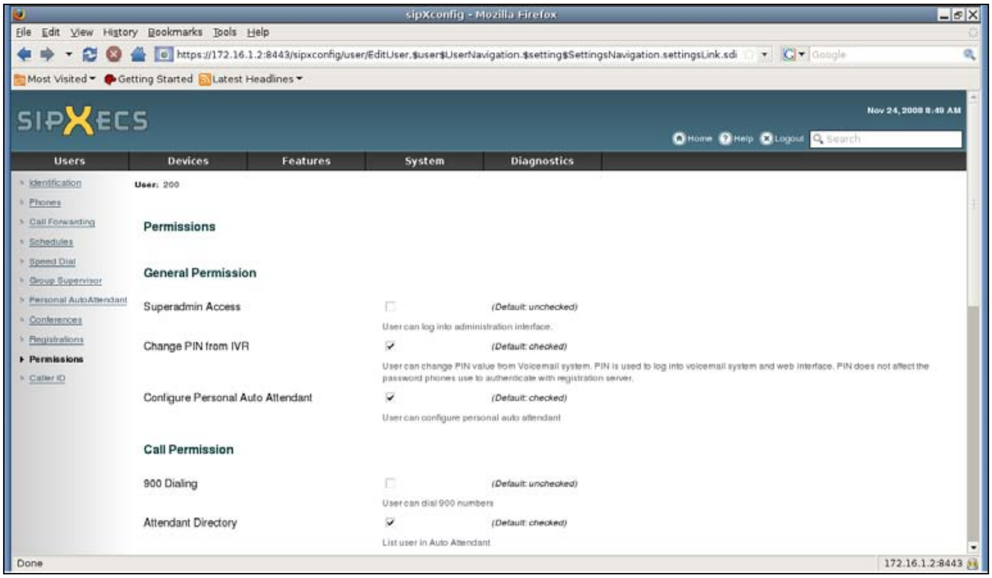


Individual conferences can be locked to prevent new participants from entering the conference.

The **Registrations** screen displays all user agents that are registered to this particular user.

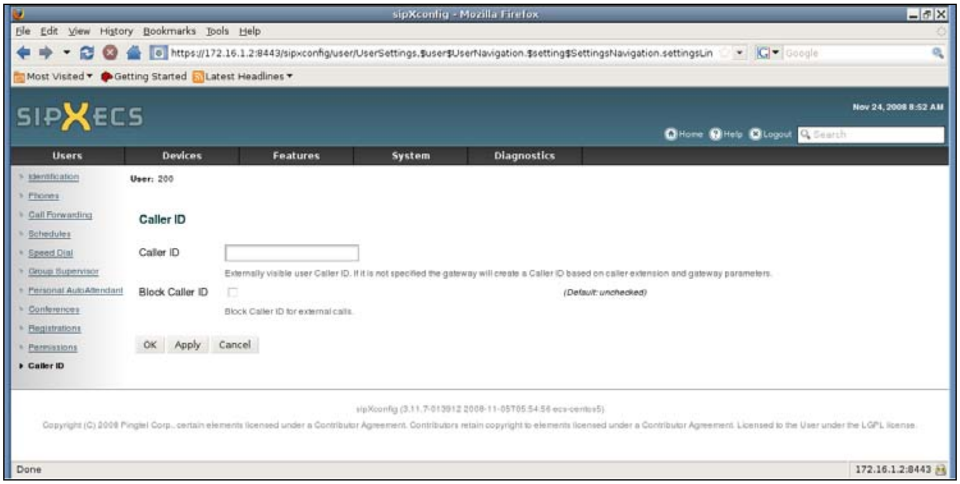


The **Permissions** screen allows the administrator to override any group settings for this particular user.



The above **Permissions** screen settings are identical to the permissions described in the *User groups* section of this chapter.

The **Caller ID** screen allows the administrator to specify the caller ID that dialed PSTN phone numbers can see (typically this can be done with a PRI type circuit or SIP trunk, but not with analog circuits). As seen on the following screenshot, the administrator can enter a unique caller ID or block the user's caller ID for external calls.



Phantom users

A Phantom user is simply a user account on the system that will never have a user agent (phone) registered to it. Phantoms can be used for voicemail-only mailboxes or for call routing purposes. Whatever their purpose be, phantoms should have any permissions that are not required removed for security.

Voicemail-only mailbox

A voicemail-only mailbox is useful for having callers deposit voicemail for a team of users. The voicemail should be checked on a regular basis (see Chapter 7) or have voicemail forwarded to an email address that is monitored.

> There is no way to set a message notification on a user's phone for anything but their own voicemail, so using email notification of messages (to an email box or cell phone) is very useful for voicemail-only mailboxes.

All permissions except voicemail permission should be removed from voicemail-only mailboxes. This prevents any SIP devices from being able to log into the proxy as the phantom user and make calls. If there are many voicemail-only mailboxes on the system, consider making a "VoicemailOnlyPhantoms" user group (see *User groups* section earlier in this chapter) with the appropriate permissions, and add the phantom users to that group.

Call routing phantom

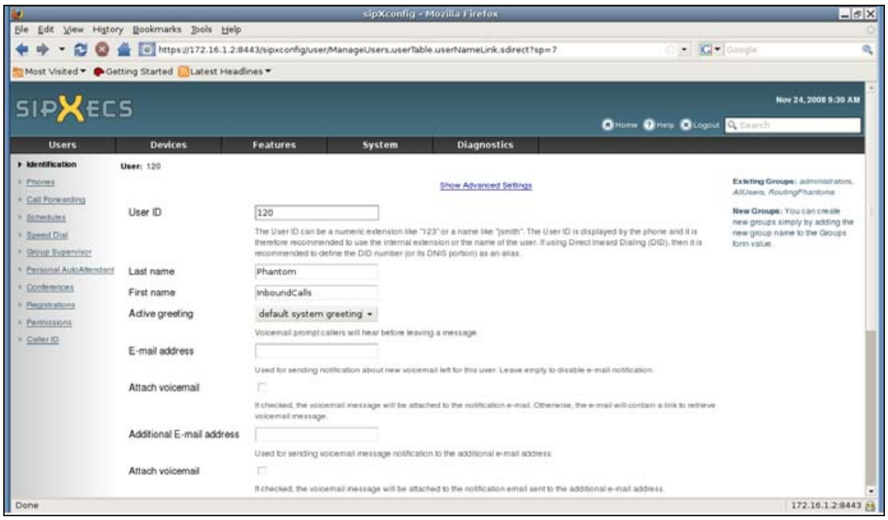
Call routing phantoms can be utilized for making important call routing decisions in the phone system. One of the most common uses is handling inbound phone calls during the day that need to be answered by a live operator, and then routed to an auto attendant during non-business hours.

For call routing phantoms, voicemail permissions are not typically required and you should only allow dialing permissions that the routing phantom will need (for example, there should be no reason that a routing phantom should be able to dial 900 numbers or need to be listed in the attendant directory). As above, this prevents any SIP devices from being able to log into the proxy as the phantom user and make calls. If there are many call routing phantoms on the system, consider making a "RoutingPhantoms" user group (see *User groups* section earlier in this chapter) with the appropriate permissions, and add the phantom users to that group.

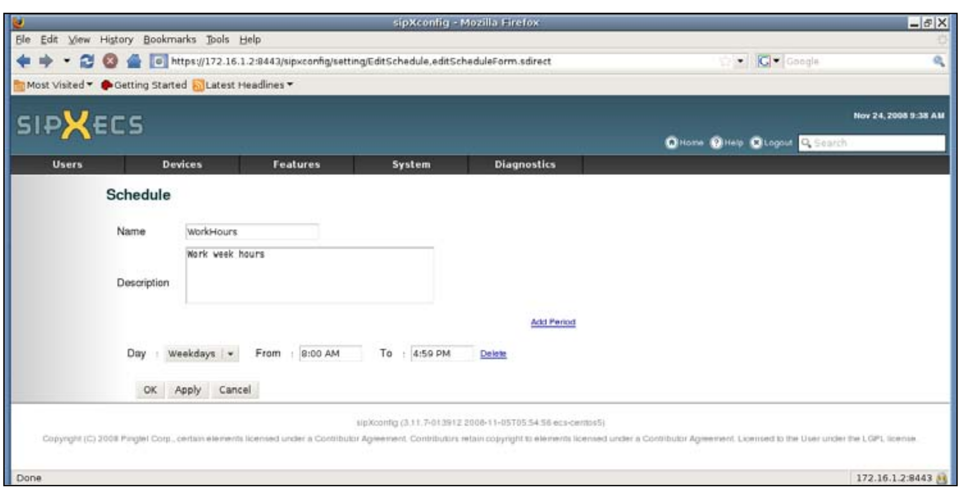
Call routing phantom example

The following example illustrates how calls are answered by a live operator during working hours, ring a hunt group on no answer during working hours, and routed to an auto attendant on no-answer or during non-business hours.

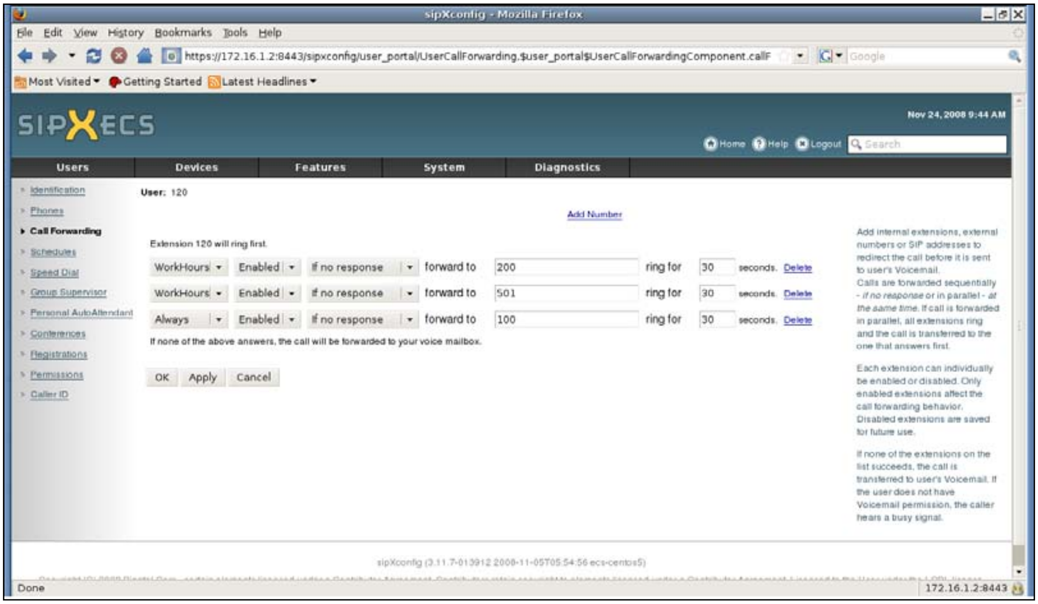
Create your call routing phantom user and assign the appropriate permissions (for this example extension 120 will be used).



On the user's configuration page click on **Schedules** and then add the appropriate schedule times to set up the work week schedule (8 a.m. to 4:59 p.m. in our example). Note that this schedule could be created in the RoutingPhantoms user group if there are many phantoms that might utilize this schedule.



Once the schedule is configured as desired, click on **OK** and then click on the **Call Forwarding** hyperlink on the left of the screen. Then click on the **Add Number** hyperlink to add in the extensions that will be forwarded, shown as follows (in this example, the main answering extension is extension **200**, a hunt group is set up on extension **501**, and the default auto attendant for the system is at extension **100**).



Lastly, configure any gateways on the system (see Chapter 5) to ring in to the phantom extension that was just created.

Summary

In this chapter we covered in depth how to create users and groups. We also explored how to use phantom users for voicemail-only mailboxes and for some advanced call routing needs.

5

Configuring Phones in sipXecs

Any IP telephone (also referred to as a User Agent in the SIP world) that conforms to accepted SIP standards can interoperate with the sipXecs system. There are literally hundreds of hardware and software-based phones that will work. If there is any question whether a device will work with the system, SIPfoundry offers an automated interoperability testing server (`http://interop.pingtel.com`).

Types of phones

When most hardware-based phones boot, they can check a configuration server for a configuration file. The configuration file is generally transferred by the phone with TFTP, FTP, or HTTP. The configuration file format varies for each phone vendor but typically the configuration file will have the **MAC** address (**Media Access Control** address, or more commonly known as the Ethernet hardware address, which is unique to every Ethernet device) of the phone in its name.

The sipXecs system knows how to generate configuration files for many different types of IP phones. The currently supported IP phones were covered in Chapter 2 in the *Equipment selection* section. Any phone for which sipXecs generates a configuration file is considered to be a *managed phone*.

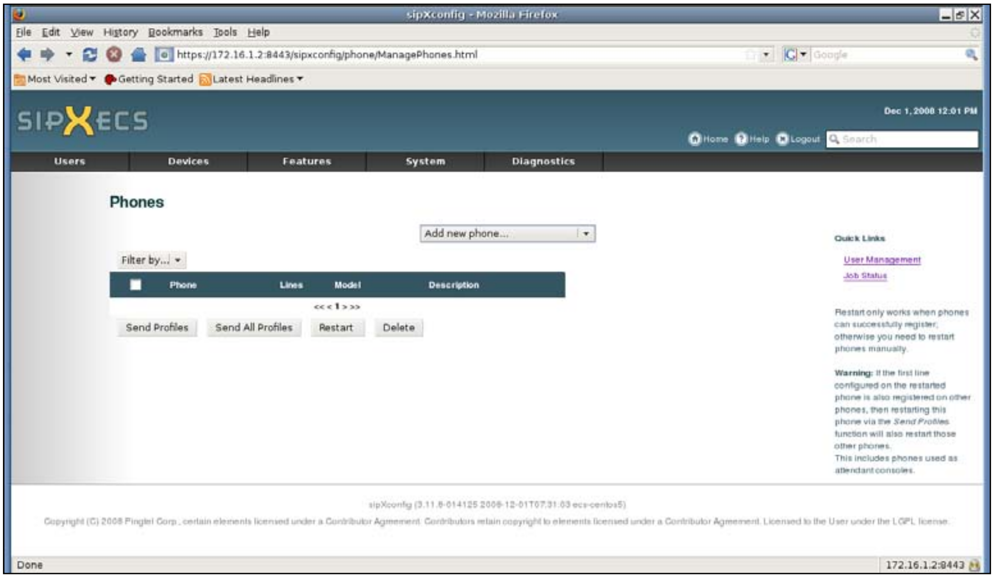
Unmanaged phones are devices for which sipXecs cannot generate the configuration files. These devices need to be manually configured or the administrator must generate his or her own configuration files and place them in the phone configuration file folder (`/var/sipxdata/configserver/phone/profile/tftproot`).

Since space restrictions prohibit covering every phone that sipXecs supports in the next couple of sections, the examples of the Polycom 650 hardware phone as a managed device and the Counterpath xLite software phone as an unmanaged device will be used.

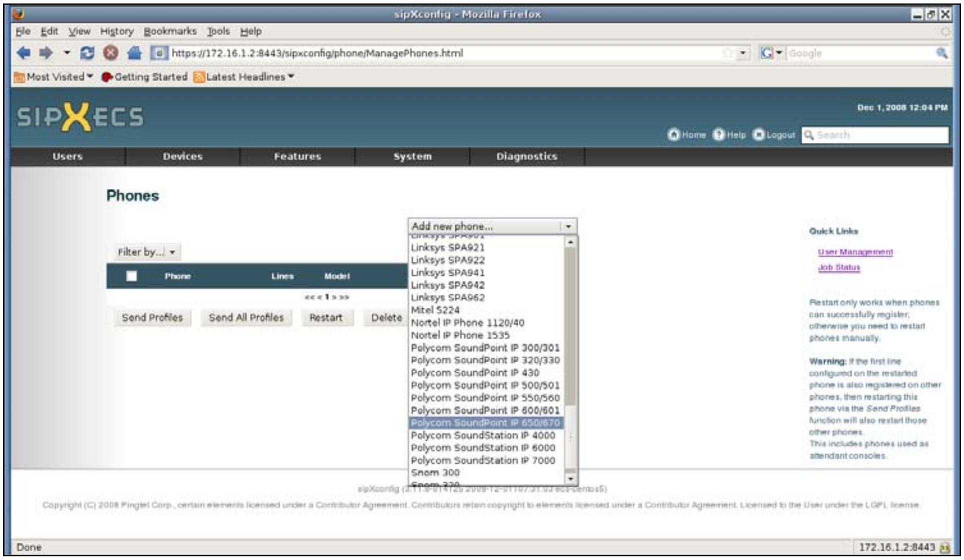
Managed phones

The process for adding a managed phone is creating the phone within the system, assigning a user (the term line is used interchangeably with user) to the phone, generating the configuration file (called the phone profile), and then booting the phone.

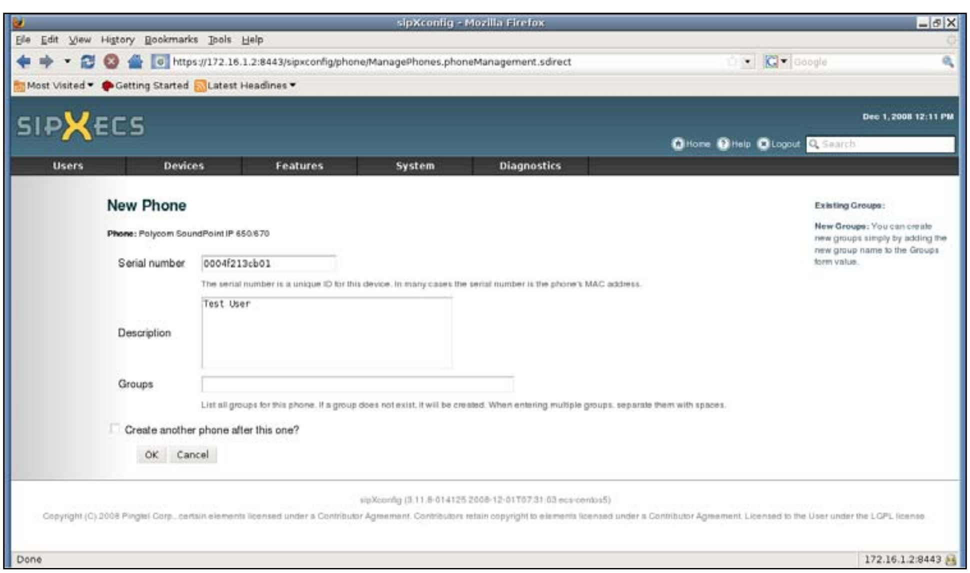
Sign into the configuration GUI of the PBX as Superadmin and click on the **Devices** menu and then select the **Phones** menu item. This should display the following screen:



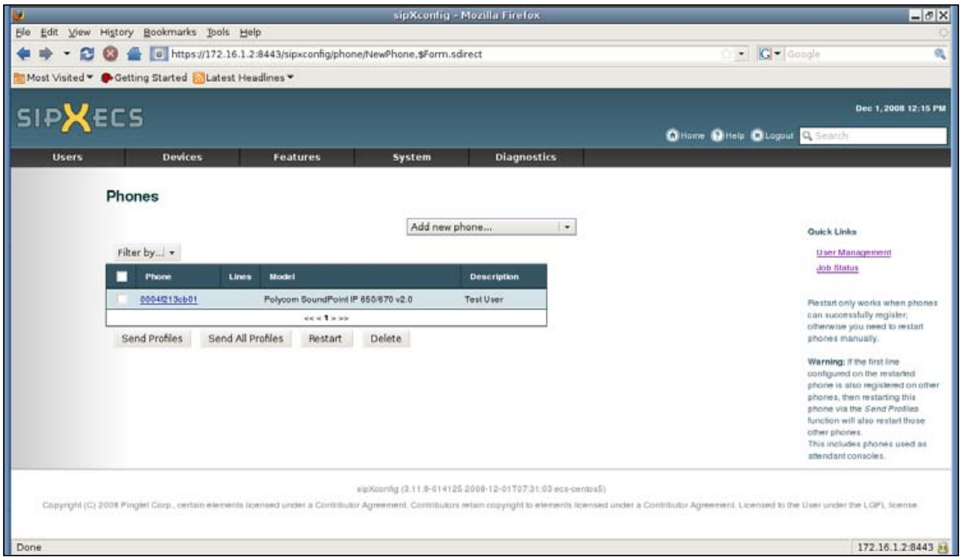
To add the new phone, click on the **Add new phone** drop-down box and select the model of phone that will be added to the system, as shown in the following screenshot:



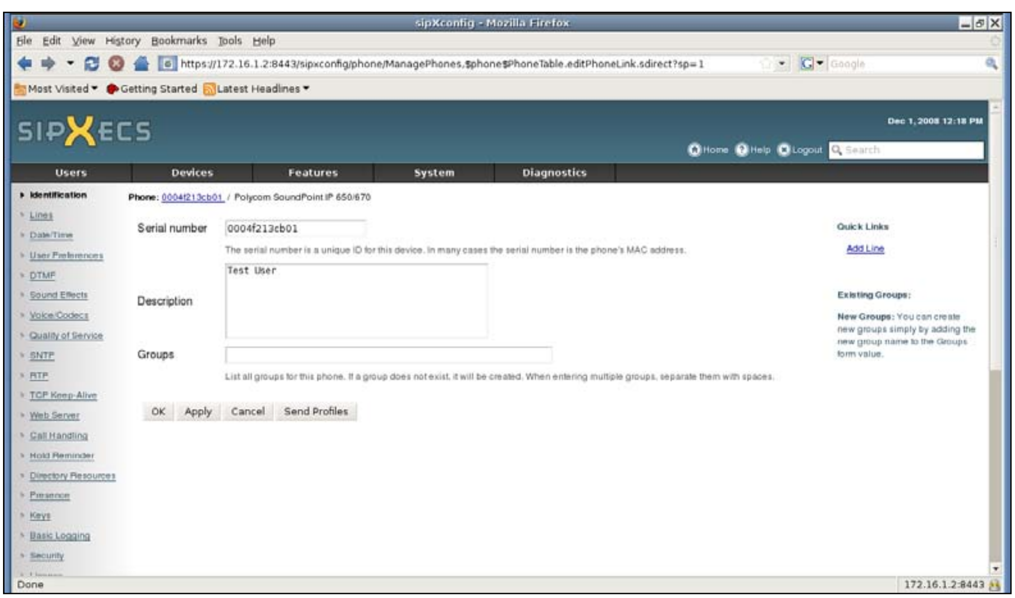
The **New Phone** page will then be displayed prompting for details about the phone. As shown in the following screenshot, enter the serial number of the phone (this is the MAC address of the phone, commonly found on a sticker on the backside of the device), a description of the phone, if desired (entering the user of the phone will make finding things easier), any groups that the phone belongs to (phone groups will be discussed later in this chapter), and use the checkbox above the **OK** button if you would like to enter multiple phones.



After clicking on the **OK** button the **Phones** page will be displayed again with the device that was just added. As shown in the following screenshot, the MAC address of the phone will be a hyperlink:

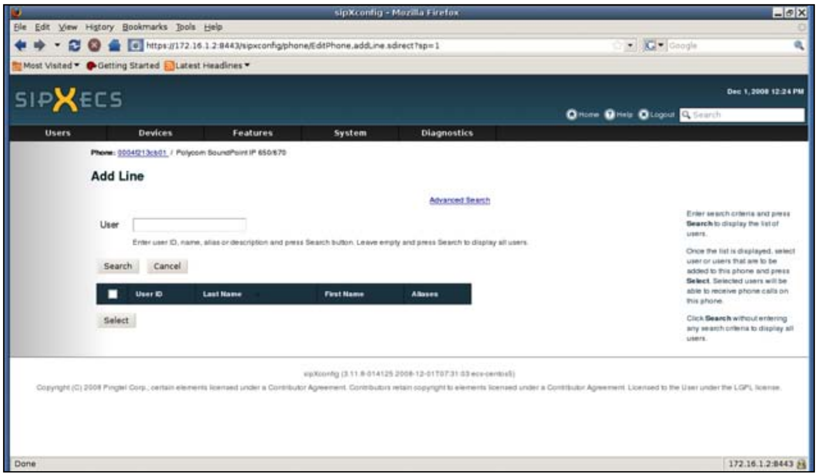


The next step adds one of the system users that were created earlier to the new phone. Click on the phone's MAC address and the phone configuration page will be opened, as follows:

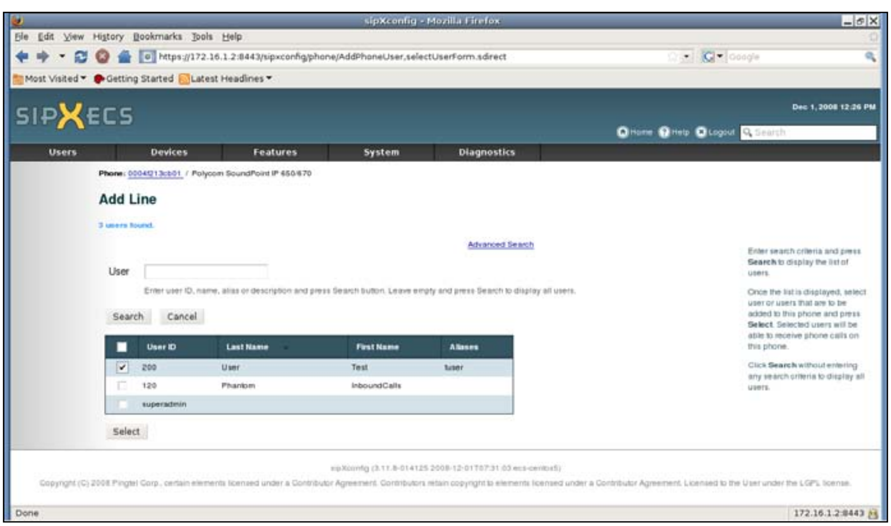


Notice the long list of configuration parameters on the lefthand side of the page. The phone parameters have been pre-configured with the most common settings for each type of phone that sipXecs knows how to manage.

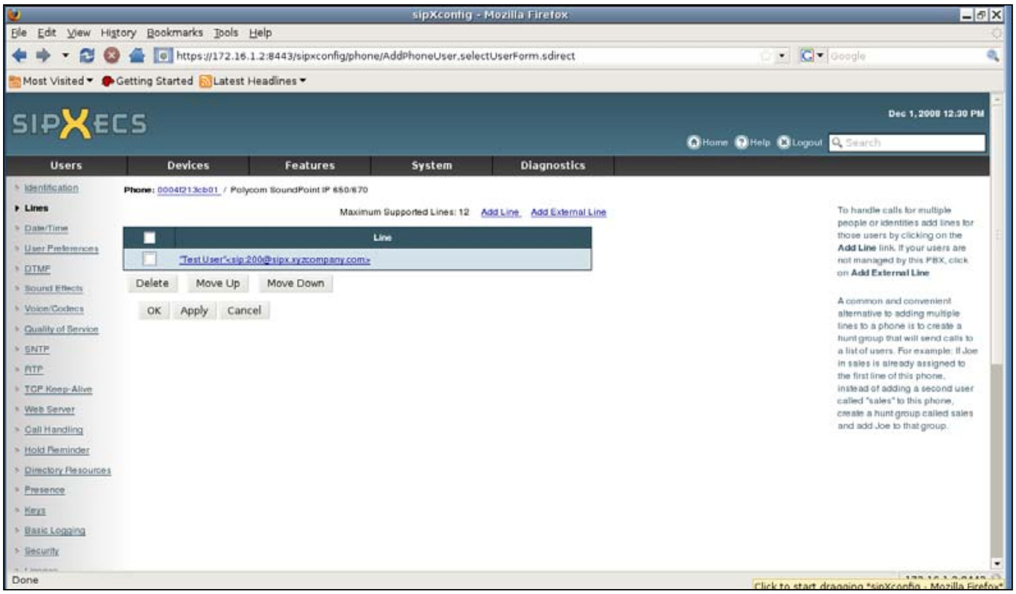
To add a user to the phone, click on the **Add Line** hyperlink under **Quick Links** on the righthand side of the page. The following page prompts the administrator to search the user:



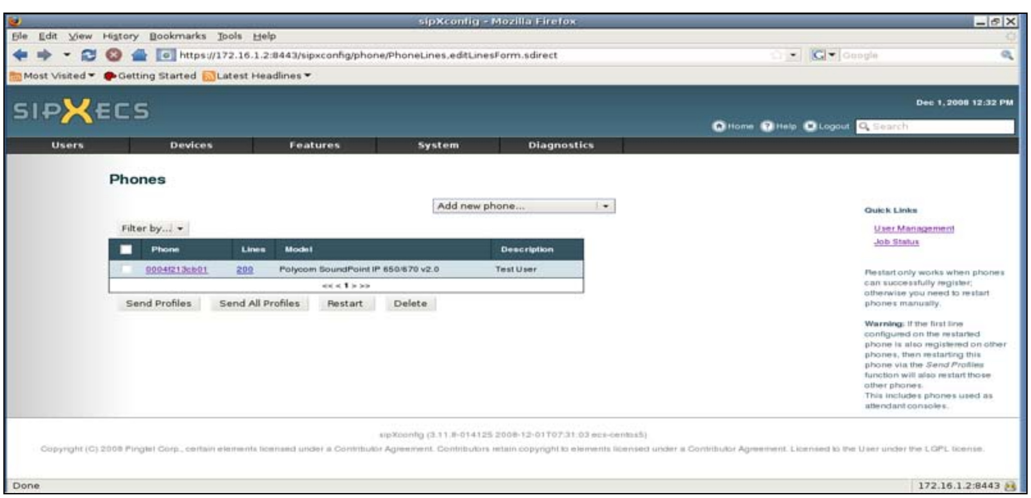
If there are many users on the system, searching will be simplified by entering some information in the **User** dialog box. Simply clicking on the **Search** button will list all users in the system. Check the box next to the user to be added to the phone and click on the **Select** button below the user list.



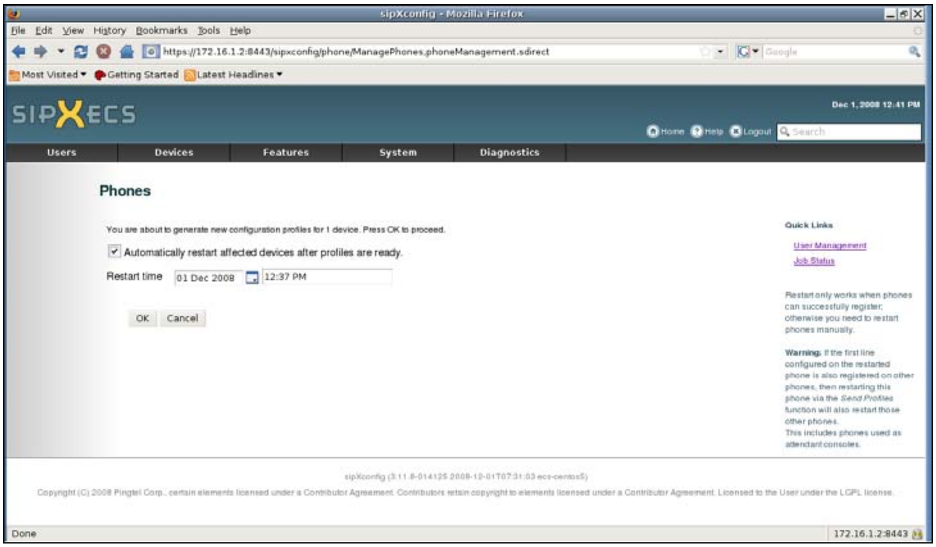
The phone configuration page will then be displayed with the user shown as a line added to the phone as seen in the following screenshot:



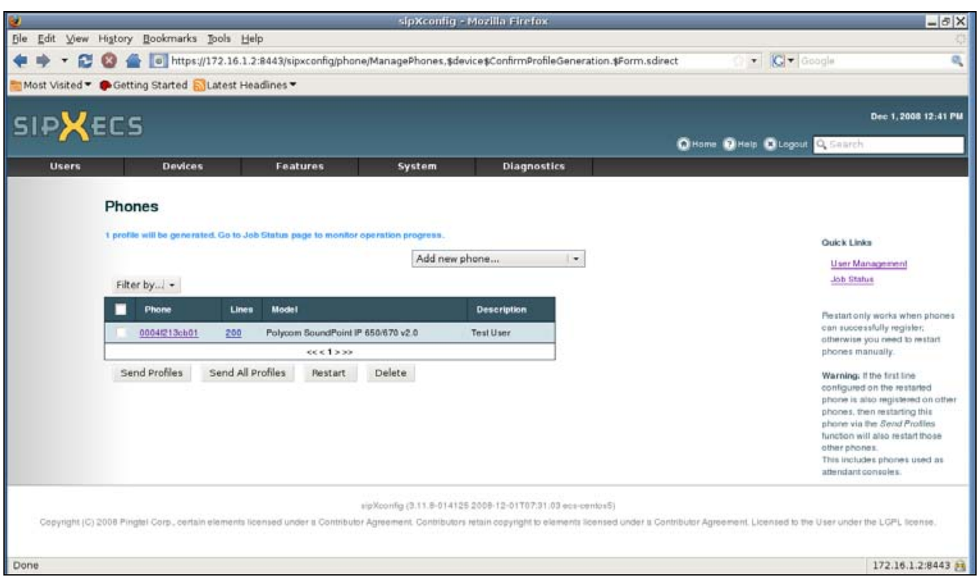
Click on the **OK** button to return to the **Phones** page, which, as seen in the following screenshot, will now show the phone with the new added line next to the phone's MAC address.



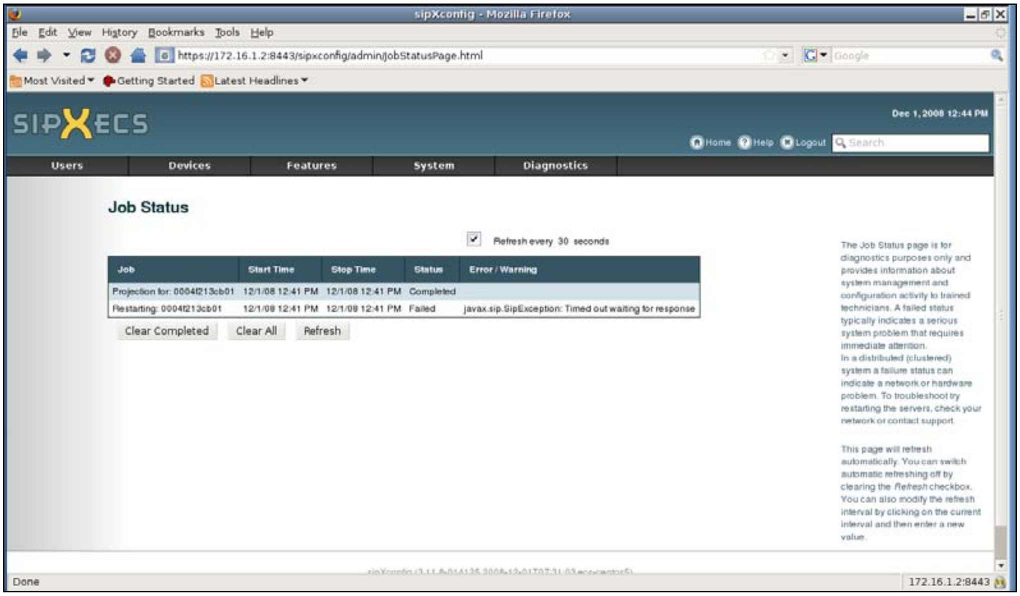
The **Send Profiles** button will create configuration files for any phone with a check in the box before the MAC address. The **Send All Profiles** button will re-create profiles for all phones on the system. The following page will then be displayed, which allows phone reboots to be scheduled at a pre-determined date and time (phone reboots will interrupt users' phone conversations, so plan appropriately).



Clicking on **OK** will return to the **Phones** page with a notification near the top of the page indicating how many profiles are to be generated.



To monitor the progress of the phone profile creation, click on the **Diagnostics** menu and then select the **Job Status** menu item. The following screenshot shows the phone profile creation (called the **Projection**) and then the command to restart the phone. If the phone is not plugged in, the **Status** of the phone restart will show **Failed**, as seen in the following screenshot:



A couple of important subtleties that an administrator should be aware of:

- The sipX administrator is unable to force the reboot of any phone that has not registered yet. Creating phone profiles is strongly suggested even before plugging in the phone.
- The TFTP and FTP server will not provide firmware/bootrom files if needed, until the first phone has been configured with a profile pushed out.

All that is remaining at this point is to boot the phone and verify that it can communicate with the sipXecs server. If you are utilizing VLANs, make sure that the phone is either in a port that is statically in the phone system VLAN or the phone is tagging its traffic for the appropriate VLAN. (With Polycom phones at boot, press the **Setup** softkey, select the **Ethernet** menu and scroll down to select **VLan**, and enter the VLAN number.)

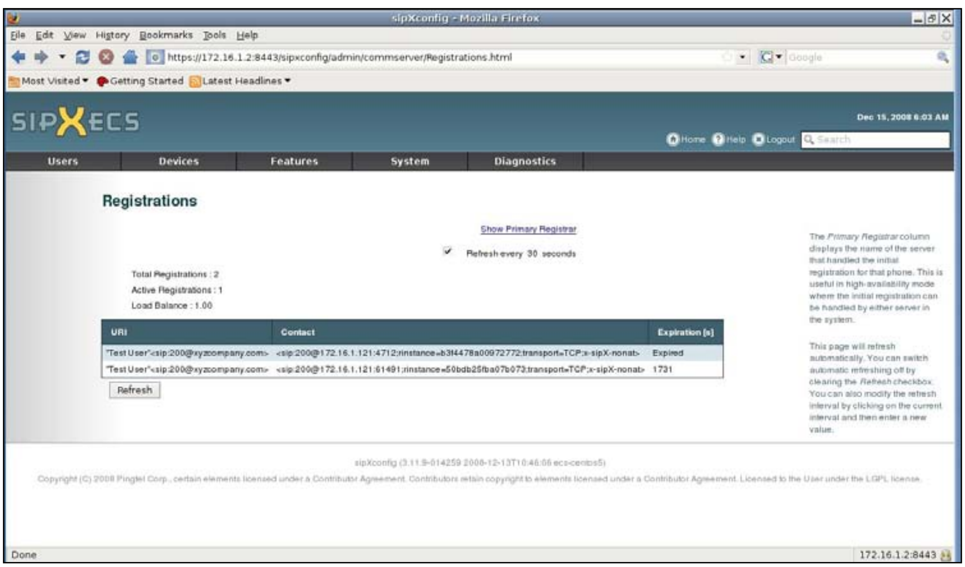
On boot, with most IP hardware phones, the IP address will be displayed. As the phone is booting, verify that the IP address is proper for your phone system network. If it is not, then verify your VLAN settings.

The PBX pre-configures the DHCP service with an option directing the phone to get its configuration information from the sipXecs server. If you are configuring your own DHCP server, this is typically DHCP option 'tftp-server-name' or option number 66.

Once the phone boots, the line number that was assigned to it should appear next to one of the line keys (if your phone has a display). In the case of polycom phones, there is a small phone icon beside the phone extension. If the phone is solid black, then the line has registered (logged in) to the PBX properly. If there is just an outline of a phone, the extension is not registering properly with the PBX.

If the IP phone does not register with the PBX the most common problem is with getting DNS working properly. Revisit Chapter 3 and verify whether DNS and DHCP are working properly.

To verify that the phone is registered properly, click on the **Registrations** menu item in the **Diagnostics** menu. The resulting **Registrations** page should look as follows:



To test calling, place a test call to extension 100. Dial 100 and press **Send** or **Dial**, if required by the phone being used.

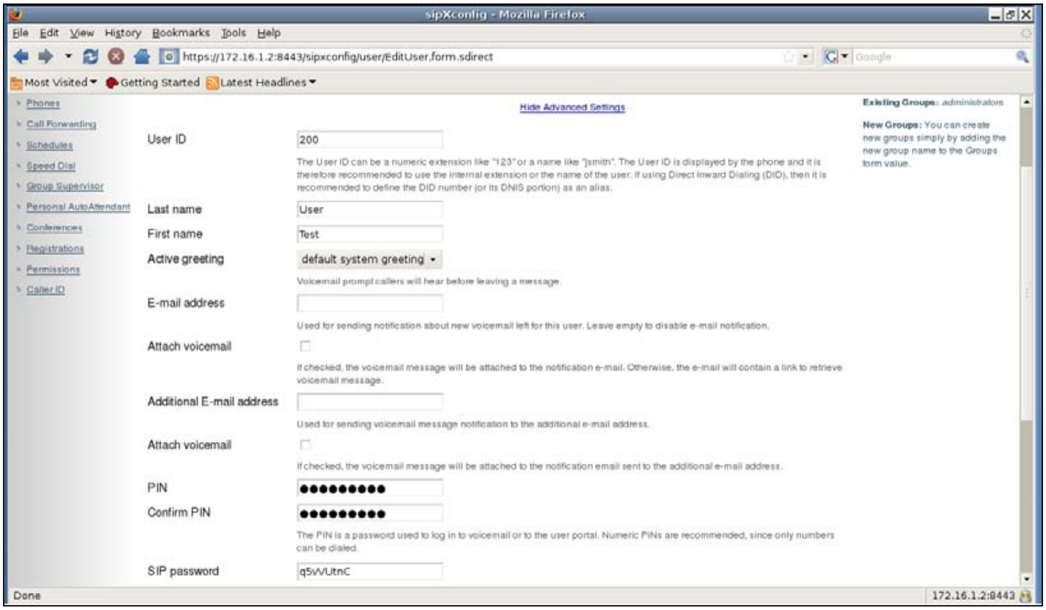
> For large deployments of phones and users, administrators can explore utilizing the sipXecs user and phone CSV file import. Phone suppliers can provide the serial numbers for phones before deployment and the phones along with users can be imported into the system.

Unmanaged phones

As mentioned previously, unmanaged phones are the SIP devices that cannot be automatically configured for use with sipXecs. Since these devices cannot be managed, there is no reason to add them into the sipXecs configuration GUI.

Many devices fall into this category. Unfortunately there is no standard method for manually configuring these devices. One potential source of information is the *Phones and Gateways* page in the sipX Wiki (`http://sipx-wiki.calivia.com/index.php/Phones_%26_Gateways`).

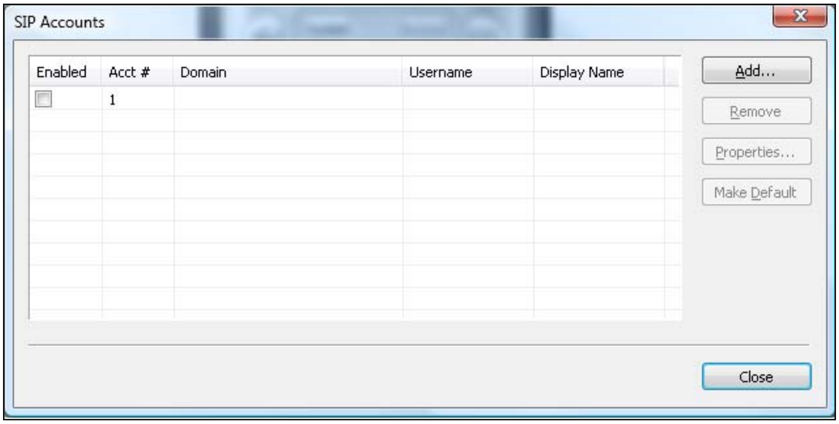
The typical pieces of information required are the SIP username, the SIP password, the domain name, and the PBX fully qualified domain name (FQDN, for example, `sipx.xyzcompany.com`). The SIP username is the user's extension and the SIP password can be displayed on the **User** configuration page (in the **Users** menu, select the **Users** menu item and then click on the individual user hyperlink) by clicking on the **Show Advanced Settings** hyperlink near the top-center of the page. The SIP password for the user will then be displayed directly under the PIN for the user as seen in the following screenshot:



> The **PIN** and **SIP password** reflect two different things. The **PIN** is the voicemail pin for accessing the system, while the **SIP password** is only a phone setting that allows the phone to register. The user would have no way to alter the **SIP password** without the sipX admin.

Counterpath's X-Lite softphone is one of the most popular softphones available and a good example of an unmanaged device. While it is not open source, it is free to use for personal or business use. Binary versions are available for all modern versions of Microsoft Windows, Mac, and Linux. X-Lite supports voice and video calls to a variety of different end-points.

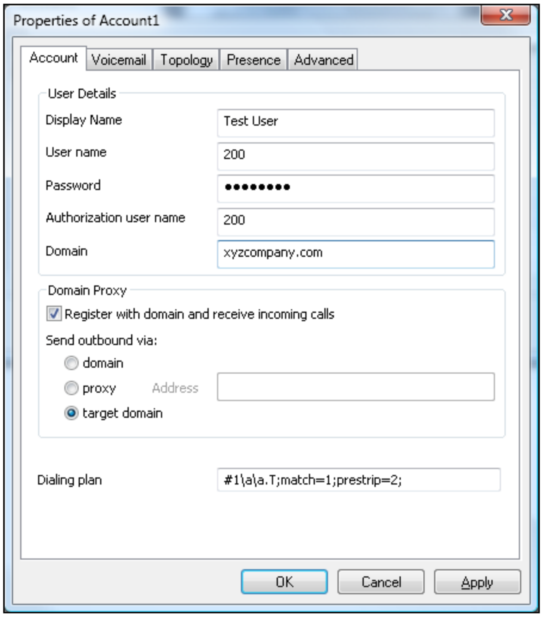
After installing X-Lite, the user will be prompted to enter SIP account information, seen as follows:



Click on the **Add** button to set up the properties for SIP account number **1** (commercial versions of the X-Lite client can register to multiple lines as well as to multiple SIP phone systems). On the **Account** tab enter the following information:

- **Display Name**: Text field that will appear on other phones when the user dials out
- **User Name**: The user's extension
- **Password**: The user's SIP password (not their PIN)

- **Authorization user name**: Same as the user's extension
- **Domain**: The SIP domain (for example, `xyzcompany.com`)



Next, click on the **Voicemail** tab and fill in the following fields (shown as follows):

- **Check for voice mail**: Checked
- **Number to dial for checking voicemail**: 101 (dialing 101 from any phone checks that extension's voicemail)
- **Number for sending calls to voicemail**: 8200 (8 and the extension of the user)

Click on the **OK** button to accept the settings and then click on the **Close** button back on the **SIP Accounts** window. The phone should show that it is registering and then come back with a **Ready** message, as shown in the next screenshot:

[If configuring video calls is required, on the **Advanced** tab, disable **SIP keepalives** and enable **rport**.]

The X-Lite softphone supports the ability to have **Contacts** stored on the righthand side tab and **Video** conversations can be seen on the left. The fully expanded display is shown in the following screenshot:

X-Lite also has the ability to choose different audio sources. It is recommended to get a quality USB headset to use with softphones. To choose or alter the audio devices used with X-Lite, right-click on the phone's user interface, choose **OPTIONS,** and then **Devices** on the left.

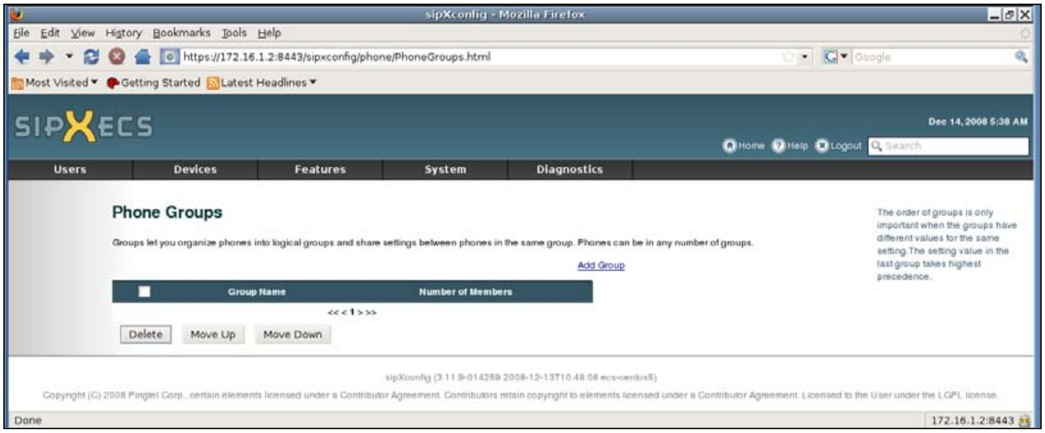
If you are calling X-Lite to X-Lite or to another phone that supports the H.263 video codec, and you have video devices installed and available, video calls are also easily achieved. As with audio, a good USB camera device goes a long way to a good quality experience. If the camera has audio capabilities, the user has the ability in X-Lite to decide how they want the audio to connect to the system. For example, the headset might be used for speaker and microphone on phone calls. In speakerphone mode, perhaps the speakers on the PC and the microphone on a camera would be used instead.

Phone groups

Managing individual phones for any more than a few phones will quickly become cumbersome and error prone. Managed phones can be placed in groups to utilize the same settings across all phones in the group. The administrator can pick and choose how he or she would like to group phones. Common methods of choosing phone groups include phone model (Polycom330, Polycom650), phone purpose (Receptionists, HelpDesk), or physical location (Boston, NewYork).

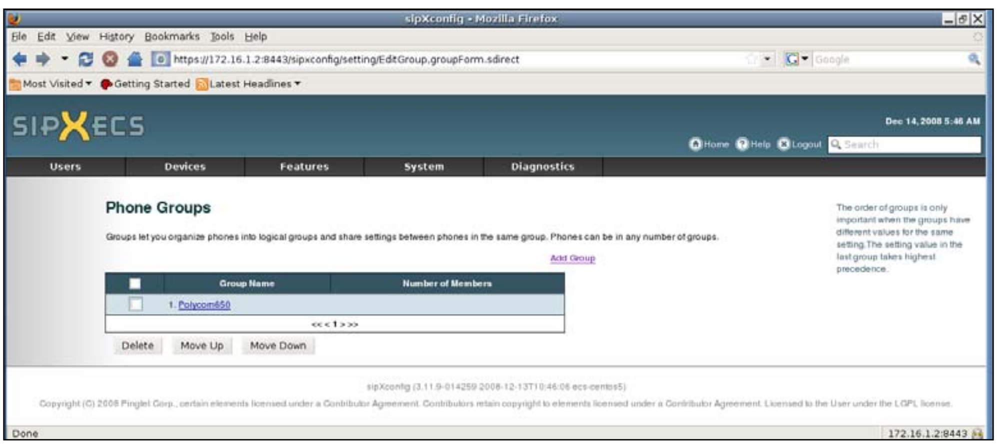
Phones can be in any number of groups. For instance, it may be desirable for all Polycom 650 phones in Boston to have just a few different settings from Polycom 650 Phones in New York. Only the order of the groups is important when groups have different values for the same setting. The last group in the list of groups will take the highest priority.

To get to the **Phone Groups** page, select the menu option for it in the **Devices** menu. The following page will be displayed:



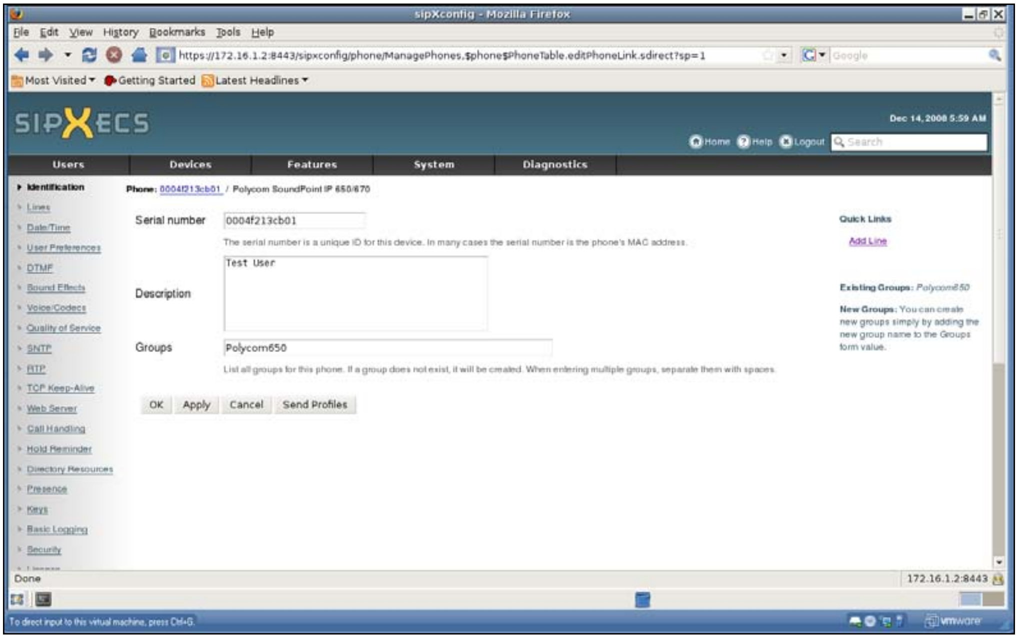
To add a new group, click on the **Add Group** hyperlink near the middle of the page. As seen in the following screenshot, the **Add new Group** page will be displayed where the name will be entered (no spaces are allowed in group names), and a description, if desired.

After clicking on **OK**, the **Phone Groups** page will be displayed again with the new group shown in the list of groups as shown in the following screenshot:



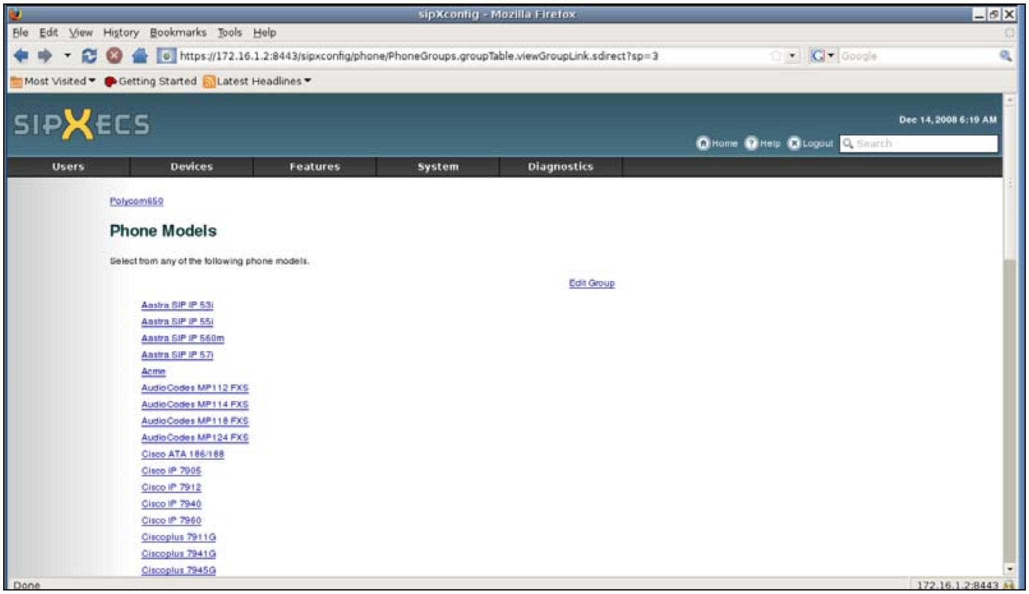
If multiple groups are defined, their order can be changed by placing check marks next to the group names and moving them up and down in the list of groups. For instance if some different settings were desired for Boston and New York users of Polycom 650 phones, the groups should have the group containing the Polycom 650s first in the list of groups and then Boston and New York groups after that group. This would first impose the common settings for all Polycom 650s across all phones and then any settings configured in the Boston and New York groups would take precedence over the more generic Polycom 650 settings.

Once the group is defined, click on the **Devices** menu and select the **Phones** menu item. Select the phone to add to the newly created group and enter the group name exactly as it was created in the groups menu (capitalization is important). As shown in the following screenshot, the list of phone groups defined can be seen in the right side of the page after **Existing Groups**.

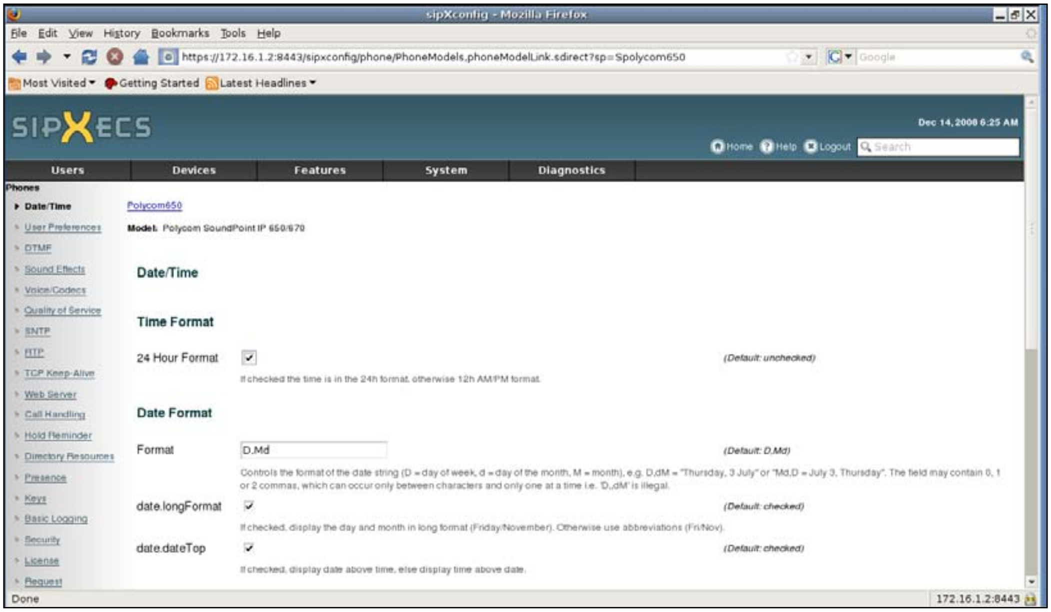


As with user groups, phone groups can be created on the fly while creating or editing phones by simply putting a group name in the **Groups** dialog box of any phone.

Once a group is defined and phones have been assigned to it, group settings still need to be made for the group. To get to the settings for the group, click on the **Devices** menu and select the **Phone Groups** menu item. On the **Phone Groups** page click on the group name and a list of phones will be displayed as follows:



Select the phone model for which you would like to make settings and click on the hyperlink. The settings that sipxconfig can set for that model phone will be displayed as follows:



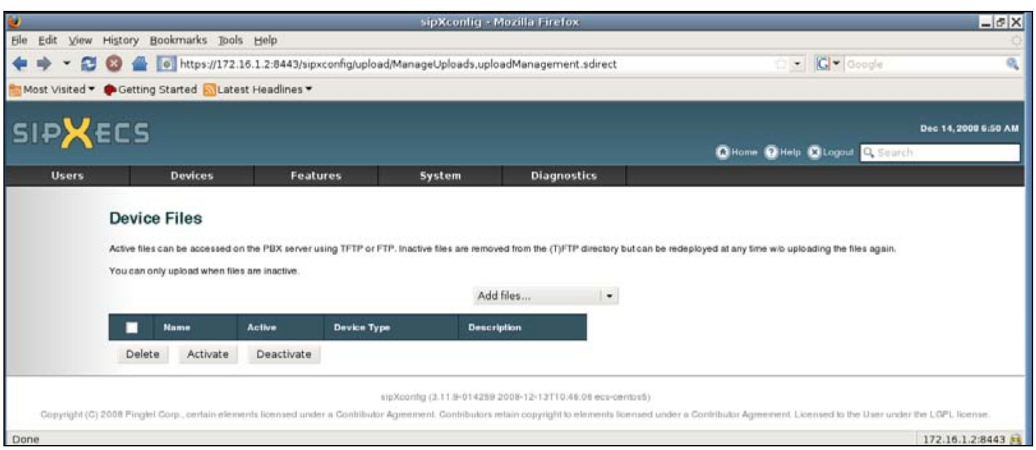
Make any desired changes (see the *Advanced phone configuration* section for some examples) by clicking on the **Apply** button between page changes and then clicking on the **OK** button when complete. If all the desired changes are made but some changes are required in the future, the phone configuration files must be regenerated (**Devices** menu, **Phones** menu item, either click on the **Send All Profiles** button or select the affected phones and click on the **Send Profiles** button).

Phone firmware

Hardware phone vendors update the software that operates their phones fairly regularly. This software is called firmware. Some vendors also have separate code called a bootrom to initially boot the phones. sipXecs has the ability to maintain these files for administrators in the phone profile download folder (`/var/sipxdata/configserver/phone/profile/tftproot`).

Different versions of the files can be maintained in the system, but typically, only one set of device files for each vendor is allowed at each time. For example, sipXecs can have only one set of polycom software for all polycom phones in the system.

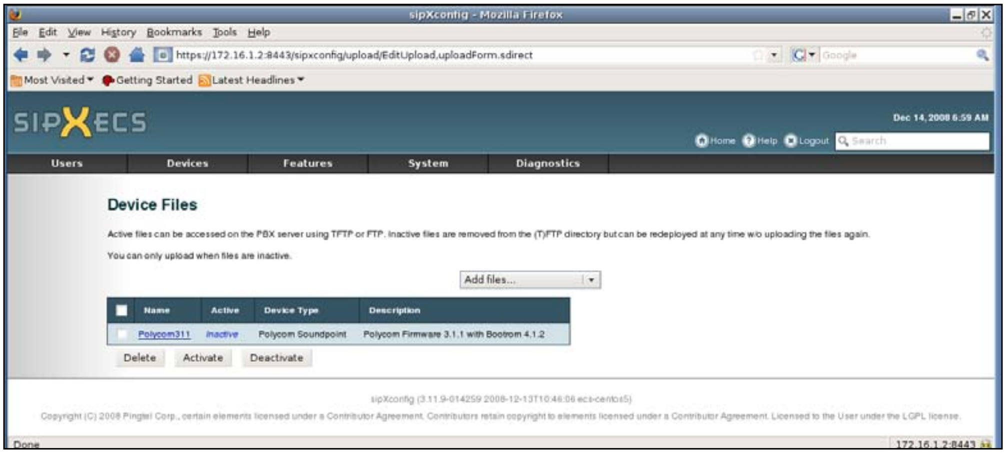
To create a device file set, click on the **Devices** menu and select the **Device Files** menu item. The **Device Files** page will appear as follows:



Clicking on the **Add files** drop-down menu will reveal the list of devices for which sipXecs knows how to maintain device files. If the devices you are using are not listed, raw files can be placed in the phone profile download folder using the **Unmanaged (T)FTP Files** menu item.

Once a menu item is selected, the following page will be displayed. This will prompt the administrator to enter the **Name** and an optional **Description**, of the device file set, as seen in the following screenshot:

Click on **OK** and the **Device Files** page will be displayed again with the new device file set listed and in an **Inactive** state, as follows:



Click on the device file set name hyperlink and then browse for the firmware files on your computer and upload them by clicking on **OK**.

After the files are uploaded, place a check mark next to the device file set and click on the **Activate** button. The system will then uncompress the files (if they are in a compressed state) and move them to the phone profile download folder.

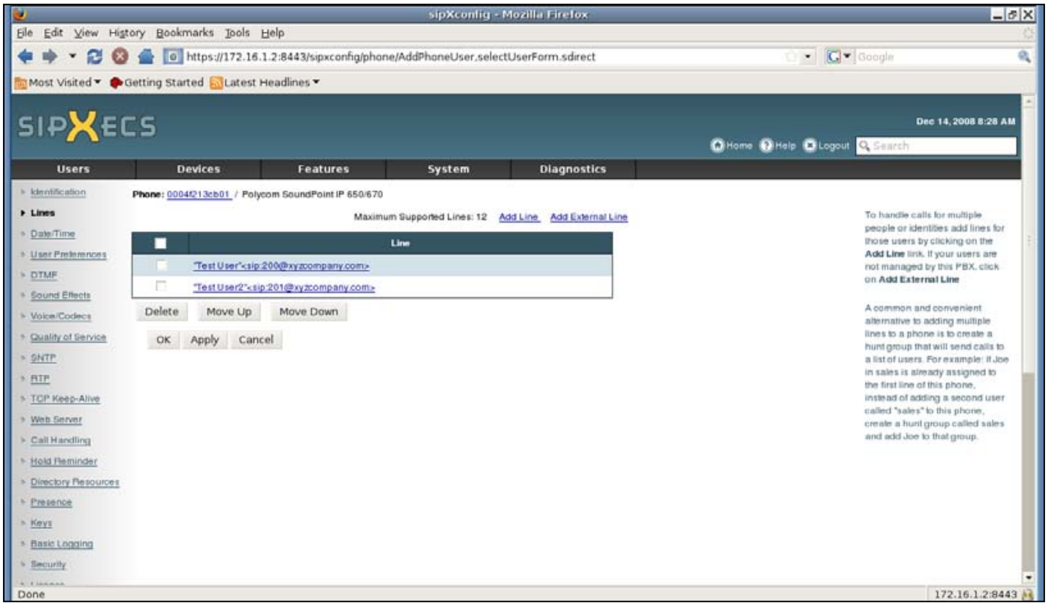
Advanced phone configuration

Most IP hardware and software phones are highly customizable devices. Polycom devices have 32 different settings menus available for the administrator to explore and tweak to their hearts content. Finding the proper settings for the system being deployed is usually a matter of trial and error. The following is a list of common user requests:

Multiple lines on a phone

For phones that support multiple lines, adding the extra lines is an easy task. In the sipXecs administration screen under the **Devices** menu select **Phones** then click on the phone to which you would like to add the additional line.

Under **Quick Links** on the right side of the page is an **Add Line** hyperlink. Clicking on that hyperlink will display the **Add Line** page where you can click on the **Search** button to bring up a list of all extensions in the system. Place a check mark next to the user(s) to add to the phone and then click on the **Select** button. The phone configuration screen will then be displayed showing the additional line, as follows:



Click on the **OK** button to return to the phone list, select the phone with the check box next to it and then click on the **Send Profiles** button to generate the new configuration file for the phone.

Multiple phones for a user

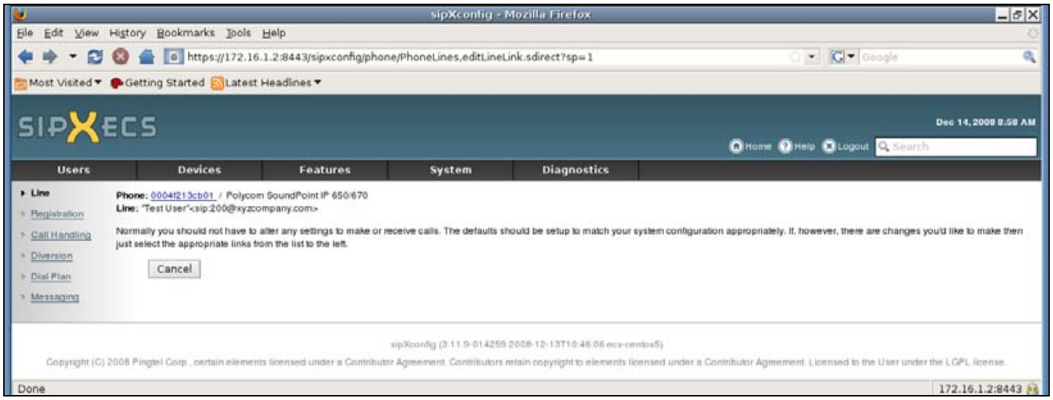
The sipXecs system supports a SIP proxy feature known as *parallel forking*. Parallel forking allows a single SIP user account to register on up to 8 devices. The system will then ring all of those devices simultaneously when that user is dialed. Note that different phone vendor's phones may behave differently and not allow quite as many phones registered to the same line.

This feature is useful when users have a desk phone and a software-based phone. If the user is travelling with their laptop or portable device and has the software phone running, they will be able to receive calls.

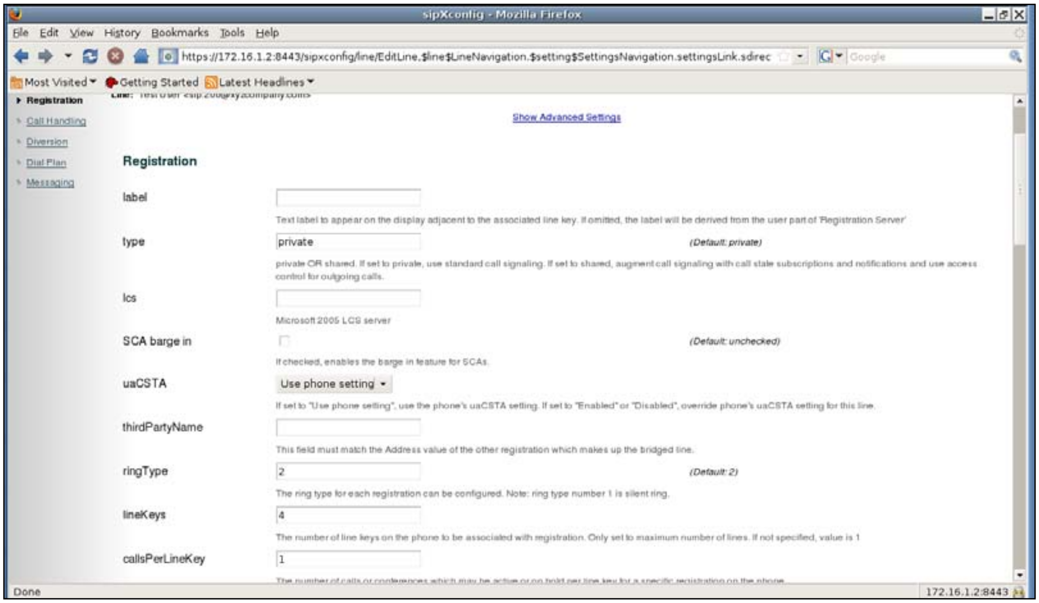
Multiple line appearances on a phone

Most multiple line IP hardware phones allow multiple calls to a single line. This can be quite confusing for the average phone user and difficult to deal with at an answering position. To remedy this problem it is easier for the user to have multiple appearances of the same line on their telephone. Each successive call will ring on the next line appearance.

To configure this functionality, click on the desired phone on the **Phones** page (**Devices** menu, **Phones** menu item). On the lefthand side of the page, select the **Lines** hyperlink and then click on the line for which multiple appearances are desired. This should bring you to the following screen:



Click on the **Registration** hyperlink to the left and then scroll down to find the **lineKeys** and **callsPerLineKey** dialog boxes, shown in the following screenshot:



The preceding example shows that this phone will have four line appearances for this line and only one call will be allowed on each line. Assign the desired values, click on the **OK** button at the bottom of the page, and then send the profile for the phone (select the phone with the checkbox next to it and click on the **Send Profiles** button to generate the new configuration file for the phone).

Summary

Chapters 4 and 5 cover 95% of the typical day-to-day functions that a communications systems manager will be performing. The reader should now have a good basic knowledge of adding users and phones to the system. A fully functional phone system is one more chapter away, when the system is connected to the outside world.

6

Connecting to the World with sipXecs

Eventually your users will want to dial out of the system. Gateways provide the connectivity required to reach other systems. These systems can be other sipXecs PBX's, traditional phone lines, or **Internet Telephony Service Providers** (**ITSP**s).

Connecting the IP phone system to the outside world is one of the most difficult tasks in making the phone system work. If the network infrastructure is configured properly for quality of service, the connection to the outside world can most likely be the source of any call quality problems.

Traditional analog **Plain Old Telephone Service** (**POTS**) lines are the largest source of frustration. If you can avoid them by utilizing a digital type of service or an ITSP, by all means take that avenue. For those not so lucky, you'll learn more about them then you ever thought you needed to. Typically, volume levels, line disconnect, and echo are the most common problems. Most gateways will have some advanced settings for dealing with these issues but they are different for every manufacturer.

In this chapter we will cover the following topics:

- Adding managed and unmanaged gateways
- Setting up the Session Border Controller
- Working with Dial Plans

Adding gateways

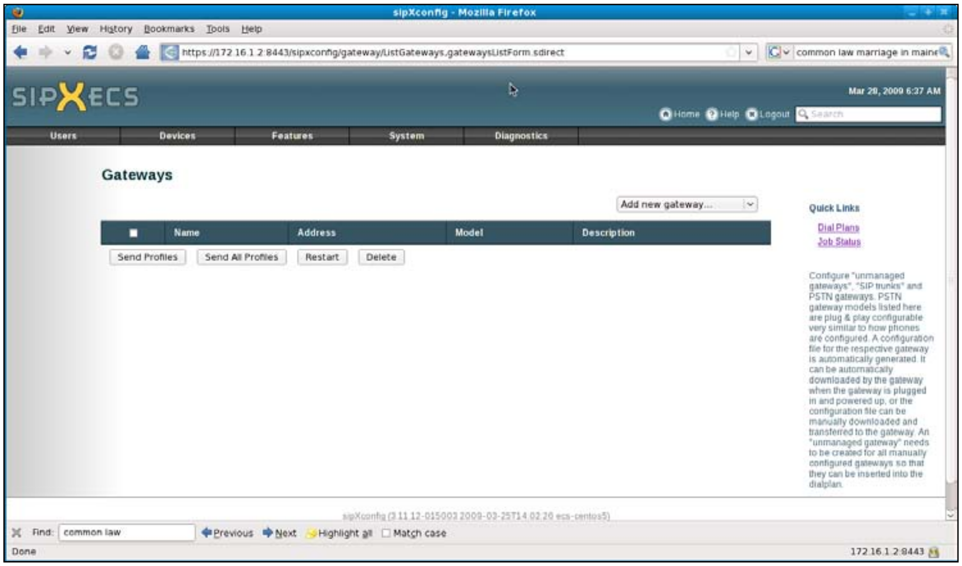
There are three types of gateways that can be configured to work in sipXecs; managed, unmanaged, and SIP Trunks. A managed gateway is a hardware device that connects to a traditional phone line. sipXecs knows how to generate configuration files (plug and play) for it. An unmanaged gateway is either a hardware device for which sipXecs doesn't know how to generate configuration files, or it may be another SIP PBX (such as another sipXecs system, see the *Connecting two sipXecs servers* section in Chapter 9). A SIP Trunk is a connection to an ITSP.

Managed gateways

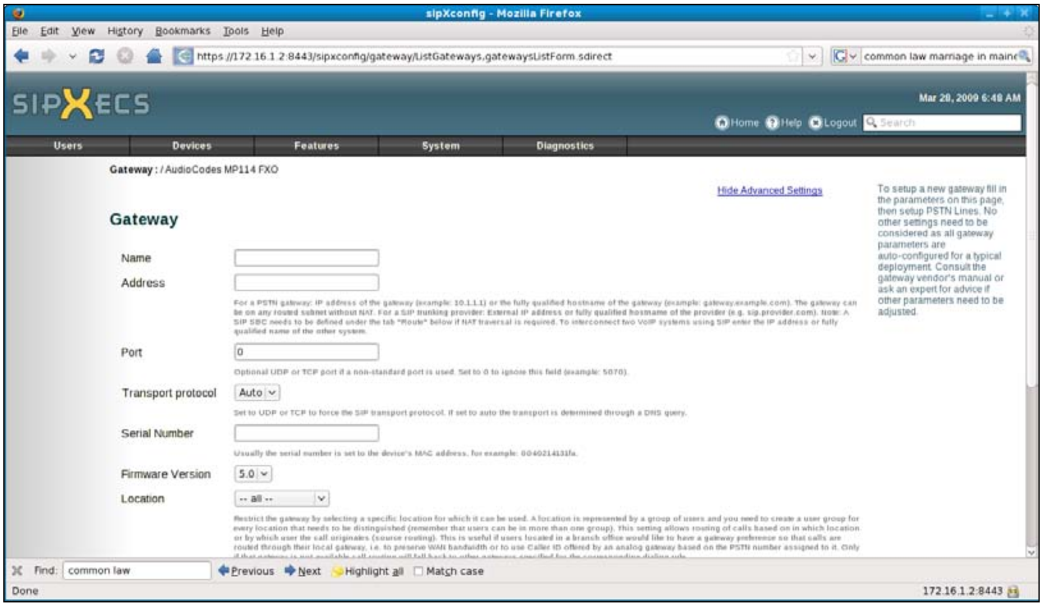
At present, there are eight gateways for which sipXecs generates configuration information (ACME 1000 and AudioCodes Models MP114, MP118, Mediant 1000/2000/3000/BRI, and TP260). This is just a small cross section of gateways available in the market. If your gateway is not in this list, see the following *Unmanaged gateways* subsection. The following detailed information about managed gateways may prove to be useful in setting up an unmanaged gateway.

For the following example screens, we'll utilize an AudioCodes MP114 **FXO** (**Foreign Exchange Office**) gateway. This particular gateway has four analog ports for connecting to POTS lines. Information on the gateway is available at `http://www.audiocodes.com/products/mediapack-1xx`.

To add the gateway, click on the **Gateways** menu item in the **Devices** menu. As shown in the following screenshot, there are no gateways configured by default.



To add a managed gateway, click on the **Add new gateway** drop-down box and select the appropriate gateway. The gateway configuration page will be displayed as follows:

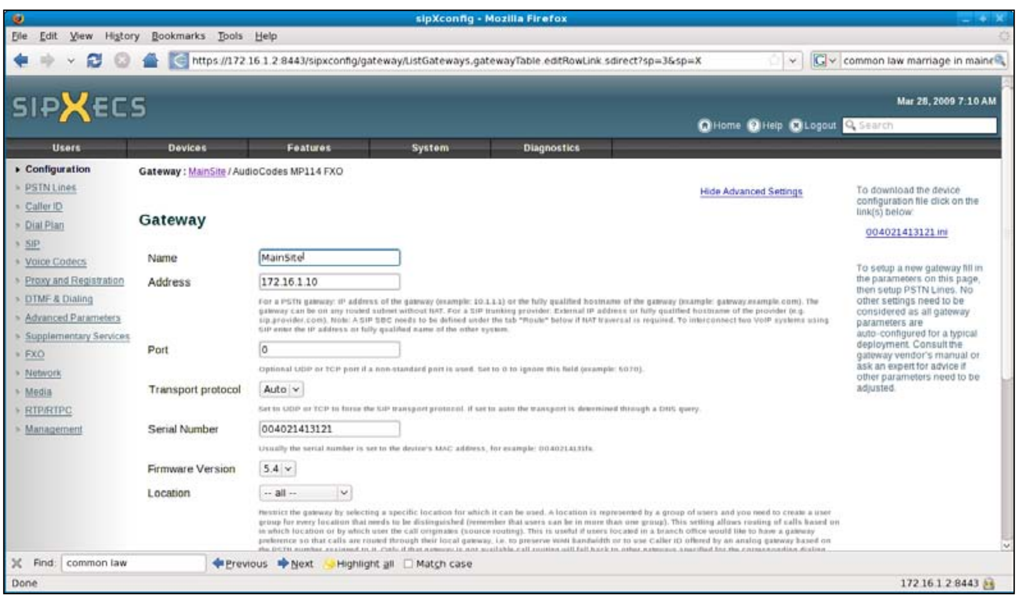


The following configuration information can be configured on this page (click on the **Show Advanced Settings** hyperlink to display all configuration items):

- **Name**: A name given to the gateway (no spaces).
- **Address**: The IP address of the gateway or the fully qualified hostname of the gateway (see manufacturer's documentation for information on configuring IP address and other basic settings).
- **Port**: An optional setting for UDP or TCP port if a non-standard port is used. Set to 0 to ignore this field.
- **Transport protocol**: This can be manually configured to UDP or TCP to force the SIP transport protocol. If it is set to **Auto**, the transport is determined through a DNS query.
- **Serial Number**: This is the Ethernet MAC address of the gateway.
- **Firmware Version**: Certain gateways may have different configuration file information or formats depending on the version of firmware in the device. Select the version of firmware that is loaded in the gateway (see manufacturer's documentation).

- **Location**: It is possible to restrict the gateway by selecting a specific location for which it can be used. A location is represented by a group of users. A user group must be created for every location that needs to be distinguished (remember that users can be in more than one group). This setting allows routing of calls based on the location or the user from which the call originates (source routing). This is useful if users located in a branch office would like to have a gateway preference so that calls are routed through their local gateway, for example, to preserve WAN bandwidth or to use caller ID offered by an analog gateway based on the PSTN number assigned to it. Only if that gateway is not available, will call routing fall back to other gateways specified for the corresponding dialing rule.
- **Shared**: If this setting is checked, this gateway can be used by any user in any location, even if a specific location is selected. This setting is checked by default so that users in an identified location still use their preferred gateway, but the gateway can also be used by other users in other locations.
- **Description**: This is for documenting the system configuration. Information about the lines connected to the gateway is very useful here.

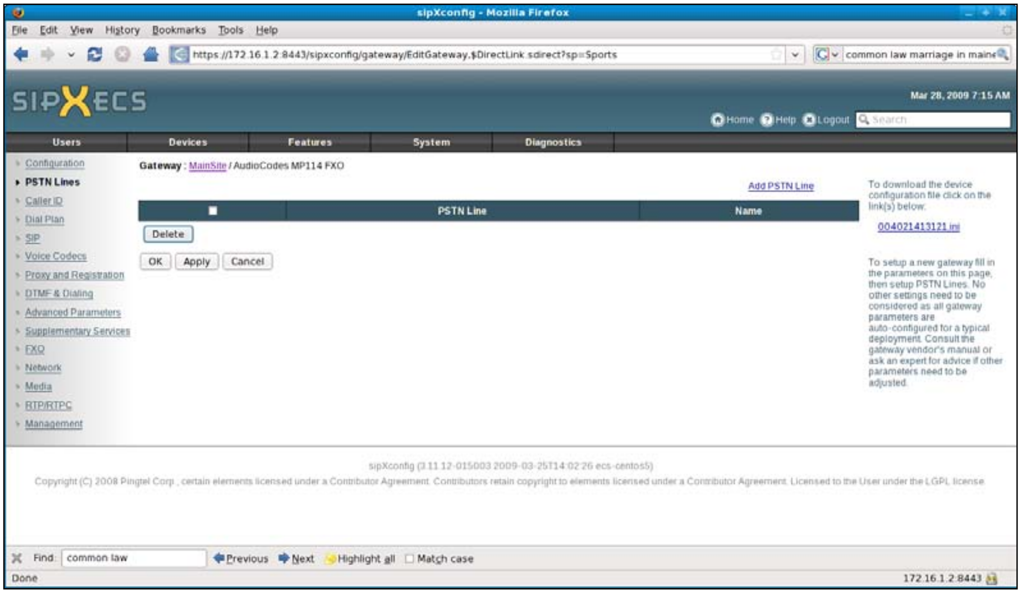
With all of the configuration information entered, click on the **OK** button and the **Gateway** page will be displayed as follows with the new gateway on it. Click on the gateway name to reveal more configuration options, as shown in the following screenshot:



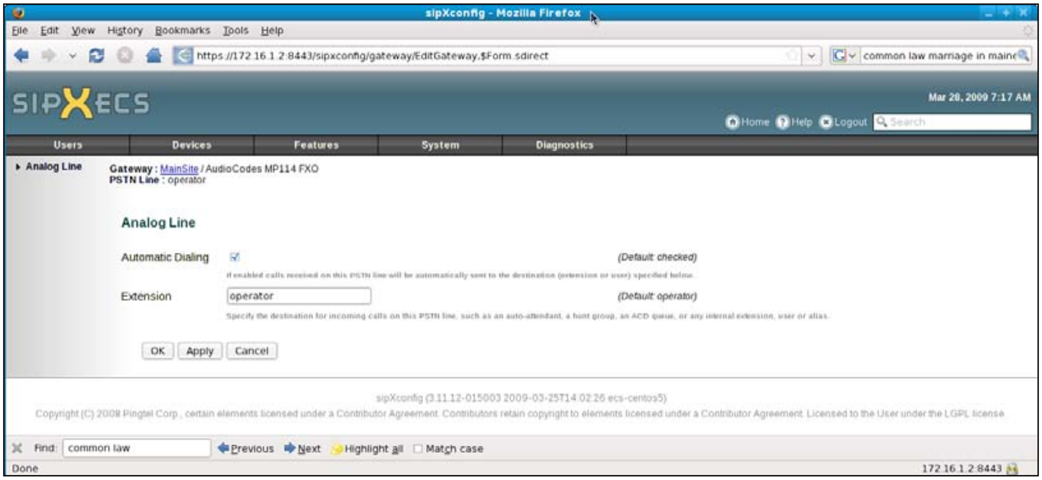
In the following subsections we'll explore the managed gateway settings available.

PSTN Lines

Click on the **PSTN Lines** item on the lefthand menu. As shown below, there are no lines defined on the gateway by default.



Click on the **Add PSTN Line** hyperlink and the following page will be displayed:



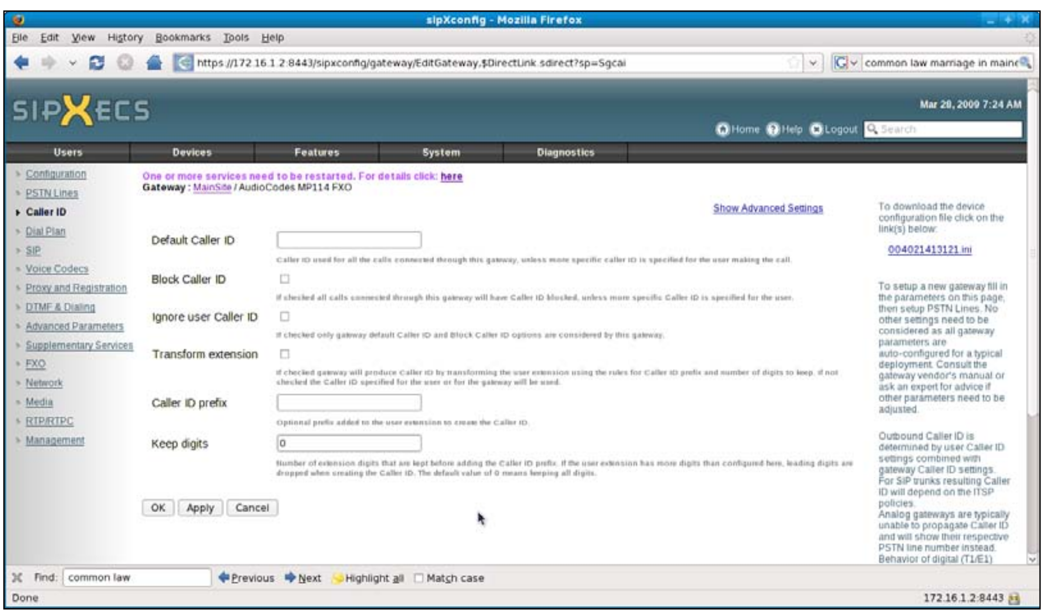
This page has two configuration options:

- **Automatic Dialing**: If this is enabled, calls received on this PSTN line will be automatically sent to the destination (extension or user) specified below it. The default is enabled. If it is not enabled, incoming calls will ring and never be forwarded.
- **Extension**: This is the destination extension for incoming calls on this PSTN line, such as an auto attendant, a hunt group, an ACD queue, or any internal extension, user, or alias. The default value is **operator**, which is an alias on the auto attendant.

Click on **OK** to add the line to the gateway. Repeat for the number of lines that are in use on the gateway.

Caller ID

The **Caller ID** page allows the administrator to set outbound caller ID information. This isn't particularly useful for analog lines as this is not a function that can be utilized. With a T1/PRI/BRI gateway, the administrator can insert whatever is necessary for caller ID informaton to the outgoing calls.



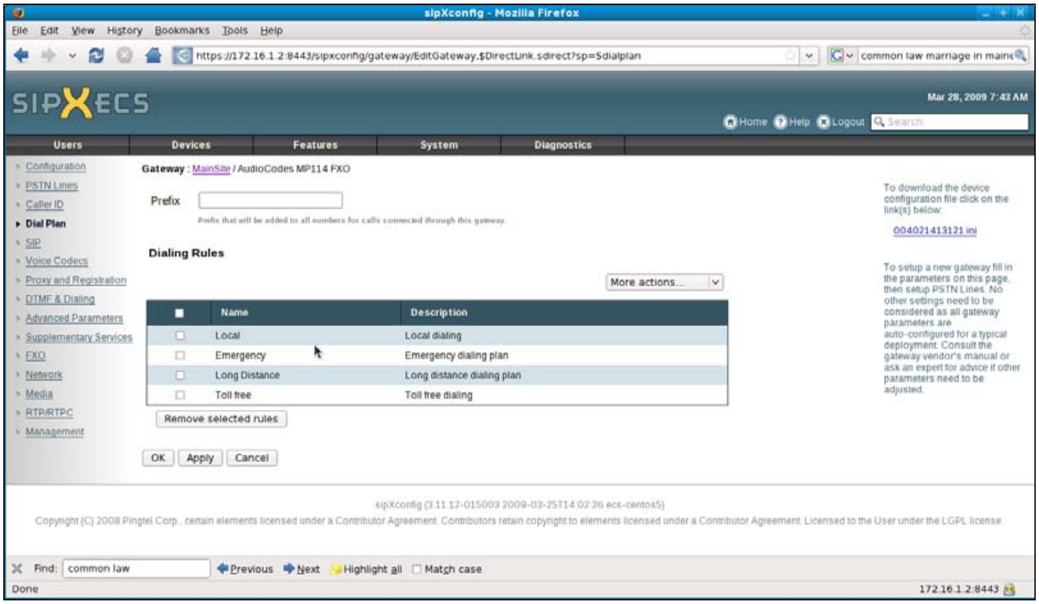
The following options are available on the preceding **Caller ID** page.

- **Default Caller ID**: This is the outgoing caller ID used for all the calls connected through this gateway, unless a more specific caller ID is specified for the user making the call (specified in the user configuration; see Chapter 4).
- **Block Caller ID**: If this is checked, all calls connected through this gateway will have outbound caller ID blocked, unless a more specific caller ID is specified for the user.
- **Ignore user Caller ID**: If this setting is checked, only the gateway **Default Caller ID** and **Block Caller ID** options are used for outgoing calls through this gateway.
- **Transform extension**: If this setting is checked, the gateway will produce the caller ID by transforming the dialing user's extension using the rules for caller ID prefix and number of digits to keep. If it is not checked, the caller ID specified for the user or for the gateway will be used.
- **Caller ID prefix**: This is an optional prefix added to the user extension to create the caller ID.
- **Keep digits**: This is the number of user extension digits that are kept before adding the **Caller ID prefix**. If the user extension has more digits than configured, then the leading digits are dropped while creating the caller ID. The default value of 0 means keep all of the digits.

Click on the **Apply** button to keep any changes made on this page.

Dial Plan

The **Dial Plan** page, as shown in the following screenshot, allows the administrator to add a dial prefix for outbound calls and also add the gateway to any pre-configured system dialing rules (see the *Dial plan* section under *Unmanged gateways*, later in this chapter).



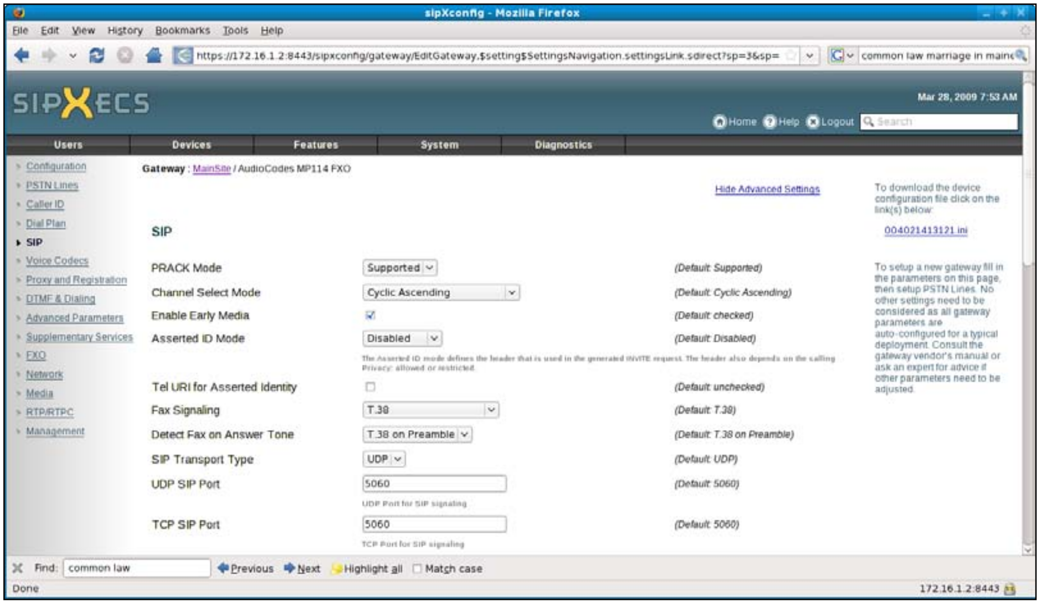
The following configuration options are available on this page:

- **Prefix**: The administrator can configure an outbound dialing prefix that will be added to all numbers for calls connected through this gateway. This is useful if centrex lines are in use.
- **Dialing Rules**: The system dialing rules that should use this gateway can be specified in this section. Click on the **More actions** drop-down box to select the dial plan entries that are defined in the system.

Click on the **Apply** button to keep any changes made on this page.

SIP

The SIP configuration page allows fine-grained control over SIP parameters in the gateway, if **Show Advanced Settings** is clicked. Most commonly, all of the default settings can be used.



The following configuration options are available on this page. Click on the **Show Advanced Settings** hyperlink to reveal all options. (For more detailed information about how all of these settings affect the gateway, please refer to the manufacturer's documentation.)

- **PRACK Mode**: **PRACK** stands for **Provisional Response Acknowledgement** support for the gateway. PRACK is defined in RFC 3262. Provisional responses provide information on the progress of the request processing. The default setting for this mode is **Supported** (checked).
- **Channel Select Mode**: This mode determines how the outbound phone lines are selected. The commonly used settings are **Ascending** (starting from line 1 and progressing up in line numbers, each time resetting to the lowest available number line that is not in use), **Cyclic Ascending** (starting from line 1 and ascending in line numbers for each call and wrapping around to line 1 again after each line has been used), **Descending** (starting at the highest line number available and descending to line 1, each time resetting to the highest available number line that is not in use) and **Cyclic Descending** (starting at the highest line number available and descending in line numbers for each call and wrapping around to line 1). The default value is **Cyclic Ascending**. Note that it is best to use the opposite direction to show how the lines ring into the system from the outside provider's inbound hunt group. This helps to avoid a condition referred to as glare. Glare occurs if the phone system picks up a line to dial out that is ringing in at the same time.

- **Enable Early Media**: Early Media refers to the ability of two SIP user agents to communicate before a SIP call is actually established, which is generally for call setup with a PSTN or PBX connection. The default is enabled (checked).
- **Asserted ID Mode**: This mode defines the header that is used in the generated INVITE request. The header also depends on the calling privacy—it can be allowed or restricted. The default setting is disabled for this mode.
- **Tel URI for Asserted Identity**: If "Asserted Identity" is selected, the telephone URI will be used for the AI. The default is to not use the Tel URI (unchecked).
- **Fax Signaling**: Fax machines (and modems for that matter) have a difficult time communicating over a normal G.711 voice path. The T.38 protocol allows fax machines to communicate between gateways. The default is to have T.38 enabled.
- **Detect Fax on Answer Tone**: If T.38 is enabled above, a fax machine can be detected when the call is answered with this setting. The default is T.38 on Preamble.
- **SIP Transport Type**: This selects UDP, TCP, or TLS for the SIP transport type. The default is UDP.
- **UDP SIP Port**: This allows the SIP UDP signaling port to be changed. The default is 5060.
- **TCP SIP Port**: This allows the SIP TCP signaling port to be changed. The default is 5060.
- **TLS SIP Port**: This allows the SIP TLS signaling port to be changed. The default is 5061.
- **TCP Connection Reuse**: If TCP is reused, a SIP client behind a NAT'd network can keep a TCP connection open and both client and server can reuse it. This makes TCP communication potentially easier when NAT is in use. The default is to not reuse the TCP connection (unchecked).
- **Tel to IP No Answer Timeout**: This is the timeout for a phone call ringing into a SIP extension. The default value is 180 seconds. This may need to be increased if the inbound calls need to ring longer.
- **Remote Party ID**: This setting is not used by sipXecs but might be used in a gateway-to-gateway configuration. It allows the receiving gateway to identify a remote gateway by its ID. The default value is to not send it (unchecked).

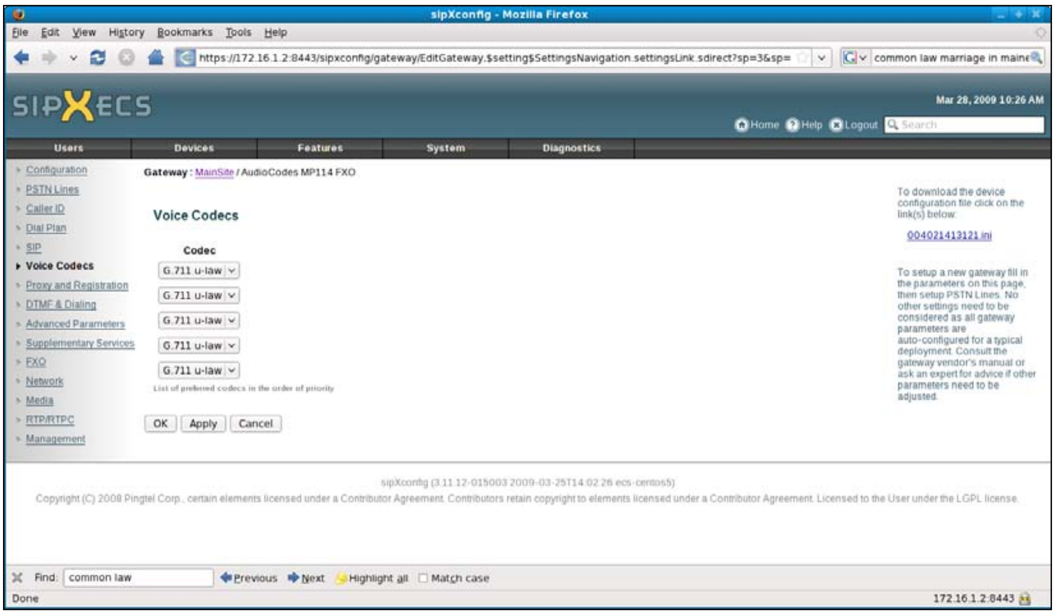
- **RPI Header Content**: Used with the above setting. The default is set to "Include Number Plan" and "Type".
- **History-Info Header**: From RFS 4244—*a standard mechanism for capturing the history information associated with a* **Session Initiation Protocol** (**SIP**) *request. This capability enables many enhanced services by providing the information as to how and why a call arrives at a specific application or user*. This information is not used by sipXecs and is disabled by default (unchecked),
- **Use Source Number as Display Name**: This uses the source phone number as the display name on inbound calls to the PBX. The default setting is "No".
- **Use Display Name as Source Number**: This uses the configured display name as the source number on inbound calls. The default is disabled (unchecked).
- **Play Ringback Tone to IP**: Allows the gateway to play the ringing tone to the IP side of the gateway. The default is disabled (unchecked).
- **Play Ringback Tone to Tel**: Allows the gateway to pick up a phone call and then continue playing a ring tone to the caller. Valid settings are "Don't Play", "Always Play", "Play" according to 180/183, and "Play" according to PI (default). See Audiocodes manual for more detailed information.
- **Enable GRUU**: A URI that routes to a specific UA instance is called a **Globally Routable UA URI** (**GRUU**). The default is disabled (unchecked). See Audiocodes manual for more detailed information.
- **User-Agent Information**: Defines the string that is used in the SIP request header "User-Agent" and SIP response header "Server". If it is not configured, the default string "AudioCodes product name s/w-version" is used. The default is blank (not configured).
- **SDP Session Owner**: The value of the Session Owner line ("o" field) in outgoing **Session Description Protocol** (**SDP**) bodies. May be up to 39 characters. The default value is AudiocodesGW.
- **Subject**: Defines the value of the subject header in outgoing INVITE messages. If it is not specified, the subject header isn't included. The default is blank (not specified).
- **Multiple Packetization Time Format**: This setting enables the IP gateway to define a separate Packetization period for each negotiated coder in the SDP. The "mptime" attribute is included only if this parameter is enabled, even if the remote side includes it in the SDP offer. The default is disabled (unchecked).
- **Reason Header**: This enables or disables the use of the SIP reason header. The default is enabled (checked).

- **3xxBehavior**: Determines the gateway's behavior when a SIP 3xx response is received for an outgoing INVITE request. The gateway can either use the same call identifiers (Call ID, branch, to and from tags) or change them in the new initiated INVITE. If this is disabled, the gateway will use different call identifiers for a redirected INVITE message. If it is enabled, the gateway will use the same call identifiers. The default is set to disabled (unchecked).
- **Enable P-Charging-Vector**: From RFC 3455—*P-Headers are a set of private Session Initiation Protocol (SIP) headers (P-headers) used by the* **3rd-Generation Partnership Project** (**3GPP**). *The P-Charging-Vector header is used to convey charging related information, such as the globally unique IMS charging identifier (ICID) value*. This value is used primarily for call accounting but not used by sipXecs and thus the default is set to disabled (unchecked).
- **Enable Voicemail URI**: This enables or disables the interworking of target and cause for redirection from Tel to IP and vice versa, according to RFC 4468. The default is disabled (unchecked).
- **SIP T1 Retransmission Timer [msec]**: This is the time interval (in milliseconds) between the first transmission of a SIP message and the first retransmission of the same message. The default is 500 ms.
- **SIP T2 Retransmission Timer [msec]**: This is the maximum interval (in milliseconds) between retransmissions of SIP messages. The time interval between subsequent retransmissions of the same SIP message starts with **SIP T1 Retransmission Timer** and is multiplied by two until the **SIP T2 Retransmission Timer** is reached. The default is 4000.
- **SIP Maximum RTX**: This is the number of UDP transmissions (first transmission + retransmissions) of SIP message. The range is 1 to 7. The default value is 7.

Click on the **Apply** button to keep any changes made on this page.

Voice Codecs

The **Voice Codecs** page allows the administrator to specify what Codecs (compression / decompression algorithms) the gateway is allowed to use. By default, the sipXecs media services only support G.711 uLaw and aLaw Codecs (64 to 80 Kbps per call).

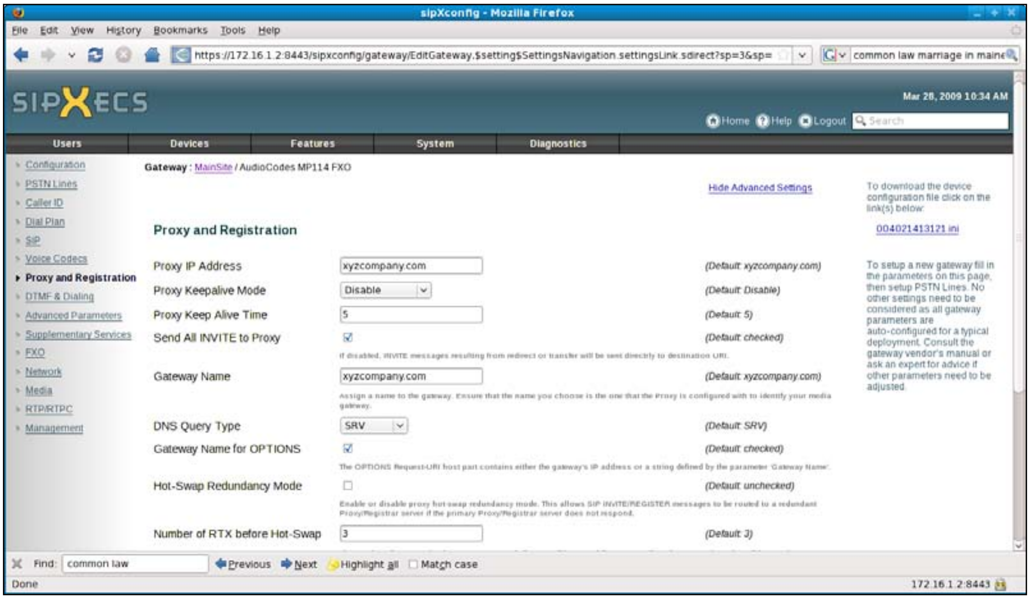


From the drop-down boxes select the protocols required on the gateway.
If a remote phone is being used for the outgoing calls through this gateway, it may be advantageous to select **G.729** as the second **Codec** (8 to 12 Kbps per call).

Click on the **Apply** button to keep any changes made on this page.

Proxy and Registration

The **Proxy and Registration** page determines how the gateway interacts with the PBX. In the sipXecs world, gateways do not register with the PBX (however, individual lines on an FXS gateway do).



The following configuration options are available on this page (click on **Show Advanced Settings** to reveal all options):

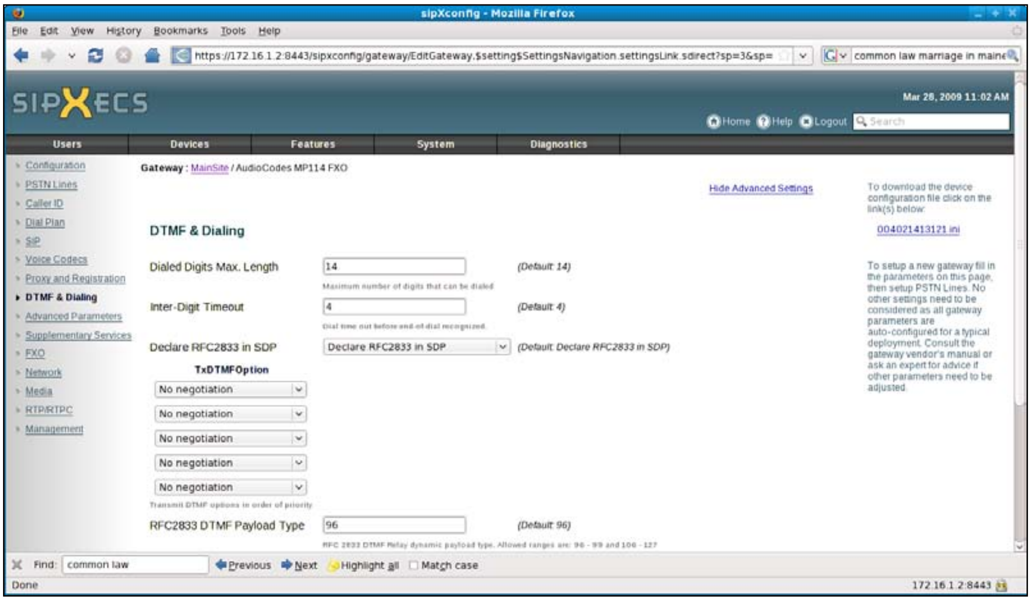
- **Proxy IP Address**: This should be set to the SIP domain of the PBX. (With the example system that has been used, this would be **xyzcompany.com**.)
- **Proxy Keepalive Mode**: If this is set to "Options", a SIP OPTIONS message is sent every **Proxy Keep Alive Time**. If set to "Register", a SIP REGISTER message is sent every registration time. Any response from the proxy, either success (200 OK) or failure (4xx response) is considered as if the proxy is correctly communicating. Since gateways don't need to register with sipXecs, this value is not needed and is set to disabled by default.
- **Proxy Keep Alive Time**: This defines the proxy keep-alive time interval (in seconds) between keep-alive messages. The default is set to 5 seconds but is not used because **Proxy Keepalive Mode** is set to disabled.
- **Send All INVITE to Proxy**: If this is disabled, INVITE messages resulting from redirect or transfer will be sent directly to the destination URI. The default is set to enabled (checked) so that all INVITE messages are transmitted to the proxy server (to the PBX).

- **Gateway Name**: This is the name of the gateway. Ensure that the name you choose is the one that the Proxy is configured with to identify your media gateway. The default is set to the SIP domain name (from the example that has been used it would be set to **xyzcompany.com**).
- **DNS Query Type**: This is for querying the SIP domain. It can be set to A-Record, DNS NAPTR, or SRV records. The default setting is set to SRV.
- **Gateway Name for OPTIONS**: The OPTIONS Request-URI host part contains either the gateway's IP address or a string defined by the parameter "Gateway Name". If this is enabled, the gateway sends its name as the host part of the SIP URI. If it is disabled, the IP address is used. The default is enabled (checked).
- **Hot-Swap Redundancy Mode**: The user can enable or disable proxy hot-swap redundancy mode. This allows SIP INVITE/REGISTER messages to be routed to a redundant proxy/registrar server if the primary proxy/registrar server does not respond. This is not required by sipXecs (unchecked) because SRV records are used for routing between redundant SIP proxies.
- **Number of RTX before Hot-Swap**: The AudioCodes default value is 3 retransmits before switching to a redundant SIP Proxy. This setting is not needed either because of the use of SRV records.
- **Challenge Caching Mode**: To reduce the number of SIP messages, challenges can be cached. Select the desired level of challenge caching to use with SIP proxies. The default is set to none (challenges are not cached).
- **Mutual Authentication Mode**: This mode selects whether **Authentication** and **Key Agreement** (**AKA**) digest authentication information are optional or mandatory for incoming requests. If it is set to "Mandatory", incoming requests without AKA information will be rejected. The default setting is "Optional".

Click on the **Apply** button to keep any changes made on this page.

DTMF & Dialing

The Gateway **DTMF & Dialing** page is used to configure how the gateway interacts with dialed digits.



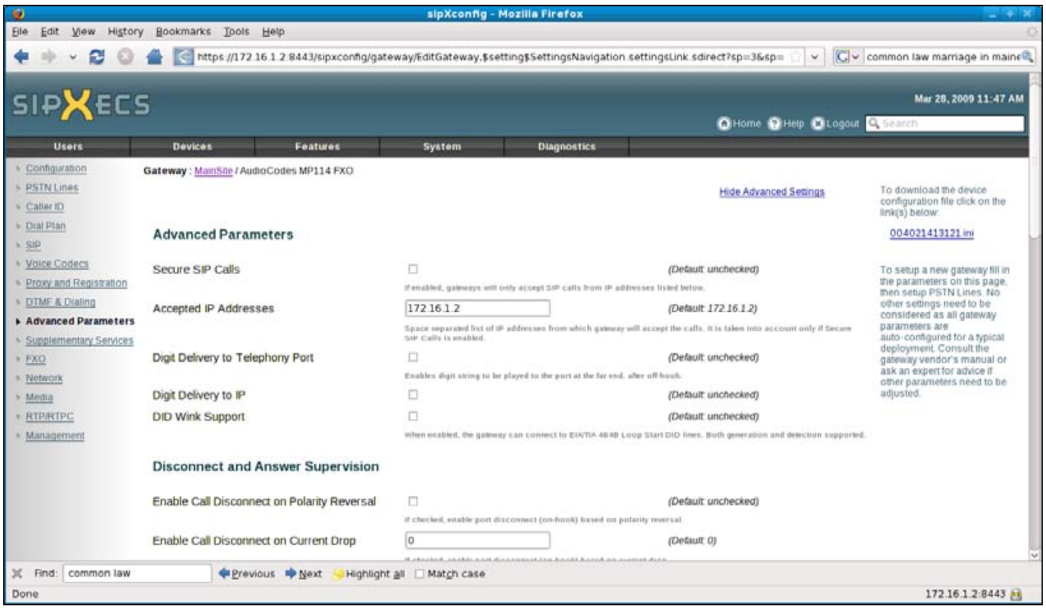
The following configuration options are available on this page (click on **Show Advanced Settings** to reveal all options):

- **Dialed Digits Max. Length**: The maximum dialed number length allowed. The default is set to 14 digits.
- **Inter-Digit Timeout**: The gateway's dial time-out before end of dialed string is automatically set. The default is 4 seconds.
- **Declare RFC2833 in SDP**: RFC2833 determines how dialed digits (DTMF) are dealt with within a phone call. The gateway needs to be set to declare RFC2833 in the **Session Description Protocol** (**SDP**). DTMF is done in-band with the media services.
- **TxDTMFOption**: Transmit DTMF options in order of priority (all are set to no negotiation).
- **RFC2833 DTMF Payload Type**: The RFC2833 DTMF Relay dynamic payload type. Allowed ranges are: 96-99 and 106-27. The default value is 96.
- **Flash Hook Detection**: Reported Period—the flash-hook period (in milliseconds) that is reported to the FXO port. The default value is 790 ms.

Click on the **Apply** button to keep any changes made on this page.

Advanced Parameters

The **Advanced Parameters** settings, shown as follows, are accessed by clicking on the **Advanced Parameters** item in the lefthand menu and are a collection of AudiCodes-specific settings.



The following configuration options are available on this page (click on **Show Advanced Settings** to reveal all options):

- **Secure SIP Calls**: If this is enabled, gateways will only accept SIP calls from IP addresses listed below. The default is disabled (unchecked)
- **Accepted IP Addresses**: They are used in conjunction with the above setting. It is a space-separated list of IP addresses from which gateway will accept the calls. It is taken into account only if **Secure SIP Calls** is enabled. The default is the IP address provided for the PBX during install.
- **Digit Delivery to Telephony Port**: This setting enables a digit string to be played to the port at the far end, after off-hook. The default is disabled (unchecked).
- **Digit Delivery to IP**: This setting enables a digit string to be played to the port at the far end, after off-hook. The default is disabled (unchecked).
- **DID Wink Support**: When this is enabled, the gateway can connect to EIA/TIA 464B Loop Start DID lines. Both generation and detection are supported. The default setting is disabled (unchecked).

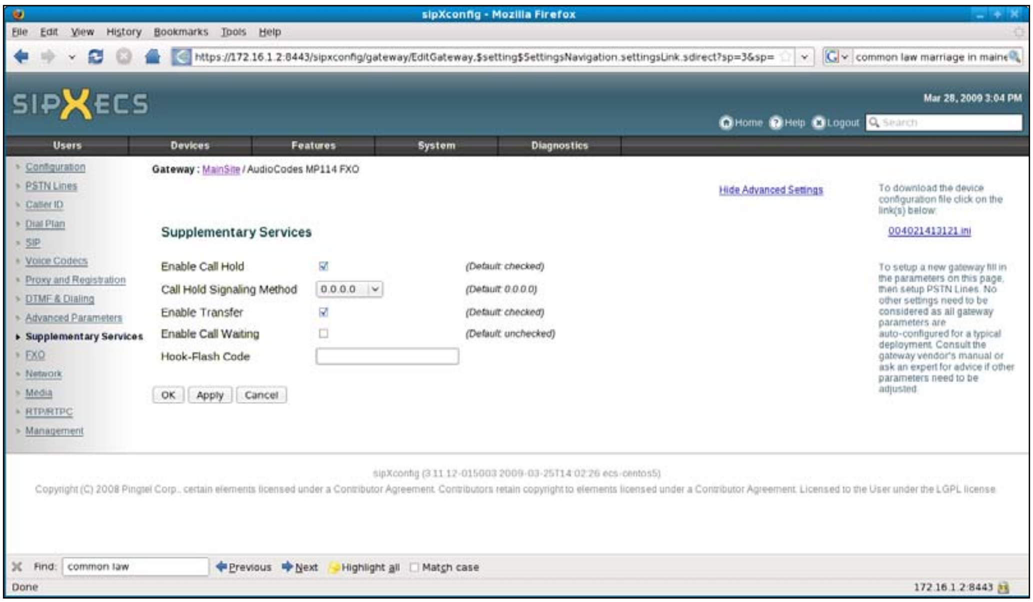
- **Enable Call Disconnect on Polarity Reversal**: If this is checked, enables port disconnect (on-hook) based on polarity reversal. Some POTS providers will reverse the polarity of the analog phone line to signal disconnection to a PBX. The default is disabled (unchecked).
- **Enable Call Disconnect on Current Drop**: If this is set to 1, enables port disconnect (on-hook) based on current drop. The default setting is disabled (0).
- **Enable Call Disconnect on Broken Connection**: If this is checked, the call is released if the gateway stops receiving RTP for a period of time. The default is enabled (checked).
- **Broken Connection Timeout (10msec)**: The amount of time for which RTP is not received, before the call is cleared. In 10 ms steps, the default is 500, 10 ms steps (5 seconds).
- **Enable Call Disconnect on Far End Silence**: If this checked, enables disconnection of call based on silence. The default is disabled (unchecked).
- **Silence Period for Disconnect**: The detection period, in seconds, before the call is released based on silence. The default is 120 seconds.
- **Silence Detection Method**: This setting can be set to "None" (silence detection option is disabled), "Packets Count" (according to packet count), "Voice/Energy Detectors" (according to energy and voice detectors (default)) or "All" (according to packet count and energy / voice detectors).
- **Silence Threshold**: The threshold of packet count, in percentage, below which is considered as silence. The default setting is 8 packets.
- **Detail Level in Debug Log**: The detail level of the log messages sent to syslog server. Default is 0 (off), max is 5 (full).
- **CDR Server IP Address**: An optional separate syslog server to collect CDRs only. If null and CDR is enabled, the output is mixed with the log messages and is routed to the syslog server IP. (Default: 0.0.0.0)
- **CDR Report Level**: This can be set to "None", (**Call Detail Recording** or **CDR** information isn't sent to the Syslog server, which is the default value), "End Call" (CDR information is sent to the Syslog server at the end of each Call) and, "Start & End Call" (CDR information is sent to the Syslog server at the start and at the end of each Call).

- **Port Busy-Out Method**: If there is a network-side failure on the gateway, the POTS interfaces can be set to busy. If this is checked, telephony ports are busied out (special tone) in case of LAN failure or proxy communication failure. The default is disabled (unchecked).
- **Delay After Reset [sec]**: Amount of time delay before answering calls after gateway reset. The default is 7 seconds.
- **Max Number of Active Calls**: This is the maximum number of active calls the PBX can process. It should be set to the number of PSTN lines active.
- **Max Call Duration [min]**: This is the maximum duration of a phone call. The default is 0, which means no maximum.
- **Enable LAN Watchdog**: When **LAN Watchdog** is enabled, the gateway's overall communication integrity is checked periodically. If no communication for about 3 minutes is detected, the gateway performs a self test. If the self test succeeds, the problem is logical link down (for example, Ethernet cable disconnected on the switch side), and the "Busy Out" mechanism is activated if enabled (EnableBusyOut = 1). Lifeline is activated if enabled. If the self test fails, the gateway restarts to overcome an internal fatal communication error (default: unchecked).
- **Enable SAS**: This setting is to enable/disable **Stand-Alone Survivability** (**SAS**) (default: unchecked).
- **SAS Registration Time**: This is the time after which SAS is enabled (default: 20 seconds).
- **SAS Local SIP UDP port**: This is the UDP Port for SAS SIP signaling (default: 5080).
- **SAS Local SIP TCP port**: This is the TCP Port for SAS SIP signaling (default: 5080).
- **SAS Local SIP TLS port**: This is the TLS Port for SAS SIP signaling (default: 5081).
- **SAS Default Gateway**: This is the SAS Default Gateway IP address (default blank).
- **SAS Short Number Length**: This is the SAS short number length.

Click on the **Apply** button to keep any changes made on this page.

Supplementary Services

Supplementary Services are calling services that are provided by **User Agents** (**UA**). With SIP, much of the call handling is done by the intelligent end points instead of the PBX. Clicking on the **Supplemenary Services** menu item will display the following page:



The following configuration options are available on this page (click on **Show Advanced Settings** to reveal all options):

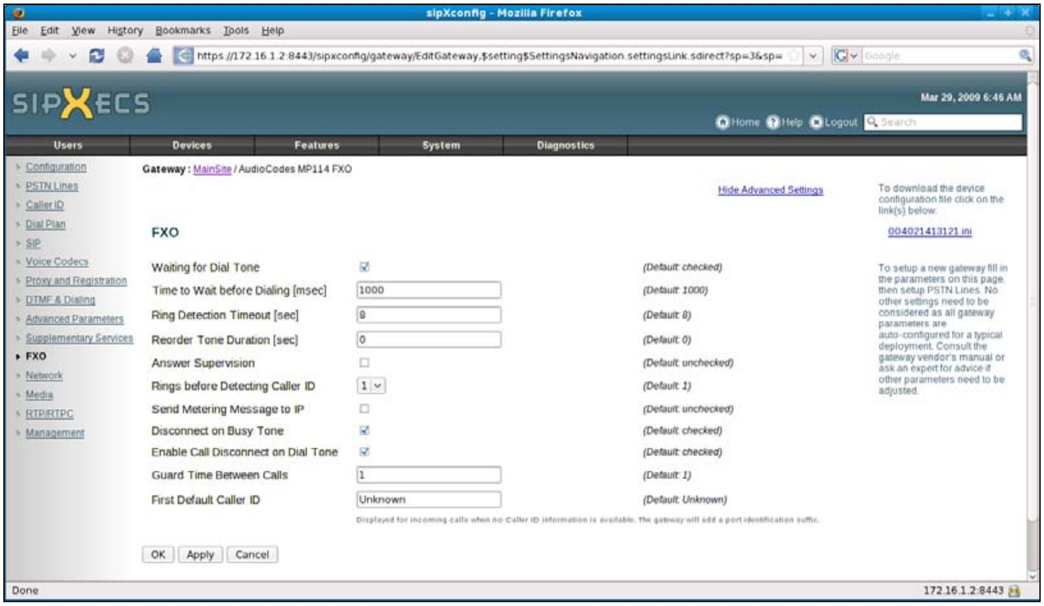
- **Enable Call Hold**: This allows the gateway to enable the "Call Hold" function. The default is enabled (checked).
- **Call Hold Signaling Method**: "Call Hold" can be signaled to another UA in a couple of different ways with the AudioCodes gateway. The connection IP address in SDP is 0.0.0.0 (default) or "Send Only" where the last attribute of the SDP contains 'a=sendonly'.
- **Enable Transfer**: Enables the "Call Transfer" feature in the gateway. The default is enabled (checked).
- **Enable Call Waiting**: Enables the "Call Waiting" feature in the gateway. The default is disabled (unchecked).

- **Hook-Flash Code**: Determines a digit pattern that, when received from the Telecom side, indicates a "Hook-Flash Code". The valid range is a 25-character string. The default is blank (don't look for hook flash from the Telecom side).

Click on the **Apply** button to keep any changes made on this page.

FXO

The FXO settings page (shown as follows) allows some tuning of the interface with the telecommunications provider.



The following configuration options are available on this page (click on **Show Advanced Settings** to reveal all options):

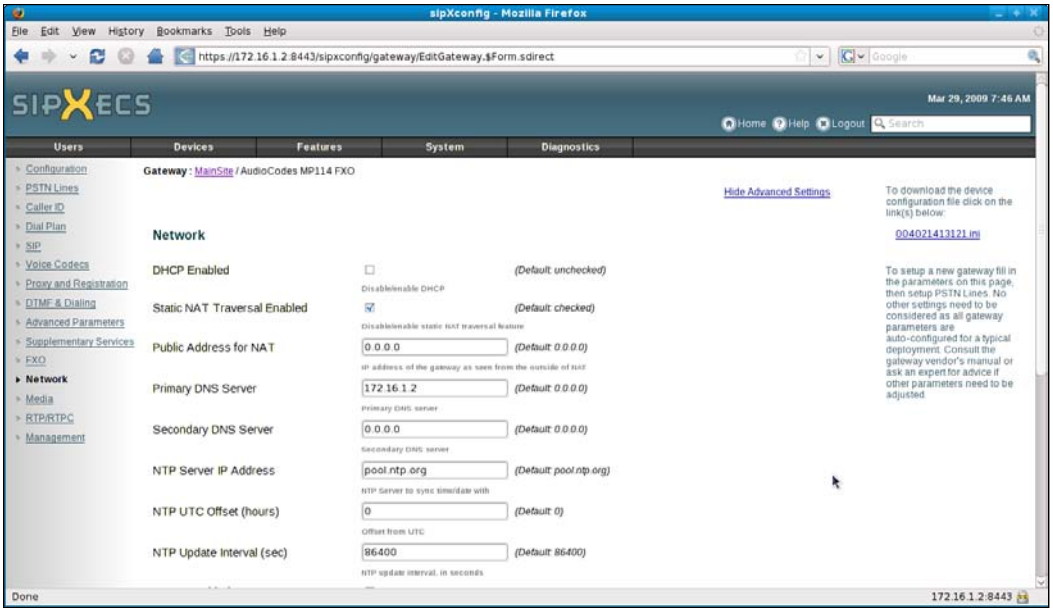
- **Waiting for Dial Tone**: When an outgoing call is made, the gateway waits to hear the dial tone on the line before dialing. The default is enabled (checked).
- **Time to Wait before Dialing [msec]**: After the gateway goes off-hook to dial out, it will wait for this amount of time before dialing the phone number. The default setting is 1000 milliseconds (1 second).

- **Ring Detection Timeout [seconds]**: **Ring Detection Timeout** is used in conjunction with inbound caller ID detection. If **Caller ID** is enabled, then the FXO gateway seizes the line after detection of the second ring signal (allowing detection of caller ID, sent between the first and the second rings). If the second ring signal doesn't arrive for **Ring Detection Timeout**, the gateway doesn't initiate a call to IP. The default setting is 8 seconds.
- **Reorder Tone Duration [seconds]**: Before releasing the line, FXO gateway plays a "Busy" or "Reorder" tone, which has duration in seconds. The default is 0 seconds disabling the reorder tone.
- **Answer Supervision**: If this is enabled (checked), the FXO gateway sends a SIP 200 OK (to INVITE) messages when speech/fax/modem is detected. If it is disabled, a SIP 200 OK is sent immediately after the FXO gateway finishes dialing. The default setting is disabled (unchecked).
- **Rings before Detecting Caller ID**: Determines the number of rings to wait for the caller ID from the phone company. The default is 1 ring.
- **Send Metering Message to IP**: Sends a metering tone INFO message to the IP of 12/16 kHz metering pulse. Not used by sipXecs, so the default is disabled (unchecked).
- **Disconnect on Busy Tone**: If the gateway detects a busy tone it will interpret this as a disconnect signal and hang up the line. The default is enabled (checked).
- **Enable Call Disconnect on Dial Tone**: If the gateway detects a dial tone on the phone line, it will interpret this as a disconnect signal and hang up the line. The default is enabled (checked).
- **Guard Time Between Calls**: Sometimes, after a call is ended and the gateway goes on-hook, a delay is required before placing a new call (and performing the subsequent off-hook). This is necessary to prevent the phone company thinking that the gateway is trying to perform a hook-flash. The default is 1 second.
- **First Default Caller ID**: The value that is displayed for incoming calls when no caller ID information is available. The gateway will add a port identification suffix. The default value is set to "Unknown".

Click on the **Apply** button to keep any changes made on this page.

Network

The **Network** settings page has some typical network settings. They are given as follows:



The following configuration options are available on this page (click on **Show Advanced Settings** to reveal all options):

- **DHCP Enabled**: The default is disabled (unchecked).
- **Static NAT Traversal Enabled**: Disable/enable static NAT traversal feature. The default is enabled (checked).
- **Public Address for NAT**: This is the IP address of the gateway as seen from the outside of NAT. The default is no IP address (0.0.0.0).
- **Primary DNS Server**: The Primary DNS server (default: 0.0.0.0).
- **Secondary DNS Server**: The Secondary DNS server (default: 0.0.0.0).
- **NTP Server IP Address**: The NTP Server to sync time/date with (default: `pool.ntp.org`).
- **NTP UTC Offset (hours)**: The gateway's location offset from UTC (default: 0).
- **NTP Update Interval (sec)**: The NTP update interval, in seconds (default: 86400 seconds).
- **STUN Enabled**: Enable/disable STUN (default: unchecked).

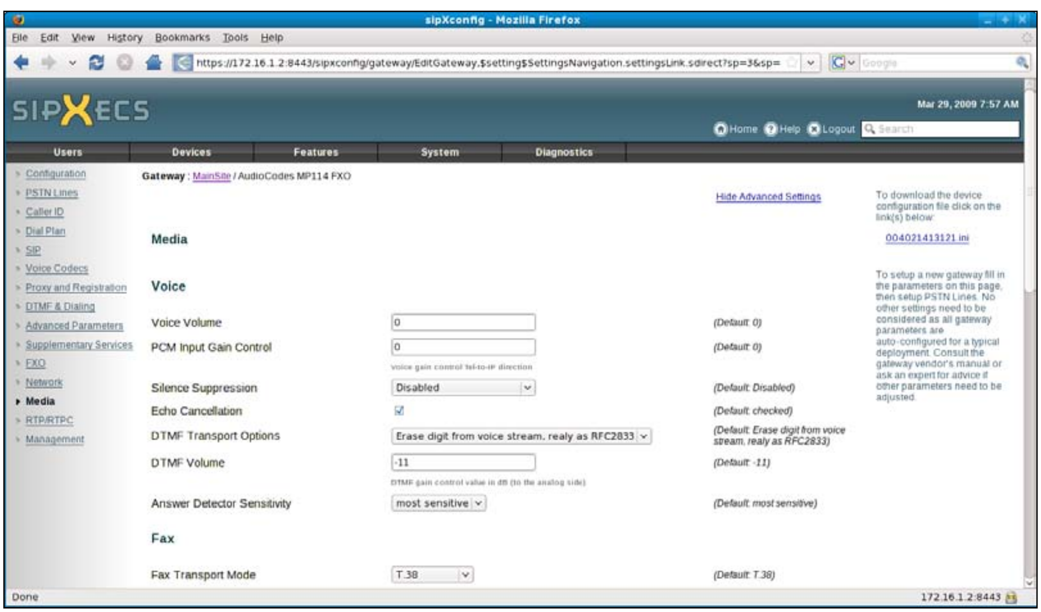
- **Primary STUN Server IP Address**: IP address of the primary STUN server (default: 0.0.0.0).
- **Secondary STUN Server IP Address**: The IP address of the secondary STUN server (default: 0.0.0.0).
- **Syslog Output Enabled**: Enable/disable syslog facility for diagnostics (default: unchecked).
- **Syslog Server IP address**: The IP address of the syslog server (default: 0.0.0.0).
- **Syslog Server Port**: The Default syslog port (default: 514).

Click on the **Apply** button to keep any changes made on this page.

Note that with the gateways, most of these parameters should be hard-coded into the gateway configuration rather than relying on the gateway to download the settings. Please refer to your manufacturer's documentation for detailed information as to how to do this.

Media

The **Media** section of the gateway configuration allows fine-grained control over the audio portion of a call through the gateway. The top of the **Media** settings page is shown as follows:



The following configuration options are available on this page (click on the **Show Advanced Settings** hyperlink to reveal all options):

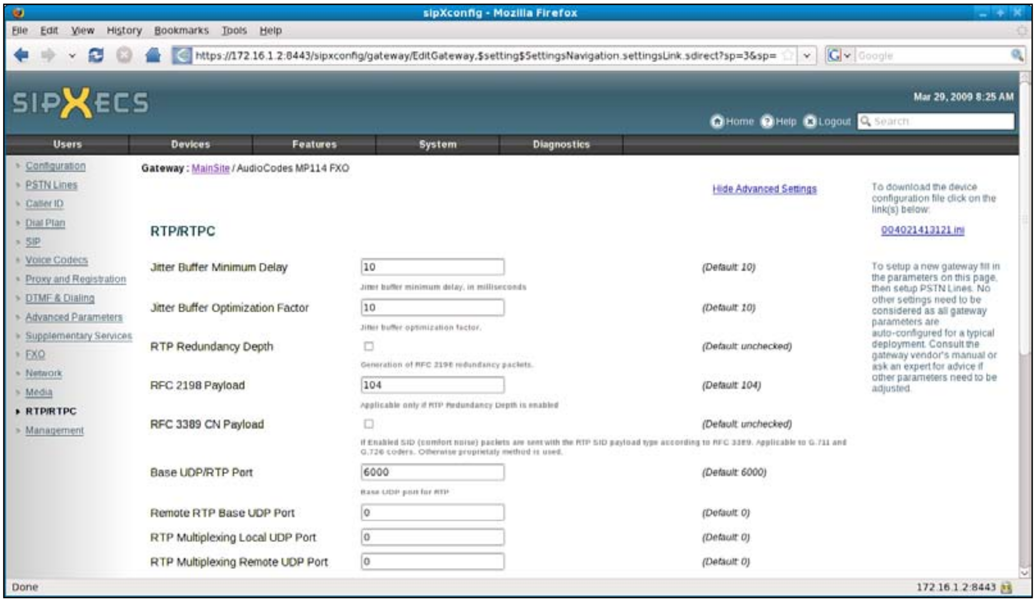
- **Voice Volume**: The voice gain control is given in decibels. This parameter sets the level for the transmitted **Voice Volume** (IP to Telecom direction) signal. The default is no gain (0). Increase this value if the far-end party is complaining of low volume.
- **PCM Input Gain Control**: The voice gain control (Tel-to-IP direction). The default is no gain (0). Increase this value, if your local callers complain about low volume with calls through the gateway. Increasing the volume too much, however, will increase static and echo will be heard on calls.
- **Silence Suppression**: This suppresses transmission of silence (default: disabled).
- **Echo Cancellation**: This enables echo cancellation on the gateway (default: checked).
- **DTMF Transport Options**: This determines how DTMF is handled (default: Erase digit from voice stream, relay as RFC2833).
- **DTMF Volume**: The DTMF gain control value in dB (to the analog side) (default: -11). Increase if DTMF is not being recognized when dialing out to another system and DTMF digits need to be sent by the caller.
- **Answer Detector Sensitivity**: This helps the gateway to detect if an outbound call has been answered (default: most sensitive).
- **Fax Transport Mode**: This mode shows how faxes are transported over IP (default: T.38).
- **Fax Transport Codec in By-Pass Mode**: (default: G711 u-Law).
- **Fax Transport Payload ID in By-Pass Mode**: Payload type for by-pass fax transport, 96 through 120 (default: 102).
- **Fax Relay Redundancy Depth**: The number of times each fax relay payload is retransmitted to the network (default: 0).
- **Fax Relay Enhanced Redundancy Depth**: The number of times the control packets are retransmitted when using the T.38 standard (default: 2).
- **Fax Relay ECM**: **Error Correction Mode** or **ECM** is enabled or disabled (default: checked).
- **Fax Relay Max Rate**: The maximum rate at which fax relay messages are transmitted (outgoing calls) (default: 14.4 kbps).
- **Fax/Modem Bypass Packing Factor**: The number of (20 millisecond) coder payloads that are used to generate a fax/modem bypass packet (default: 1).

- **CNG Detector Mode**: In "Relay" mode, CNG (fax tones) are detected on the originating side. CNG packets are sent to the remote side according to T.38 and the fax session is started. In "Events Only" mode, CNG is detected on the originating side. The CNG signal passes transparently to the remote side and the fax session is started. (Default: Disable)
- **Enable Caller ID**: This will enable generation (FXS) and detection (FXO) of caller ID on the telephony ports (Default: checked).
- **Caller ID Display Type**: (Default: Bellcore).
- **V.21 Modem Transport Type**: (Default: Disable (Transparent)).
- **V.22 Modem Transport Type**: (Default: Disable (Transparent)).
- **V.23 Modem Transport Type**: (Default: Disable (Transparent)).
- **V.32 Modem Transport Type**: (Default: Disable (Transparent)).
- **V.34 Modem Transport Type**: (Default: Disable (Transparent)).

Click on the **Apply** button to keep any changes made on this page.

RTP/RTPC

The RTP/RTPC settings allow fine-grained cotrol over the IP side of voice conversations.



The following configuration options are available on this page (click on **Show Advanced Settings** to reveal all options):

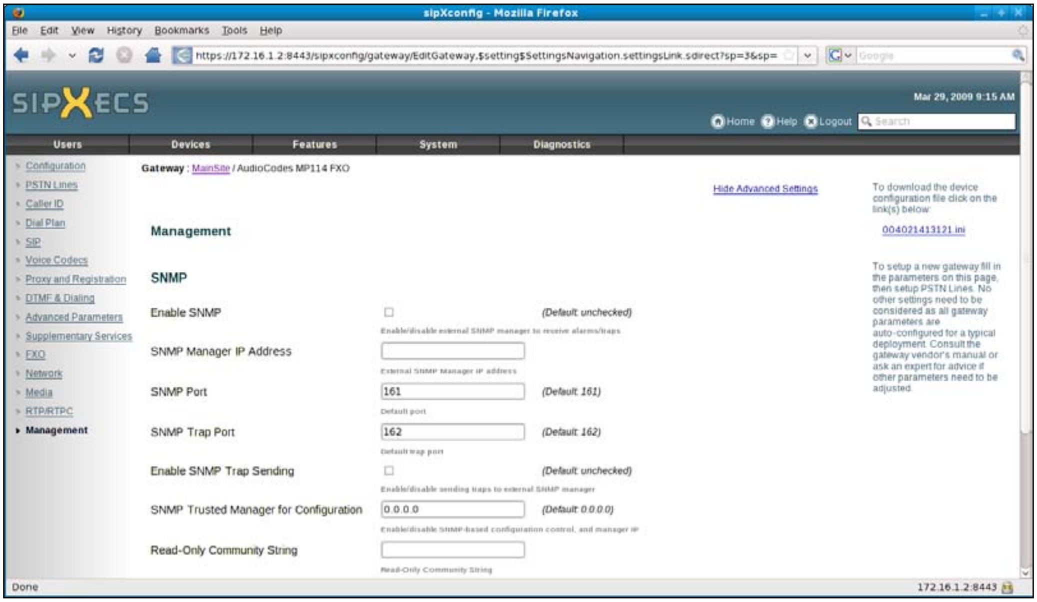
- **Jitter Buffer Minimum Delay**: The Jitter Buffer minimum delay, in milliseconds. The default is 10 milliseconds. Packet jitter is an average of the deviation from the network mean latency (a network that has a constant latency has no jitter). A jitter buffer helps compensate for changes in latency on the network by providing a buffer (queue).
- **Jitter Buffer Optimization Factor**: AudioCodes Dynamic Jitter Buffer frame error / delay optimization factor. Valid values are 0 through 13 with the default being 10.
- **RTP Redundancy Depth**: Enable or disable the generation of RFC 2198 redundancy packets (default: unchecked).
- **RFC 2198 Payload**: Applicable only if **RTP Redundancy Depth** is enabled (default: 104).
- **RFC 3389 CN Payload**: If this is enabled, SID (comfort noise) packets are sent with the RTP SID payload type according to RFC 3389. Applicable to G.711 and G.726 coders. Otherwise a proprietary method is used. The default is disabled (unchecked). Comfort noise is white noise generated by a gateway so that the person on the phone knows that a call is still active.
- **Base UDP/RTP Port**: The base UDP port for RTP (default: 6000).
- **Remote RTP Base UDP Port**: (Default: 0.)
- **RTP Multiplexing Local UDP Port**: (Default: 0.)
- **RTP Multiplexing Remote UDP Port**: (Default: 0.)
- **Comfort Noise Generation Negotiation**: The use of CN is indicated by including a payload type for CN on the media description line of the SDP. The gateway can use CN with a codec whose RTP timestamp clock rate is 8,000 Hz (G.711/G.726). The static payload type 13 is used. The use of CN is negotiated between sides; therefore, if the remote side doesn't support CN, it is not used. Note: Silence Suppression must be enabled to generate CN. (Default: unchecked.)
- **Call Progress Tones Filename**: A region-specific, telephone exchange-dependent file that contains the call progress tone levels and frequencies that the VoIP gateway uses. The default CPT file is U.S.A. A different CPT file can be uploaded and will be placed in the TFTP folder and loaded during boot.
- **FXS Loop Characteristics Filename**: Used for FXS (station) gateways, the name of the FXS loop characteristics definition file, to be TFTP-loaded during boot (default: MP11x-02-1-FXS_16KHZ.dat).

- **Country Variant**: A definition for country variant for line characteristics. North America = 70 (default: 70).
- **LifeLine Type**: On FXS gateways, a single Lifeline, connected to port #1 via a splitter (not supplied), is available. On combined FXS/FXO gateways, a splitter isn't required. All FXS ports are automatically connected to FXO ports (FXS port 0 to FXO port 4 and so forth). On FXO gateways a Lifeline isn't available. The Lifeline is activated on: 0 = power down (default), 1 = power down, or when link is down (physical disconnect), 2 = power down or when link is down, or on network failure (logical link disconnect).

Click on the **Apply** button to keep any changes made on this page.

Management

The **Management** configuration settings for gateways allow some network managemet parameters to be configured for use with the network tools.



The following configuration options are available on this page (click on **Show Advanced Settings** to reveal all options):

- **Enable SNMP**: The user can enable/disable an external SNMP manager to receive alarms/traps (default: unchecked).
- **SNMP Manager IP Address**: The external SNMP Manager IP address (default: blank).
- **SNMP Port**: TCP/IP default port for listening for SNMP (default: 161).
- **SNMP Trap Port**: TCP/IP default trap port destination (default: 162).
- **Enable SNMP Trap Sending**: Enable/disable sending traps to the external SNMP manager (default: unchecked).
- **SNMP Trusted Manager for Configuration**: Enable/disable SNMP-based configuration control and trusted manager IP (default: 0.0.0.0).
- **Read-Only Community String**: The SNMP management system uses the read only community string.
- **Read-Write Community String**: The SNMP management system uses the read/write community string.
- **Trap Community string**: The SNMP management system uses the trap community string.

Click the **Apply** button to keep any changes made on this page.

Unmanaged gateways

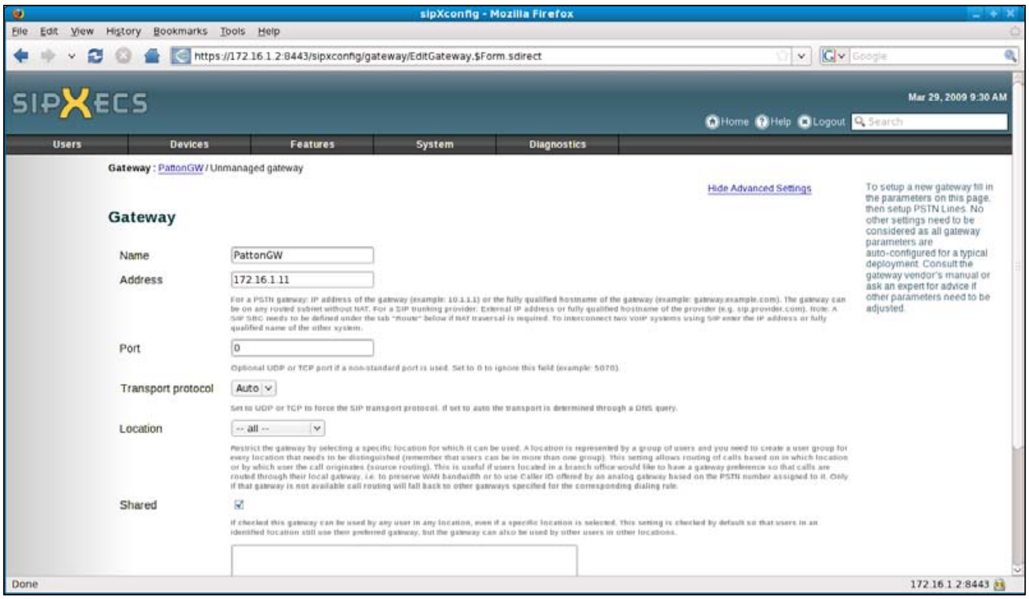
The initial configuration of unmanaged gateways looks quite similar to that of a managed gateway. There is, however, no detail that can be set because configuration files are not built for these gateways.

It is up to the system administrator to manually configure any unmanaged gateways. If there are settings that you are not sure about, refer to the *Managed gateway* settings for a possible answer.

The sipXecs community Wiki has a section for common gateway configurations. The Wiki can be accessed from `http://www.sipfoundry.org`. Since there are only a couple of managed gateway manufacturers supported at present in sipXecs, many installations utilize unmanaged gateways. There are many gateway manufacturers with products to meet every need.

Add gateway

To add an unmanaged gateway, click on the **Add new gateway** drop-down box and select **Unmanaged gatway**. The unmanaged gateway configuration page will be displayed as follows:

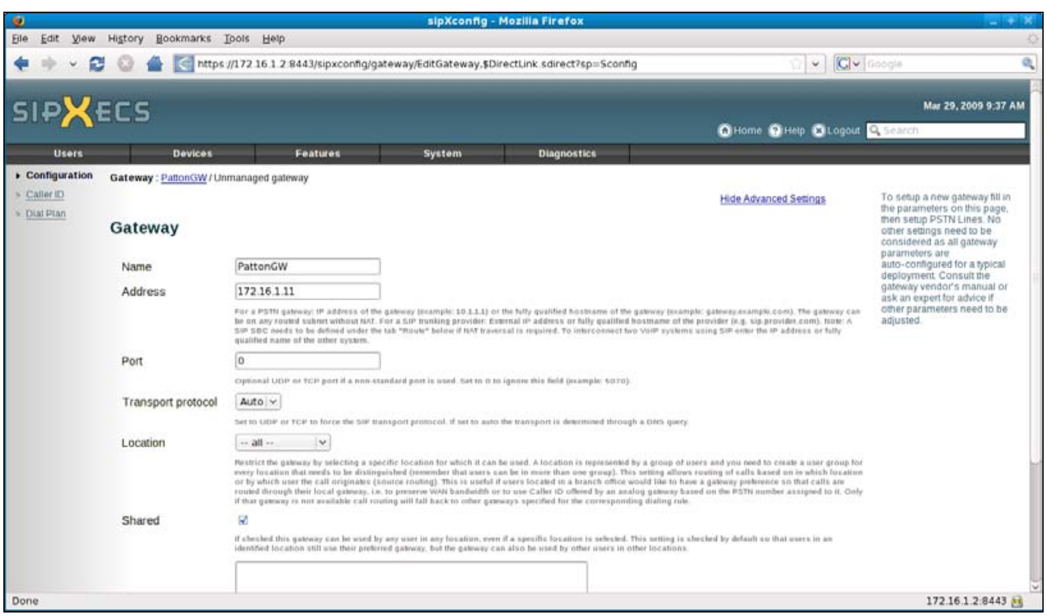


The following configuration information can be configured on this page (click on **Show Advanced Settings** to display all configuration items):

- **Name**: A name is given to the gateway (no spaces).
- **Address**: The IP address of the gateway or the fully qualified hostname of the gateway (see manufacturer's documentation for information on configuring IP addressing and other basic settings).
- **Port**: An optional setting for UDP or TCP port if a non-standard port is used. Set to 0 to ignore this field.
- **Transport protocol**: This can be manually configured to UDP or TCP to force the SIP transport protocol. If it is set to **Auto**, the transport is determined through a DNS query.

- **Location**: It is possible to restrict the gateway by selecting a specific location for which it can be used. A location is represented by a group of users. A user group must be created for every location that needs to be distinguished (remember that users can be in more than one group). This setting allows routing of calls based on in which location or from which user the call originates (source routing). This is useful if users located in a branch office would like to have a gateway preference so that calls are routed through their local gateway. That is done to preserve WAN bandwidth or to use the caller ID offered by an analog gateway based on the PSTN number assigned to it. Only if that gateway is not available, call will routing fall back to other gateways specified for the corresponding dialing rule.
- **Shared**: If this setting is checked, this gateway can be used by any user in any location, even if a specific location is selected. This setting is checked by default so that users in an identified location still use their preferred gateway, but the gateway can also be used by other users in other locations.
- **Description**: This is for documenting the system configuration. Information about the lines connected to the gateway is very useful here.

With all of the configuration information entered, click on the **OK** button and the **Gateway** page will be displayed as follows with the new gateway on it. Click on the new unmanaged gateway's name to reveal more configuration options, as shown in the following screenshot:



In the following subsections, we'll explore the unmanaged gateway settings available (luckily there aren't as many as with the managed gateways).

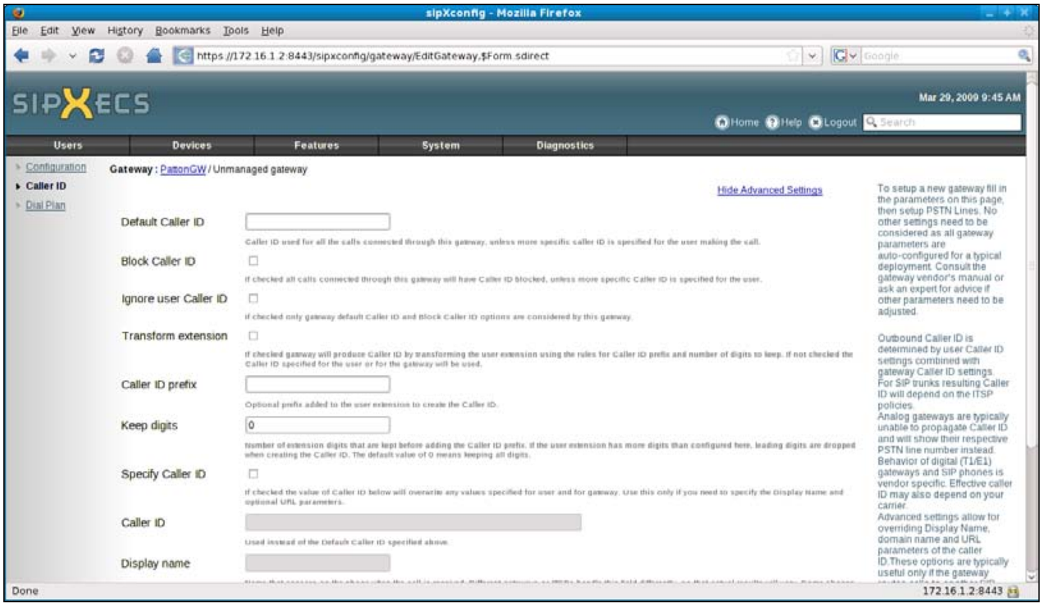
Caller ID

Outbound caller ID is determined by user caller ID settings combined with gateway caller ID settings. For SIP trunks, the resulting caller ID will depend on the ITSP policies.

Analog gateways are typically unable to transmit caller ID and will show their respective PSTN line number instead. This is generated on the telecom provider's side.

Behavior of digital (T1/E1) gateways and SIP phones is vendor specific. Effective caller ID may also depend on your telecom provider.

Advanced settings allow for overriding **Display Name**, domain name, and URL parameters of the caller ID. These options are typically useful only if the gateway routes calls to another SIP system



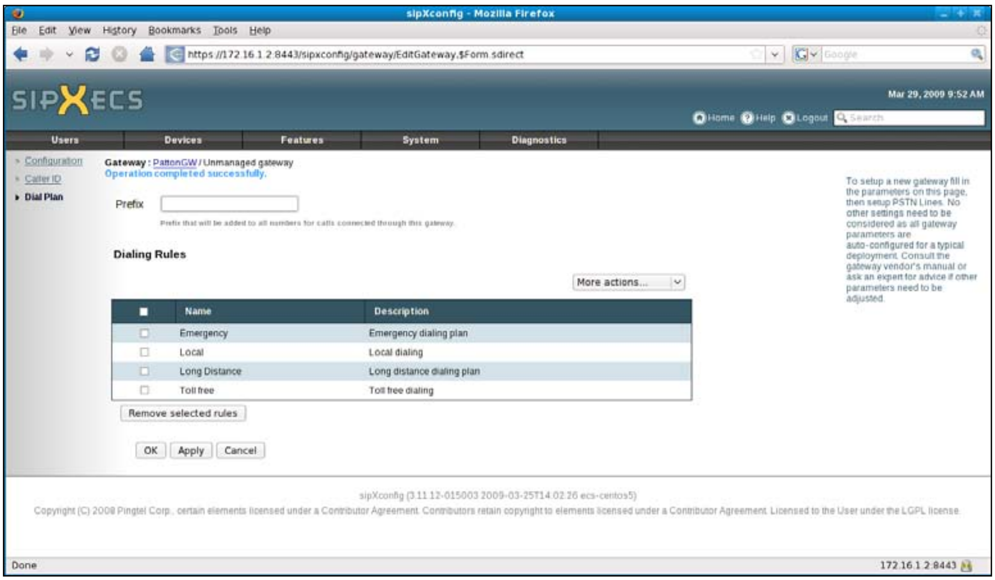
The following configuration information can be set on this page (click on **Show Advanced Settings** to display all configuration items):

- **Default Caller ID**: The **Caller ID** used for all the calls connected through this gateway, unless a more specific caller ID is specified for the user making the call.
- **Block Caller ID**: If this is checked, all calls connected through this gateway will have caller ID blocked, unless a more specific caller ID is specified for the user.
- **Ignore user Caller ID**: If this is checked, only the gateway **Default Caller ID** and **Block Caller ID** options are considered by this gateway.
- **Transform extension**: If this is checked, the gateway will produce a caller ID by transforming the user extension using the rules for caller ID prefix and number of digits to keep. If not checked the caller ID specified for the user or for the gateway will be used.
- **Caller ID prefix**: Optional prefix added to the user extension to create the caller ID.
- **Keep digits**: The number of extension digits that are kept before adding the caller ID prefix. If the user extension has more digits than configured here, leading digits are dropped when creating the caller ID. The default value of 0 means keep all digits.
- **Specify Caller ID**: If this is checked, the value of **Caller ID** below will overwrite any values specified for user and for gateway. Use this only if you need to specify the **Display Name** and optional **URL parameters**.
- **Caller ID**: Used instead of the **Default Caller ID** specified above.
- **Display name**: The name that appears on the phone when the call is received. Different gateways or ITSPs handle this field differently, so that actual results will vary. Some phones may not support displaying this value correctly.
- **URL parameters**: Optional SIP URI parameters of the following form: key1=value1;key2=value2.

Click on the **Apply** button to keep any changes made on this page.

Dial Plan

The **Dial Plan** page, shown as follows, allows the administrator to add a dial prefix for outbound calls and also add the unmanaged gateway to any pre-configured system dialing rules (see the *Dial plans* section later in this chapter).



The following configuration options are available on this page:

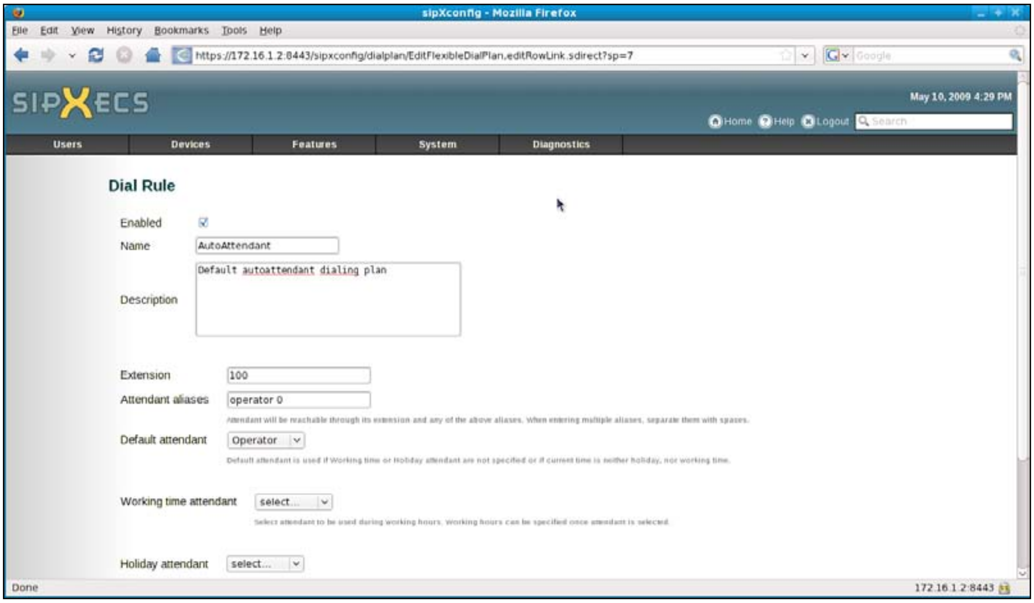
- **Prefix**: The administrator can configure an outbound dialing prefix that will be added to all numbers for calls connected through this gateway. This is useful if centrex lines are in use.
- **Dialing Rules**: The system dialing rules that should use this gateway can be specified in this section. Click on the **More actions** drop-down box to select the dial plan entries that are defined in the system.

Click on the **Apply** button to keep any changes made on this page.

SIP Trunks

Increasingly, communications connectivity is being delivered to customers via SIP trunks across the Internet instead via traditional copper lines. A special gateway is included in the system that allows for connecting the sipXecs system to SIP trunks without any additional hardware required (see the *Session Border Controllers* section later in this chapter).

A SIP trunk can be added to the system in the **Gateway** screen by selecting the **Add new gateway** drop-down menu and cliking on **SIP Trunk**.



The following settings are available for SIP trunk gateways (click on **Show Advanced Settings** to see all of the **SIP trunk**'s options):

- **Name**: This is a descriptive name for the gateway.
- **Use provider template**: Some pre-configured templates are available for popular SIP Trunk providers. Gateway settings will be pre-filled if your SIP trunking provider (ITSP) is on the list. To enter your own settings, or if your provider is not on the list, select "None". At the time of writing this, the available templates are: ATT, BT, Bandtel, bandwidth.com, CallWithUs, Cbeyond, Eutelia, LES.NET, sipcall.ch, Vitelity, VoIP User, and Voxitas.
- **Address**: For a PSTN gateway—IP address of the gateway (example: 10.1.1.1), or the fully qualified hostname of the gateway (example: `gateway.example.com`). The gateway can be on any routed subnet without NAT. For a SIP trunking provider—External IP address or fully qualified hostname of the provider (for example, `sip.provider.com`).

> A SIP Session Border Controller (see later in this chapter) needs to be defined under the tab **Route**, if NAT traversal is required. To interconnect two VoIP systems using SIP, enter the IP address or fully qualified name of the other system.

- **Port**: Optional UDP or TCP port if a non-standard port is used. Set to 0 to ignore this field (example: 5070).
- **Transport protocol**: Set to UDP or TCP to force the SIP transport protocol. If set to "Auto", the transport is determined through a DNS query.
- **Location**: The gateway use can be restricted by selecting a specific location for which it can be used. A location is represented by a group of users and you need to create a user group for every location that needs to be distinguished (remember that users can be in more than one group). This setting allows routing of calls based on in which location or from which user the call originates (source routing). This is useful if users located in a branch office would like to have a gateway preference so that calls are routed through their local gateway, for example, to preserve WAN bandwidth or to use caller ID offered by an analog gateway based on the PSTN number assigned to it. Only if that gateway is not available, will call routing fall back to other gateways specified for the corresponding dialing rule.
- **Shared**: If this is checked, this gateway can be used by any user in any location, even if a specific location is selected. This setting is checked by default so that users in an identified location still use their preferred gateway, but the gateway can also be used by other users in other locations.
- **Description**: This is used to document the gateway. Important information about the provider can be inserted here including tech support numbers or any other important and hard-to-locate information.
- **Route**: How calls are routed to the SIP provider. **Session Border Controller** (**SBC**), SIP aware firewall or SIP proxy that processes calls directed at the provider served by this SIP tgrunk. Unless your system is on a public IP address, you will need an SBC. If in doubt, create an Internal SBC (see later in this chapter).

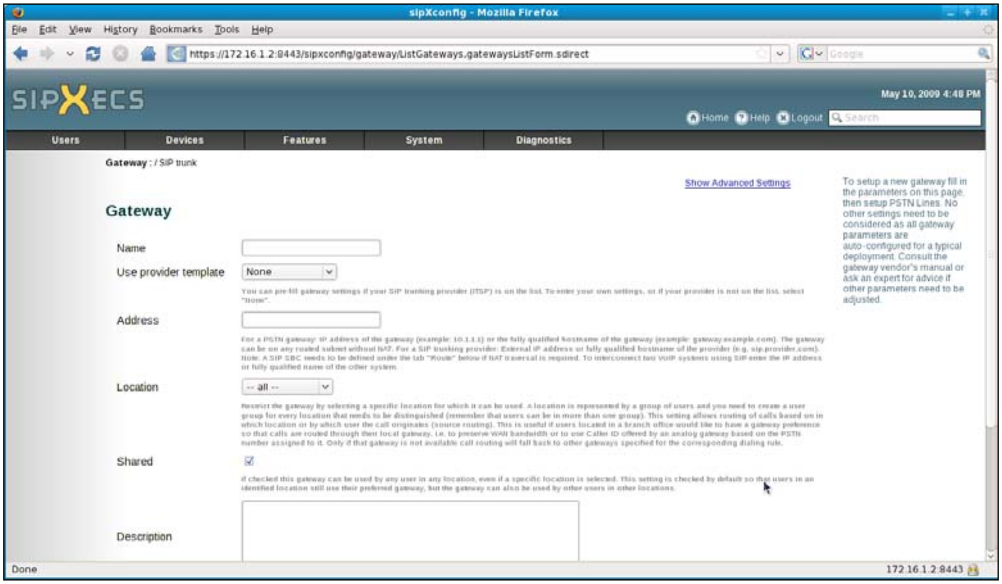
Dial Plans

The communication system's **Dial Plan** is a collection of **Dial Rules**. The purpose of the **Dial Plan** is to control the routing of calls based on dialed numbers. Different **Dial Rules** within the **Dial Plan** are selected by matching dialed number patterns (the user part of a SIP URL).

The following types of dial rules can be created in sipXecs:

- **Voicemail**: This is used to configure the system Voicemail server.
- **Custom**: This is used to build custom call routing to gateways.
- **Long Distance**: This is used to route long-distance dialed calls.
- **Local**: This is used to route local phone calls to gateways.
- **Emergency**: This is used for emergency call routing to gateways.
- **International**: This is used for routing calls to international destinations to gateways.
- **Attendant**: This is used for routing calls to auto attendants defined in the system.

Dial Plan configuration is located under the **System** menu. Clicking on the **Dial Plan** menu item will display the following page:



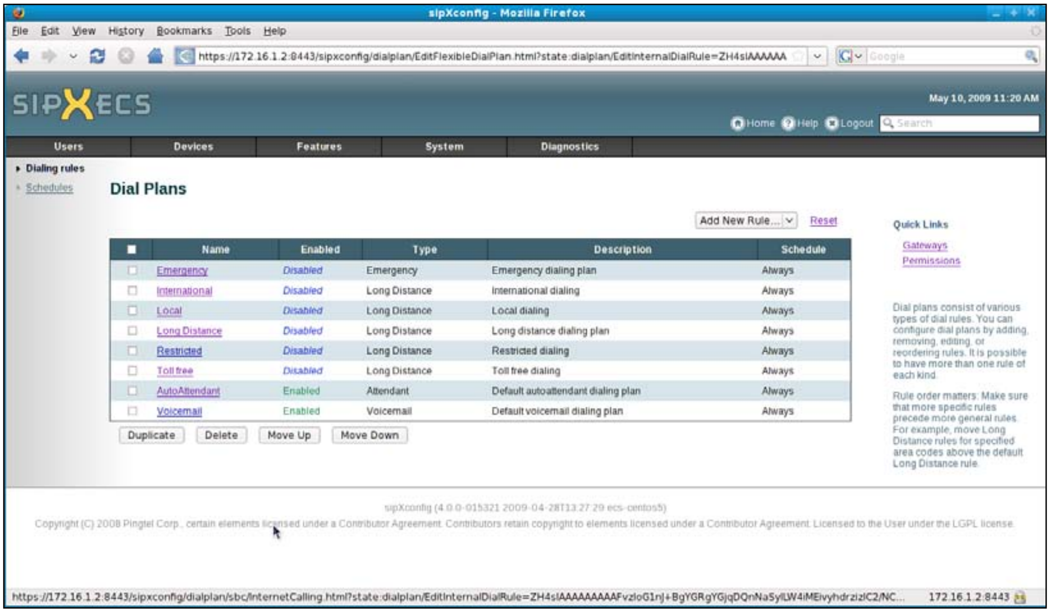
As seen in the above screenshot, there are some default dial rules already created, that allow the administration to simply add gateways and enable them.

Existing **Dial Rules** can be edited by clicking on the rule's name. Additionally new rules can be created with the **Add New Rule** drop-down menu.

Dial rules are processed in the order that they are listed so more specific dial plan entries should be listed near the top. Additionally, if a dial rule is matched and the user does not have permission to use the dial plan entry the call will fail.

Voicemail dial rule

There is typically only one Voicemail per phone system. Its purpose is to control how voicemail is routed for mailboxes and how the voicemail system is accessed. The following screenshot shows the default Voicemail system settings:



The following options are available in **Voicemail Dial Rules**:

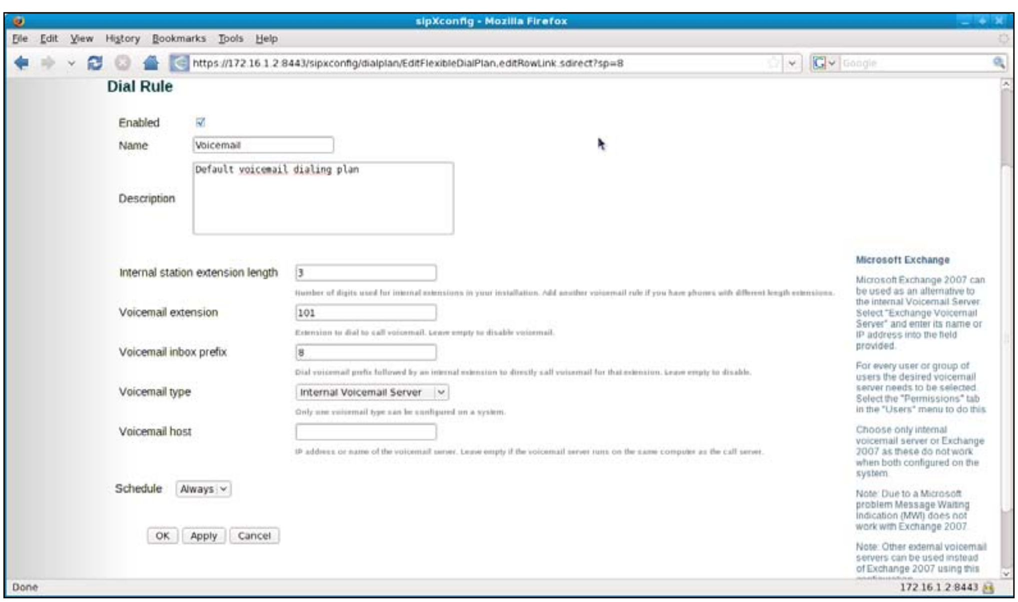
- **Enabled**: Dial rules can be enabled or disabled in the system as the administrator wishes. A rule might be disabled if it is being tested or if a temporary rule gets created to address a particular problem.
- **Name**: This is a descriptive name for the dial rule.
- **Description**: This is a description of what the dial rule is for, to help in documentation.
- **Internal station extension length**: The number of digits used for internal extensions in your installation. Add another voicemail rule if you have phones with different length extensions.
- **Voicemail extension**: The number dialed to reach the voicemail server. This can be left empty to disable Voicemail.
- **Voicemail inbox prefix**: The number dialed when directly dialing or forwarding a call to a user's voicemail box.

- **Voicemail type**: The **Voicemail type** can be set to **Internal Voicemail Server** or **Exchange Voicemail Server**. Microsoft Exchange 2007 can be used as an alternative to the **internal Voicemail Server**. Select **Exchange Voicemail Server** and enter its name or IP address into the field provided. For every user or group of users, the desired voicemail server needs to be selected. Select the **Permissions** tab in the **Users** menu to do this. Choose only either the internal voicemail server or Exchange 2007 as these do not work when both configured on the system. Note: Due to a Microsoft problem **Message Waiting Indication** (**MWI**) does not work with Exchange 2007. Other external voicemail servers can be used instead of Exchange 2007 using this configuration.
- **Voicemail host**: IP address or name of the voicemail server. Leave empty if the voicemail server runs on the same computer as the call server.
- **Schedule**: All dial plan entries can be allowed to operate based on a schedule. Voicemail is typically not scheduled.

Custom dial rules

Custom dial rules are very useful for controlling special call scenarios. For example, if you are connecting a gateway to another PBX that has extensions 400: 599, a custom dial rule could be configured to send calls to that gateway when a three digit number is passed that begins with a 4 or a 5.

The following screenshot show the custom **Dial Rule** page:



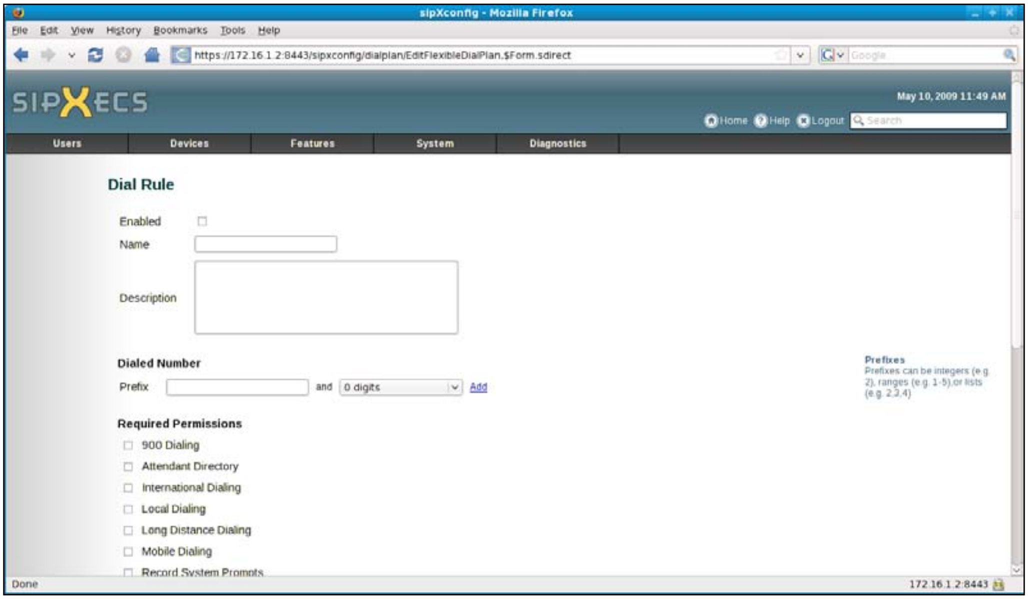
The following options are available for custom **Dial Rules**:

- **Enabled**: Dial rules can be enabled or disabled in the system as the administrator wishes. A rule might be disabled if it is being tested or if a temporary rule gets created to address a particular problem.
- **Name**: A descriptive name for the dial rule.
- **Description**: More information about this dial rule and what it is used for.
- **Dialed Numbe**r: Defines the digits that this rule will match. Any number of prefixes and trailing digits can be added with the **Add** hyperlink.
    - **Prefixes**: Prefixes are the initial part of a dialed number (or SIP URL). A prefix can be integers (for example, 2), ranges (for example, 1-5), or lists (for example, 2, 3, 4).
    - **Any number of digits (Suffix)**: Defines how many digits will follow the prefix. Values from 0 to 18 or **Any Number of Digits** can be selected.
- **Required Permissions**: Defines the user permissions required to access the dial rule. 900 Dialing, Attendant Directory, International Dialing, Local Dialing, Long Distance Dialing, Mobile Dialing, Record System Prompts, Toll Free, or Voice Mail.
- **Resulting Call**: Defines what digits besides the dialed digits will be sent to the gateway.
    - **Dial (new prefix)**: Allows the administrator to change the prefix that will be passed to the gateway. This entry may be left blank to drop the prefix that was detected (when Matched suffix is selected in the following drop-down menu).
    - **And append (Suffix)**: The **and append** drop-down menu item can have one of three values; **Nothing**, **Matched suffix**, or **Entire dialed number**.
- **Schedule**: A schedule can be defined that determines when the custom dial rule can be used.
- **Gateways**: A list of gateways available to this dial rule. See the *Adding gateways* section earlier in this chapter for information about gateway selection and user locations.

Long distance dial rules

Long distance dial rules are used by the system to control whether the users are permitted to dial long-distance numbers or to select different gateways for least-cost routing of calls.

The default long distance **Dial Rule** is disabled by default in the system. The rule is triggered by a number consisting of a PSTN prefix followed by the **Long Distance** prefix and a variable part starting wth one of the patterns specified in the **Area Codes** field.



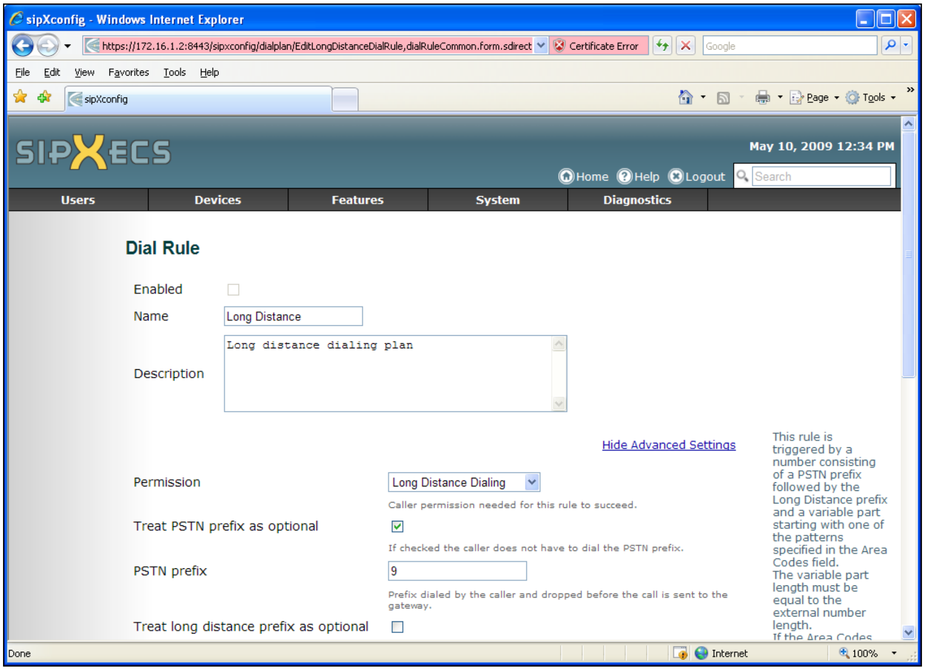
The following settings are available for long distance dial rules (click on **Show Advanced Settings** to see all of the dial rule's options):

- **Enabled**: Dial rules can be enabled or disabled in the system as the administrator wishes. A rule might be disabled if it is being tested or if a temporary rule gets created to address a particular problem.
- **Name**: A descriptive name for the dial rule.
- **Description**: More information about this dial rule and what it is used for.
- **Permission**: Defines the user permissions a user must have to use this dial rule.

- **Treat PSTN prefix as optional**: If this is checked the caller does not have to dial the PSTN prefix (following). Dialing the PSTN prefix is optional by default. This item is only shown if **Show Advanced Options** is selected.
- **PSTN prefix**: The prefix dialed by the caller and dropped before the call is sent to the gateway. The Long Distance prefix is always sent to the gateway.
- **Treat long distance prefix as optional**: If this is checked the caller does not have to dial the long distance prefix. This item is only shown if **Show Advanced Options** is selected.
- **Long distance prefix**: The prefix dialed by the caller and sent to the gateway.
- **Area codes**: Optional comma-separated list of prefixes that specify the dialed numbers to which this rule applies. If the **Area Codes** field is empty the rule will match any number starting with the PSTN prefix followed by the **Long distance prefix**.
- **External number length**: The number of digits in the resulting number sent to the gateway. The PSTN prefix and the long distance prefix are not counted. Valid values are—**Any number of digits** and 5-15 digits.
- **Schedule:** A schedule can be defined that determines when the custom dial rule can be used.
- **Gateways**: A list of gateways available to this dial rule. See the *Adding gateway* section earlier in this chapter for information about gateway selection and user locations. The resulting call is sent to the gateways specified in the gateway list in the order gateways are listed. List the preferred gateway first and backup gateways below it.

Local dial rules

The local dial rule is utilized to control how phone numbers are routed for calls that are deemed as local (without toll) to the system. The local dial rule is triggered by a number consisting of a PSTN prefix followed by the **Long Distance prefix** and a variable part starting with one of the patterns specified in the **Area Codes** field.



The following settings are available for local dial rules (click on **Show Advanced Settings** to see all of the **Dial Rule**'s options):

- **Enabled**: Dial rules can be enabled or disabled in the system as the administrator wishes. A rule might be disabled if it is being tested or if a temporary rule gets created to address a particular problem.
- **Name**: This is a descriptive name for the dial rule.
- **Description**: More information about this dial rule and what it is used for.
- **Permission**: Defines the user permissions a user must have to use this dial rule.
- **Treat PSTN prefix as optional**: If this is checked the caller does not have to dial the **PSTN prefix** (following). Dialing the **PSTN prefix** is optional by default. This item is only shown if **Show Advanced Options** is selected.
- **PSTN prefix**: The prefix dialed by the caller and dropped before the call is sent to the gateway.
- **Area codes**: An optional comma-separated list of prefixes that specify dialed numbers to which this rule applies.
- **External number length**: The number of digits in the resulting number sent to the gateway. The PSTN prefix and the long distance prefix are not counted.

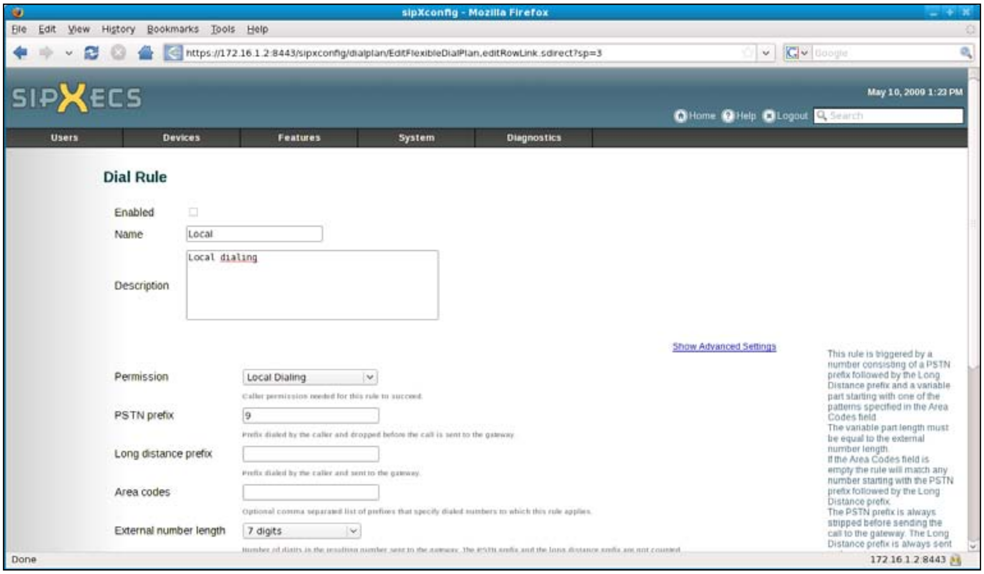
- **Schedule**: A schedule can be defined that determines when the custom dial rule can be used.
- **Gateways**: A list of gateways available to this dial rule. See the *Adding gateways* section earlier in this chapter for information about gateway selection and user locations. The resulting call is sent to the gateways specified in the gateway list in the order gateways are listed. List the preferred gateway first and backup gateways below it.

Emergency dial rules

The Emergency dial rule is for emergency calls. Many phones can be programmed to dial 911 directly to a gateway (in case the PBX is not available). For those that can't, this dial rule will handle the call routing. This dial rule is typically first in the list of the overall Dial Plan.

Administrators should take the time to evaluate requirements for 911 dialing for their locale and make sure that the system is in compliance with local laws.

The **Emergency Dial Rule** can be seen in the following image:



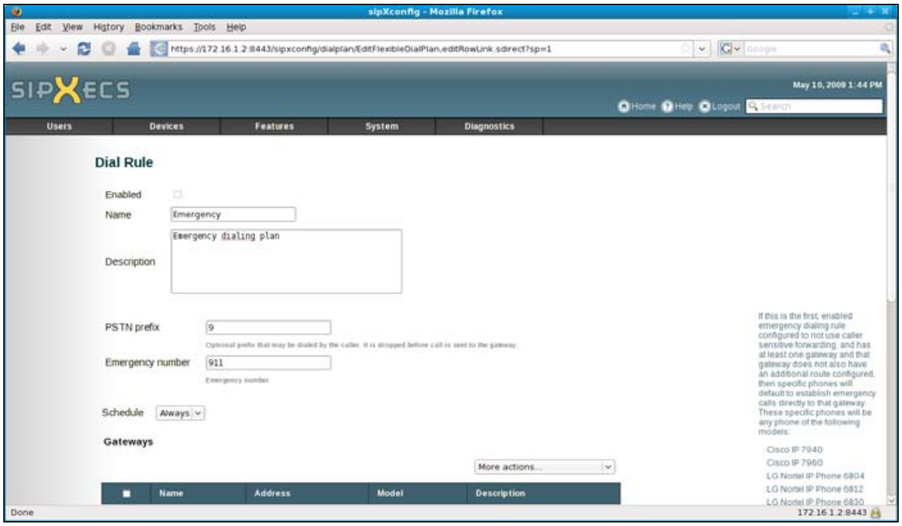
The following settings are available for **Emergency Dial Rules**:

- **Enabled**: Dial rules can be enabled or disabled in the system as the administrator wishes. A rule might be disabled if it is being tested or if a temporary rule gets created to address a particular problem.
- **Name**: This is a descriptive name for the dial rule.
- **Description**: More information about this dial rule and what it is used for.
- **Permission**: Defines the user permissions a user must have to use this dial rule.
- **PSTN prefix**: The optional prefix dialed by the caller and dropped before the call is sent to the gateway (in the previous example screen the user can dial 9911 or 911).
- **Schedule**: A schedule can be defined that determines when the custom dial rule can be used. In general no schedule should be applied to an Emergency dial rule.
- **Gateways**: A list of gateways available to this dial rule. See the *Adding gateways* section earlier in this chapter for information about gateway selection and user locations. The resulting call is sent to the gateways specified in the gateway list in the order gateways are listed. List the preferred gateway first and backup gateways below it.

> Always test Emergency Dial plan after system is setup (before go-live) and if any gateway changes are made.

International dial rules

The **International Dial Rule** is much like the Long Distance dial rule. The rule is triggered by a number consisting of a PSTN prefix followed by the Long Distance prefix (international code) and a variable part starting with one of the patterns specified in the **Area Codes** field.



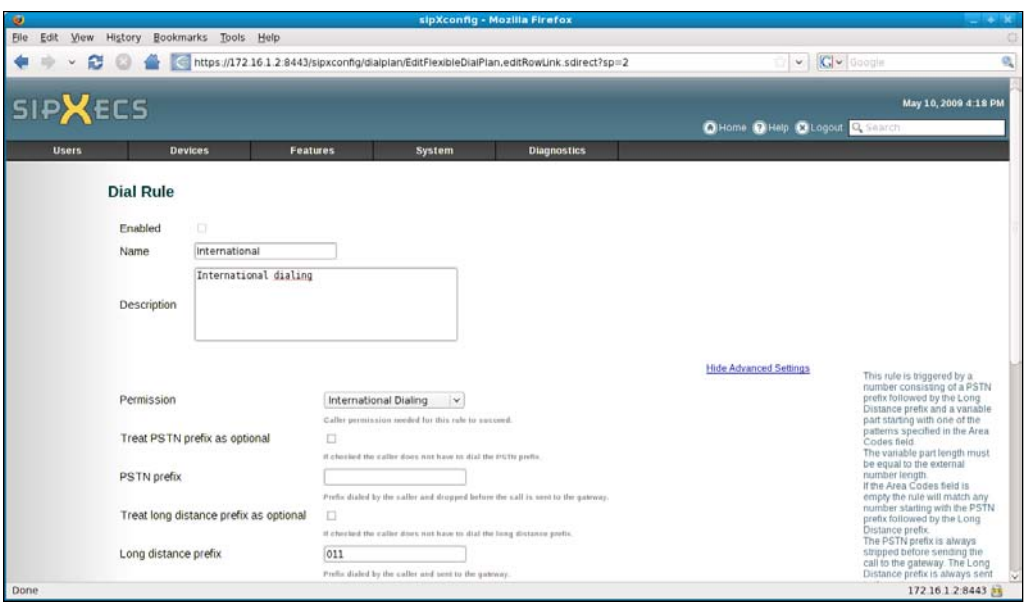
The following settings are available for International dial rules (click on **Show Advanced Settings** to see all of the **Dial Rule**'s options):

- **Enabled**: Dial rules can be enabled or disabled in the system as the administrator wishes. A rule might be disabled if it is being tested or if a temporary rule gets created to address a particular problem.
- **Name**: This is a descriptive name for the dial rule.
- **Description**: This has more information about this dial rule and what it is used for.
- **Permission**: Defines the user permissions a user must have to use this dial rule. This defaults to the International Dialing Permission.
- **Treat PSTN prefix as optional**: If this is checked, the caller does not have to dial the PSTN prefix (following). Dialing the PSTN prefix is optional by default. This item is only shown if **Show Advanced Options** is selected.
- **PSTN prefix**: The prefix dialed by the caller and dropped before the call is sent to the gateway. The Long Distance prefix is always sent to the gateway.
- **Treat long distance prefix as optional**: If checked the caller does not have to dial the long distance prefix. This item is only shown if **Show Advanced Options** is selected.

- **Long distance prefix**: The prefix dialed by the caller and sent to the gateway. This is the International Dialing Code.
- **Area codes**: Optional comma-separated list of prefixes that specify the dialed numbers to which this rule applies. If the **Area Codes** field is empty, the rule will match any number starting with the PSTN prefix followed by the **Long Distance** prefix.
- **External number length**: The number of digits in the resulting number sent to the gateway. The PSTN prefix and the long distance prefix are not counted. Valid values are: **Any number of digits** and 5-15 digits. For the International Dial Rule this defaults to **Any number of digits**.
- **Schedule**: A schedule can be defined that determines when the custom dial rule can be used.
- **Gateways:** A list of gateways available to this dial rule. See the *Adding gateways* section earlier in this chapter for information about gateway selection and user locations. The resulting call is sent to the gateways specified in the gateway list in the order gateways are listed. List the preferred gateway first and backup gateways below it.

Attendant dial rules

The purpose of the Attendant Dial Rule is to route calls to different auto attendants based on the time of day. See Chapter 7 for informaion on configuring auto attendants.



The following settings are available for **Attendant Dial Rules** (click on **Show Advanced Settings** to see all of the Dial Rule's options):

- **Enabled**: Dial rules can be enabled or disabled in the system as the administrator wishes. A rule might be disabled if it is being tested or if a temporary rule gets created to address a particular problem.
- **Name**: This is a descriptive name for the dial rule.
- **Description**: This has more information about this dial rule and what it is used for.
- **Extension**: The extension number to be dialed to reach the auto attendant.
- **Attendant aliases**: The attendant will be reachable through its extension and any of the **Attendant aliases**. When entering multiple aliases, separate them with spaces. These may also be DIDs if utilized in this system.
- **Default attendant**: The default attendant to be routed to if neither the working time nor the holiday date is matched. This would typically be considered the after-hours attendant.
- **Working time attendant**: This is typically the daytime greeting played to all callers. When an attendant is specified fields are displayed for Sunday through Saturday in which the administrator can specify typical work hours.
- **Holiday attendant**: If a holiday attendant is specified an **Add** hyperlink will be displayed allowing the administrator to add specific dates that require a different auto attendant message be played.

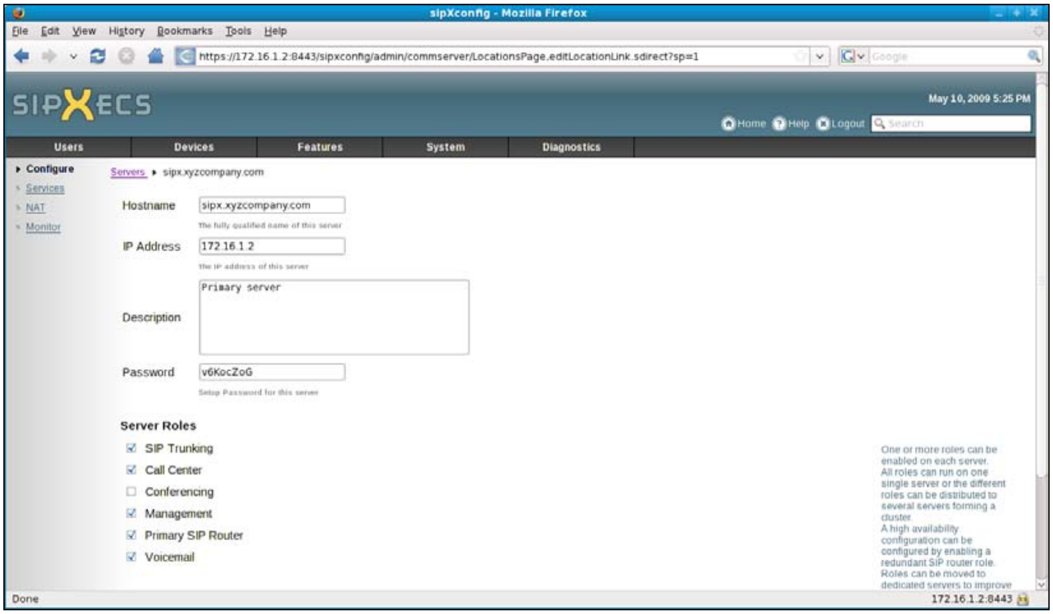
Session Border Controllers

Session Border Controllers (**SBC**) allow SIP calls to traverse network boundaries (firewalls). Because SIP traffic contains IP-specific information, SIP messages need to be modified when they traverse a **NAT**'d (**Network Address Translation**) network connection. With the 4.x release of sipXecs, an internal Session Border Controller has been included. SBC functionality is important if you are planning on utilizing ITSP phone system connectivity (SIP Trunks) or if IP phones need to connect to the system across the Internet.

Unmanaged Session Border Controllers from third-party vendors can also be utilized by the system. These SBCs in most cases provide additional security and functionality beyond the integrated SBC.

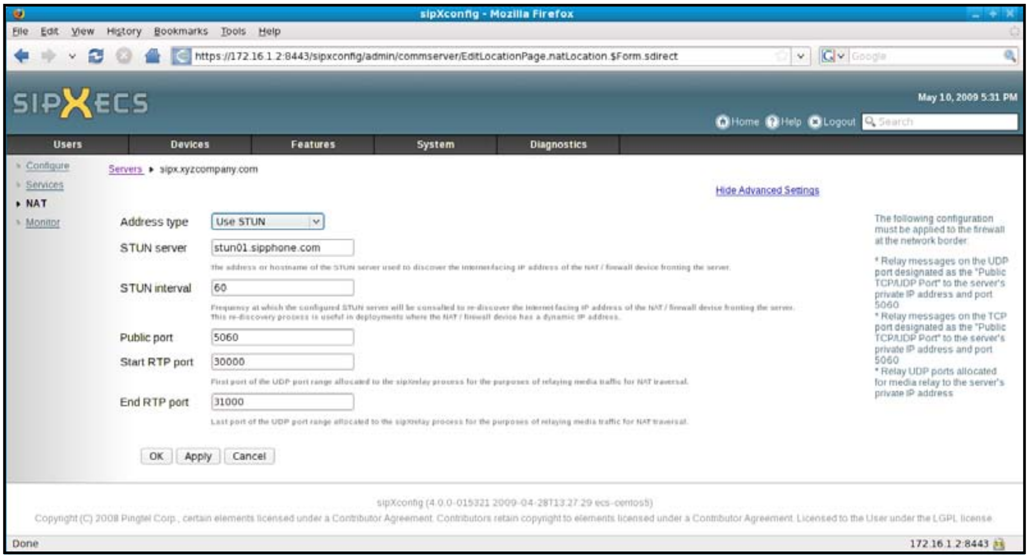
sipXecs Session Border Controller

To enable internal SBC functionality, the service must first be enabled on the server. To enable the service, select the **Servers** menu item in the system menu. On the next screen, click on the PBX that will house the SBC and then select **Configure** from the lefthand menu. The following page should be displayed:



Place a check mark next to **SIP Trunking** and then click on **Apply** at the bottom of the page. If prompted, restart any services required.

Next, click on the **NAT** item in the lefthand menu. The following page will be displayed, which allows the administrator to configure ho the external IP address of the PBX is determined.



The following settings are available for NAT configuration (click on **Show Advanced Settings** to see all of the options):

- **Address type**: Select either **Specify IP address** or use **STUN** (**Simple Traversal** of **UDP** over **NAT**). Simply put, a STUN server allows an internal server to determine what IP address the greater Internet is seeing the server come from. Several free-for-use STUN servers are available on the Internet.
- **STUN server**: The address or hostname of the STUN server used to discover the Internet-facing IP address of the NAT / firewall device fronting the server. By default the service uses the very popular server at `stun01.sipphone.com`.
- **STUN interval**: The frequency at which the configured STUN server will be consulted to re-discover the Internet-facing IP address of the NAT / firewall device fronting the server. This re-discovery process is useful in deployments where the NAT / firewall device has a dynamic IP address.
- **Public port**: This is the port is used for SIP traffic.
- **Start RTP port**: The first port of the UDP port range allocated to the sipxrelay process for the purposes of relaying media traffic for NAT traversal.

- **End RTP port**: The last port of the UDP port range allocated to the sipxrelay process for the purposes of relaying media traffic for NAT traversal.

To complete the NAT traversal configuration the following configuration must be applied to the firewall at the network border:

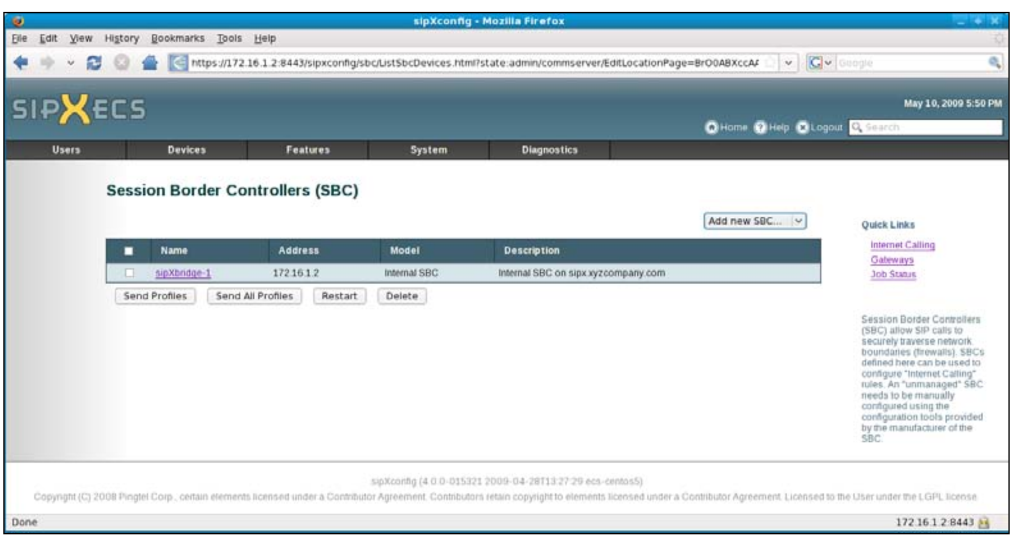
- Relay messages on the UDP port designated as the "Public TCP/UDP Port" to the server's private IP address and port 5060.
- Relay messages on the TCP port designated as the "Public TCP/UDP Port" to the server's private IP address and port 5060.
- Relay the UDP port range allocated for media relay to the server's private IP address.

A relay is also known as a *port forward*.

> If you have a SIP-aware firewall it may be necessary to disable that functionality so that it does not interfere with the NAT traversal services in sipXecs.

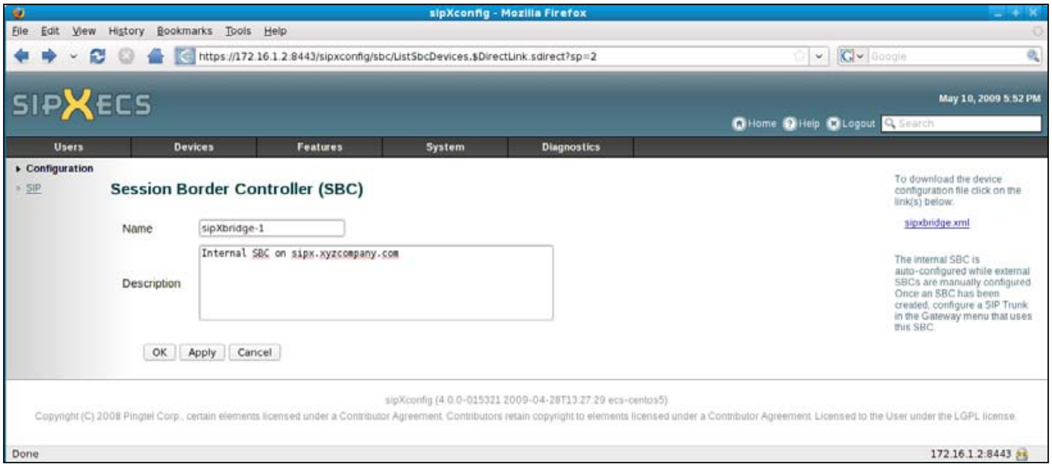
Defining Session Border Controllers

Session Border Controllers can be added to the system by selecting the **SBCs** menu item in the **Devices** menu. As seen in the following screenshot, the sipXbridge-1 Internal SBC will be displayed if the SIP Trunk service was added to the sipXecs server.

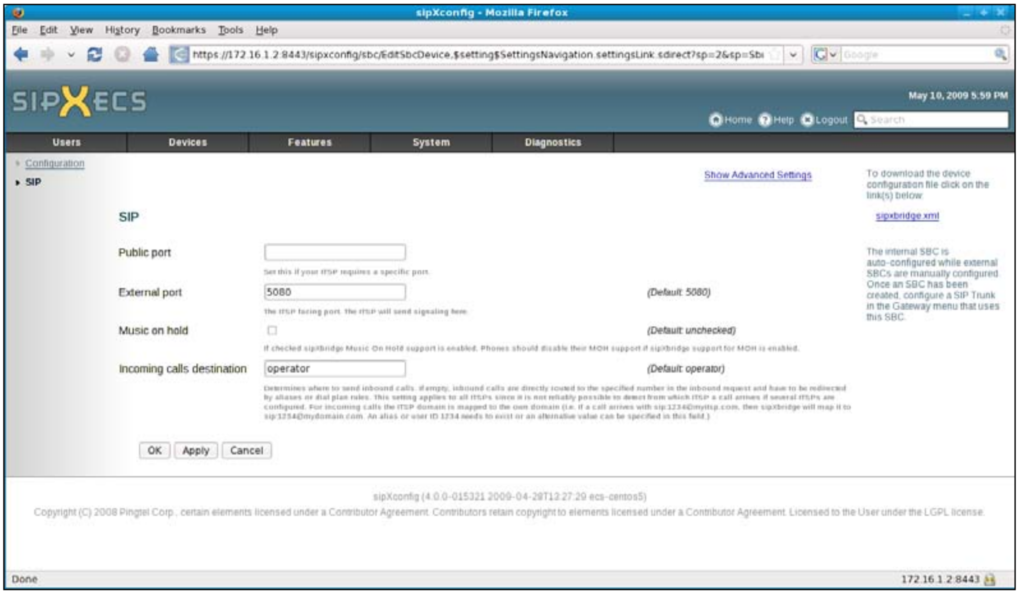


SBCs defined here can be used to configure "Internet Calling" rules. To add a third-party SBC, click on the **Add new SBC** drop-down menu and select **Unmanaged SBC**. An "unmanaged" SBC needs to be manually configured using the configuration tools provided by the manufacturer of the SBC.

The sipXbridge SBC has some settings that can be configured. Click on **sipXbridge-1** and the bridge configuration screen will be displayed as follows:



The name and description of the sipXbridge can be changed here. Clicking on **SIP** on the lefthand menu will reveal the following page:



The following SIP settings are available for the sipXbridge SBC (click on **Show Advanced Settings** to see all of the options):

- **Public port**: Set this if your ITSP requires a specific port.
- **External port**: The ITSP-facing port that the ITSP will send signaling to (default: 5080).
- **Signaling keep-alive interval**: The keep-alive timer for SIP Signaling. sipXbridge will re-register with each ITSP to keep the NAT pinhole open on the near-end firewall. The default is 20 seconds.
- **Media keep-alive interval**: A keep-alive timer for RTP. Each RTP stream facing the ITSP will start a timer that runs with this timeout (in milliseconds). The default is 1 millisecond.
- **Music on hold**: If this is checked, the sipXbridge Music on Hold support is enabled. Phones should disable their MOH support if sipXbridge support for MOH is enabled.
- **Incoming calls destination**: Determines where to send inbound calls. If it is empty, inbound calls are directly routed to the specified number in the inbound request and have to be redirected by aliases or dial plan rules. This setting applies to all ITSPs since it is not reliably possible to detect from which ITSP a call arrives if several ITSPs are configured. For incoming calls the ITSP domain is mapped to the local domain (that is, if a call arrives with `sip:1234@myitsp.com`, then sipXbridge will map it to `sip:1234@mydomain.com`. An alias or user ID 1234 needs to exist or an alternative value can be specified in this field). The default is to route calls to the operator alias.
- **Logging level**: The debug level for the sipXbridge gateway is set here. Valid values are: OFF, INFO, WARN, ERROR, DEBUG, and TRACE. The default setting is INFO. Logs can be found on the sipXecs server in the `/var/logs/sipxpbx` folder.

Summary

One of the most difficult tasks in getting a new communications system operating is interfacing it with the outside world. Patience and testing will be required to make any communication system interoperate with you phone trunk providers.

In this rather large chapter we covered Gateways, Dial Plans, and sipXecs's integrated Session Border Controller. You should have garnered enough knowledge to begin making these necessary settings.

7
Configuring sipXecs Server Features

sipXecs has several server-side features that provide additional functionality. These functionalities are not otherwise available in the phones themselves. Many of the basic features will be covered in this chapter, while some of the more advanced features will be described in Chapter 9. This ever-increasing list of system features helps set sipXecs apart from its competition. As you will discover in this chapter, the features are easy to configure and they are easy for the end user to utilize.

In this chapter we will cover configuration of the following services:

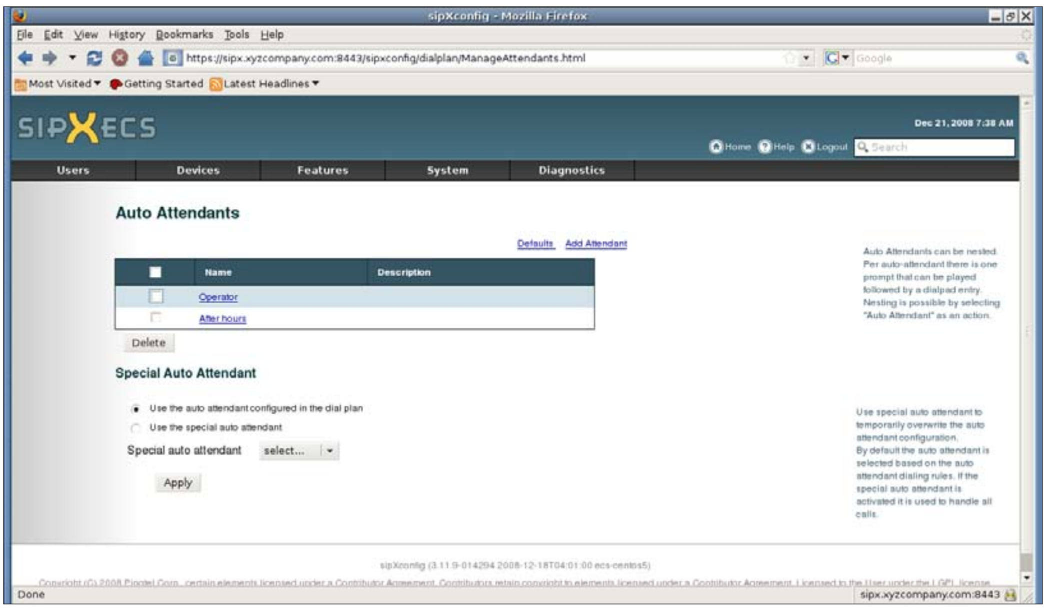
- Auto attendant
- Intercom
- Paging Groups
- Call Park Orbits
- Music on Hold

Auto Attendant

As mentioned in Chapter 1, the multi-level auto attendant service provides system-wide answering of incoming calls, dial-by-name abilities, automated transfer to local extensions, access to remote voicemail retrieval, and transfer to other auto attendants.

The auto attendant is often the first impression your callers will have of your organization, so designing a menu structure that is clear and concise is critically important. For good auto attendant design, try not to have more than two auto attendants deep. Callers quickly become annoyed if they have to go through too many menu layers.

The auto attendant configuration is accessed through the system administration screen by clicking on the **Features** menu and then selecting the **Auto Attendants** menu item. The **Auto Attendants** page will be displayed as follows:

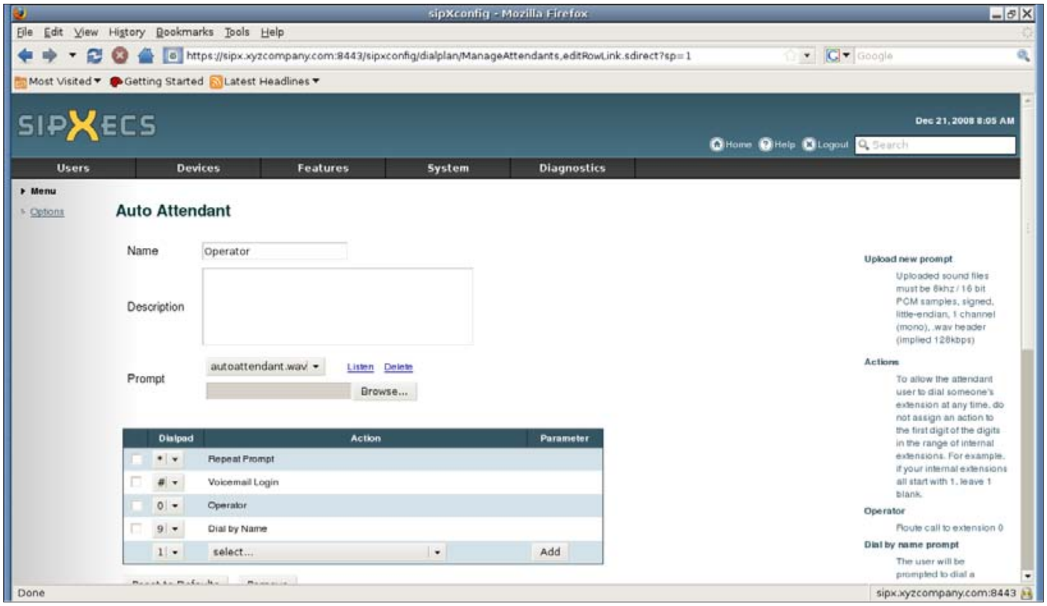


By default there are two auto attendants defined, but only the **Operator** auto attendant (AA) is in use. The administrator is free to create as many auto attendants as he or she would like. Auto attendants can be cascaded to create multiple levels.

Which auto attendant answers initially for the system is specified in the Dial Plan settings (see Chapter 6). Default Auto Attendant, Working Hours Auto Attendant, and Holiday Auto Attendant can all be specified as part of the Dial Plan configuration.

On the **Auto Attendants** page a **Special Auto Attendant** may be selected with the **select** drop-down menu. This feature is useful if the organization is unexpectedly closed. In addition to activating the **Special Auto Attendant** on this page, it can also be activated remotely through the voicemail system by a system administrator or a user with the Record System Prompts permission (see Chapter 8).

To edit an existing attendant, click on its name. To add a new auto attendant, click on the **Add Attendant** hyperlink. The default **Operator** auto attendant has been selected for editing in the following screenshot:



The name of the auto attendant can be changed and a more detailed description added if desired. To listen to the existing prompt, click on the **Listen** hyperlink. To upload a new prompt to play click on the **Browse** button and locate the file on your local computer.

Auto attendant prompt sound files must be 8khz / 16 bit PCM samples, signed, little-endian, 1 channel (mono), `.wav` header (implied 128kbps). There are many products available for manipulating audio files. MediaCoder (`http://www.meoderhq.com`) works very well for exchanging between different audio formats. Audacity (`http://audacity.sourceforge.net/`) is a sound mixer that allows mixing in music along with recorded voice.

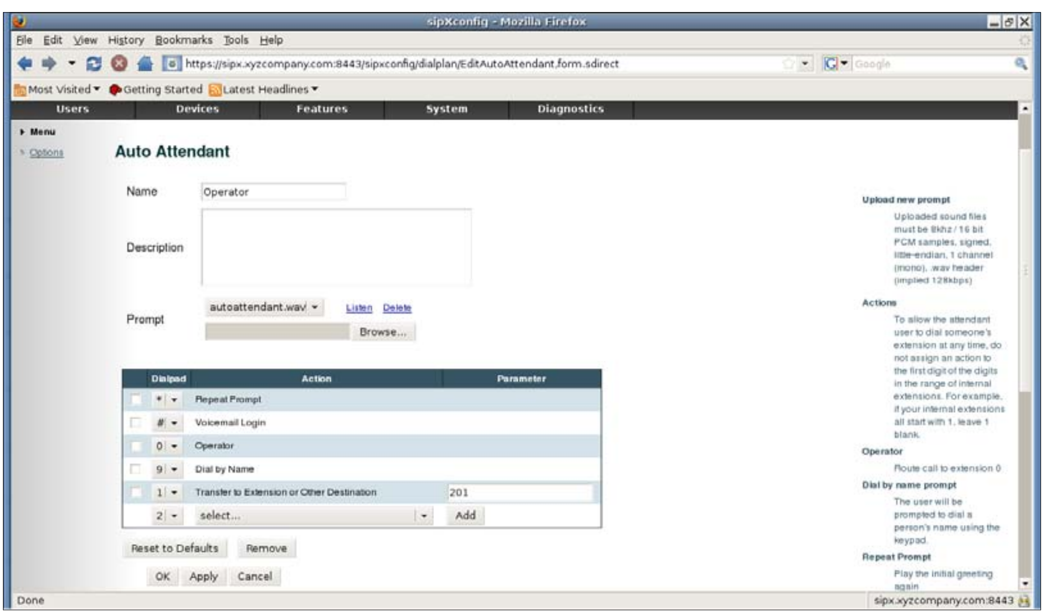
> An easy way to record AA prompts is to record them into a user's voicemail box. Once recorded, use the User Web Portal (see Chapter 8) to save the WAV file to your local computer and then upload it on the auto attendant page.

The following actions may be assigned to the phone dial pad keys (0 through 9, asterisk—* and pound—#):

- **Operator**: Routes the call to extension zero (0).
- **Dial by Name**: Connects the caller to the dial-by-name directory.
- **Repeat Prompt**: Replay the greeting that was just heard.
- **Voicemail Login**: The caller will be directed to the voicemail system and prompted to log in.
- **Disconnect**: Plays a good-bye message and ends the call.
- **Auto Attendant**: Routes the caller to another auto attendant.
- **Transfer to Extension or Other Destination**: Routes the call to an extension. This can be a user on the system, hunt group, ACD queue, or an external phone number.
- **Deposit Voicemail**: Directs the caller directly to a voicemail box, plays the voicemail box greeting, and the user can leave a message.

To add an action, click on the **Dialpad** drop-down box at the bottom of the table to select the digit desired, select the **Action** with the drop-down box, and click on the **Add** button.

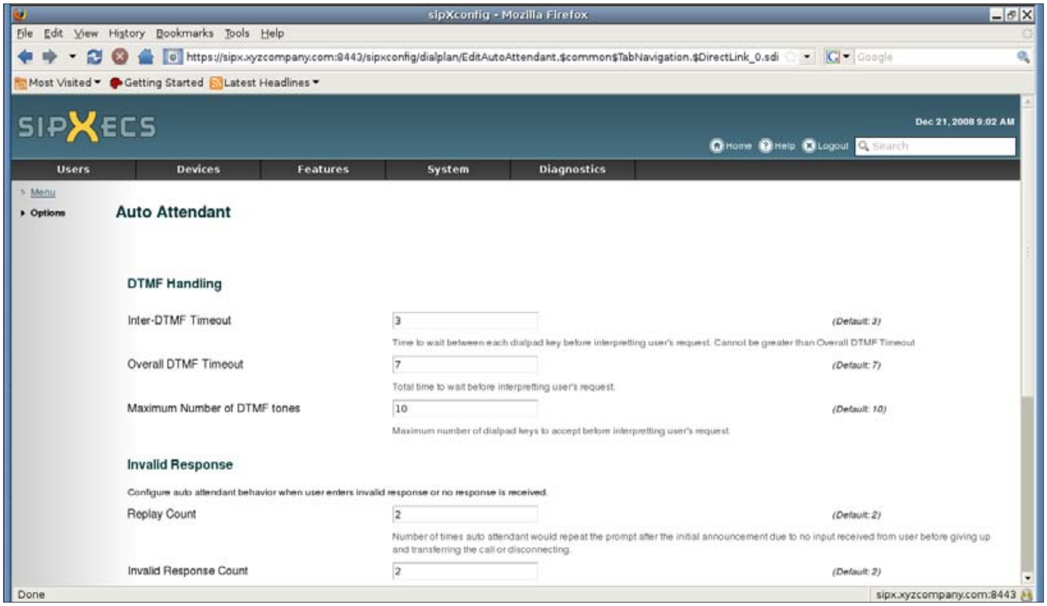
If a parameter is required a dialog or drop-down box will appear in the **Parameter** column shown as follows:



Click on the **OK** or **Apply** button to make the changes take effect. The changes will become live after a short delay for the system to generate the new **VXML** (**Voice XML**) code in the background.

To remove an action, place a check mark next to the action and click on the **Remove** button. Likewise, to reset the menu back to its default settings click on the **Reset to Defaults** button.

Clicking on the **Options** link on the left side of the page allows the administrator to customize **DTMF** (**Dial Tone Multi Frequency**) handling and **Auto Attendant Invalid Response** handling. The **Auto Attendant Options** page is shown as follows:



The following DTMF handling settings are available:

- **Inter-DTMF Timeout**: The time to wait between each dial pad key press before interpreting the caller's request. This value cannot be greater than **Overall DTMF Timeout**. (Default: 3 seconds.)
- **Overall DTMF Timeout**: The total time to wait before interpreting the caller's request. (Default: 7 seconds.)
- **Maximum Number of DTMF tones**: The maximum number of dial pad key presses to accept before interpreting caller's request. (Default: 10 key presses.)

The **Invalid Response** settings allow the administrator to configure the auto attendant's behavior when callers enter an invalid response or no response is received.

- **Replay Count**: The number of times the auto attendant prompt will be repeated after the initial announcement due to no input being received. (Default: 2 times.)
- **Invalid Response Count**: The number of times the caller can input an invalid response before the auto attendant transfers or disconnects the call. (Default: 2 times.)
- **Transfer on Failures**: If this setting is enabled, the auto attendant will transfer the call to a designated extension if no valid response is received. If disabled, the call will be disconnected. (Default: unchecked.)
- **Transfer Extension**: The extension to be used when transfer on failure is enabled.
- **Prompt to play when transferring call after failure**: The administrator can specify a WAV file to play before transferring the call after a user input error.

After the desired settings are modified click **OK** or **Apply** to make them active.

Auto Attendant example

As mentioned in Chapter 2, when designing an auto attendant, the best policy is to keep the menu structure as simple as possible. Most of us have experienced examples of poorly designed auto attendants and they never result in a positive experience for the caller.

The following is an example flow diagram of a multilevel auto attendant for a typical widget company.

Operator Auto Attendant (ext. 100)

Menu Option	Description	Action	Parameter
1	Customer Service ACD Queue	Transfer to Extension	550
2	Sales Auto Attendant	Auto Attendant	SalesAA
3	Accounting Department Hunt Group	Transfer to Extension	501
4	Human Resources	Transfer to Extension	230
9	Dial by Name Directory	Dial by Name	Dial by Name
0	Operator	Operator	Operator
#	Voicemail Login	Voicemail Login	Voicemail Login
*	Repeat Menu	Repeat Prompt	Repeat Prompt

Sales Auto Attendant (SalesAA)

Menu Option	Description	Action	Parameter
1	Product A Sales Group ACD	Transfer to Extension	551
2	Product B Sales Group ACD	Transfer to Extension	552
3	Product C Sales Group ACD	Transfer to Extension	553
0	Operator	Operator	Operator
#	Voicemail Login	Voicemail Login	Voicemail Login
*	Repeat Menu	Repeat Prompt	Repeat Prompt

The above example shows how an **Auto Attendant** menu structure would be created and flow in sipXecs. This auto attendant is referred to as a multilevel auto attendant because main menu option 2 calls yet another auto attendant.

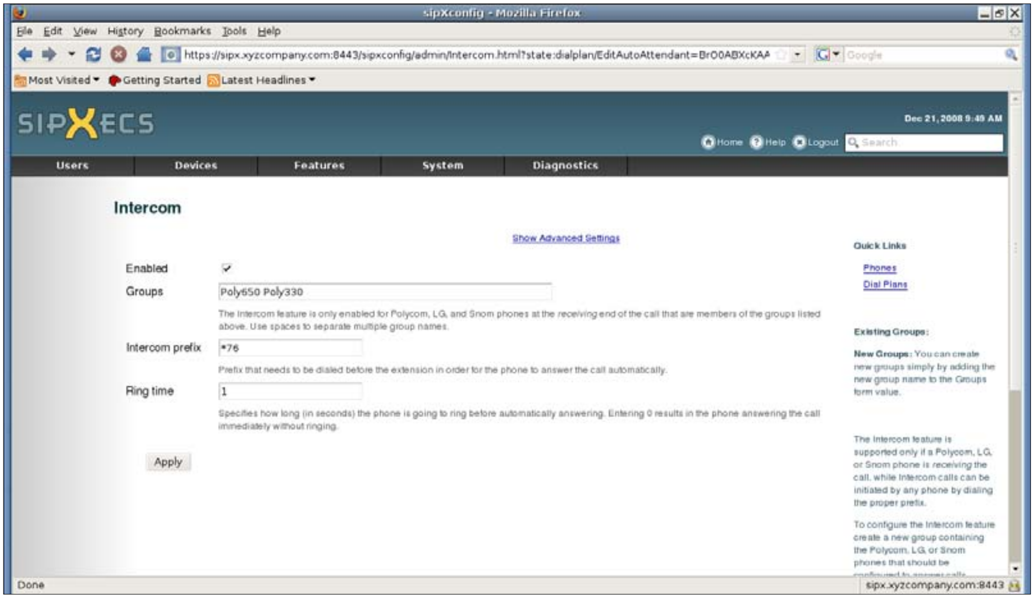
The preceding call flow has calls getting to the main auto attendant from the gateway to extension 100. Users have menu options 1 to 4 for various departments, 9 for the dial by name directory, 0 will dial the system operator extension, # is the option for a caller to get to the voicemail system login, and * allows the user to repeat the auto attendant prompt. The options 9, 0, #, and * are fairly common across different voicemail systems.

> It is not necessary to announce all options available to users in the recorded auto attendant prompt. For example, when recording the AA prompt you may choose to not let users know that they can get to a voicemail prompt by pressing the # key.

Intercom

The intercom feature allows a caller to dial an extension, and have the called extension automatically go off hook so the two parties can then have a conversation. This feature only works with Polycom, LG Nortel, and snom phones on the receiving end of an intercom call.

To configure the intercom feature, in system administration click on the **Features** menu and select the **Intercom** menu item. The following screenshot shows the intercom feature enabled for the phones in the **Poly650** and **Poly330** phone groups.



The available settings are as follows:

- **Groups**: This contains list of phone groups for which the receiving end of an intercom call is allowed. The intercom feature only works with Polycom, LG Nortel, and snom phones at the receiving end of the call that are members of the groups listed. As in other places in the configuration server, use spaces to separate multiple group names and groups can be defined on-the-fly.
- **Intercom prefix**: This allows the administrator to customize the intercom feature code. This is the prefix that needs to be dialed before the extension in order to make the phone answer the call automatically.

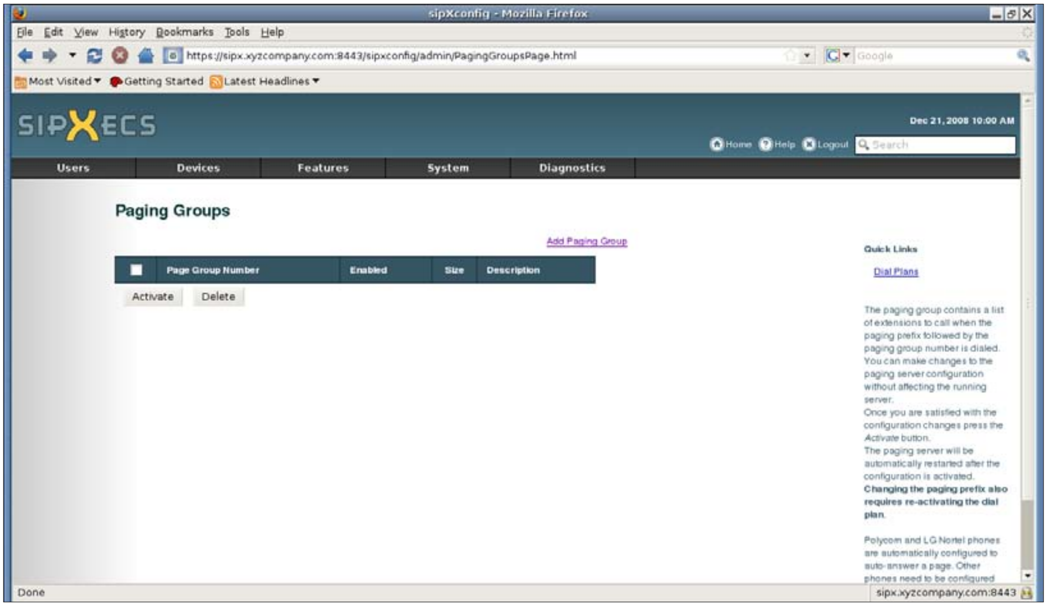
- **Ring time**: This is the amount of time (in seconds) the receiving phone is going to ring before automatically answering and going off-hook. Entering 0 results in the phone answering the call immediately without ringing.
- **Alert info** (Displayed by clicking on **Show Advanced Settings**): This is an internal configuration value, used by Polycom phones, to determine if the call is to be answered automatically.

Click on the **Apply** button to save the changes. The dial plan must be reactivated and the affected phones must have their configuration profiles regenerated.

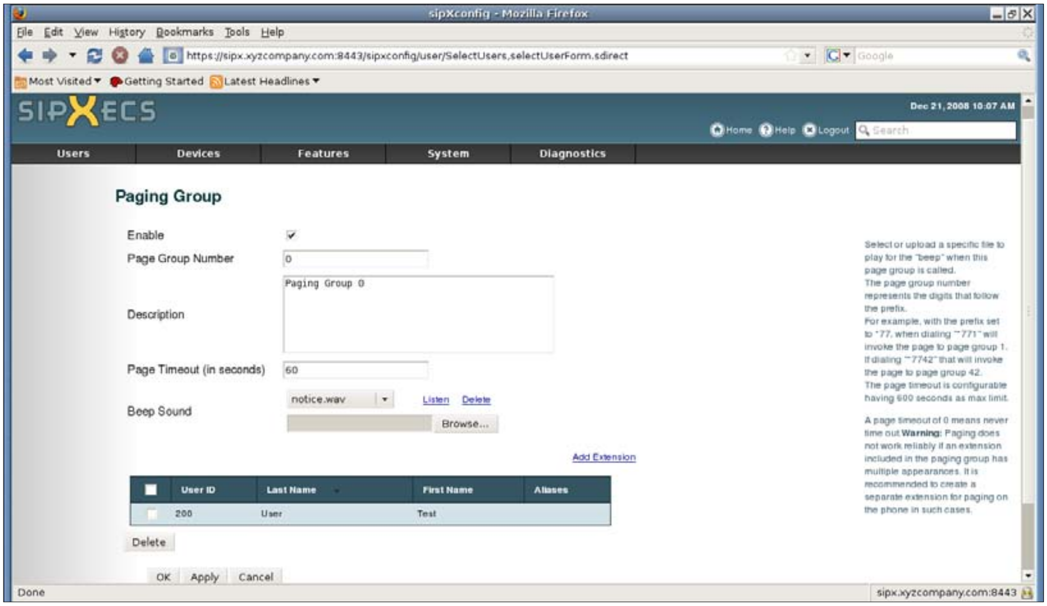
Paging Groups

A paging group is a group of extensions that will be contacted, automatically go off hook, and have an announcement message played. Polycom and LG Nortel phones are automatically configured to automatically answer a page. Other phones may need to be configured manually to receive a page.

The **Paging Groups** feature is accessed from the System Administration page by clicking on the **Features** menu and selecting the **Paging Groups** menu item. The following page will be displayed:



Click on the **Add Paging Group** hyperlink near the middle of the page and the **Paging Group** configuration page will be dislayed as seen in the following screenshot:



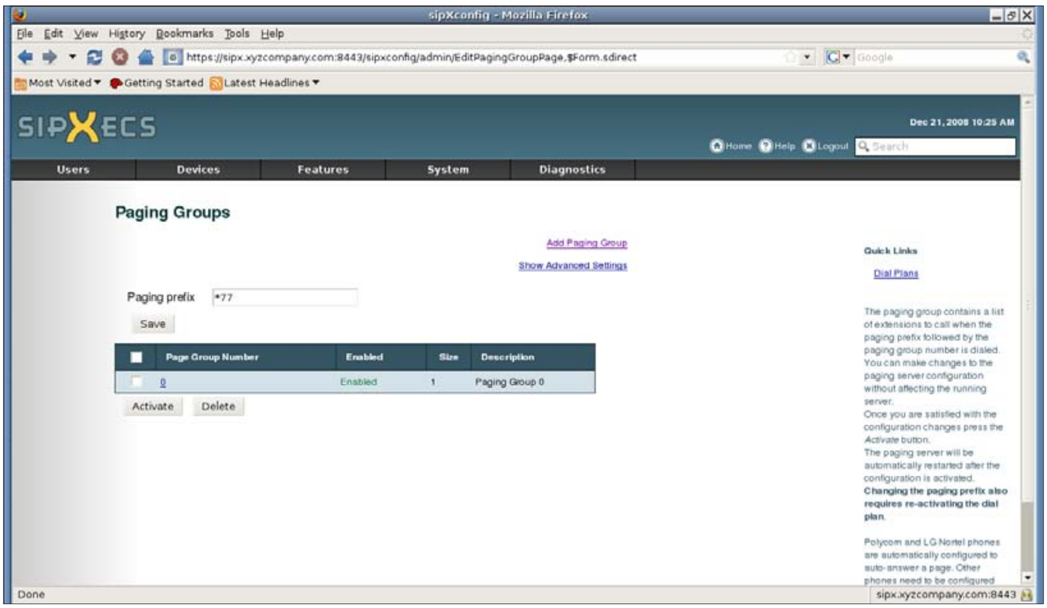
The following settings are available for configuration:

- **Page Group Number**: This is the number that will be dialed after the paging group feature code (the default feature code is *77). If the system will have many paging groups then start with double-digit codes and adjust your phone dial plans accordingly.
- **Description**: This is a text explanation regarding what this paging group is for.
- **Page Timeout**: This is a value in seconds after which a page will timeout if the caller has not hung up the call. The page timeout can have a maximum value of 600 seconds. A page timeout of zero means that the page will never time out.
- **Beep Sound**: This is a WAV file that will be played preceding the page.

Once the settings are configured as desired, enter a list of extensions with the **Add Extension** hyperlink.

Note that paging does not work reliably if a paging group member extension has multiple appearances. Add a separate extension used just for paging on any phones that require multiple appearances of the same extension.

Click on the **OK** button to save the configuration changes and return to the **Paging Groups** page. As seen in the following screenshot, the page group will now be listed along with the ability to change the paging feature code prefix.

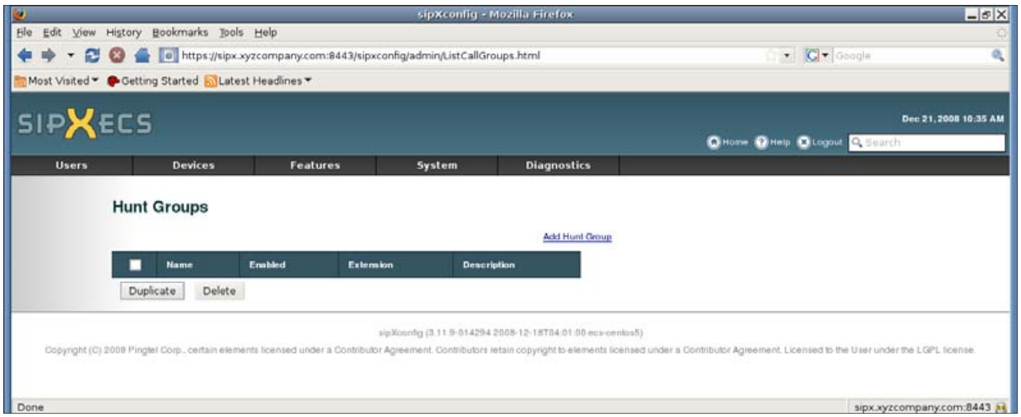


Clicking on **Show Advanced Settings** will reveal a **SIP Trace Level** drop-down box, which enables trace or debug logging for the paging service. This can be helpful for debugging if a phone is having difficulty receiving pages. Log files can be found in the `/var/log/sipxpbx` folder.

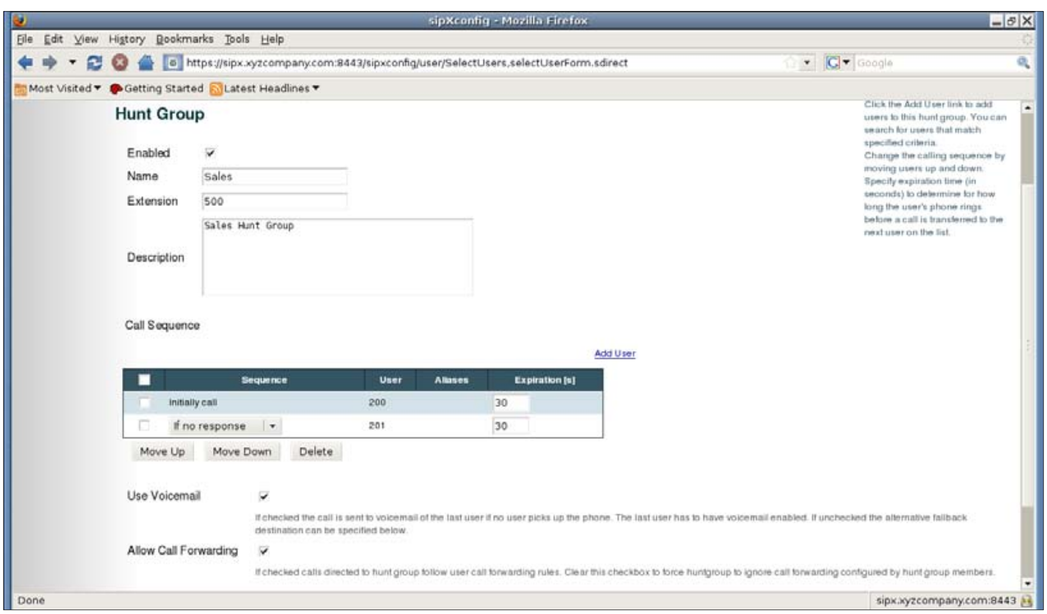
Once the paging server changes are complete the **Activate** button must be clicked to restart the paging service. If the paging feature code prefix is changed, the system dial plan must also be reactivated.

Hunt Groups

A hunt group is a collection of extensions that ring in a particular order when the hunt group number is dialed. To access the **Hunt Groups** page, from the System Administration page click on the **Features** menu and select the **Hunt Groups** menu item. The **Hunt Groups** page will be displayed as follows.



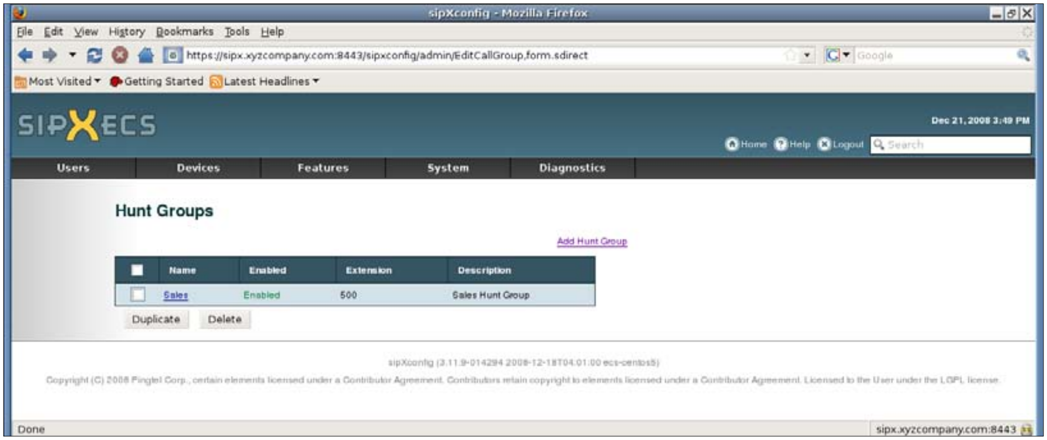
To add a hunt group, click on the **Add Hunt Group** hyperlink near the middle of the page. The **Hunt Group** page will be displayed as follows:



Hunt groups are configured with the following information:

- **Name**: This is the text name for the hunt group.
- **Extension**: This is the extension that is dialed to reach the hunt group, often referred to as the pilot number for the hunt group.
- **Description**: This is the text description to help document the system configuration.
- **Call Sequence**: This is the order in which extensions ring and for how long they ring. Check the box and use the **Move Up** and **Move Down** buttons to change the order of extensions. The drop-down box under **Sequence** can have values of **If no response** and **At the same time**. Specify expiration time for each call. Users may only appear once in the hunt group.
- **Use Voicemail**: If this box is checked, the call is sent to the voicemail box of the last extension in the list if the call is not answered. If it is not checked, an alternative fallback destination can be specified.
- **Fallback Destination**: This will be visible only if **Use Voicemail** is unchecked. The value entered can be an extension, SIP address, auto attendant, park orbit, or another hunt group.
- **Allow Call Forwarding**: If this box is checked, calls to the hunt group will also follow user call forwarding rules. Clear the checkbox to force the hunt group to ignore user call forwarding (most often this is preferable).

Click **OK** or **Apply** to accept all changes to the hunt group. After clicking **OK** the **Hunt Group** page will be displayed as shown in the following screenshot:



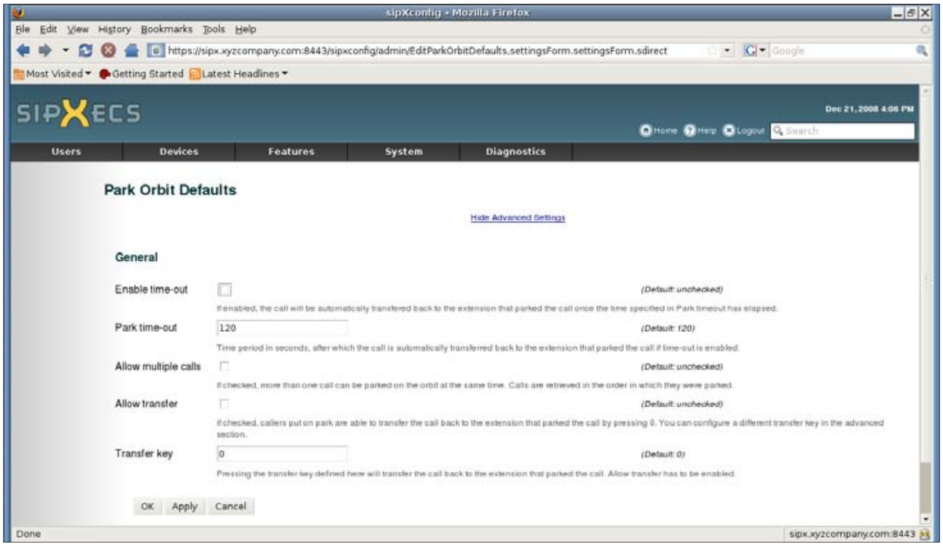
Hunt groups can be duplicated by checking the box next to the hunt group name and clicking on the **Duplicate** button.

Call Park Orbits

A call park orbit is a queue that is intended to temporarily hold on to a call so that it can be picked up at any extension. The caller that is placed in a call park orbit will hear music or whatever message the administrator specifies. Once the desired party is located, they can retrieve the parked call from any phone they happen to be near.

To get to the **Call Park** configuration, from the System Administration screen, click on the **Features** menu and then the **Call Park** menu item. The following page will be displayed on entry to the **Call Park** feature:

The defaults for call park orbits can be set by clicking on the **Defaults** hyperlink near the middle of the page. The following screenshot shows the **Park Orbit Defaults** page after **Show Advanced Settings** was selected.

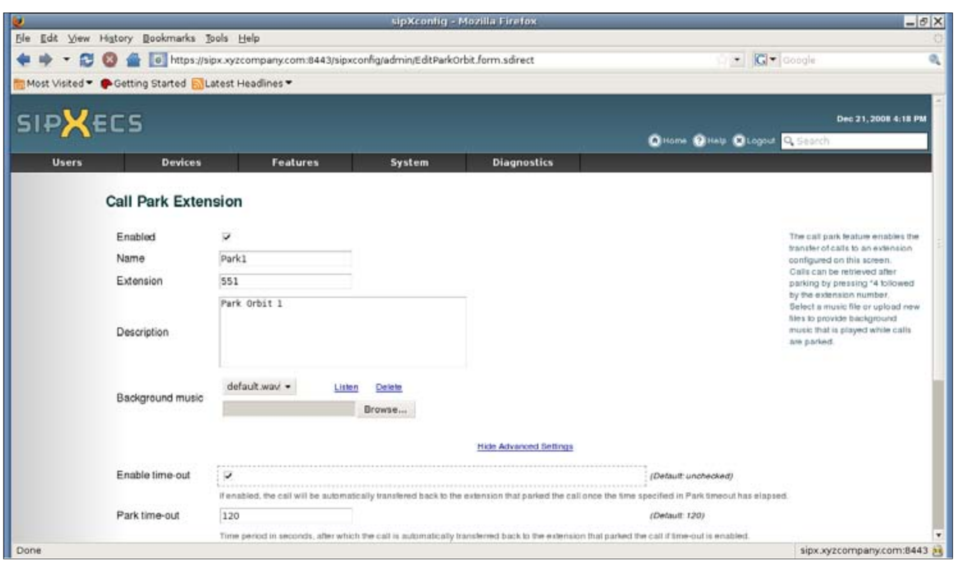


The following default settings can be configured for the **Call Park Orbits**. (Each call park orbit can have different settings. These are just the default settings that will be presented when call park orbits are created.)

- **Enable time-out**: If this is enabled, the call will be automatically transferred back to the extension that parked the call once the time specified in **Park time-out** has elapsed. (Default: unchecked.)
- **Park time-out**: This is the time period in (in seconds), after which the call is automatically transferred back to the extension that parked the call if time-out is enabled. (Default: 120 seconds.)
- **Allow multiple calls**: If this is checked, more than one call can be parked on the orbit at the same time. Calls are retrieved in the order in which they were parked. (Default: unchecked.)
- **Allow transfer**: If this is checked, callers put on park are able to transfer the call back to the extension that parked the call by pressing zero (0). The administrator can configure a different transfer key in the advanced section. (Default: unchecked.)
- **Transfer key**: Pressing the transfer key defined here will transfer the call back to the extension that parked the call if **Allow transfer** is enabled. (Default: 0.)

Clicking on the **OK** button will accept the changes to the call park orbit defaults. The **Call Park** page will be displayed again.

To create a call park orbit, click on the **Add Call Park Extension** hyperlink near the middle of the page. The **Call Park Extension** page will be displayed as shown in the following screenshot:



The following settings can be set for each call park orbit:

- **Name**: A text name given to the call park orbit.
- **Extension**: This is the extension number that can be dialed to transfer a call to the call park orbit.
- **Description**: This is the text description of the call park orbit to help with documenting the system.
- **Background music**: This is the audio that will be played to the callers waiting in the call park orbit. As with a call on hold, call park will play the audio file from the beginning of the file for each user.
- All of the settings from the default **Call Park** page as described above.

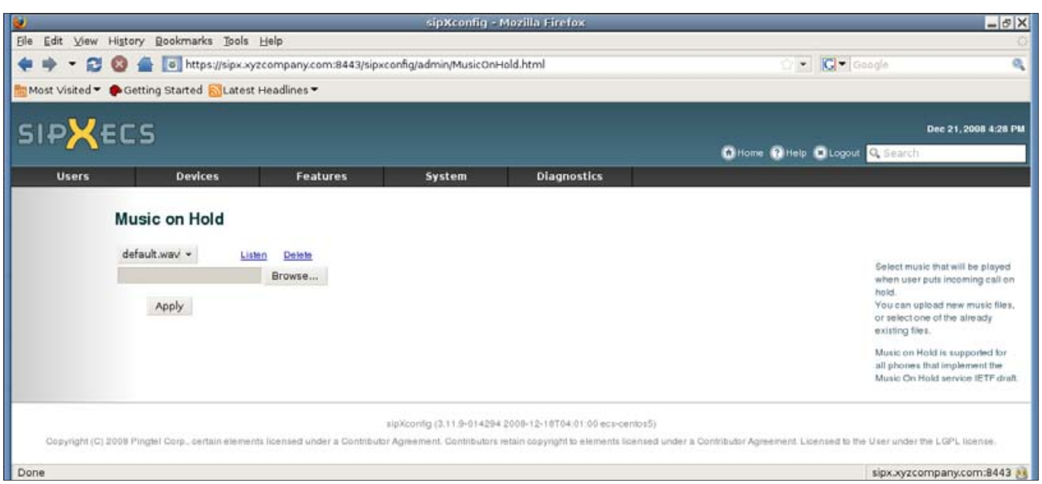
Click on **OK** to accept the changes and activate the Call Park Orbit.

Calls are placed into a call orbit by an unattended (blind) transfer to the **Call Park Orbit** extension number. Calls can be retrieved by any phone on the system after parking by pressing *4, followed by the extension number.

Music on Hold

As of this writing there is no one standard for supporting music on hold with a pure SIP phone system. Polycom and snom phones are known to support the same Music on Hold service IETF draft that Sipfoundry chose to support in sipXecs.

To change the Music on Hold audio, from the System Administration page, click on the **Features** menu and select the **Music on Hold** menu item. The following page will be displayed where the administrator can select a WAV file already present on the system or click on the **Browse** button to select a WAV file on his/her local computer.



Clicking the **Apply** button activates any change to **Music on Hold**.

Each call placed on hold will hear its own instance of the music on hold audio file starting from the beginning of the file.

Information on the IETF draft can be found at `http://svn.resiprocate.org/rep/ietf-drafts/worley/draft-worley-service-example-01.html`.

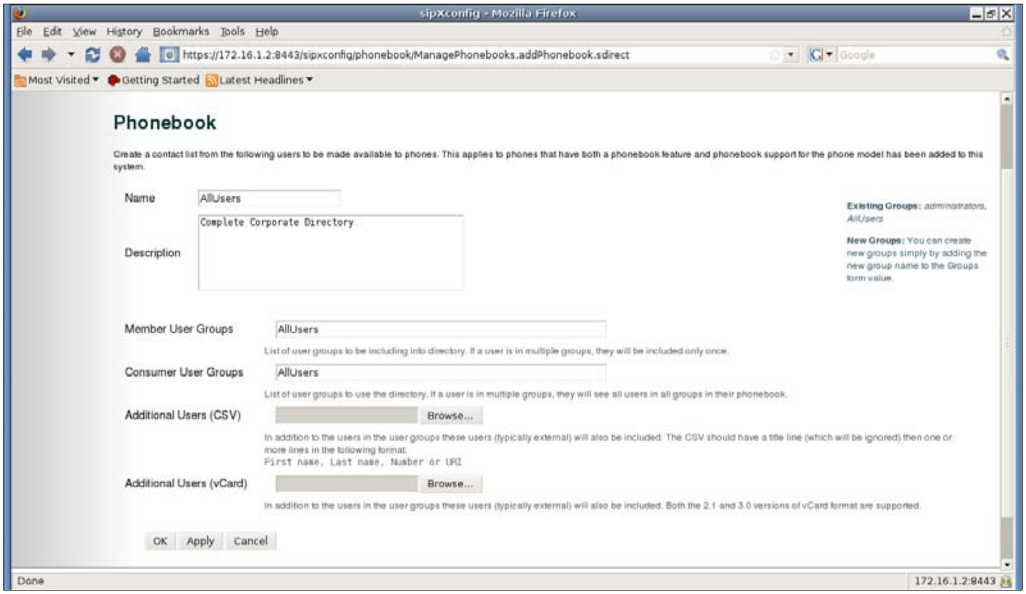
Phonebooks

The Phonebook feature in sipXecs allows centralized management of phone number directories within the phone system. This allows users to look up phone extensions and phone numbers by name, and dial directly from the directory.

The administrator can create different directories per department, user group, or for individual users. In addition to being able to maintain a list of internal users, lists of external phone numbers can be imported for often-needed phone numbers. At present, this feature is supported on Polycom, snom, and ClearOne MAX IP phones.

To create a system phonebook, from the System Administration page click on the **Features** menu and select the **Phonebooks** menu item. The following page will then be displayed:

Click on the **Add Phonebook** link near the middle of the page and the **Phonebook** page, as shown in the following screenshot, will be displayed:



The following settings can be set for each phonebook:

- **Name**: This is a text name given to the phonebook.
- **Description**: This is a text description of the phonebook to help with documenting the system.
- **Member User Groups**: This is the groups of users to be included into the directory. If a user happens to be in multiple groups they will only be added once.
- **Consumer User Groups**: These are the users who are allowed to use the directory. If the user has a compatible phone the directory will be downloaded to the phone when the phone boots.
- **Additional Users (CSV)**: In addition to the users in the user groups these users (typically external phone numbers) will also be included.
- **Additional Users (vCard)**: This is another method for importing external phone numbers into the system.

For importing external phone numbers the **Comma Separated Values** (**CSV**) file should have a title line (which will be ignored) then one or more lines in the following format:

First name, Last name, Number or URI

The following is an example CSV file that could be imported to the system:

First name, Last name, Number or URI

Antonios, Pizza, 5555551212

TellMe, News, 411@sipphone.com

Weather, Phone, 5555551212

The vCard file format is a standards-based file format that provides an electronic equivalent of a business card. It is supported by many different applications and often exchanged in emails. The vCard format is owned and maintained by the **IMC** (**Internet Mail Consortium**) (`http://www.imc.org/`).

Summary

We've now covered most of the basic system-provided features of the phone system. As highlighted in many of the features, phone selection is very important as not all features are supported on all makes and models of phones. This will continue to be one of the underlying challenges of a 'standards'-based phone system.

8

Using sipXecs—The User Perspective

Sooner or later you will to have to let the users start using the cool, new communications system you have built. sipXecs is not only easy for administrators to maintain and implement, it also provides a great experience to the user. In this chapter we will explore the following points:

- How users access the phone system features from their phones
- How users can leverage the user web portal

The Telephone User Interface (TUI)

The most common interface to the phone system for the user is the telephone. While the user web portal is a great way for the user to make changes to their phone and manage their voicemail, at the end of the day, the user wants to make phone calls.

Each hardware or software phone will have different methods for accessing features that are handled at the phone level. Features such as dialing a call, putting a call on hold, transferring a call, and setting up a multi-party (conference) call are all handled in the phone. How to use these features is different for every phone and will be documented in the user guides for your respective device.

Other calling features such as paging, intercom, and park orbits are handled by the phone system. These features are accessed by entering what are called feature codes. A feature code usually starts with an asterisk (*) followed by a one or two digit feature code. The features outlined in this section are described with their default feature codes.

For some of these features to work with minimal user keystrokes on hardware phones, the administrator may have to adjust the phone dial plans. This would usually be done within a phone group (see Chapter 5). The dial plans tell the phone when to send a call without the user having to press a dial key. Refer to the administrators guide for your phones to determine the appropriate dial plans.

Transfer a call directly to voice mail

Users can transfer calls directly to another user's voicemail by performing a blind transfer (refer to Chapter 1 for a description of the types of call transfers) to extension 8, followed by the user's extension. For example, to transfer a call to extension 201's voicemail, perform a blind transfer to 8201.

On a Polycom hardware phone the procedure is as follows:

- While on a call, press *Trnsfr* softkey
- Press *Blind* softkey
- Dial 8 + extension number
- Hang up

Directed call pickup

Directed call pickup is picking up another ringing extension. In sipXecs there is no ability to perform a general call pickup (pick up any ringing phone) or have call pickup groups (pick up any ringing phone in a particular group of phones) at this time. The reason for this is because with SIP a phone would have to query every phone on the network to determine if it is ringing. This would create a huge amount of network traffic overhead.

Directed call pickup uses feature code 78 by default. Dial *78 and the extension to pick up another ringing phone. So, for example, if extension 205 was ringing, a user would pick up his or her phone and dial *78 and the extension.

Because of some limitations in SIP and sipXecs, call pickup is not reliable if the targeted pickup line appears on more than one phone device.

Parking a call

The method of parking a call is a blind transfer of the call to a park orbit number. Chapter 7 described the configuration of park orbits. Park orbits each have an extension associated with them.

On a Polycom hardware phone the procedure is as follows:

- While on a call, press the *Trnsfr* softkey
- Press *Blind*
- Dial the orbit number (xxx - xxx)

Picking up a parked call

Picking up a parked call is a little different than parking a call. This function relies on the phone system to transfer the call from the park orbit to the extension from which it is being requested. To pick up a parked call dial *4 and the park orbit extension. For example, if a call was parked on 501, dial *4501.

On a Polycom hardware phone the procedure is as follows:

- Dial *4 then the park orbit number (xxx - xxx)

Intercom

The intercom feature allows a phone to ring another phone, have the receiving phone automatically go off-hook (on speakerphone unless the receiving party picks up the handset) and begin a two way conversation. To access this feature dial *76 followed by the extension you would like to call. So, to intercom to extension 203, dial *76203 and begin the conversation.

Paging groups

The paging group feature allows a single phone to broadcast a message to a group of phones. On the receiving end, the phone will play a predetermined tone and then the caller's message. To page a group of phones, dial *77 and then the paging group number. To page group 1, dial *771, wait for the tone, and then begin speaking.

Conference room controls

Users who are in a conference room controlled by sipXecs have the ability to affect their leg of the conference call. The following in-conference DTMF keys are defined:

- # (Hangup code): Hangup (leave) the conference call
- 0 (Mute): Mutes the input of the user's call leg microphone
- * (Deaf Mute): Mutes the input of the user's call leg microphone and speaker
- 9 (Energy Up): Increase the minimum voice energy required to be heard

- 8 (Energy Reset): Reset the minimum voice energy required to be heard
- 7 (Energy Down): Decrease the minimum voice energy required to be heard
- 6 (Volume Up): Increase the volume of the call on the user's call leg
- 5 (Volume Reset): Reset the volume of the call on the user's call leg
- 4 (Volume Down): Decrease the volume of the call on the user's call leg
- 3 (Talk Volume Up): Increase the sensitivity of the user's microphone
- 2 (Talk Volume Reset): Reset the sensitivity of the user's microphone
- 1 (Talk Volume Down): Decrease the sensitivity of the user's microphone

ACD sign in and out

If the user is a member of an ACD Queue (see Chapter 10 for ACD Queue specifics), the user can sign in and out of the queue with feature codes *86 and *88 respectively. If the user is a member of multiple call queues, they are signed into or out of all of them.

Using the sipXecs voicemail service

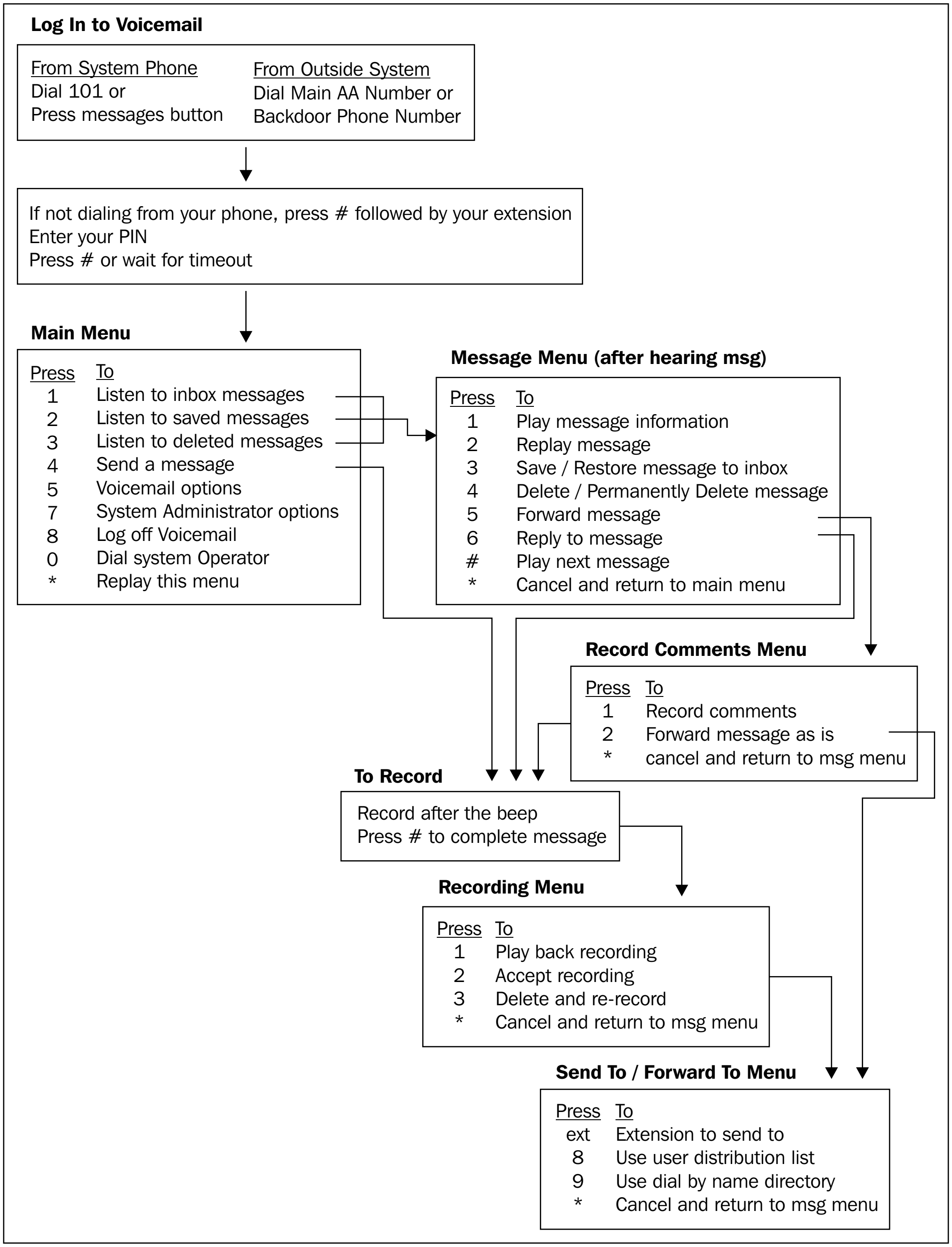
The sipXecs voicemail service is very easy for users to navigate. All user options are read to the user by the voicemail system.

To contact the voicemail service, the user may have a button programmed on the phone for messages or the user may have to dial 101 and enter their PIN when prompted. If a user would like to check his or her voicemail from a different phone, they would dial 101, press #, and then, when prompted, his or her extension and PIN respectively.

The following flowcharts demonstrate all of the voicemail system's features and menu structure.

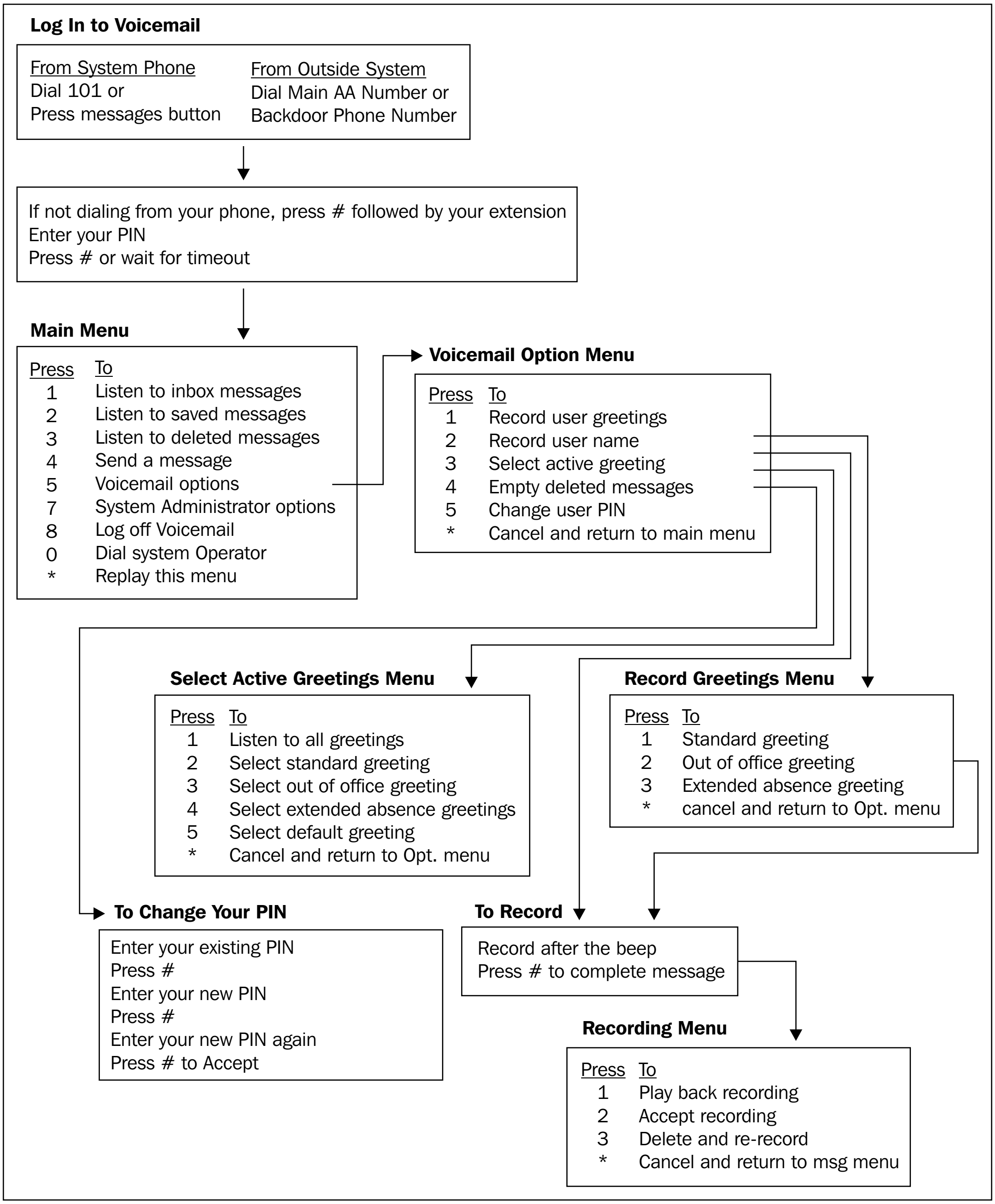
Voicemail messages menu structure

The following flowchart illustrates menu options when listening to voicemail messages:


Log In to Voicemail
From System Phone
Dial 101 or
Press messages button
From Outside System
Dial Main AA Number or
Backdoor Phone Number
If not dialing from your phone, press # followed by your extension
Enter your PIN
Press # or wait for timeout
Main Menu
Press To
1 Listen to inbox messages
2 Listen to saved messages
3 Listen to deleted messages
4 Send a message
5 Voicemail options
7 System Administrator options
8 Log off Voicemail
0 Dial system Operator
* Replay this menu
Message Menu (after hearing msg)
Press To
1 Play message information
2 Replay message
3 Save / Restore message to inbox
4 Delete / Permanently Delete message
5 Forward message
6 Reply to message
Play next message
* Cancel and return to main menu
Record Comments Menu
Press To
1 Record comments
2 Forward message as is
* cancel and return to msg menu
To Record
Record after the beep
Press # to complete message
Recording Menu
Press To
1 Play back recording
2 Accept recording
3 Delete and re-record
* Cancel and return to msg menu
Send To / Forward To Menu
Press To
ext Extension to send to
8 Use user distribution list
9 Use dial by name directory
* Cancel and return to msg menu

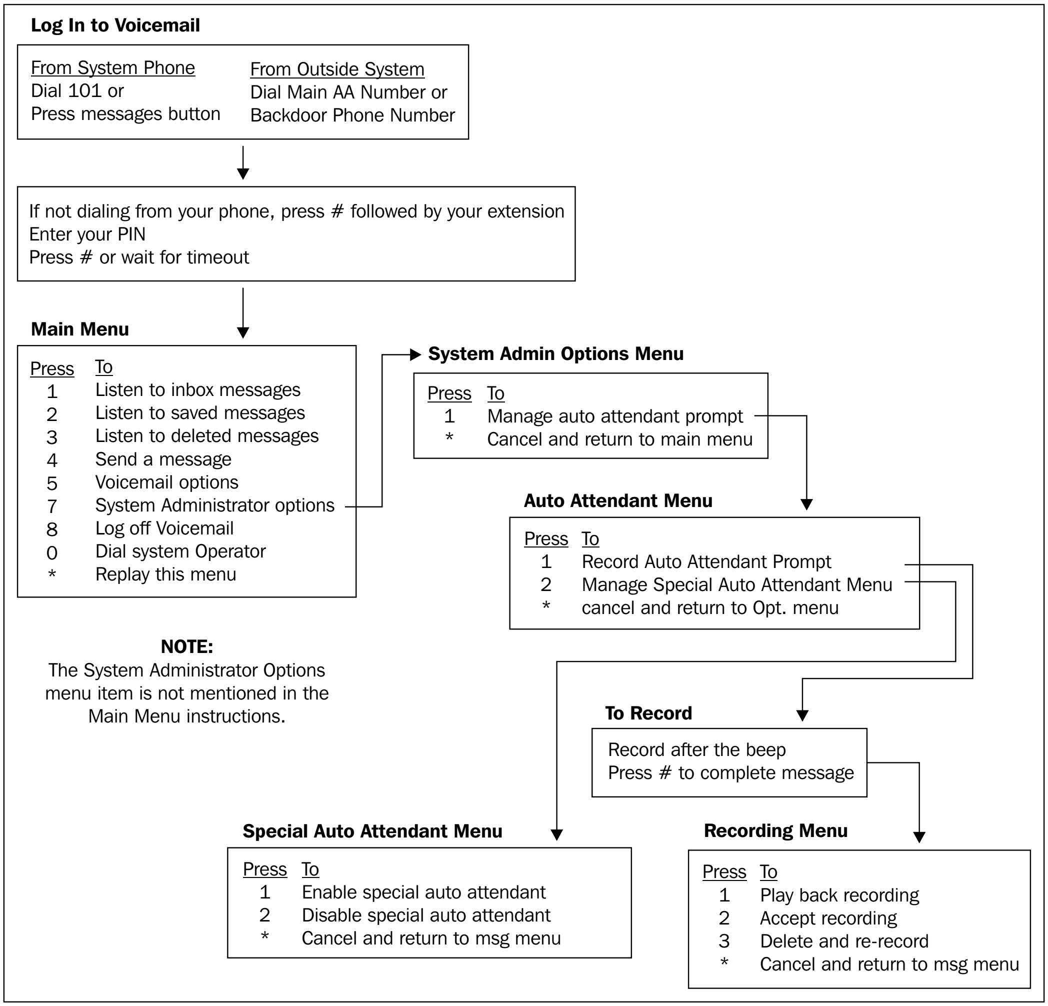
Voicemail options menu

The following menu flowchart illustrates the voicemail options menu:



Voicemail system administrator options

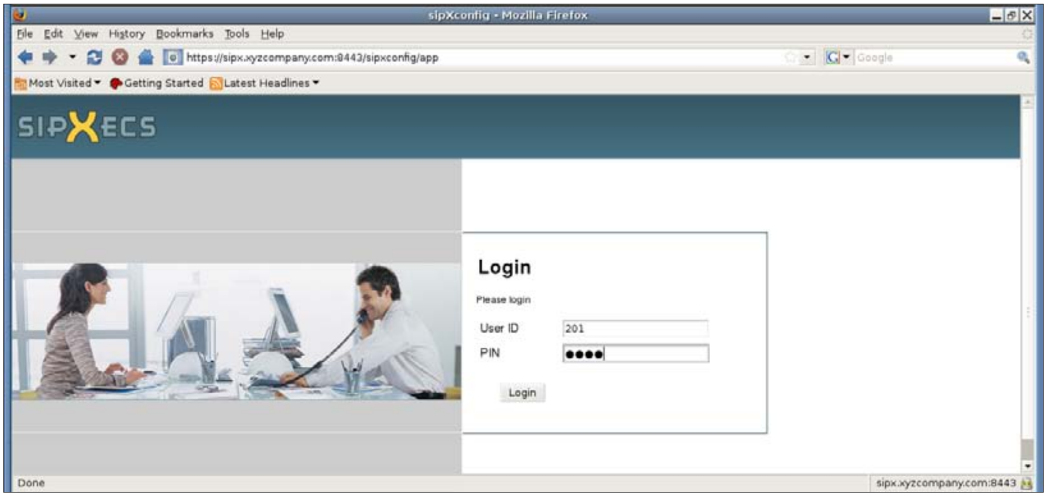
The following menu flowchart illustrates voicemail menu options available to the voicemail system administrator:



The user web portal

The user web portal allows the user to interact with the sipXecs system in a manner they may never have thought of before with a traditional phone system. While not all users will take to interacting with their phone system through a web browser, the savvy computer users will relish the opportunity to control their communications in a manner familiar to them.

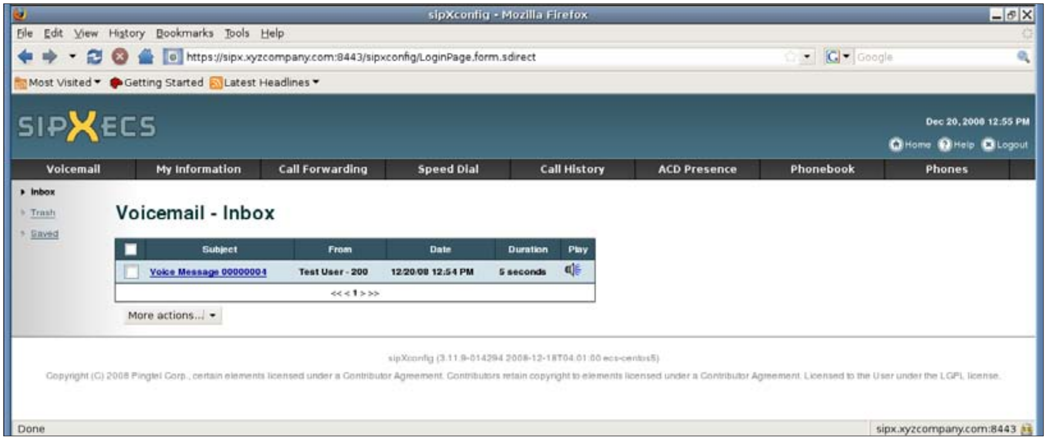
For users to get to the web server, they should go to the same web page as the administrator does to log in to manage the phone system (from our examples in previous sections `http://sipx.xyzcompany.com`). As shown in the following screenshot, the user enters his or her extension and PIN (the same PIN used to log in to voicemail, not the SIP password).



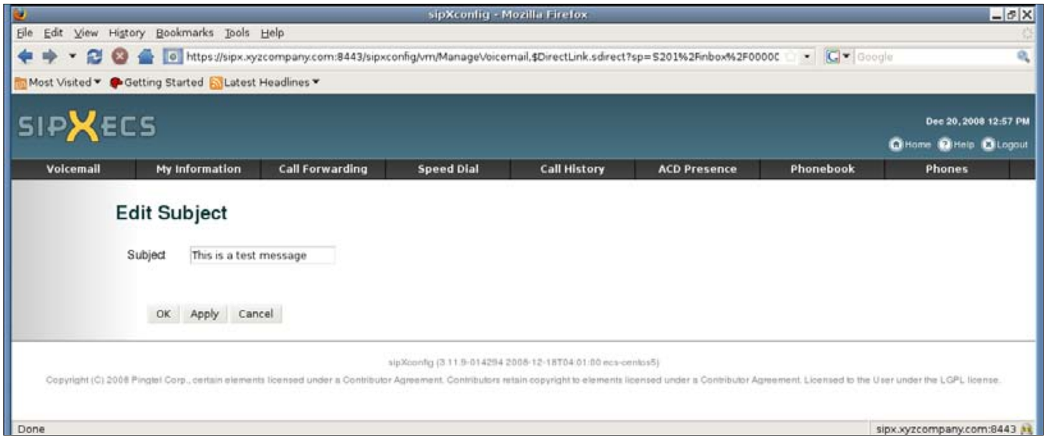
Upon login the user is directed to his or her voicemail inbox.

Voicemail

Any new voicemail will be shown in bold with caller ID as the sender's address (if available). The following screenshot shows user 201's inbox with a voicemail from user 200.



If the user clicks on the hyperlink under subject, he or she can change the subject of the message to something more descriptive, as shown in the following screenshot:



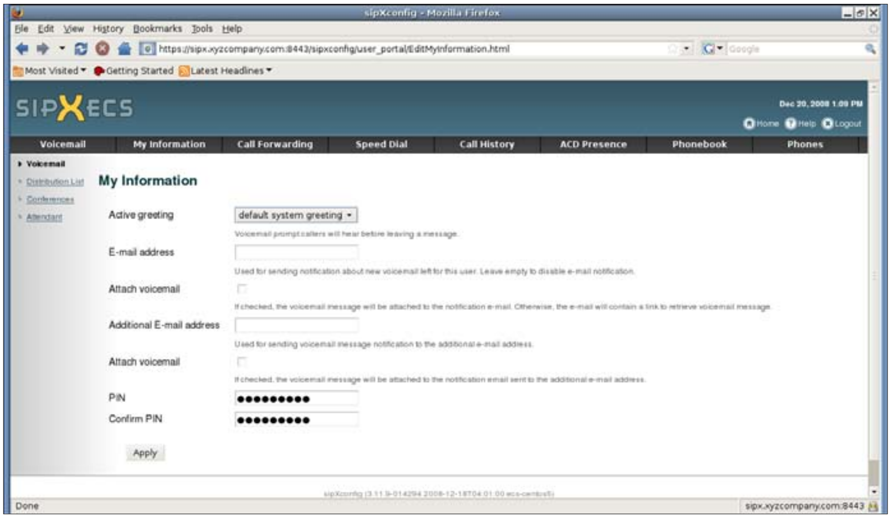
To play the voicemail, click on the small speaker icon in the play column. The voicemail is a WAV file; so as long as the user's computer can play that type of file, the message should begin being played through the computer's speakers.

The user can also right-click on the message icon and choose to save it to long-term storage on his or her computer or network.

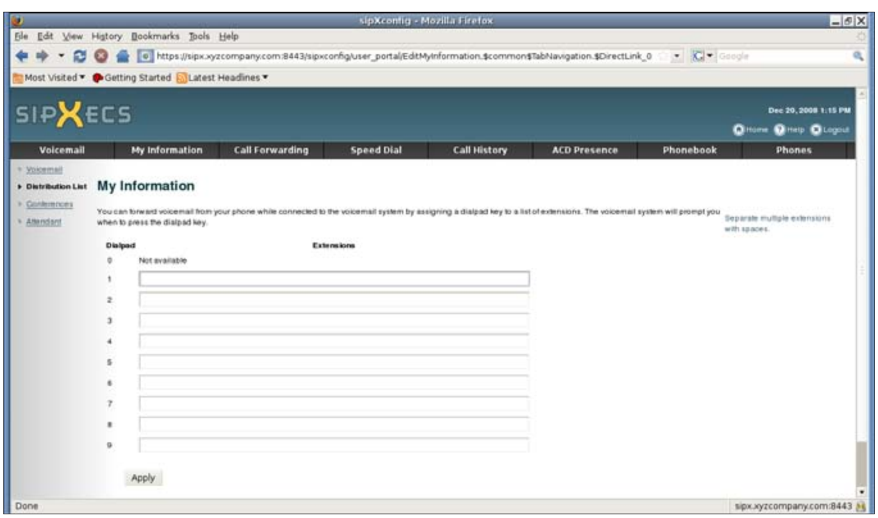
To delete or save the message, check the box to the left of the message, click on the drop-down box labeled **More actions** and pick the action desired. The **Trash** and **Saved** folders on the left work similarly.

User information

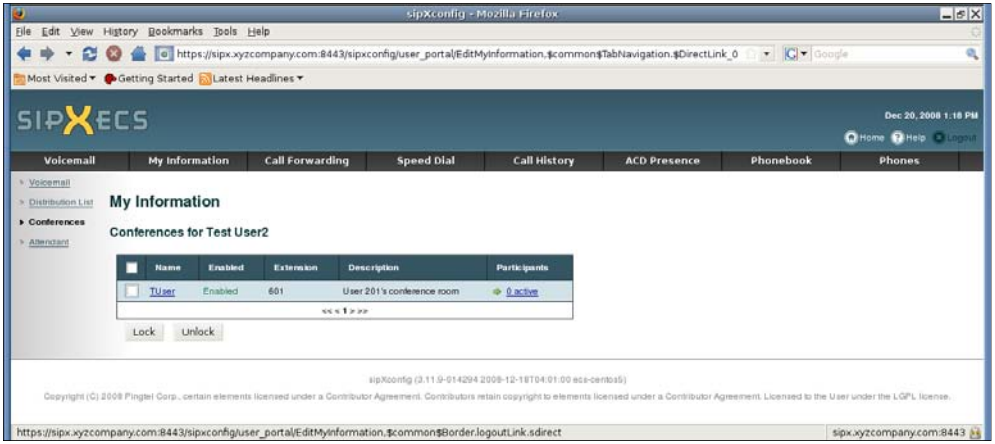
Clicking on the **My Information** tab near the top of the page displays settings the user can modify with regards to their voicemail configuration. The following screenshot shows that the users can modify their two voicemail notification email addresses, whether they want voicemails attached to the emails, and change their PIN.



Clicking on **Distribution List** on the left allows the user to modify their own voicemail distribution lists for sending voicemail to multiple system users at once. The distribution list page is then seen as follows:

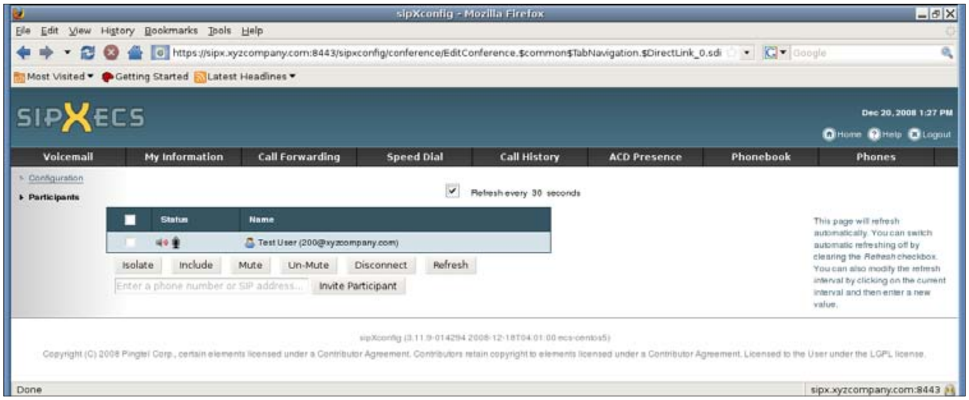


Clicking on the **Conferences** option at the left side of the page gives the user control over any conference rooms that have been assigned to him or her. The following screenshot shows a conference room named TUser with an extension of 601 and no active participants. The conference can be locked or unlocked for new participants joining by checking the box to the left of the conference and clicking on the respective button.

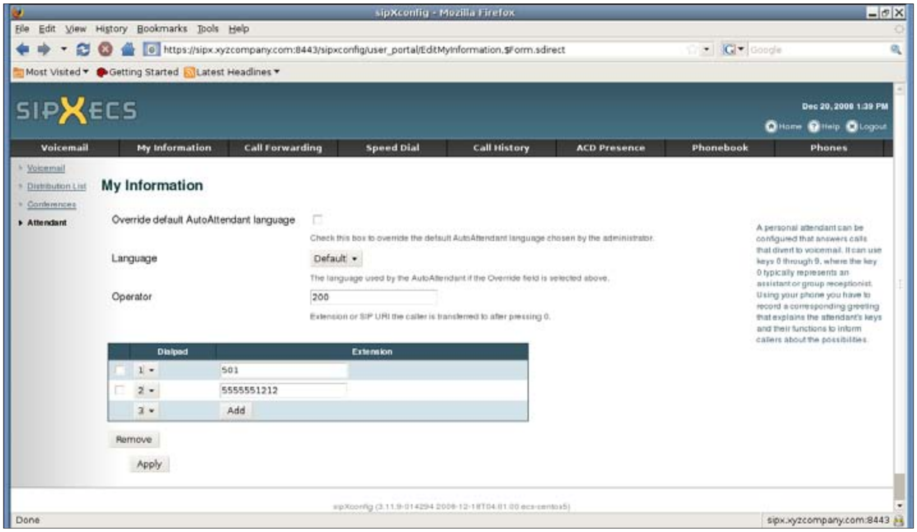


Clicking on the conference room name reveals configuration information for the room that the user is allowed to modify, as seen in the following screenshot. The user can choose to have a PIN for users to get into the conference and if the number of users in the conference is limited or not.

Clicking on **Participants** to the left or on the previous page allows the user to control individual users in the conference as well as invite new participants to the conference.

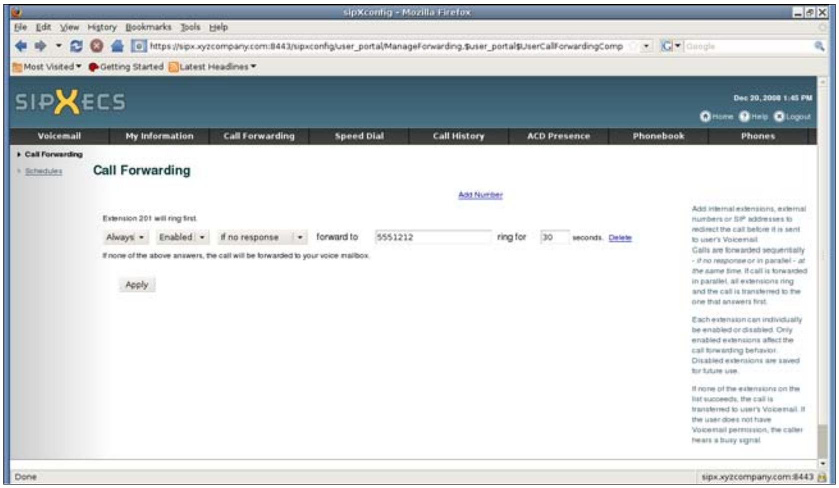


Clicking on the **My Information** tab and then selecting **Attendant** on the lefthand menu will allow the users to configure their own automated attendant and operator. As seen in the following example, the user can select actions for dialpad entries 0 to 9. It is up to the user to record the information for his or her personal auto attendant in his or her mailbox greeting.



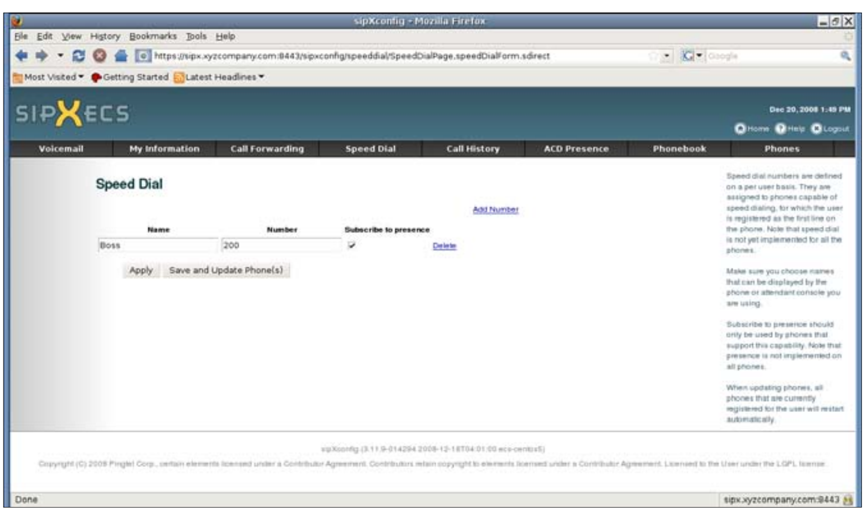
Call forwarding

The user has the ability to configure his or her own call forwarding by clicking on the **Call Forwarding** tab near the top of the page. The call forwarding and corresponding scheduling, as shown in the following screenshot, were covered in depth in Chapter 4.



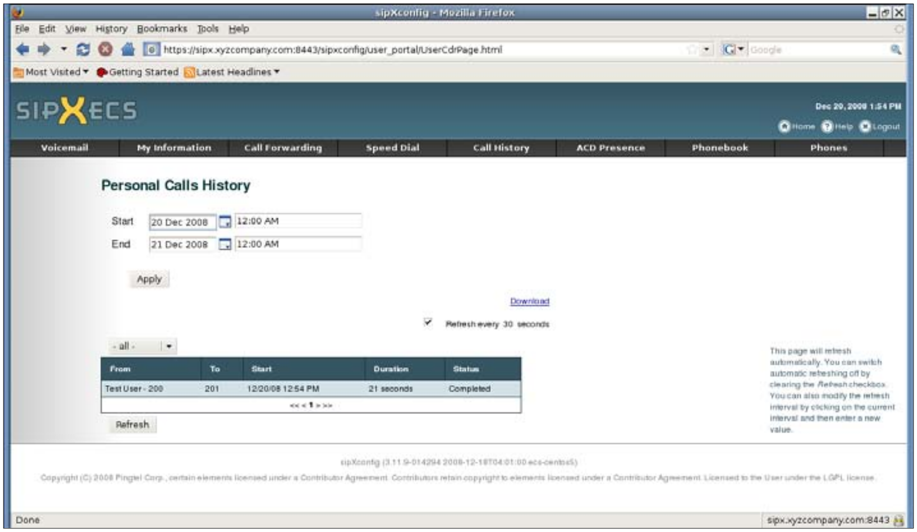
User speed dials

The **Speed Dial** tab at the top of the page allows the user to affect the buttons available on his or her phone. The **Speed Dial** page shown in the following screenshot is identical in function to that shown in Chapter 4. The user must click on the **Save and Update Phone(s)** button, which will update the phone profile and reboot the phone.



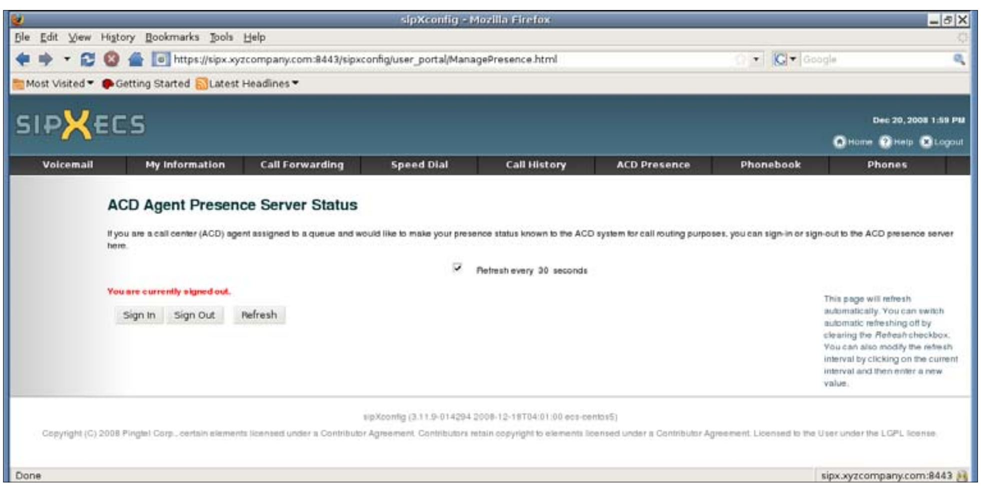
Call history

The **Call History** tab at the top of the page gives the user the ability to review all of the calls made to them or from them for any desired date range. As shown in the following screenshot, the current day is displayed on entry to the page.



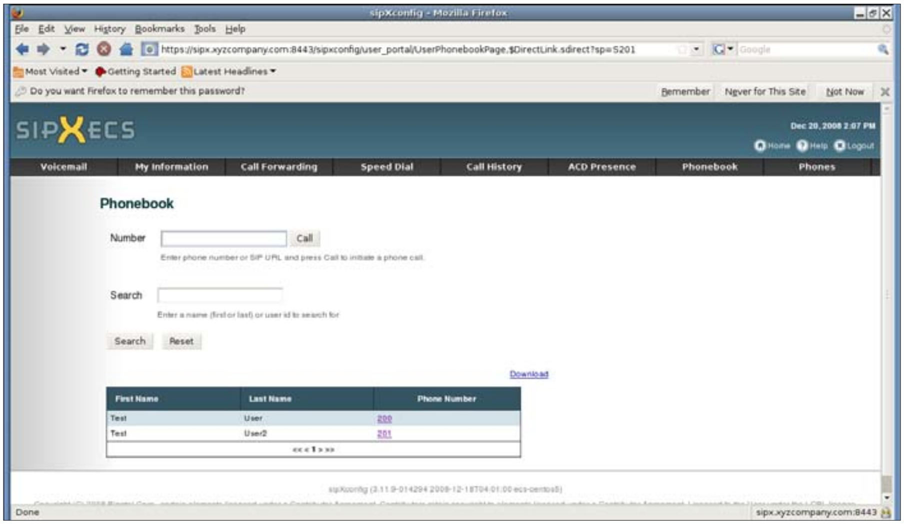
ACD presence

If the user is a member of an ACD Queue (see Chapter 10 for ACD Queue specifics), the user can use the **ACD Presence** page to sign in or out. The user's current status is also displayed on the page as seen in the following screenshot:



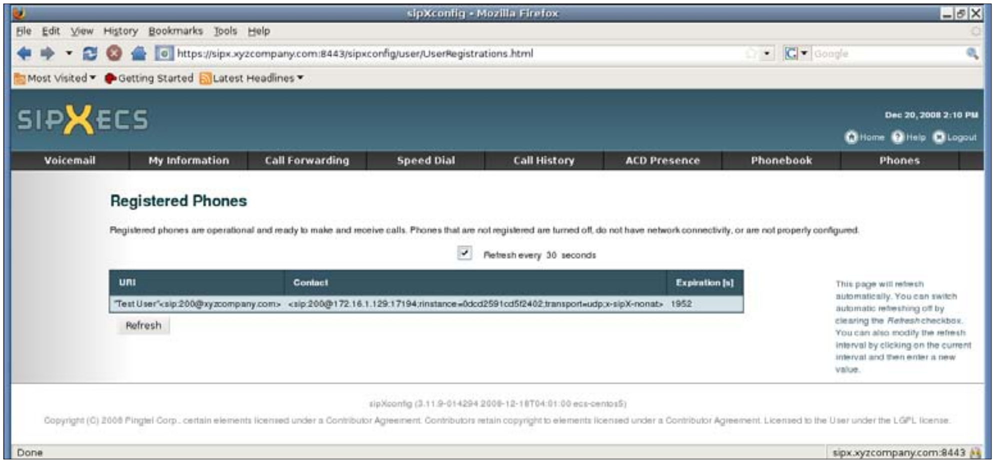
Phonebook

The **Phonebook** page gives the user access to the phone system directories published by the system administrator. The page also provides click-to-dial capabilities. If the user enters a number to dial, or clicks on a user phone number, the user's phone will ring. When the user picks it up, a call will be initiated to the called number.



Phones

The information contained on the **Phones** page allows the user to identify on what phones his or her user account is logged.



User training

Without proper end-user training any phone system deployment, no matter how well it has been designed, will be doomed to failure. The users need to be given live instructions in front of a phone and need some take-away instructions for future reference when they forget everything they were taught. Some users learn through doing, some through reading and studying. Give users the option to do both.

Training materials

The user manuals that come with phones are typically very large and confusing to most users. To help your users along it is a good idea to develop some small tri-fold or single page instructions for each type of phone being deployed. Make sure to cover even the basics of dialing numbers and adjusting the phone volume. The following is an example of a tri-fold that was created for the Polycom 650. The first page contains the outside document description, a section for the end user to add custom notes, and instructions for dialing.

Dialing

Station to Station: Dial the 4 digit extension.

Outside Calls: Dial 9 and the number.

Emergency: Dial 911 or 9 and then 911.

Voicemail: Dial 101

Voice Mail:

1. Log into voicemail by dialing ______.
   PIN (Password) is 2008#.
   OR
2. Press "Messages"
   Press "Connect"
   PIN (2008#)
3. Press "**1**" to Listen to messages
4. Dial 5 – Voice Mail Options
   1 – Greeting
   2 – Name
   5 – Change PIN (Password)

USERS WITHOUT VOICE MAIL:

1. Log in to voice mail by dialing 101
2. Dial # when voice mail answers
3. Dial your mailbox number
4. Enter your PIN (2008) #

sipXecs IP Voice System

Quick Reference Guide

Instructions for Polycom 650

December 2008

XYZ Company
555 West Street
Somewhere, ME 04000

1-800-555-1212

www.xyzcompany.com

Logo Here

As seen in the following screenshot, the second page (or 'inside') of the tri-fold contains information about using system features.

Feature Instructions Polycom 650

Make a Call

- Dial the number then press the **Dial** button (or)
- Press "New Call" and dial the number
- (or)
- Lift handset and dial the number

Receive a Call

- Pick up the handset
- (or) Press **Answer**

Put a Call on Hold

- Press the **Hold** soft button.
- To retrieve a held call, press **Resume** or the flashing line button.

Transfer – Blind (Without announcing)

- While on a call, press **Trnsfr**.
- Press **Blind**.
- Dial the extension number.
- Press **Send**

Transfer a Call – Screened (Head's Up)

- While on a call, press the **Trnsfr** soft button.
- Dial the target extension.
- Press **Send**
- Wait for the target to answer the call to tell them who is calling.
- Press **Trnsfr** then hang up.
- To cancel a transfer and return to the original party, press the **Cancel** soft button before pressing **Trnsfr** the second time.

Transfer to Voice Mail

- While on a call, press **Trnsfr**
- Press **Blind**
- Dial 8 + extension number
- **Hang up**

Call Forward (Current Incoming Call – Reject)

- When receiving a call, press **Reject**
- Call will go to your voicemail

Directed Call Pickup

- Dial *78 and the extension number ringing
- Press **Dial**

Parking a Call

- While on a call, press the **Trnsfr** soft button.
- Press **Blind**.
- Dial the orbit number (501-502)
- Press **Send**

Picking up a Parked Call

- Dial *4 then (501-502)
- Press **Dial**

Conference Call

- While on a call, press the **Conference** soft button.
- Dial the next party.
- Wait for an answer the call and then press **Conference**.

Do Not Disturb

- Press the **Do Not Disturb** button to turn on this feature.
- You will not be alerted to incoming calls; all calls will immediately go to voicemail.
- Press **Do Not Disturb** again to turn this feature off.

Mute a Call

- Press the **Mute** button while on the call – Mute icon will appear on the screen indicating that muting is in progress.
- Press **Mute** again to deactivate muting.

MENU

1. Features
    - Call List
    - Messages
3. Settings
    - Basic
        - Preferences (Date)
        - Contrast
        - Ring Type

Classroom training

Standing up in front of the room of students with the only phone in the room is not a recipe for a successful training session. Small classes of users with each user having the type of phone they will be getting on their desks seem to be the best format for system training. Walk the users through all of the functionality of the phone, following the handouts you have prepared.

Additionally, launch the User Web Portal on a system for all to see and walk through the functionality they will experience. Follow up the training with an email containing the link to their new web portal and instructions for how to log in to it.

Summary

The telephone user interface and user web portal are what really matters to the end users of the phone system. Providing them with the proper end-user training and documentation is the key to make sure that you have a successful project. In this chapter we covered all of the information you will need as an administrator to help your users acclimatize to their new communications system. In Chapter 9 we will move into configuring the advanced features provided by the sipXecs communications system, including the all-new conferencing service.

9
Configuring Advanced sipXecs Features

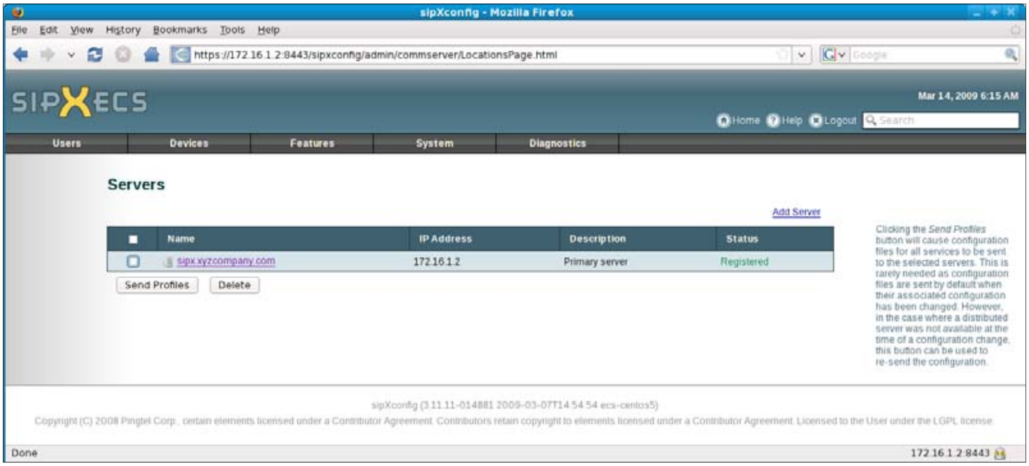
In this chapter we'll explore the built-in conference services provided by sipXecs and then explore some more advanced sipXecs call routing features. This chapter will include:

- Utilizing the cnference service
- How to configure DIDs
- Using phantom users for call routing
- Connecting two sipXecs servers

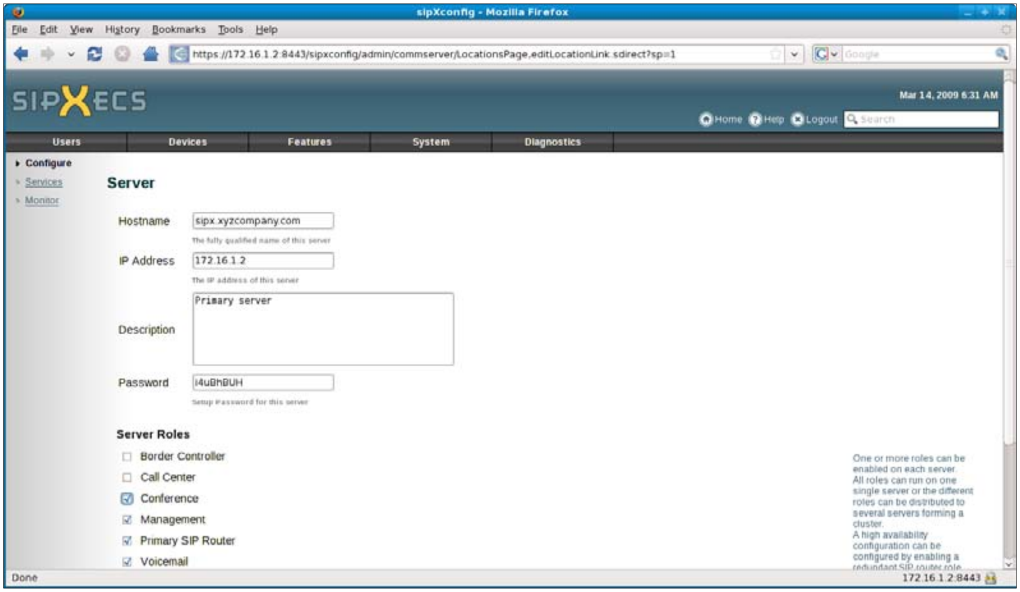
Conference service

Companies can spend hundreds of dollars monthly on conferencing services. sipXecs's built-in conference bridge can satisfy most conferencing needs for even the largest organizations. The conference service is built on top of Freeswitch (`www.freeswitch.org`).

The conference server is not enabled by default, so to enable it, click on the **System** menu and then select the **Servers** menu item. The following page will be displayed:



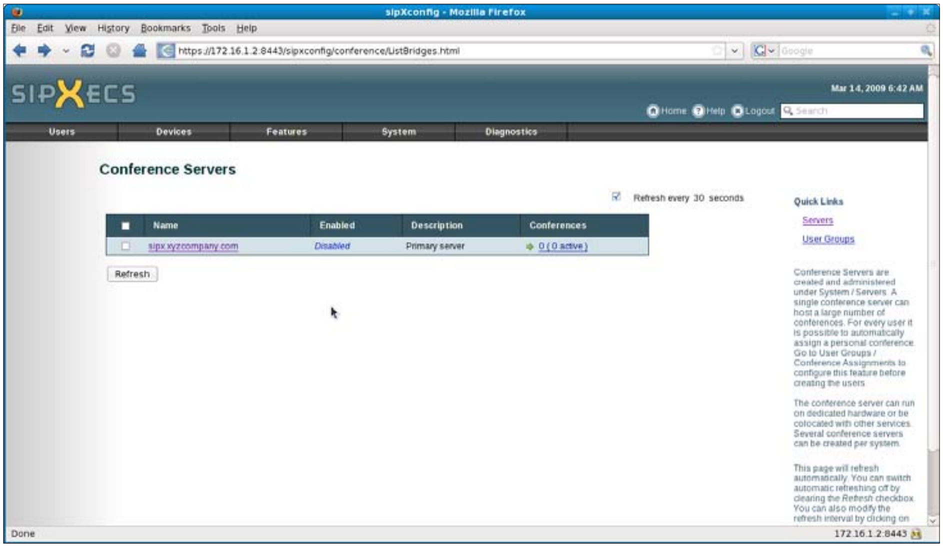
Click on the server name to display the services that are enabled on the server. As shown in the following screenshot, click on the checkbox next to **Conference,** and click on **OK** at the bottom of the page.



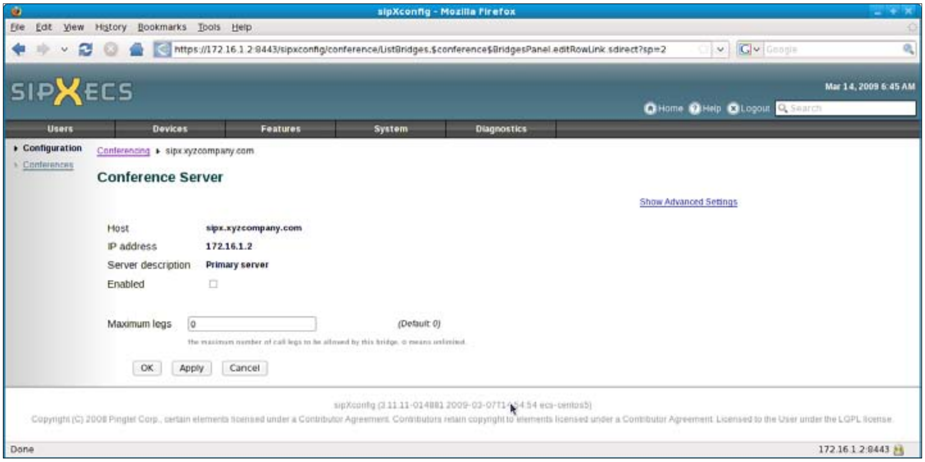
Once the Conference service is enabled, the server configuration profile must be built. The following page will be displayed after the **OK** button is clicked on the previous page. Place a check mark next to the server name and click on **Send Profiles**. Clicking on the **Send Profiles** button will cause configuration files for all services to be sent to the selected servers.

Sending profiles is not required often because service configuration files are sent by default when their associated configuration is changed. However, in the case where a distributed server is not available at the time of a configuration change, this button can be used to re-send the configuration.

Clicking on the **Conferencing** menu item under the **Features** menu will allow the administrator to configure the conference service as shown in the following screenshot:

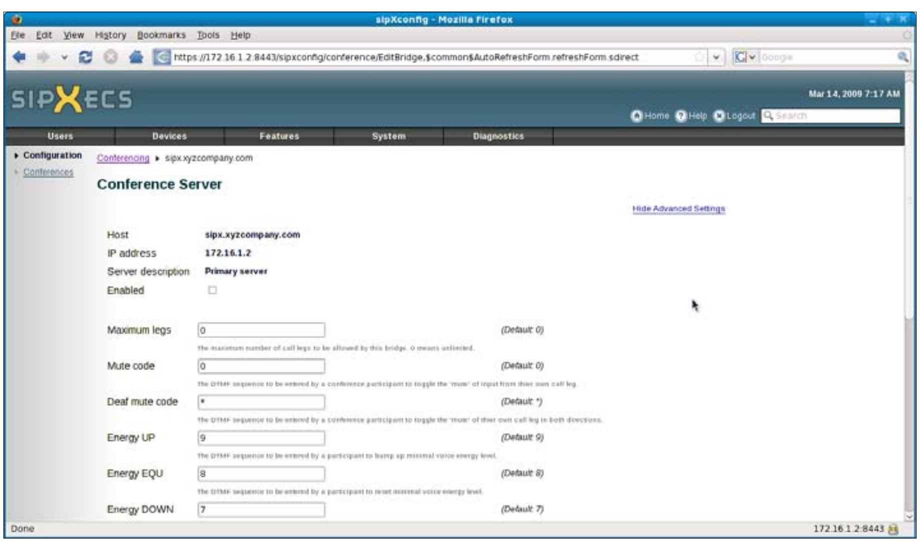


By default the service is disabled. To enable the service and configure it, click on the server name, which will display the following page:



Click on the **Enabled** checkbox and click on **OK** to turn on conferencing. The other setting available on this page is the setting for **Maximum Legs**. The **Maximum Legs** setting controls how many participants are allowed on the conference server across all conferences. By default this is set to 0, meaning that the number of participants is not limited.

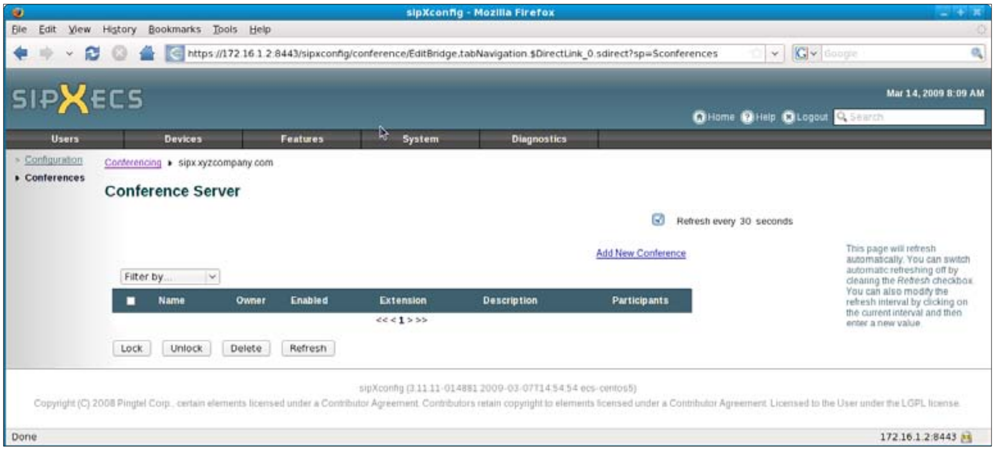
Some advanced customization options are available by clicking on the **Show Advanced Settings** hyperlink. As shown in the following screenshot, the advanced settings allow the system administrator to change the conference control options that are available to participants during a call.



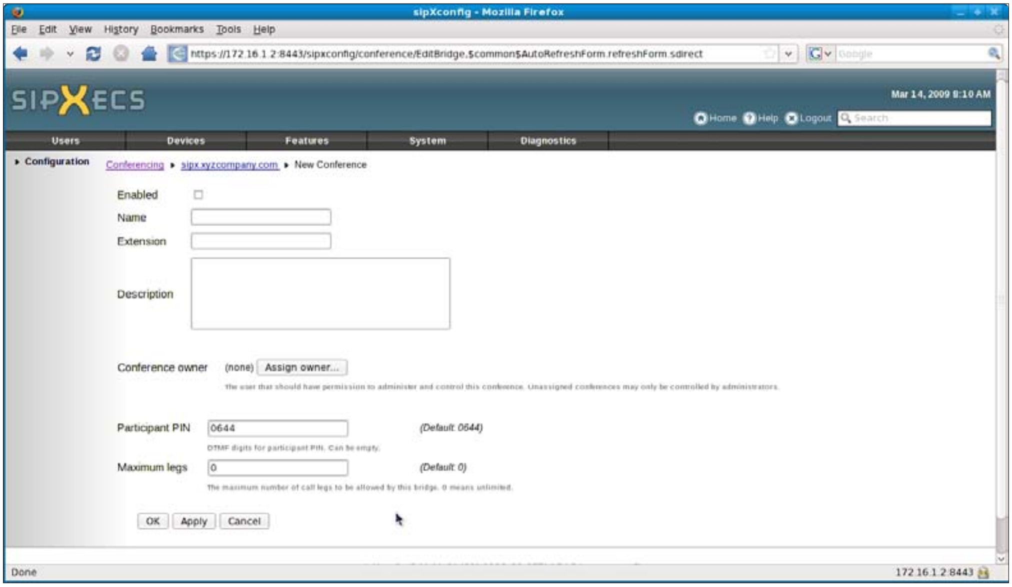
In a conference, the user has the following call control options by default:

- **Mute code** (Default is 0): The DTMF sequence to be entered by a conference participant to toggle the 'mute' of input from his or her own call leg
- **Deaf mute code** (Default is *): The DTMF sequence to be entered by a conference participant to toggle the 'mute' of his or her own call leg in both directions
- **Energy UP** (Default is 9): The DTMF sequence to be entered by a participant to bump up minimal voice energy level
- **Energy EQU**: (Default is 8): The DTMF sequence to be entered by a participant to reset minimal voice energy level
- **Energy DOWN** (Default is 7): The DTMF sequence to be entered by a participant to turn down minimal voice energy level
- **Volume UP** (Default is 6): The DTMF sequence to be entered by a participant to bump up the volume
- **Volume RESET** (Default is 5): The DTMF sequence to be entered by a participant to reset the volume level
- **Volume DOWN** (Default is 4): The DTMF sequence to be entered by a participant to turn down the volume
- **Talk volume UP** (Default is 3): The DTMF sequence to be entered by a participant to bump up microphone sensitivity (that is, his or her talk volume)
- **Talk volume RESET** (Default is 2): The DTMF sequence to be entered by a participant to reset microphone sensitivity
- **Talk volume DOWN** (Default is 1): The DTMF sequence to be entered by a participant to turn down microphone sensitivity
- **Hang-up code** (Default is #): The DTMF sequence to be entered by a participant to leave the conference

Now that conferencing is enabled, conferences must be created. To create a conference, click on **Conferencing** in the **Features** menu, click on the conference server name, and then click on the **Conferences** hyperlink on the lefthand menu. This will display the following page:



Click on the **Add New Conference** hyperlink to display the **New Conference** page as shown in the following screenshot:



The following options are available when configuring each conference:

- **Enabled**: This shows whether the conference is enabled or not.
- **Name**: This is a friendly name for the conference
- **Extension**: This is the extension assigned to the conference.
- **Description**: This is a text description of what this conference room is for.
- **Conference owner**: The user that has permission to administer and control this conference. Unassigned conferences may only be controlled by administrators.
- **Participant PIN**: The DTMF digits for conference participants to dial on entering the conference. This can be left empty for no PIN.
- **Maximum legs**: This is the maximum number of call participants allowed by this conference bridge. 0 (which is the default) means unlimited.

Controlling the conference while it is in progress can be done through the user portal (if the conference is assigned to a user). If the conference is not assigned to a user, only the administrator can control the conference by clicking on the conference name on the **Conference Servers** page. See Chapter 8 for information on controlling conferences.

Utilizing DIDs

A **DID** (**Direct Inward Dialing**) is a method that allows companies to own large blocks of telephone numbers that can be allocated to system users or services. DID services are most commonly used with digital circuits such as T1/E1/PRIs but may be available in certain areas on other circuit types.

Just before a call rings in on one of the available channels, the phone number that was dialed is transmitted. T1/E1/PRI gateways that are connected to the sipXecs PBX should then be configured to forward the dialed number to `DID@sip.domain`.

Routing the call to a particular user is easily accomplished by adding the DID as an alias on the user account or auto attendant that owns that DID. If the DID is to be used to access other resources on the PBX, consider using a phantom user as shown in the next section.

Phantom users

Phantom users (phantoms) are user accounts on the system that don't really ever have phones logged into them. These phantoms can be used for general delivery voicemail mailboxes, for departmental control over an auto attendant, or for routing phone calls. Just as with regular uses, DIDs can also be assigned to phantom users for additional call routing functionality.

Live daytime attendant

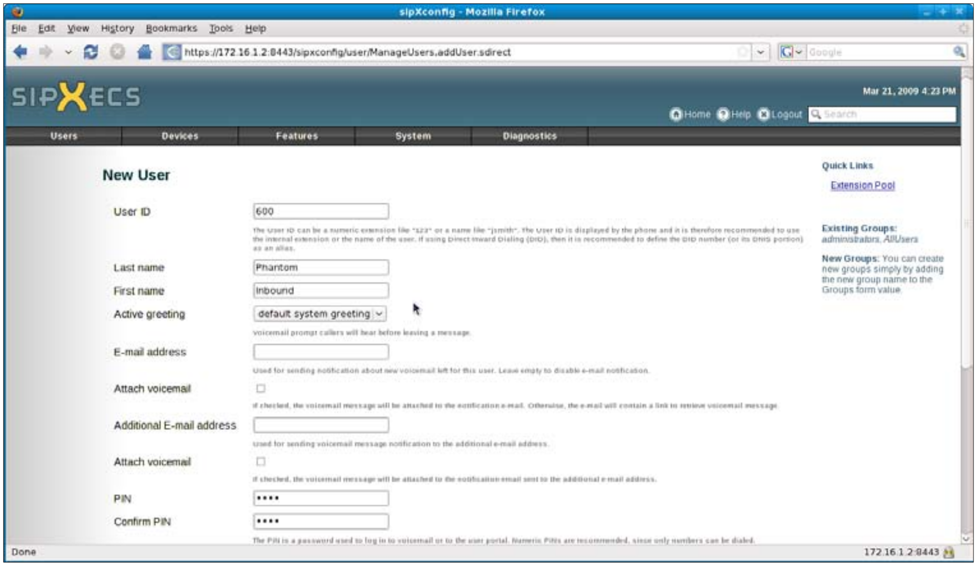
One common use for phantoms is for handling the inbound routing of calls from gateways. Since there is no way from the system auto attendant to have calls routed to a live operator during the day, a routing phantom can be utilized to accomplish this task.

The following steps are required to make this work:

1. Create a new user account
2. Disable voicemail for the phantom user
3. Create a working day schedule in the user account
4. Set up forwarding on the user account to the answering extension during the working day schedule and an 'if no answer' route to the auto attendant dial plan entry
5. Configure system gateways to route inbound calls to the phantom user

Create new user account

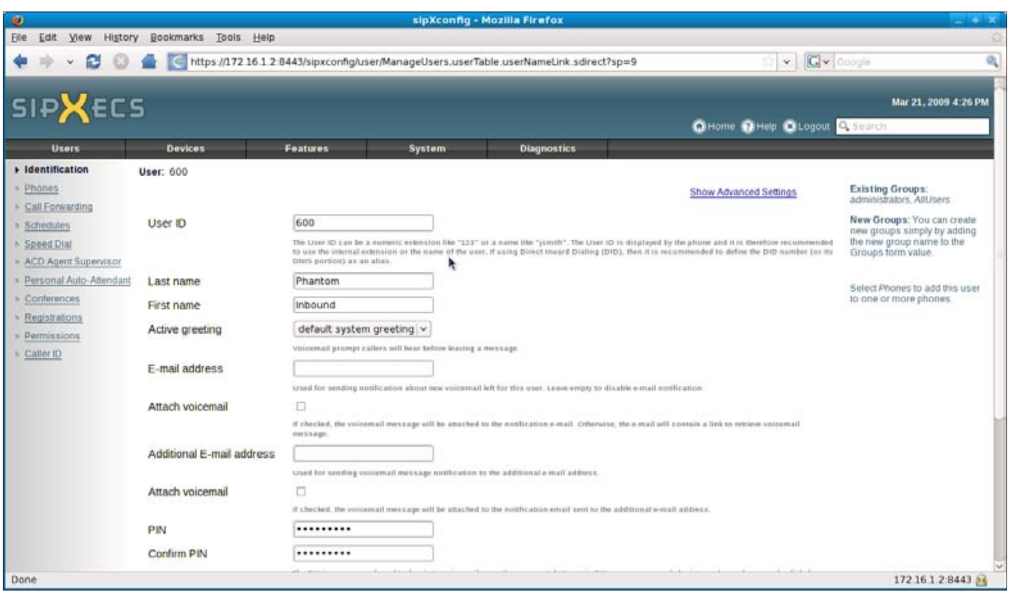
Create a new user account in the number range planned for system extensions. The following screenshot shows the creation of a user 600.



Other than a **User ID**, the only other required information is a PIN. Click on the **OK** button at the bottom of the page to create the user.

Turn off voicemail

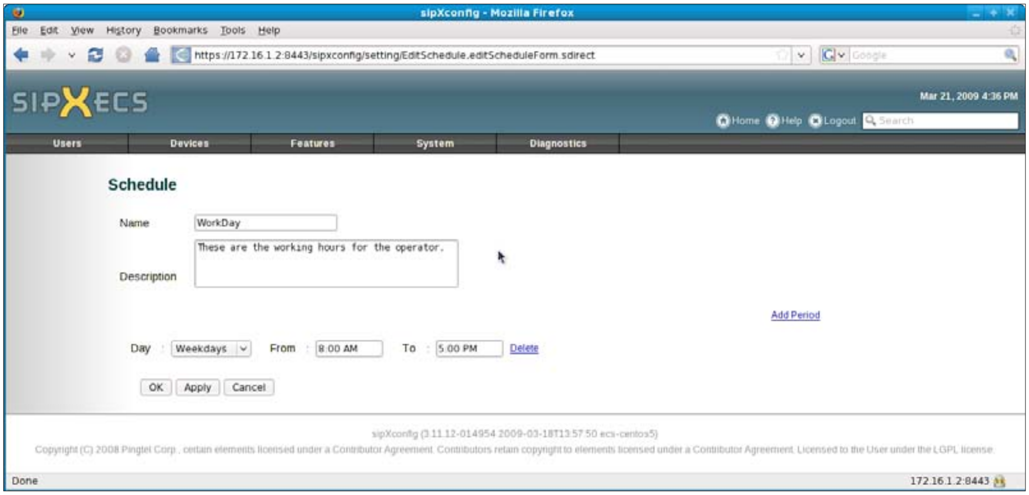
On the **User** page, click on the newly created phantom user to display the details of the user account, shown as follows:



Click on **Permissions** on the lefthand side menu and uncheck the voicemail permission and click on the **Apply** button.

Set up the work day schedule

Click on **Schedules** on the lefthand side menu and then click on the **Add schedule** hyperlink near the middle of the page. Set up the **WorkDay** schedule similar to how it is shown in the following screenshot:



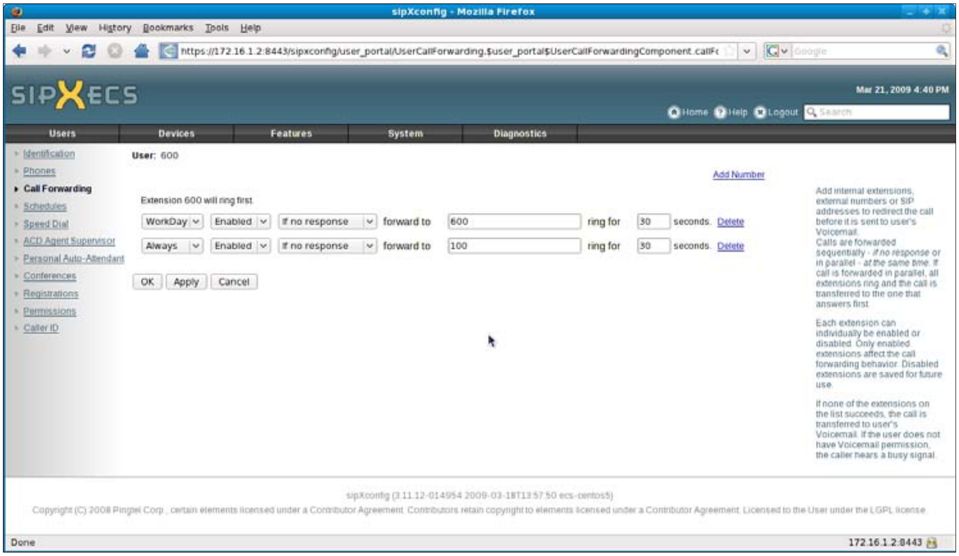
Click the on the **OK** button when completed.

Set up call forwarding

Click on the **Call Forwarding** menu item in the lefthand side menu and then the **Add Number** hyperlink near the middle of the page. In the first drop-down box select the schedule item that was created in the previous step and enter the phantom user extension in the **Forward to** dialog box.

Click on the **Add Number** hyperlink again and in the **Forward to** dialog box enter the extension of the auto attendant that you'd like the call to route to (the default system AA is on extension 100, 0, and operator).

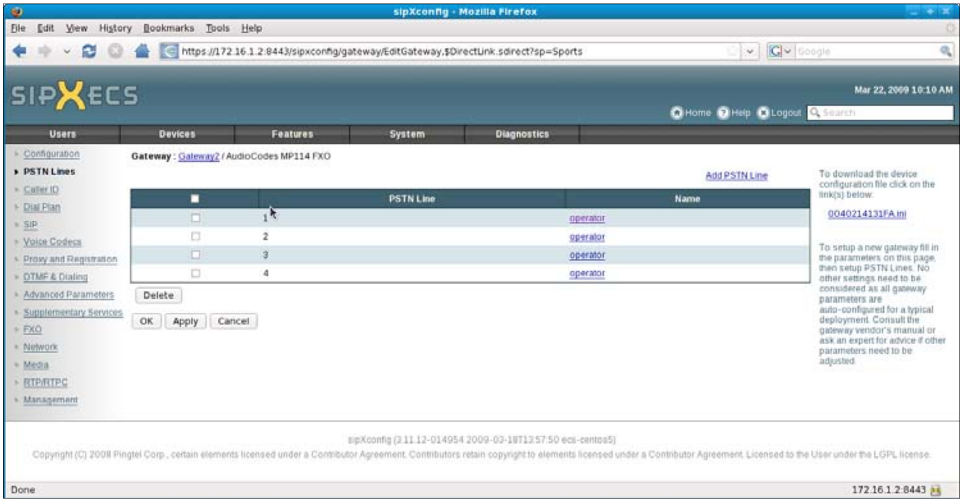
The resulting forwarding configuration should look similar to the following screenshot:



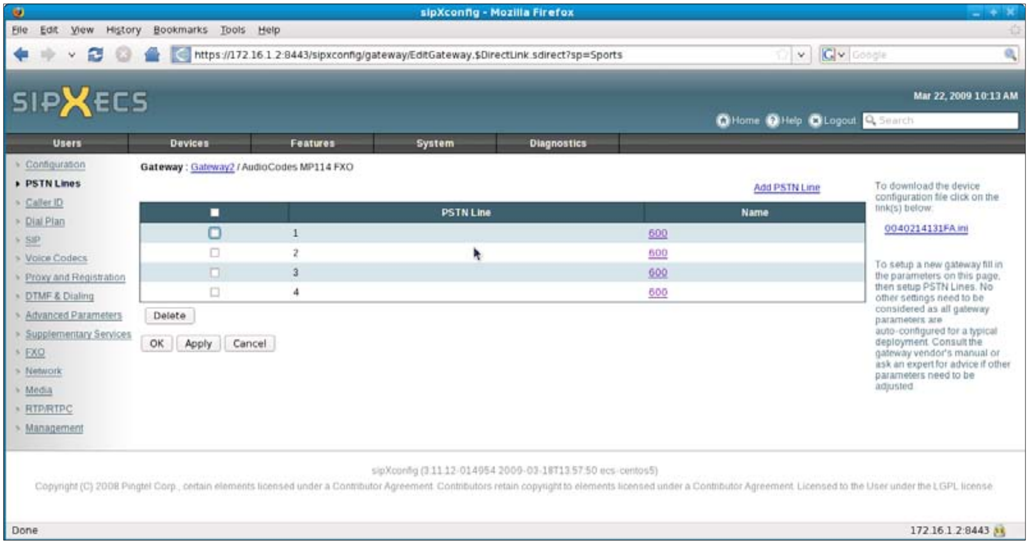
Change gateway destination extension

If an unmanaged SIP gateway is being utilized, its configuration will have to be manually set to dial the new inbound routing phantom (that is, `600@xyzcompany.com`). If a managed gateway is being utilized, its configuration can be modified in the **Gateways** page.

In the **Devices** menu select the **Gateways** menu item and then select the inbound gateway that needs to be modified and then select **PSTN Lines** on the lefthand side menu. The following page will be displayed:



Modify each PSTN line by clicking on the **operator** hyperlink and changing it to your new inbound phantom. The lines will look similar to the following screenshot:



Connecting two sipXecs servers

Two separate sipXecs servers can be configured to be able to dial each other across the Internet or across a WAN.

To enable calling between two (or more) sipXecs PBXs, there are three steps:

1. Make sure each PBX can resolve pertinent DNS records for the other's domain (SRV if you are using SRV).
2. Set up an unmanaged gateway on each PBX pointing to the other PBX.
3. Set up a dial plan used to select the other PBX.

DNS resolution

Each PBX needs to be able to resolve the other server's SIP domain information. The DNS tests described in Chapter 3 must work for the far-side server's domain name.

For example:

sipXecs system 1 has a SIP domain of: boston.xyzcompany.com.

sipXecs system 2 has a SIP domain of: dallas.xyzcompany.com.

System 1 must be able to resolve:

```
dig –t SRV _sip._udp.dallas.xyzcompany.com
dig –t SRV _sip._tcp.dallas.xyzcompany.com
```

System 2 must be able to resolve:

```
dig –t SRV _sip._udp.boston.xyzcompany.com
dig –t SRV _sip._tcp.boston.xyzcompany.com
```

There are numerous ways to make this work. One of the easier ways is to locate the zone file for each domain, copy the zone files to the opposite site's server, and modify the `named.conf` file to also load the DNS zones for the other domain in addition to the local domain. For a system that was set up from the sipXecs ISO install CD, the zone files are in `/var/named` directory and named `sip.domain.zone`. Once the zone files are copied to their respective servers, modify the `/etc/named.conf` file duplicating the zone section but for the new zone file.

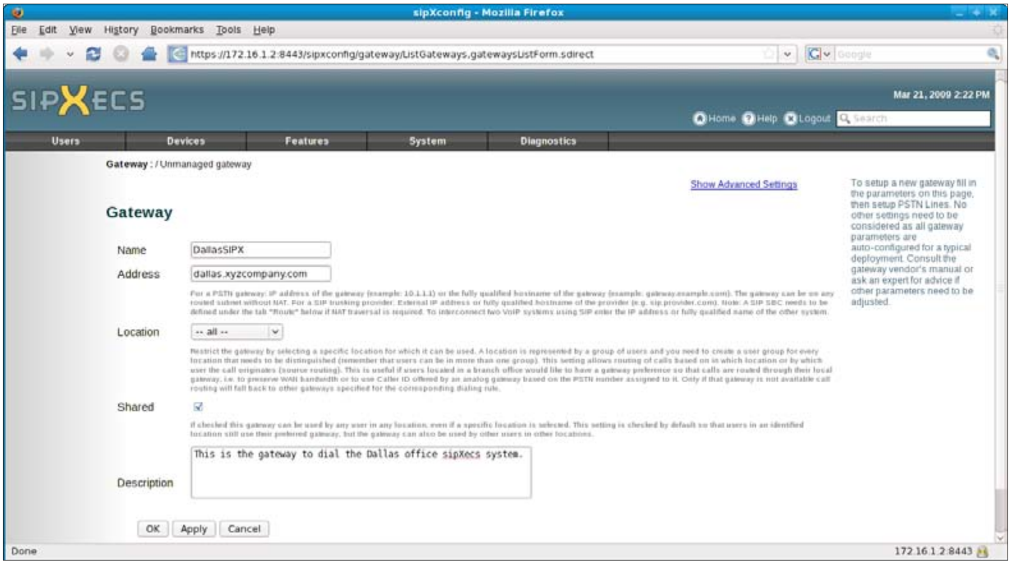
The `named.conf` file for the system 1 server would look like the following:

```
options {
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    forwarders {
        208.67.222.222;
        208.67.220.220;
    };
};
zone "boston.xyzcompany.com" IN {
   type master;
   file "boston.xyzcompany.com.zone";
   allow-update { none; };
};
zone "dallas.xyzcompany.com" IN {
   type master;
   file "dallas.xyzcompany.com.zone";
   allow-update { none; };
};
```

Once the `named.conf` file is modified, restart the DNS services with `service named restart`.

Set up gateways

An unmanaged gateway should be configured on each system pointing to the other system's SIP domain. Go to the **Gateways** menu item in the **Devices** menu and select **Unmanaged Gateway** from the **Add new gateway** drop-down box. The following page will be displayed:

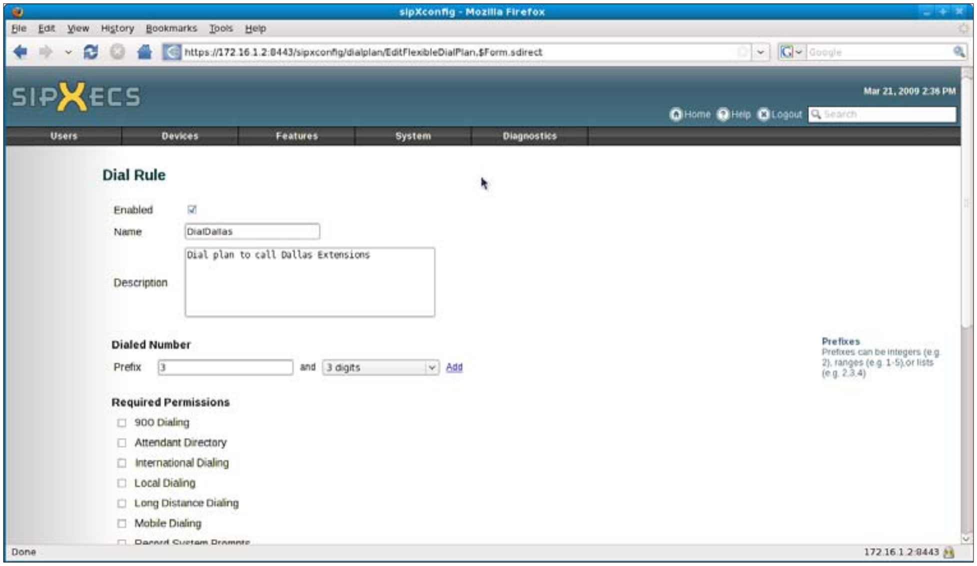


Configure the gateway as shown in the preceding screenshot and click on **OK**. Notice the **Address** field is simply the SIP domain of the remote PBX and not the IP address of the remote PBX. This will allow our resulting SIP dialed URLs to be `sip:extension@dallas.xyzcompany.com`.

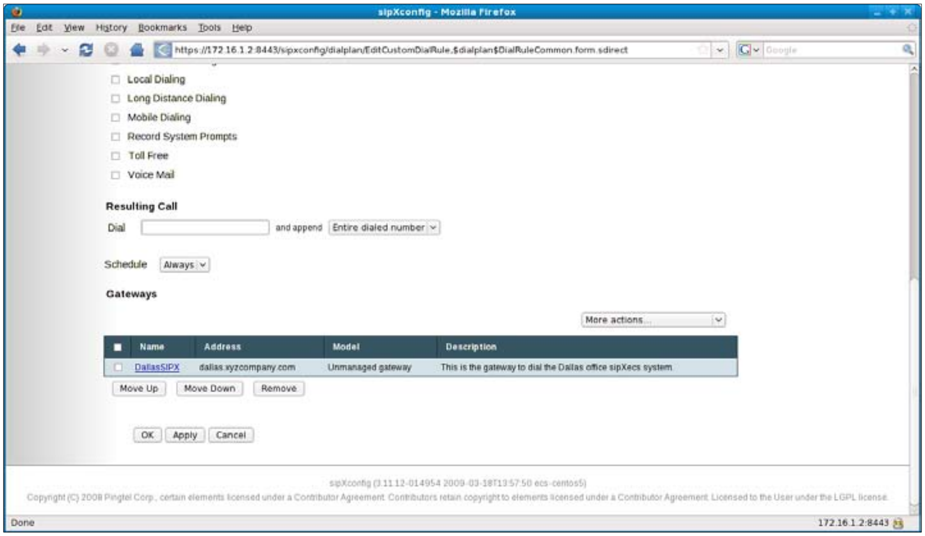
Configure custom dial plan entry

Interoffice dialing is where your dialing plan planning will pay off if you have done it correctly. For this example we will pretend that all Boston system user extensions are 2xxx and all Dallas system user extensions are 3xxx. This simplifies our custom dial plan entry greatly.

On each PBX add a custom dial plan entry: click on the **Dial Plans** menu item in the **System** menu and select **Custom** from the **Add New Rule** drop-down menu. The custom dial rule for Boston will appear as in the following two screenshots:



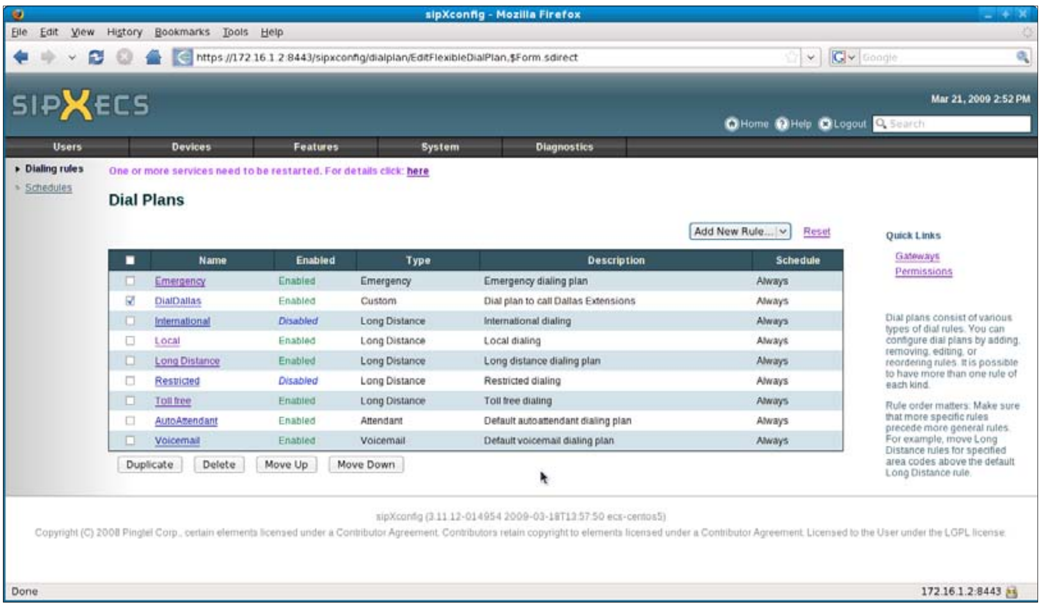
The following screenshot is the bottom half of the above screenshot:



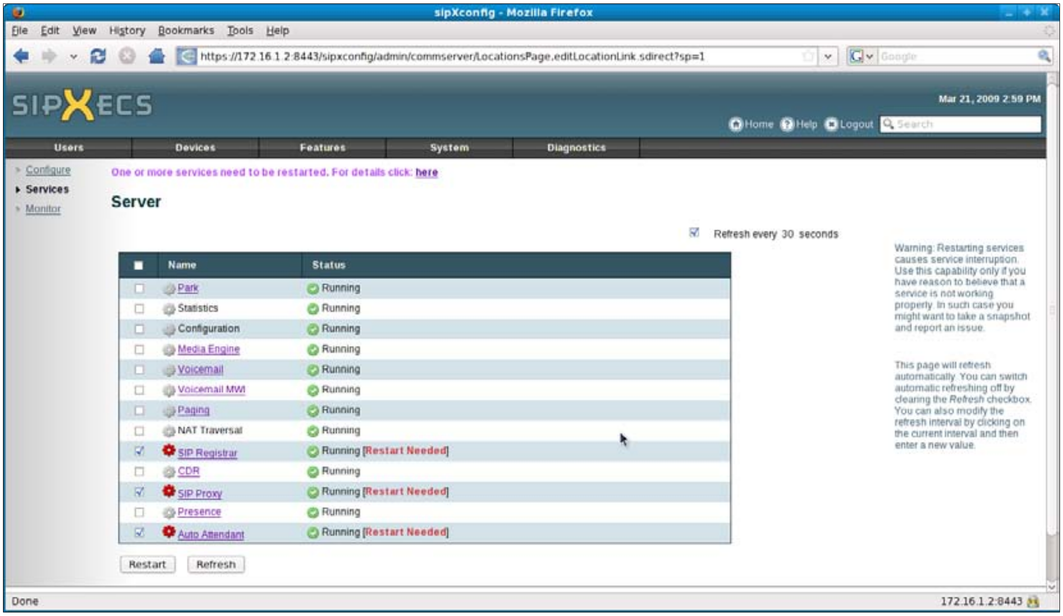
Give the dial plan entry a meaningful name and description. Using our example extensions, to reach Dallas we will be looking for the dialed number **3** followed by 3 more digits, which is set under the **Dialed Number** section as a **Prefix** of 3 and 3 digits selected in the drop-down box. No Permissions should be required to dial this extension. The **Resulting Call** section should look as above, dialing nothing and appending the **Entire dialed number**.

In the **Gateways** section, select the gateway that was added earlier from the **More actions** drop-down box. Verify that the **Enabled** checkbox at the top of the page is checked and then click on the **OK** button.

The **Dial Plans** page will be displayed after clicking on **OK**. By placing a check mark next to it and clicking on the **Move Up** button, move the new custom dial plan entry to just after the **Emergency** dial plan entry. Recall from Chapter 6 that dial plan order is important and that more specific dial rules should be higher in the dial plan list.



Once the dial plan entry is added, some of the sipXecs services must be restarted to pick up the new dial plan entry (as indicated by the notice near the top of the page). Click on the **here** hyperlink, select the **Services** menu on the left, and then select the services that need to be restarted and click the **Restart** button as shown in the following screenshot:



Assuming that the systems are connected across a VPN tunnel or across a Wide Area Network, phones on each network should now be able to call each other. If calling across the Internet, proper NAT traversal services (see Chapter 6) must be operational in the PBX, or you must have a Session Border Controller in place to handle NAT traversal.

Summary

The Conferencing Service alone in sipXecs can save hundreds of dollars a month of organizations. It is a robust and full-featured solution that will satisfy all but the most grizzled conference user.

We also covered some call routing tricks that will hopefully find use with your sipXecs installation. Utilizing phantom users and custom dial plan entries will allow the system administrator to leverage the power of sipXecs.

10

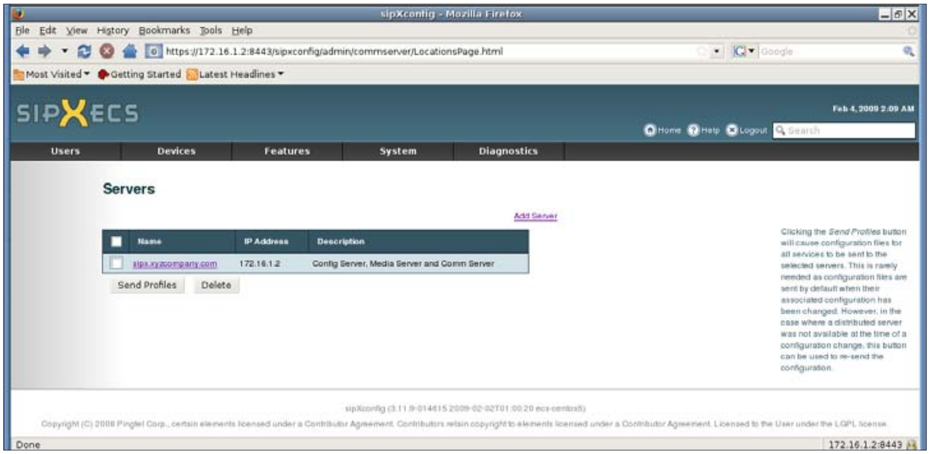
Utilizing the sipXecs ACD Service

Automatic Call Distribution (**ACD**) queues can be thought of as intelligent hunt groups. They allow phone system users (agents) to sign in when they become available take calls or sign out when they no longer want to take calls. Calls then get directed to agents based on different factors such as who is the first person in the ACD list or which agent has been idle the longest. In this chapter we'll explore how to:

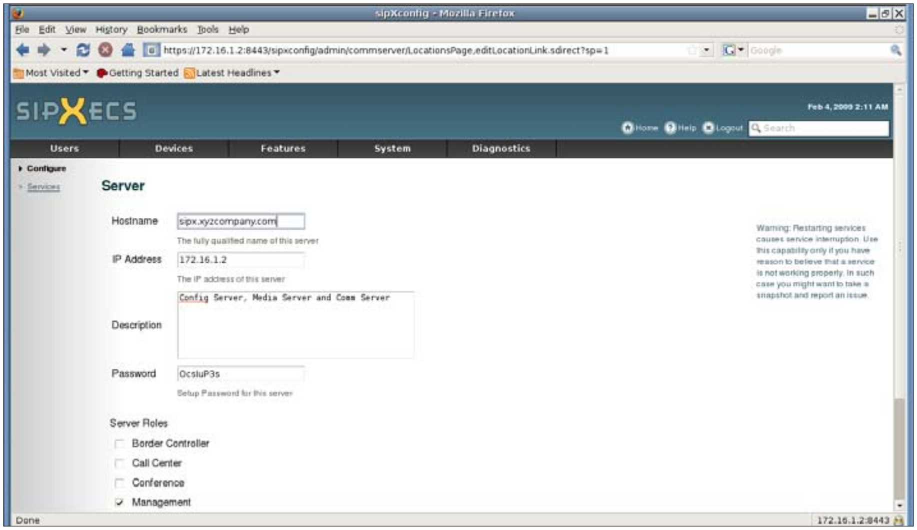
- Enable the ACD Service
- Configure the ACD Service
- Monitor ACD Agents
- Use ACD Reports

Enabling the ACD Service

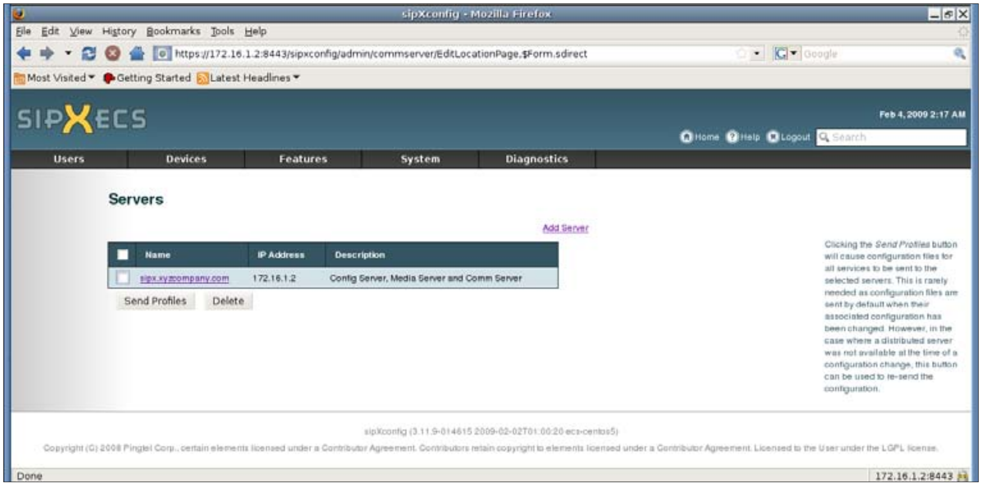
To enable the ACD Service on the sipXecs server, select the **System** menu and click on the **Servers** menu item. The following screen should be displayed showing the server name, IP address, and description:



Click on the PBX name hyperlink. This will display the following page that shows the details of the server along with what **Server Roles** are enabled (if the **Services** page is displayed, click on **Configure** in the lefthand side menu).



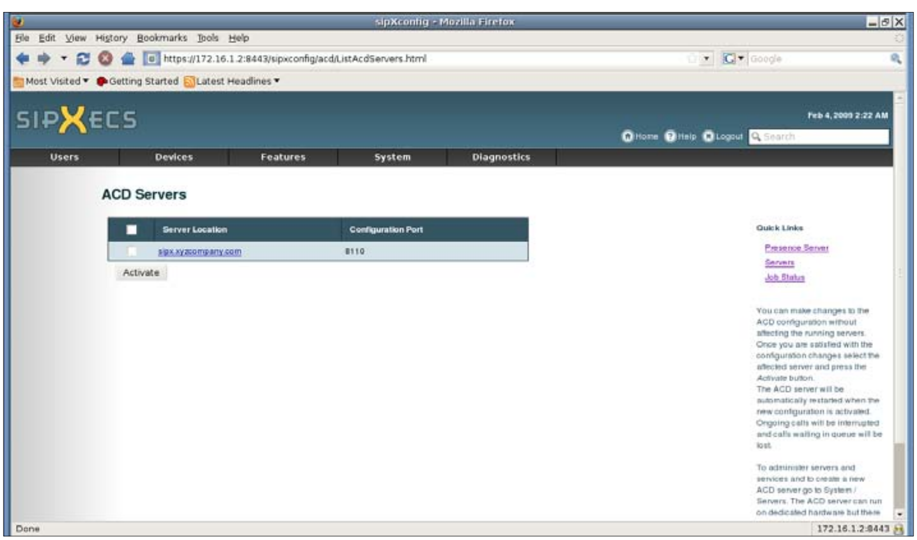
To enable the ACD services, place a check mark next to **Call Center** and click on **OK** near the bottom of the page. The **Servers** page will then be displayed as shown in the following screenshot:



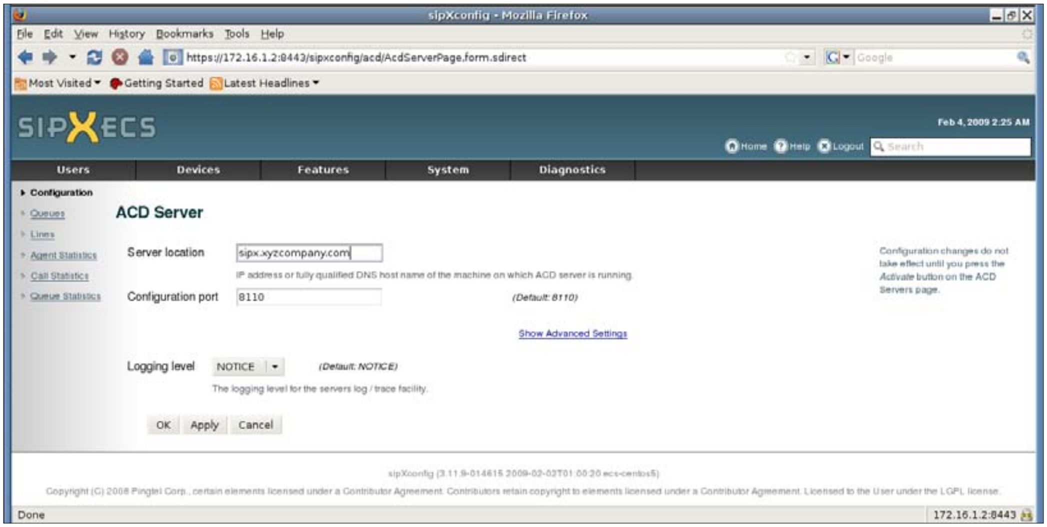
Click on the checkbox beside the server name and click on the **Send Profiles** button to complete adding the ACD service. The **Job Status** page will be updated with a message when the ACD profile creation is completed.

Configuring the ACD Service

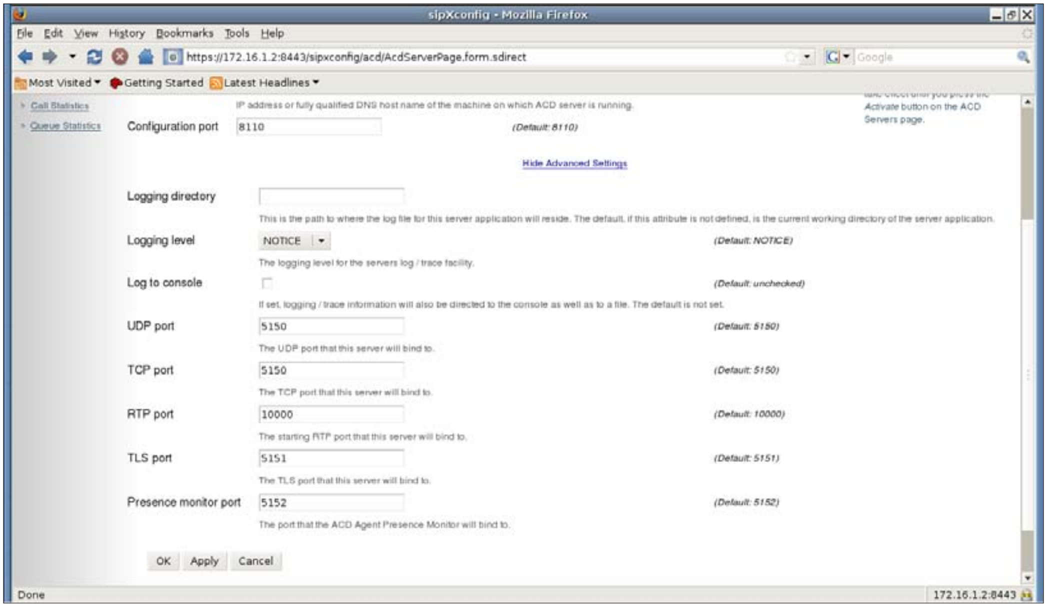
The ACD Service can be configured by selecting the **ACD Call Center** menu item under the **Features** menu. The ACD **Servers** page will be displayed showing the server name as seen here:



Clicking on the server name hyperlink reveals the **ACD Server** page as shown in the following screenshot:



The **Show Advanced Settings** hyperlink near the center of the page causes some advanced configuration options to be displayed. These settings, as shown in the following screenshot, typically do not need to be modified for most installations.

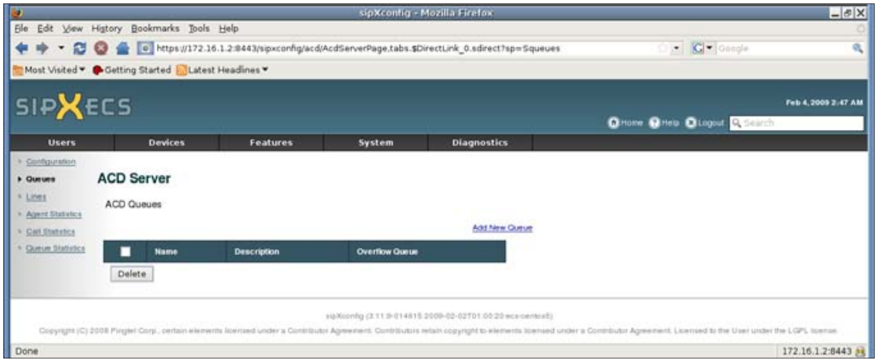


Create an ACD Queue

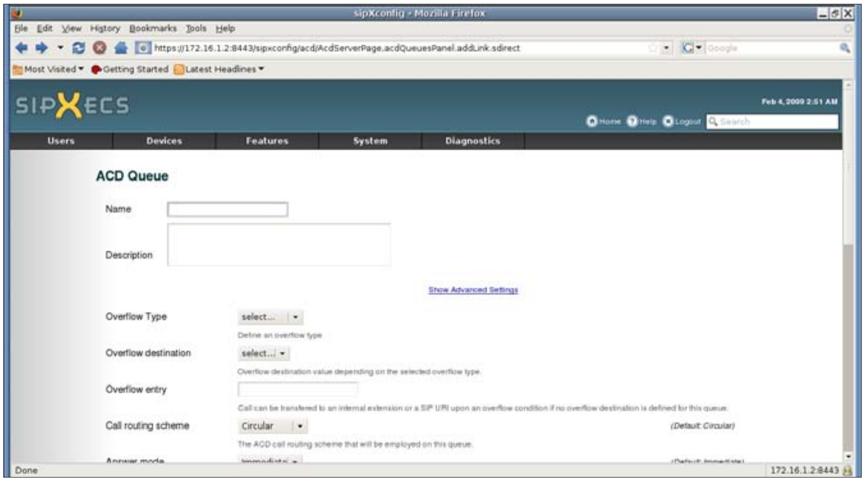
The ACD Queue configuration determines how calls are answered by the queue, what callers hear for announcements, how calls are handed out to agents of the queue and what happens when the call is completed. Any number of different queues can be configured to handle calls to individual departments differently.

Before beginning to configure the ACD Queues, refer to the information prepared in the planning phase from the *ACD Queues* section of Chapter 2.

To begin configuring an ACD Queue, click on the **Queues** hyperlink on the lefthand side menu of the **ACD Server** page. The following page will be displayed, which shows any queues that may be configured (none have been configured yet in our example system).



Click on the **Add New Queue** hyperlink near the center of the page and the following **ACD Queue** configuration page will be displayed:



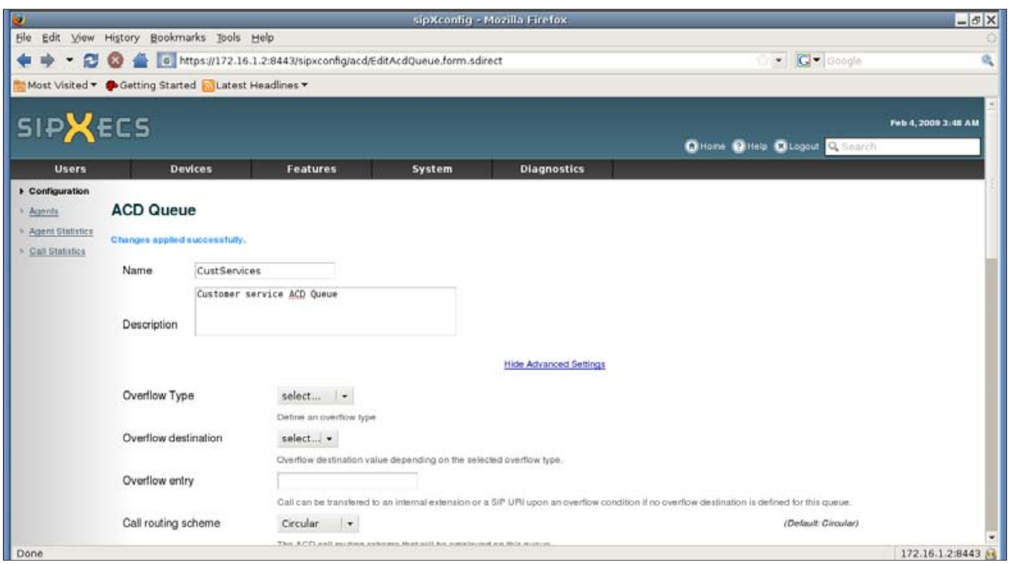
The following settings can be configured for each queue (clicking on **Show Advanced Settings** reveals all settings described below):

- **Name**: This is a descriptive text name given to the queue (for example, CustService). No spaces are allowed in the name.
- **Description**: This is used to document the purpose of the ACD Queue.
- **Overflow Type**: Overflow happens when a call cannot be handled because it has been in the queue for too long or there are too many calls in the queue. Overflow types are Queue (calls can flow to another ACD Queue) or Hunt Group (calls can flow to a Hunt Group).
- **Overflow destination**: This drop-down menu will display either all defined ACD Queues or Hunt Groups. This is determined by the **Overflow Type** setting.
- **Overflow entry**: This is used to transfer calls to an internal extension or a SIP URI upon an overflow condition if no overflow destination is defined for this queue.
- **Call routing scheme**: This is the ACD call routing scheme that is used by this queue. The permitted values are Circular (each inbound call rings the next agent in the list of agents), Ring All (rings all available agents in the list of agents), Linear (rings agents in the order of the list always starting with the first agent in the list), and Longest idle (rings the agents by the order of who has been available longest). The default queue routing scheme is **Circular**.
- **Maximum ring delay**: This value defines the maximum time (in seconds) that the queue will allow an agent phone to ring before a ring-no-answer condition is declared, and the call is rerouted to a different agent. The default value is 15 seconds.
- **Maximum queue length**: This defines the maximum number of calls that are allowed to wait in this queue. If a call arrives at this queue and the resulting call count exceeds this number, an overflow condition for this queue will be triggered. A value of -1 (negative 1) disables this limit check. The default value is 10 calls.
- **Maximum wait time**: This is the maximum time (in seconds) that a call can reside in this queue. If a waiting call exceeds this time limit, an overflow condition for this queue will be triggered. A value of zero disables timeouts. The default maximum wait time is 60 seconds.
- **FIFO overflow**: If this value is set, then upon an overflow condition, a First-In-First-Out scheme (calls that have been in the queue the longest) will be employed in to determine which call will be moved to the configured overflow-queue. If it is not set, then a Last-In-First-Out scheme (newest calls in the queue) will be employed. The default value is FIFO enabled.

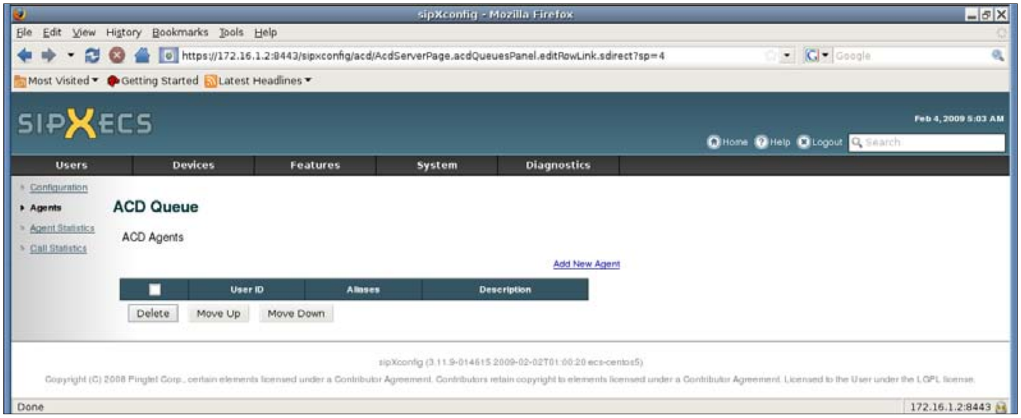
- **Answer mode**: The queue answer mode can be set to Immediate, Deferred, or Never. If it is set to Immediate, the call will be answered immediately upon arriving at this queue and the configured welcome-audio file will be played to the caller. Once the audio has completed, the queue will then attempt to route the call. If it is set to Deferred, the queue will first attempt to route the call to an agent. If it is unable to immediately route the call (because all agents are busy), it will then be answered and the welcome-audio file will be played to the caller. If it is set to Never, the call will not be answered while on this queue other than when actually connecting to an agent. The default value is set to Immediate.
- **Barge in**: If this is set, the welcome audio will be terminated early, as soon as an agent becomes available, while it is being played. The default value is unchecked (do not barge in and play the entire welcome-audio file).
- **Welcome audio**: The welcome audio played to callers upon entering the queue. If no file is specified, then silence will be played. Several files can be uploaded and selected (but only the selected one will be played).
- **Queue audio**: The queue audio is played repeatedly to the caller until the queue either routes the call to an agent or to another queue. Several files can be uploaded but only one can be selected as active.
- **Audio interval**: This is the interval, in seconds, to wait before repeating play of the specified Queue audio. The interval should be set as exactly the same length or slightly longer than the length of the queue audio (the queue audio will stop at this interval time and restart from the beginning). The default value is 15 seconds.
- **Call termination audio**: This is the message played for the caller when it has been determined that the call must be terminated. Calls may be terminated if there are no agents in the queue or if an overflow condition has occurred and there is no overflow destination. Once the audio has completed, the call will be dropped. If no audio is specified, then a busy tone will be played prior to terminating the call. The duration of the busy tone is specified by the termination-tone-duration attribute.
- **Termination tone duration**: This is the duration (in seconds) for which the termination tone (busy tone) is played if no call-termination audio is specified and the call is dropped by the queue. A value of zero indicates that no tone is to be played prior to dropping the call. The default tone duration is 2 seconds.

- **Agent wrap-up time**: The wrap-up time is a period of time (in seconds) that has to pass before the ACD transfers a new call to an agent after a previous call has been completed. This allows an agent to complete any required data input from the previous call. If set to 0, it will be disabled. The default value is 15 seconds.
- **Agent Non-Responsive time**: This value determines the period of time (in seconds) that has to pass before the ACD transfers a new call to an agent when a previous call is not answered by that agent. This prevents calls from ringing to an agent phone, if the agent has walked away temporarily. The default value is 30 seconds.
- **Maximum Bounce Count**: The maximum bounce count is the number of rejected or non-answered calls an agent may have before being "bounced" (automatically signed out) from the ACD queue. The agent must sign back in to the queue if they have been bounced. If it is set to 0, automatic sign-off will be disabled. The default number of rejected or non-answered calls is 3.

Once the basic queue settings have been configured, click on the **Apply** button at the bottom of the page and the **Agents**, **Agent Statistics**, and **Call Statistics** hyperlinks will be displayed on the lefthand side of the page as shown below:



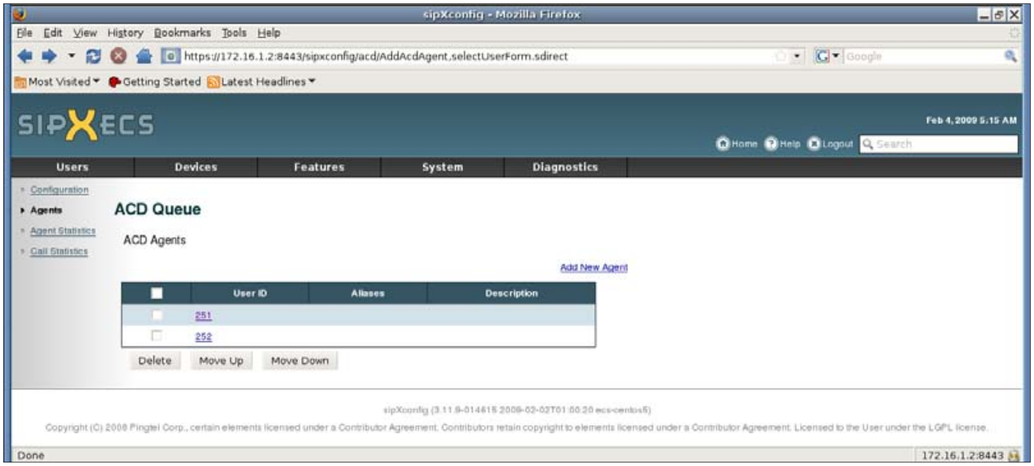
Clicking on the **Agents** hyperlink on the lefthand side of the screen displays the **ACD Agents** screen, shown as follows:



Click on the **Add New Agent** hyperlink near the center of the page and select the agents that need to be able to answer calls for this call queue.

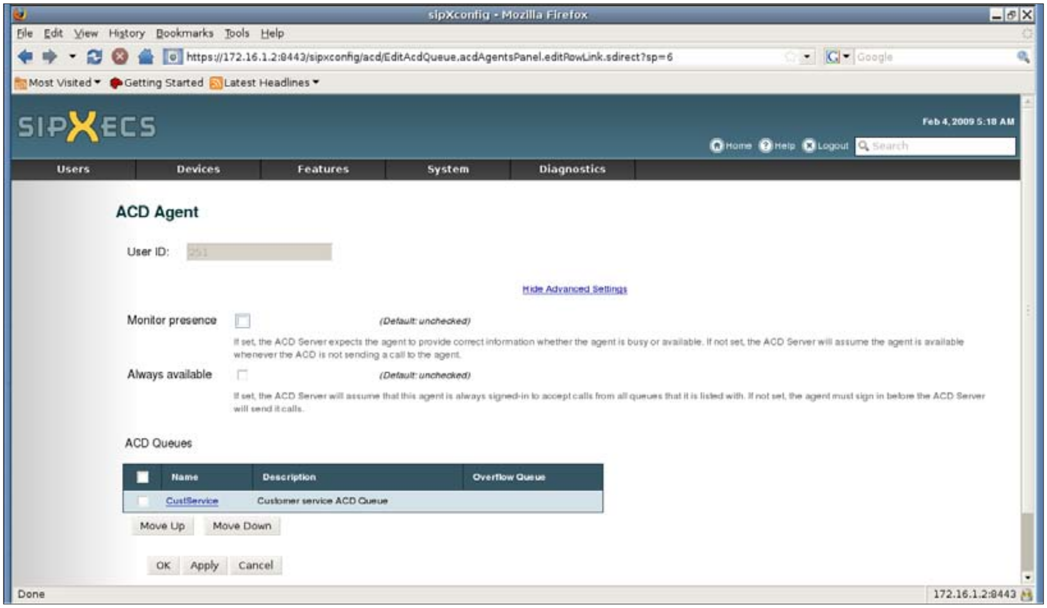
> If an agent needs to use their phone as a personal phone as well as an ACD phone, it is strongly recommended that a secondary extension be created for that phone. The secondary extension is added to the ACD queue and not the agent's personal extension. For example, extension 202 might be a personal extension for a user and extension 252 might be their ACD extension. If the user picks up the phone and makes an outgoing call, by default, it would go out over extension 202 and not interrupt ACD call traffic flow that might come in on extension 252.

The following screenshot shows that extensions 251 and 252 have been added to the queue:



The agent order can be adjusted by placing a check mark next to the extension and using the **Move Up** and **Move Down** buttons.

Clicking on the agent **User ID** in the previous screenshot allows some additional configuration on a per agent basis as shown in the following screenshot:

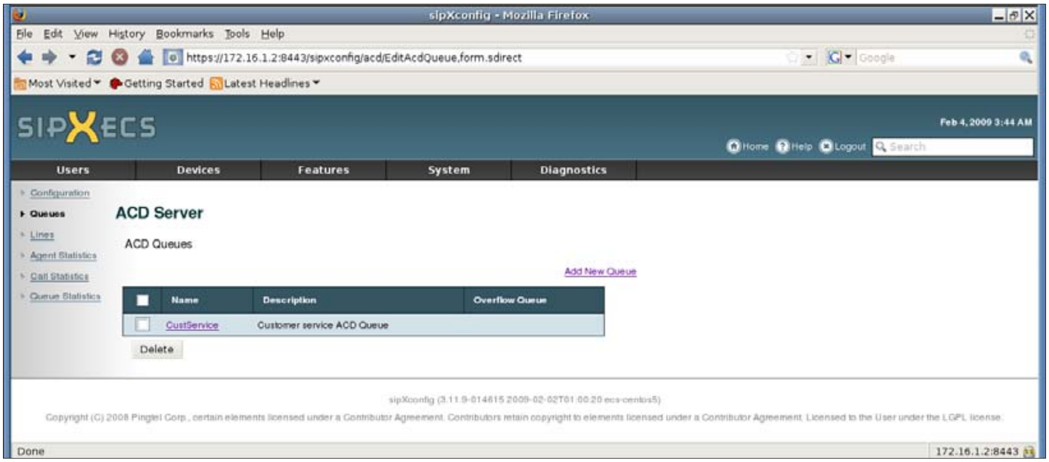


The ACD Agent settings are as follows:

- **Monitor presence**: If set, the ACD Server expects the agent to provide correct information, as to whether the agent is busy or available. If not set, the ACD Server will assume that the agent is available whenever the ACD is not sending a call to that agent. The default value is unchecked (the ACD server assumes the agent is available if not handling an ACD call).
- **Always available**: If this value is set, the ACD Server will assume that this agent is always signed-in to accept calls from all queues that it is listed with. If it is not set, the agent must sign in before the ACD Server will send it calls. The default value is unchecked.
- **ACD Queues**: This is the list of the ACD Queues that an **Agent** belongs to. Priority of the queues can be changed by placing a check mark next to the appropriate queue name and using the **Move Up** and **Move Down** buttons.

Click on the **OK** button when done configuring the agent settings.

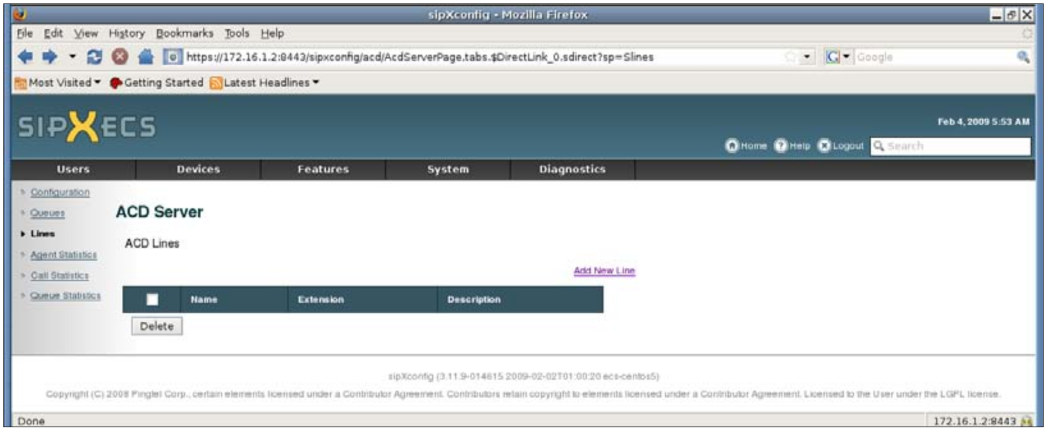
To return to the screen, click on the **Configuration** hyperlink on the lefthand side of the screen and then click on **OK** at the bottom of the page. The ACD queues page will be displayed with the new queue as shown in the following screenshot:



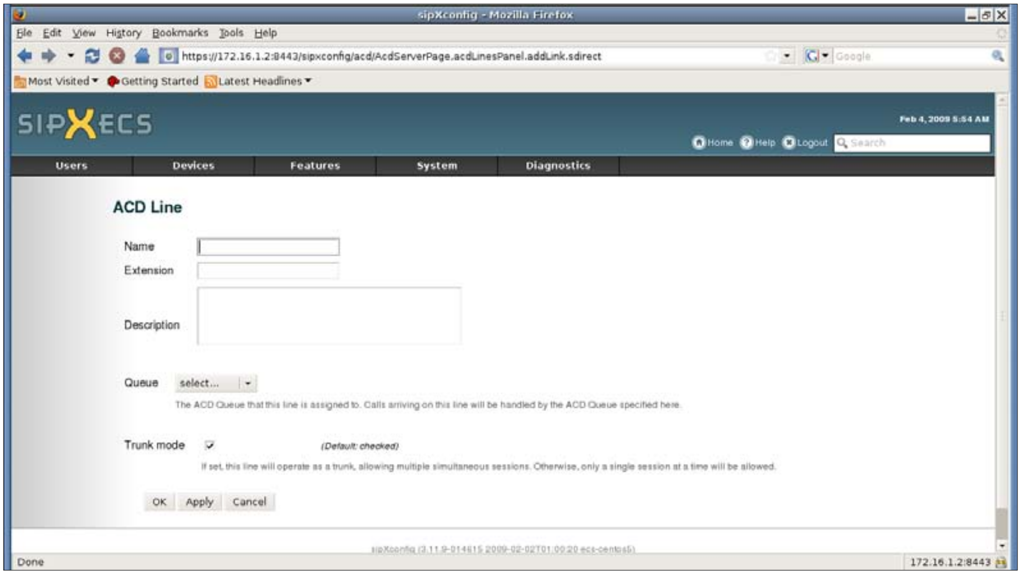
Configure lines for queues

The **Lines** setting for queues establishes a pilot number for the ACD queue. The pilot number can be referenced from an auto attendant, called directly by a gateway, or forwarded to by an extension.

To assign a line to a queue, click on the **Lines** hyperlink on the lefthand side of the **ACD Server** screen. This will display the following page:



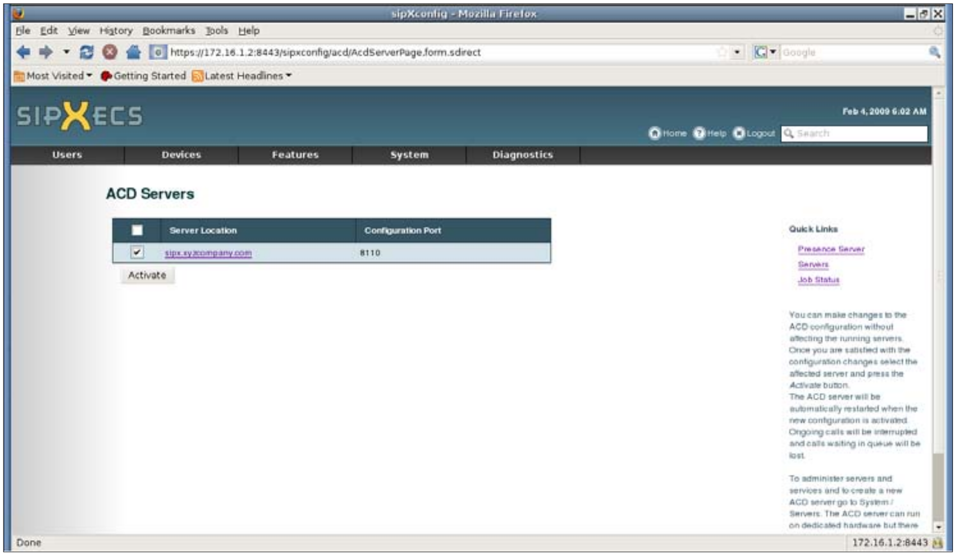
Click on the **Add New Line** hyperlink near the center of the page. This will display the following page:



The following options are available on the ACD Line page:

- **Name**: A text name for the line.
- **Extension**: The extension number of the line (pilot number). A range of these extensions should be considered in your extension plan.
- **Description**: A description for the line to help document the system.
- **Queue**: The ACD Queue that this line is assigned to. Calls arriving on this line will be handled by the ACD Queue specified here.
- **Trunk mode**: If set, this line will operate as a trunk, allowing multiple simultaneous sessions. Otherwise, only a single session at a time will be allowed. The default value is checked.

Once the settings are complete, click on the **OK** button at the bottom of the page. The **ACD Lines** screen will then be displayed with the new line in the list. To return to the ACD Servers page, click on the **Configuration** hyperlink and then **OK** at the bottom of the page. The **ACD Servers** will then be listed as shown in the following screenshot:



To apply the settings (this is necessary any time changes are made to the ACD service), place a check mark next to the server and click on the **Activate** button.

You can make changes to the ACD configuration without affecting the running servers. Once you are satisfied with the configuration changes, activate the changes, and the ACD server will be automatically restarted. It is important to note that ongoing calls will be interrupted and calls waiting in queues will be lost.

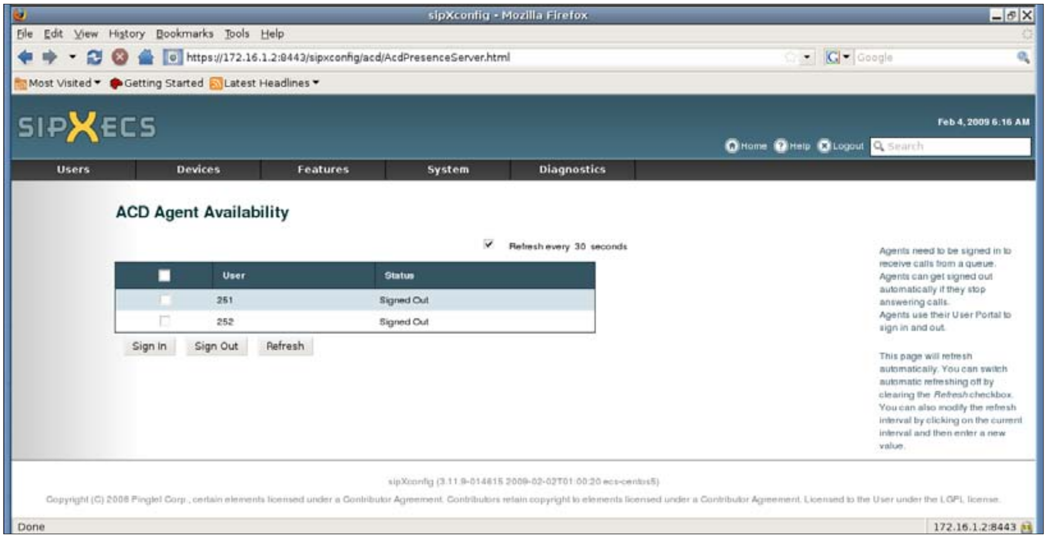
Agent Availability

Agents need to be signed in to ACD call queues when they are available to take calls. As seen previously, the agents can be set to be permanently signed in, which may be desirable for some queues.

If agents are not set to be permanently signed in to an ACD Queue, they need to sign in to the ACD service from their phone, or from the User Portal (see Chapter 8).

As described in Chapter 8, the user can sign in and out of the queue with feature codes *86 and *88 respectively. If the user is a member of multiple call queues, he or she is signed into or out of all of them. If the user is using a secondary line for his or her ACD, that line should be selected on the telephone with the line key and then the feature code should be dialed.

The system administrator can also forcibly sign agents in or out of queues on the ACD **Agent Availability** page (shown as follows). This page is accessed by selecting the **Agent Availability** menu item in the **Features** menu.



To sign in or sign out an agent, place a check mark next to the user and click on the **Sign In** or **Sign Out** button respectively.

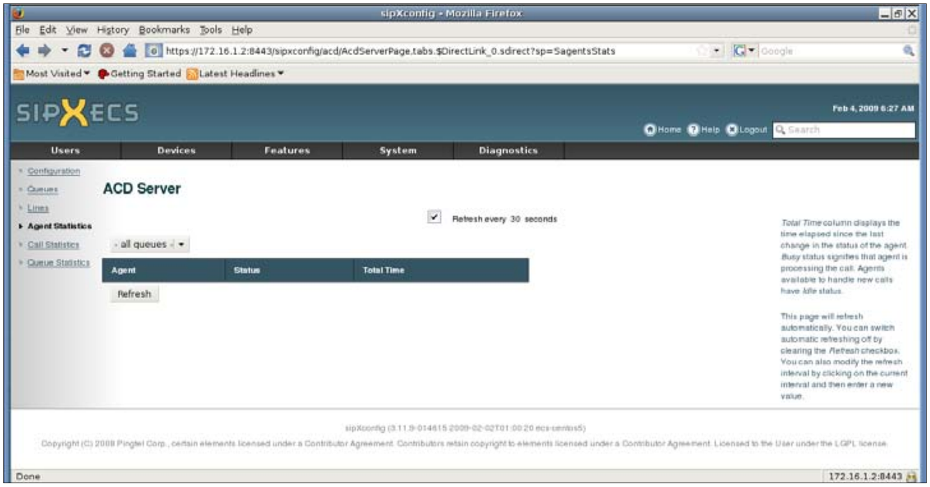
Monitoring the ACD Server

The **ACD Server** and **Agents** can be monitored in near real-time in the Administrative console. Only users in the Administrators group can view the ACD monitoring. There are three types of statistics available for monitoring: Agent, Call, and Queue Statistics.

To access the statistics pages, click on the **Features** menu, select **ACD Call Center**, and then click on the server name hyperlink. On the lefthand side of the page there will be links to the three statistics pages.

Agent Statistics

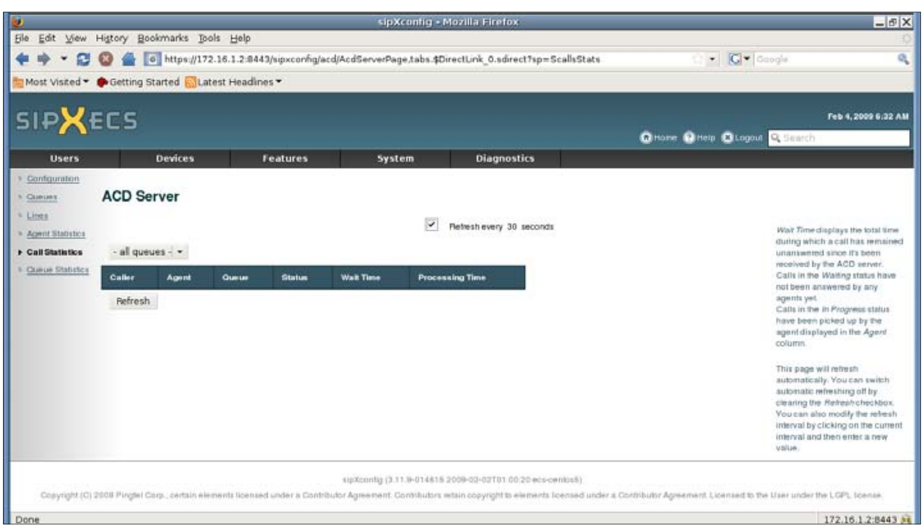
The **Agent Statistics** page (as seen in the following screenshot) is meant to give the administrator a quick view of agent status. The **Total Time** column displays the time elapsed since the last change in the status of the agent. Busy status signifies that agent is processing a call. **Agents** available to handle new calls have idle status.



This page will refresh automatically. You can switch automatic refreshing off by clearing the **Refresh** checkbox. You can also modify the refresh interval by clicking on the current interval and then entering a new value.

Call Statistics

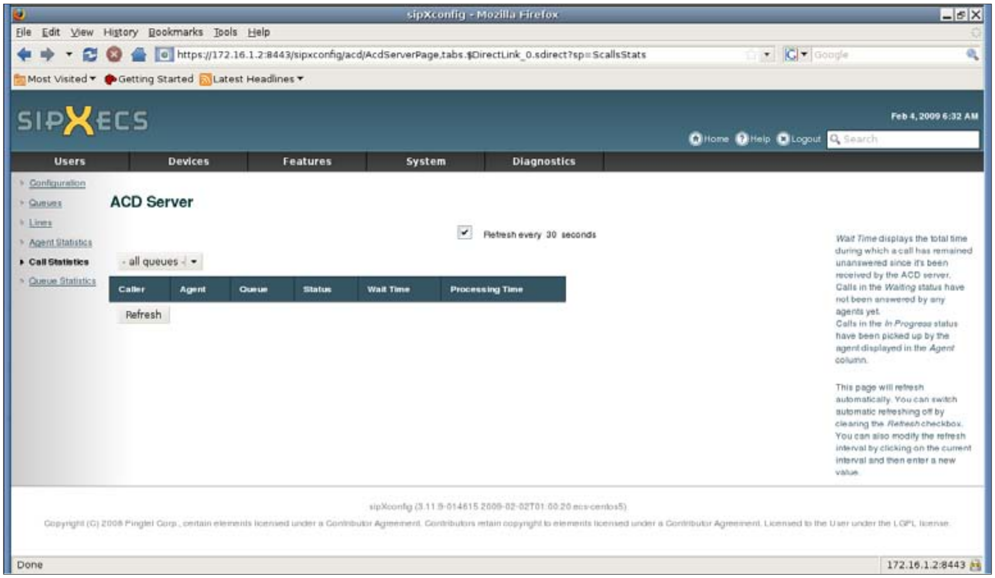
The **Call Statistics** page lets the Administrator have insight to the current call volume in the system. The **Wait Time** column displays the total time during which a call has remained unanswered since it was received by the ACD server. Calls in the **Waiting** status are the calls that have not been answered by any agent. Calls in the **In Progress** status have been picked up by the agent displayed in the **Agent** column.



This page will refresh automatically. You can switch automatic refreshing off by clearing the **Refresh** checkbox. You can also modify the refresh interval by clicking on the current interval and then entering a new value.

Queue Statistics

The **Queue Statistics** page is designed to allow the administrator to determine if all queues are operating efficiently. **Average Wait Time** is calculated based on calls received during last 30 minutes only. The **Total Agents** column displays the number of currently signed-in agents, not the number of configured agents.

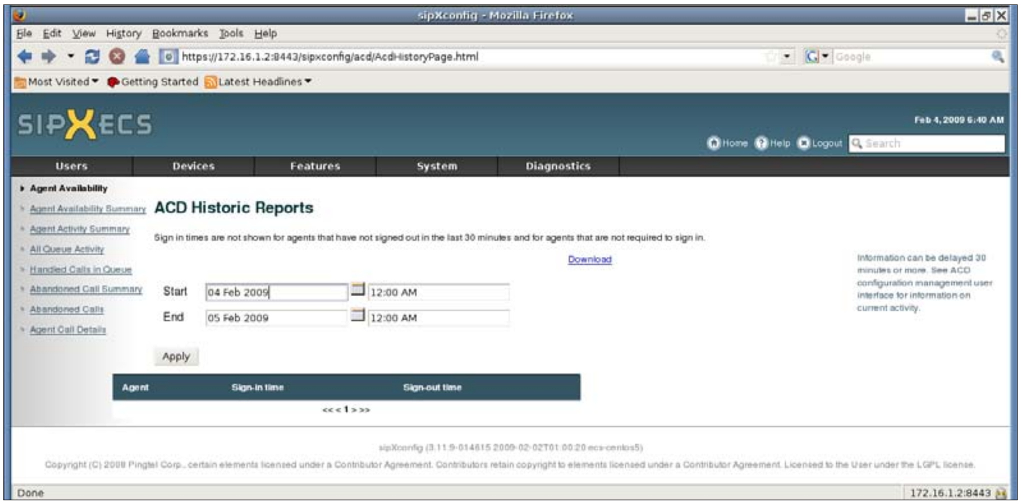


As with the other statistics pages, this page will refresh automatically. You can switch automatic refreshing off by clearing the **Refresh** checkbox. You can also modify the refresh interval by clicking on the current interval and then entering a new value.

ACD Reporting

The **ACD Reporting** functionality allows system administrators to review past statistics for future planning. The statistics are accessed through the **Diagnostics** menu by selecting the **ACD Reports** menu item.

As shown in the following screenshot, all reports allow for a date range to be entered to specify the reporting period. Additionally, a **Download** hyperlink is available for each report that allows the administrator to download a `.CSV` file for additional manipulation.



The following reports are available:

- **Agent Availability**: This is the detailed information about Agent sign-in and sign-out.
- **Agent Availability Summary**: This is the summary information about how much time an agent has spent signed in and what their maximum signed-in period was.
- **Agent Activity Summary**: This is the agent summary information about Total calls handled, total handling time, average handling time, maximum handling time, and minimum handling time.
- **All Queue Activity**: This is the summary information about each queue, the total number of calls to the queue, how many were handled, and how many were abandoned (the caller hung up before an agent got to the call).
- **Handled Calls in Queue**: This is the summary information by queue with total number of calls handled, average wait time, and maximum wait time.
- **Abandoned Call Summary**: This is the summary information about abandoned calls in each queue, including total calls abandoned, average wait time, and maximum wait time.

- **Abandoned Calls**: This is the detailed information about each abandoned call including the queue, the call start time, duration of the call, and the caller ID, if available.
- **Agent Call Details**: This is the detailed information about each agent and each call handled by the agent including which queue the call came in on, the start and end times of the call, the duration of the call, and the caller ID, if available.

Summary

While the included **Automatic Call Distribution** server is not a high-power call center solution, it meets the needs of most small and medium sized users of this system. In this chapter we learned how to configure the ACD services and monitor their operation.

We have now explored the features and functionality of sipXecs. Chapter 11 builds on this knowledge with information about maintaining and securing your installation.

11
Maintenance and Security

A couple of truisms that can be said about computer systems are: "All systems will fail at some point of time" and "The most secure computer is powered off, not plugged into anything, and is in a vault." As systems administrators it is our job to mitigate risk to the best of our ability and within budgetary constraints. In this chapter, we will explore the following system maintenance tasks and steps that can be taken to keep the phone system secure:

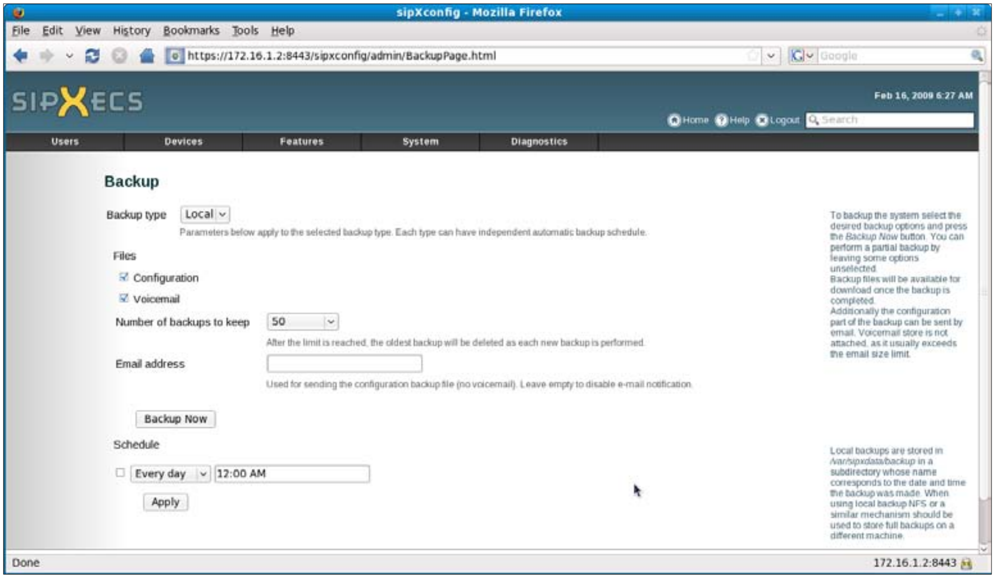
- Backing up
- Restoring
- Monitoring
- System alerts
- External monitoring
- Log files
- Snapshots
- Security
- Updating

System backup and restore

sipXecs has an integrated backup routine that allows the administrator to schedule system configuration and voicemail backups both to local files and to an FTP server. Additionally, the system configuration can be emailed on the same schedule.

Backup

To configure system backups, click on the **System** menu and select the **Backup** menu item. The following screenshot displays the backup options:



The following parameters are available on the backup page:

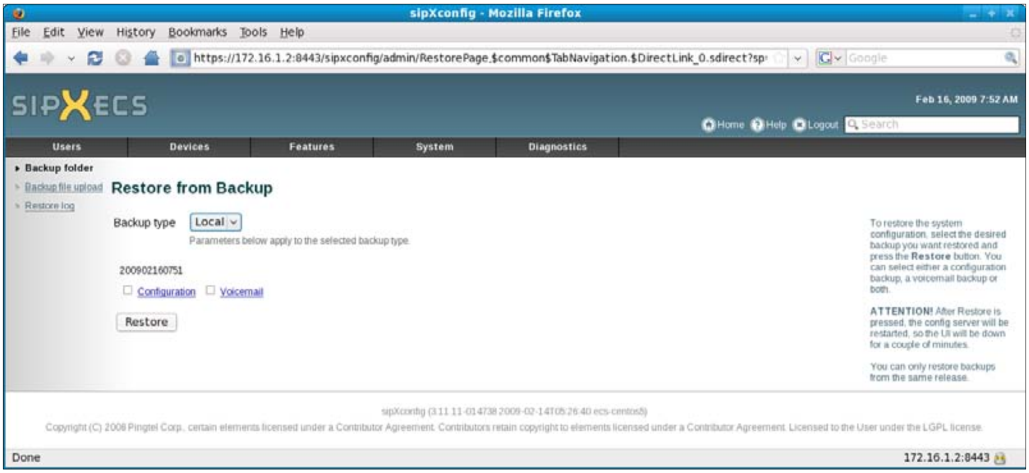
- **Backup type**: There are two types of backups available, **Local** and **FTP**. Each type can have an independent automatic backup schedule. The **Local** backup places the configuration and voicemail backup files in the `/var/sipxdata/backup` subdirectory. When using **Local** backup, **NFS** (**Network File System**) or a similar mechanism should be used to store full backups on a different machine. When selecting the **FTP** backup, the **Show FTP Settings** button will be displayed. Clicking on the button will reveal fields to enter the FTP server, username, and password.
- **Files** (**Configuration**): Sets whichever backup type selected to back up the sipXecs configuration information.
- **Files** (**Voicemail**): Sets whichever backup type selected to back up the sipXecs voicemail.
- **Number of backups to keep**: Sets whichever backup type selected to only keep this number of backups. After the limit is reached, the oldest backup will be deleted as each new backup is performed. The default value is **50** backups.

- **Email address**: Used to send the configuration backup file to an email address. Voicemail backups, because of their size, are not allowed to be emailed. Leave the field empty to disable email notification.
- **Backup Now**: The **Backup Now** button can be used to create an immediate backup of the system. When the backup is completed, hyperlinks will be presented to easily download the configuration and voicemail backup files to your local computer.
- **Schedule**: Place a check mark in the box to enable and select **Every day** or a day of the week and then the time backups should be performed.

> Mount a volume from another server or external drive to the backup folder to make sure that the system is backed up in case of drive failure.

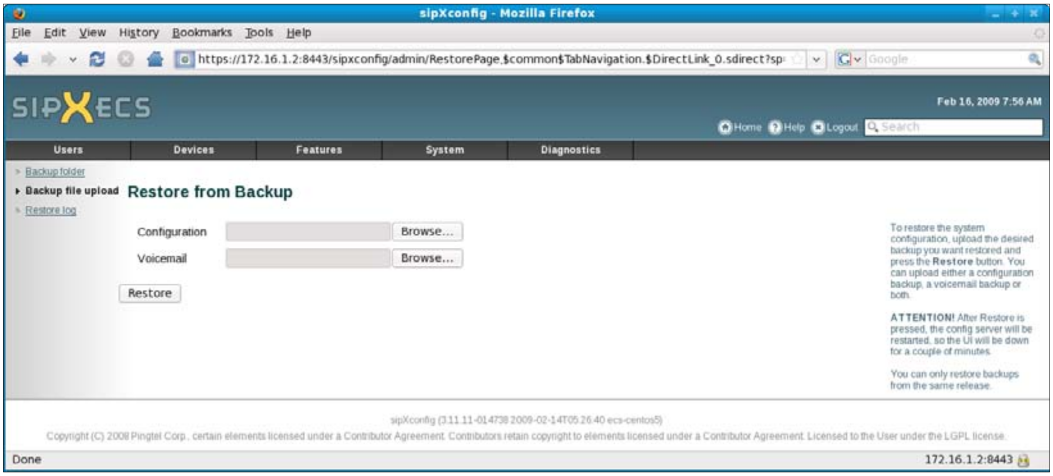
Restore

As important as a simple and reliable backup solution is, making restores easy takes some of the pressure off when the chips are down. Navigate to the **Restore** screen by clicking on the **System** menu and then select the **Restore** menu item. The following page will be displayed:



Any existing local backups found will be displayed. Selecting the drop-down box for **Backup type** will show the FTP option and the ability to specify the FTP server, username, and password. To restore, select the configuration and/or voicemail with the checkbox and click on the **Restore** button. Note that when the **Restore** button is pressed, the files will be restored and the configuration server will be restarted.

On the lefthand side of the page, there are hyperlinks for **Backup file upload** and **Restore log**. Selecting **Backup file upload** will display the following page, which allows the administrator to select files from their computer to restore:

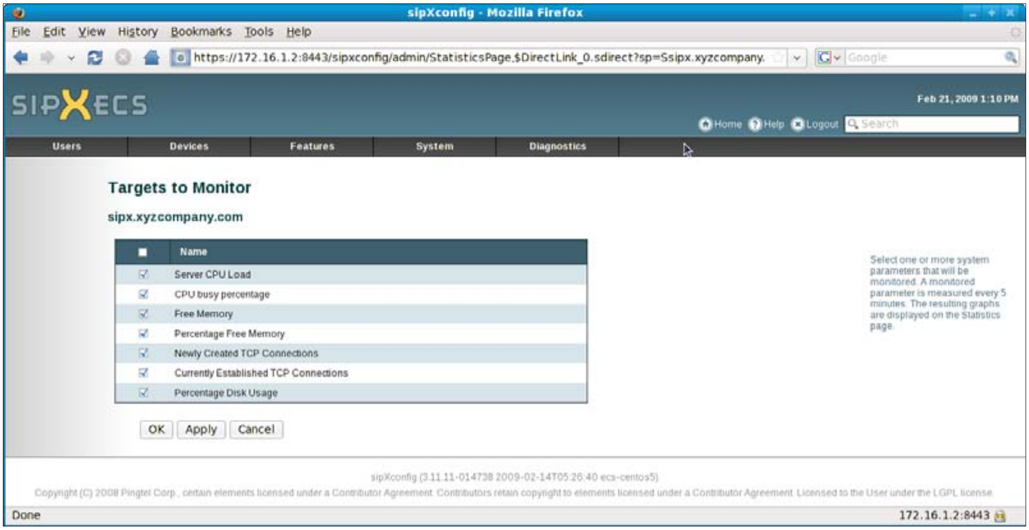


The **Restore log** option on the lefthand side of the screen will display the progress of a restore operation.

It is a good idea to keep a copy of the sipXecs installation media near the server in case of hardware failure.

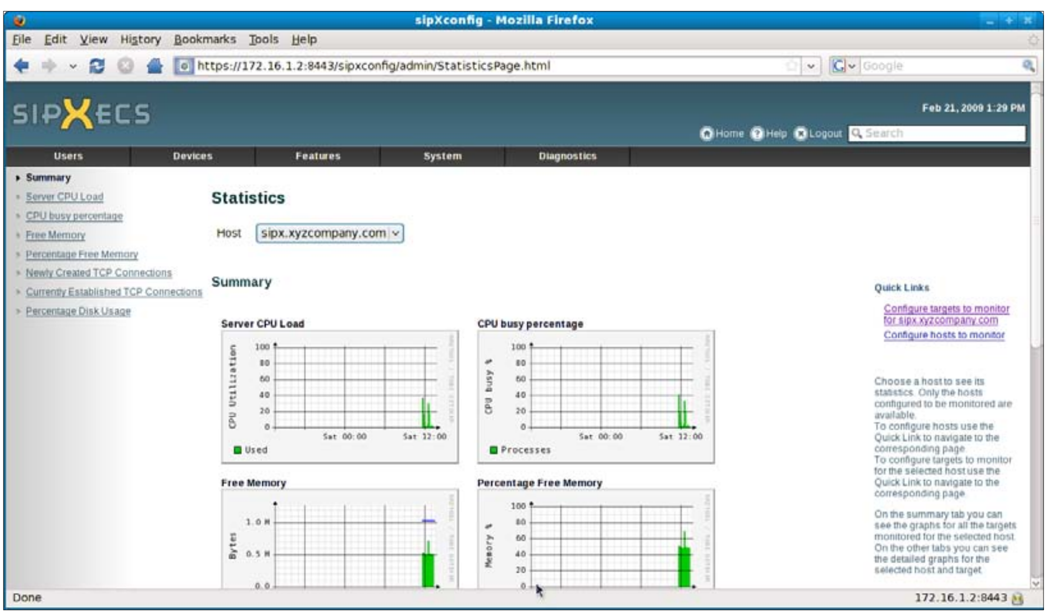
Monitoring system performance

sipXecs utilizes **MRTG** (**Multi Router Traffic Grapher**), one of the most widely used open source monitoring tools, to collect and make available historical monitoring information. Monitoring information is available in the **Statistics** menu item in the **Diagnostics** menu. The first time that you visit this menu you will need to select the server to monitor and then as shown in the following screenshot, select what system targets you would like to monitor.

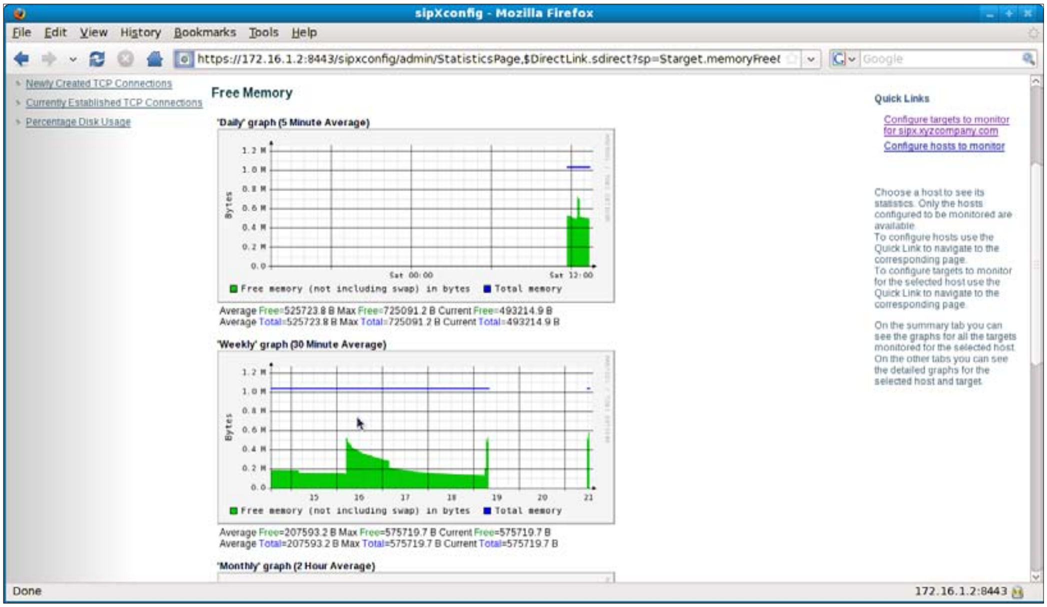


Select all appropriate items with a check mark and click on the **OK** button to begin collecting data.

Subsequent visits to the **Statistics** page will display the **Statistics Summary** page, which displays information about all monitored items for the past 24 hours.



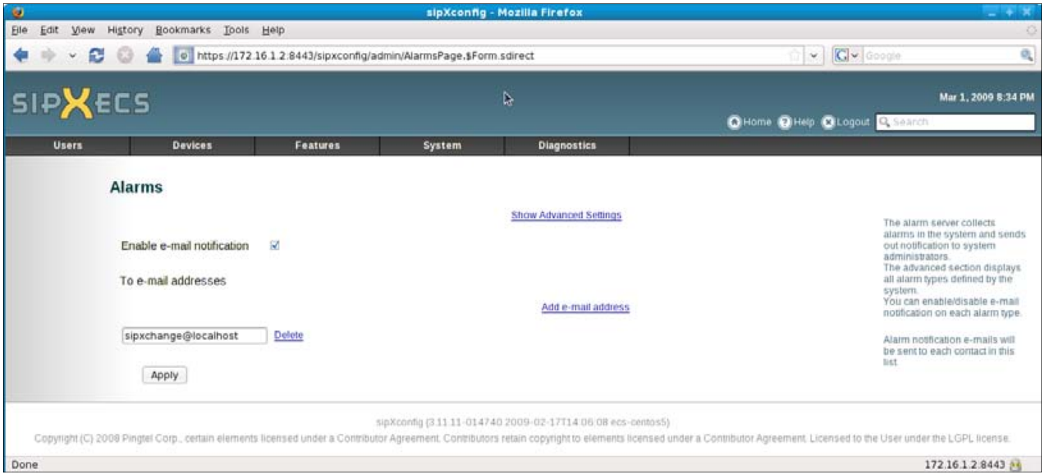
Clicking on any of the individual hyperlinks on the lefthand side of the page will display daily, weekly, monthly, and yearly statistics as seen in the following screenshot of the free memory statistical information:



Statistics should be reviewed periodically to ensure that adequate drive space and resources are available to the sipXecs services.

System alarms

sipXecs has an elaborate alarm server running on the system. The alarm server collects alarms in the system and sends out email notifications to system administrators. The alarm settings can be accessed via the **Alarms** menu item in the **Diagnostics** menu. The following screenshot shows the initial alarm screen:



Any number of email addresses can be entered to receive system alarms.

Clicking on the **Show Advanced Settings** hyperlink will allow the system administrator to specify the sending email address and enable or disable notifications for the following system alarms:

1. Emergency number dialed: Email alert of a user dialing an emergency number
2. Login failed: Failed attempt to login to PBX
3. Emergency number dialed
4. Login failed
5. Stray packets were detected by the Media Relay service
6. Failed to initialize the Media Relay
7. SipXproxy lost contact with the Media Relay
8. SipXproxy re-established connection with the Media Relay
9. SipXproxy detected a Media Relay reset but recovered
10. SipXproxy detected a Media Relay reset and is trying to recover
11. SipXproxy ran out of resources for NAT traversal
12. Process failed
13. Restarting process
14. Could not send REGISTER to the ITSP account
15. The ITSP Account has recovered
16. The ITSP disallowed an Authentication attempt

17. An ITSP account could not be found
18. The ITSP reported a server failure
19. The ITSP Account could not be reached
20. Software Updates Available
21. Public address discovery failed
22. The STUN Server recovered
23. The STUN Address cannot be resolved
24. NAT Reboot or SIPX Public Address change detected
25. CPU threshold exceeded
26. CPU threshold recovered
27. Disk usage threshold exceeded
28. Disk usage threshold recovered

External monitoring of system availability

There are several system services that are critical to sipXecs operating properly. These services should be monitored from an external monitoring solution that can provide up/down notifications and paging for support staff. There are several solutions available on the market to support this type of service, Zenoss (open source) and What's Up Gold being two of the more popular.

Services running on PBX server:

- sipxsupervisor
- sipxrls
- sipxpresence
- sipxpark
- sipxconfig-agen
- sipstatus
- sipregistrar
- sipXvxml
- sipXproxy
- ruby
- sipxacd * – only if ACD is enabled on server
- freeswitch * – only if conferencing is enabled on server

The following services may be provided by other network servers or by the PBX but are critical to proper operation of the system and should thus be monitored:

- NTP
- DNS
- NTP
- DHCP

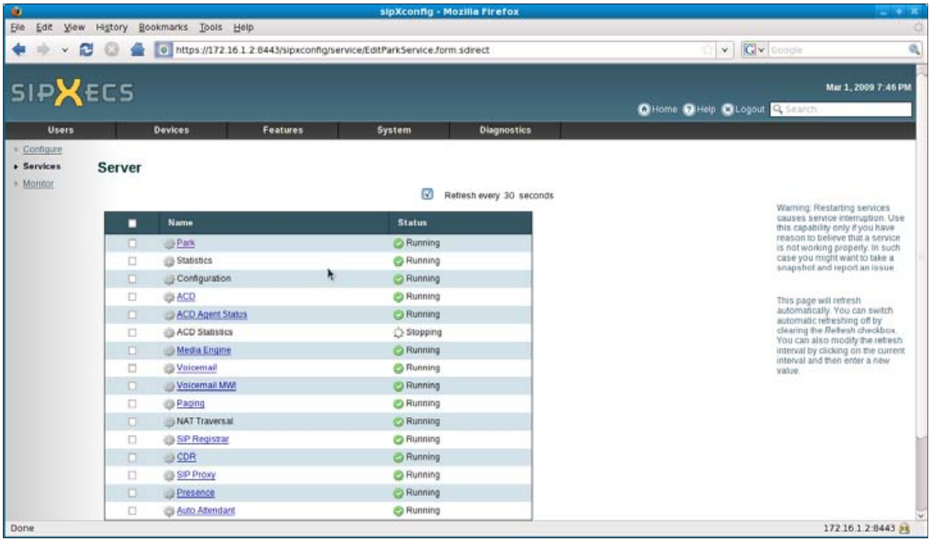
System logs

Each service in the system has the ability to create logs. Normally, this log information is kept to a minimum to reduce the processor and disk utilization by the system. If, however, there is a problem that you are trying to track down on the system, more detailed logging information might be of assistance.

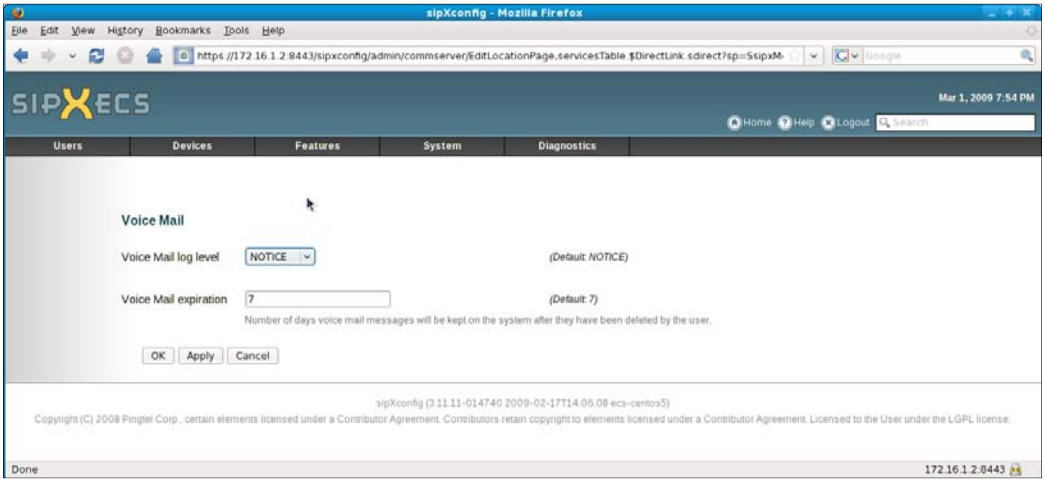
The log files for each service can be found in the `/var/log/sipxpbx` directory.

> A handy command to use to watch logs live is the `tail` command. For example `tail -f /var/log/sipxpbx/sipXproxy.log` will display the sipXproxy service log as lines are written to it.

Logging levels for each individual service running on the PBX can be set. These services can be found by clicking on the **Servers** menu item in the **System** menu. Select the server to manage (there will be only one if you have a single server system) and the following page will be displayed showing all of the services running on the server:



Click on any service with a hyperlink and the configuration information for that service will be displayed as shown in the following screenshot for the voicemail service.



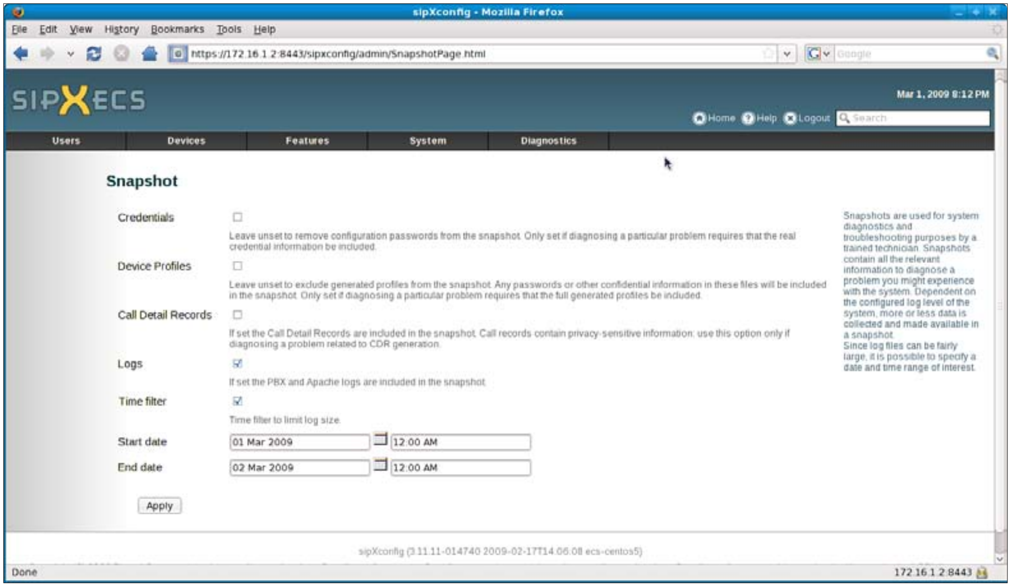
Notice on this page that the voice mail logging level can be set to Debug, Info, Notice, Warning, Error, Critical, Alert, or Emergency. Debug is the most detailed level of logging and Emergency is the least detailed level. The default level for all services is **NOTICE**.

Note that also on this page the default voice mail expiration for the system can be configured. Explore the settings available on each of the services.

System snapshots

Sometimes we just need to call for help from those 'in the know' about the system. These are the experts on the sipx-user or sipx-dev forums. A system snapshot provides detailed logging and configuration information in a single file that can be transmitted to developers in such a case.

The **Snapshot** menu item is located in the **Diagnostics** menu. Clicking on the menu item will display the following page:



The following settings are available before a snapshot is created:

Credentials: This setting will include account credentials (passwords) in the snapshot package. Leave it unchecked to remove configuration passwords from the snapshot. Check only if diagnosing a particular problem requires that the real credential information needs to be included.

Device Profiles: This setting will include device profile files in the snapshot package. Leave it unchecked to exclude generated profiles from the snapshot. Any passwords or other confidential information in these files will be included in the snapshot. Check only if diagnosing a particular problem requires that the full generated profiles be included.

Call Detail Records: This setting will add call detail information into the snapshot package. Call records may contain sensitive information so use this option only while diagnosing a problem related to CDR generation.

Logs: If this is checked, the PBX and Apache logs are included in the snapshot. The detailed level of the logs is set in each service. If you are providing a snapshot to technical personnel, you should set logging to Debug for the particular service that is experiencing problems.

Time filter: The time filter is utilized to limit log size. Logs in the system can get quite large (especially if set to Debug level). Limiting the time period of the logs forwarded to technical personnel will reduce the size of the snapshot file.

System security

The SIP protocol, like HTTP, is inherently insecure. The developers of SIP did not design it with security in mind. All messages are passed in clear-text and easily captured by any packet sniffing application. The potential security risks are:

- Private voice conversations can be captured and made public
- Potential for unauthorized calls from the system
- The ability to impersonate a caller
- Disruption of voice services

Just as HTTPS was developed to address the security issues with HTTP, SIPS has been developed to address security shortcomings with SIP. SIPS utilizes **Transport Layer Security** (**TLS**). TLS provides an encrypted channel over which a system can send SIP messages. sipXecs has support for SIPS/TLS built into the system.

The problem with TLS is that all devices in the system (phones, gateways, and PBX) must support it. At this point of time, however, not all devices provide TLS support and thus it isn't widely utilized within the SIP network (LAN) environment. This is expected to change over time.

Even if SIPS/TLS may not be used on the local network, TLS may be utilized with certain **Internet Telephony Service Providers** (**ITSPs**) to encrypt traffic across the Internet for SIP trunks. Adoption here has been slow. Many ITSPs simply restrict SIP traffic to or from their customer's firewall addresses.

Isolation

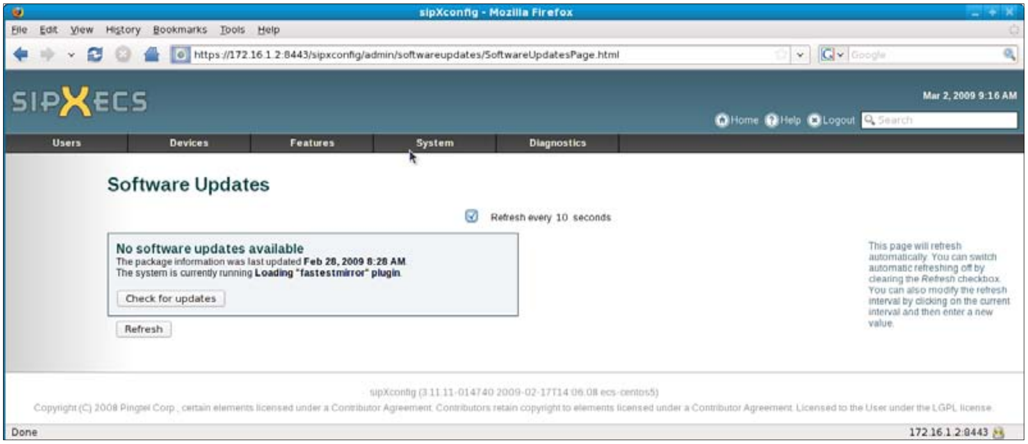
Since TLS isn't widely available the best solution for security with any SIP system is to isolate it and transmit voice between sites with secure VPN tunnels. As discussed in Chapter 2, virtual networks allow system designers to segregate voice-related network traffic from the rest of the network.

SIP passwords

When users and extensions are created in the sipXecs system they have cryptic passwords assigned automatically. The administrator can change them, to simplify them for remote users, but it is recommended that they are left cryptic. Knowing a user name/extension, and the SIP password is all that is required to log in and place calls.

Updating system software

sipXecs provides a web frontend in sipXconfig to CentOS's updating software **YUM** (**Yellowdog Updater**, **Modified**). Software updates are accessed with the **Software Updates** menu item in the **System** menu. Doing so will display the following page:



The page is refreshed by default after every 10 seconds. Unchecking the **Refresh** box will disable the automatic update. Clicking on the refresh time will allow the administrator to change the interval if desired.

A manual check for updates can be run by clicking on the **Check for updates** button.

If updates are available, the option to install them will be made available. If other YUM repos are desired, they can be added to the `/etc/yum.repos.d` directory. Information on YUM can be found at `http://yum.baseurl.org`.

Summary

Proper backups and monitoring and system maintenance will keep your sipXecs system operating reliably and put the system administrator in a position to recover easily from a disaster. Applying proven information technology processes to your company's new network-based phone system is a good practice and completes the assimilation of communications systems into information systems.

Glossary

Analog Phone: Analog phones are usually the same sort of phone you might find in a residence. They can provide signaling to the PBX for special functionality by flashing the hook switch and utilizing different DTMF codes.

Automatic Call Distribution: This can be thought of as intelligent hunt groups. They allow phone system users (agents) to sign in and out of calling queues. Calls then ring agents based on different factors such as who is the first person in the ACD list or which agent has been idle the longest.

Basic Rate ISDN (**BRI)**: A cheaper option than PRI, BRI may be offered in some areas. A BRI has two 64 Kbps B channels and a single 16 Kbps D channel for signaling. In the UK a BRI may also be called ISDN2e.

Blind Call Transfer: In a blind (also referred to as unattended) transfer, the call is simply transferred to the selected extension.

Bootrom (Boot ROM): Software that controls the booting of a device such as a phone or gateway.

Busy Lamp Field (**BLF**): This field show the status (or presence) of a call on a remote phone.

Call Detail Records (**CDR**): Information about calls that route through a phone system.

Call Forwarding: This service allows a user (or the phone system) to have a call redirected to another extension or number.

Call Hold: When a user presses a button for call hold on his or her phone, the caller is set into a mode such that neither party can hear the other.

Call Park Orbit: This was designed for PBX systems where the concepts of phone lines to users don't exist. Putting a call into a park orbit is accomplished by transferring a call to a holding queue (orbit). That call can be retrieved on any phone by dialing a pickup code and the park orbit number.

Call Pickup: This is the ability of one user to pick up another user's ringing phone.

Call Routing: How phone calls are handled and transferred through a phone system. Call routing logic evaluates calls and directs them (referred to as switching) to where they need to go based on many different factors. These factors include, but are not limited to, what number was dialed, who dialed it, and what time of day it is.

Call Transfer: This is the ability of a user to send a phone call to another extension on the phone system.

Caller-ID: Telephone number or name of caller that is passed in to a phone system.

Circular Hunt Group: This is a hunt group that "remembers" the last number that answered ringing and begins ringing on the next number in the list. When the end of the list is reached, it wraps around to the first number in the list again.

Clustering: A cluster is a collection of servers working together to act like a single system to provide high availability and load balancing.

Comma Separated Values (**CSV**): This is a data format typically used to exchange tabular data.

Compression Decompression Algorithm (**Codec**): This is a method for compressing and uncompressing media (voice / video).

Conferencing: A conference is a call between three or more parties. A conference may be a simple phone-based multi-party conversation or may be hosted by a full-featured conference server.

Consultative Call Transfer: In a consultative (also referred to as attended or supervised) transfer, the called party confers with the party that they will transfer the call to before the call is transferred.

Demarc: The demarcation point is the location in a facility at which communications facilities owned by the telecommunications provider interface with your organization's communications systems.

Dial Plans: These provide the routing logic for inbound and outbound calls from the system. The dial plans evaluate the dialed numbers, looking for patterns of digits, and direct calls to different destinations.

Dial Tone Multi Frequency (**DTMF**): This is the sound you hear when you push the dial pad buttons of a phone.

Digital Enhanced Cordless Telecommunications (**DECT**): This is a wireless standard for connecting communications equipment (headsets/phones).

Digital Phone: Digital phone sets provide higher functionality and programmability for phone systems than analog phones. They are proprietary to each vendor and type of phone system. Digital sets can be programmed centrally, provide excellent call quality, and usually have many buttons that can be programmed to provide different functionality to the user.

Direct Inward Dial (**DID**): Phone numbers assigned by a telecommunications provider that can be passed in to a phone system before the call arrives at the phone system.

Direct Station Selection (**DSS**): This is a one-touch speed dial assigned to a key on a user's telephone.

Domain Information Groper (**DIG**): This is a program, like NSLookup, that queries DNS servers.

Domain Naming System (**DNS**): This is a naming system for computers, services, or any resource participating in an IP network.

Dynamic Host Configuration Protocol (**DHCP**): This is a network protocol that allows network devices to obtain information about a network and network addressing.

E1: A physical layer protocol, much like Ethernet, that defines a 2 Mbps pipe for data or communications connectivity. This pipe can be used for data, split into 32 64 Kbps communications channels, or a mixture. If the pipe is used for communications channels, 30 of the channels can carry telephone conversations and the remaining 2 carry signaling and timing information. E1 circuits are typically found in Europe.

Firmware: Software that controls the operation of a device such as a phone or gateway.

Foreign Exchange Office (**FXO**): FXO lines are analog interfaces that connect to plain old telephone service (POTS) lines provided by the telecommunications provider.

Foreign Exchange Station (**FXS**): FXS lines are analog interfaces that connect to analog stations (phones or fax machines).

Fully Qualified Domain Name (**FQDN**): This is the combination of a DNS host name and a DNS domain name. For example with the FQDN of `www.sipfoundry.org`, www is the host name and `sipfoundry.org` is the domain name.

Ground Start Analog Circuit: Ground start circuits provide disconnect notification by actually grounding the circuit (when a caller hangs up the phone, also called answer and disconnect supervision).

Hard Phone: This is a physical telephone set.

Hunt Group: This is a collection of extensions that ring in a particular order when the hunt group number is dialed. The hunt group number is often referred to as the pilot number of the hunt group.

Intercom: The intercom function in a phone system allows a single user to dial another user's extension, have the receiving user's phone automatically go "off-hook" in speaker phone mode and have the two parties converse.

Internet Telephony Service Provider (**ITSP**): This is a company that provides telecommunications services over the Internet.

iPBX: This is a modern PBX (also referred to as a Softswitch). This name is derived from the fact that the PBX functionality is all accomplished in software running on a standard server.

ISDN: A more modern circuit signaling protocol that was designed to overcome problems that existed with T1 and E1 circuits. On E1s, EuroISDN signaling is standard. On T1s different providers utilize different standards. NI1, NI2, DMS100, and DMS250 are all examples of ISDN signaling protocols, each delivering different levels of functionality.

ISO Image: This is an archive file (or disk image) of an optical disk (CD / DVD / and so on).

Key Telephone System: This is a type of phone system that allows users to directly select outside lines through keys on the handsets. These systems were designed with smaller organizations in mind.

Linear Hunt Group: A hunt group that always starts ringing the first extension in the list and ends ringing the last in the list of extensions.

Localization: The ability of a system to localize its text and voice prompts for different regions of the world.

Loop Start Analog Circuit: Loop start analog circuits are the more typical home and key system phone lines. Loop start lines use either a polarity reversal (called battery reversal) or removal of the line voltage (battery drop) for answer and disconnect supervision.

Managed Gateway: A SIP gateway for which sipXecs can create configuration files.

Managed Phone: This is a SIP phone for which sipXecs can create configuration files.

Message Waiting Indicator (**MWI**): This is an important but seemingly simple responsibility of the voicemail system is to signify to users that they have messages waiting. This notification usually takes the form of a message waiting indicator (MWI) light that is lit on handsets.

Music on Hold (**MoH**): This is the music that is played to callers when their line is placed on hold.

Network Address Translation (**NAT**): This is a function of firewalls and routers that allows private internal IP address to be translated to one or more valid Internet IP addresses.

Network Interface Device (**NID)**: This is a box that the telecommunications provider utilizes to break-out their lines to interfaces the customer can utilize.

NSLookup: This is a program that can query DNS servers to determine address and DNS information.

Paging: Similar to intercom functionality, paging differs in that it is designed to allow a single user to broadcast a message to one or more phones without the ability for the receiving phones to talk back to the caller.

Phantom User: This is a user account on the system that will never have a User Agent (phone) registered to it. Phantoms can be used for voicemail-only mailboxes or for call routing purposes.

Ping: This is a program that allows systems to test if other systems are available across a network.

Plain Old Telephone Service (**POTS**): This is another term for analog telephone lines.

Power over Ethernet (**PoE**): This is a method to provide DC power to various devices (such as phones and wireless access points) across network cabling.

Primary Rate ISDN (**PRI**): A PRI is an E1 or T1 with ISDN signaling running on top of it. ISDN signaling provides reliable call setup and tear-down detection as well as detailed information about each call. In the UK a PRI is also referred to as ISDN30. Voice channels on a PRI are referred to as B channels and the signaling channels are referred to as the D channel. On an E1, a PRI will provide 30 B channels of voice and utilize one of the signaling channels as the D channel. Since T1s have no signaling channels, a PRI on a T1 will utilize one of the channels as a D channel and have 23 B channels for voice.

Private Branch Exchange (**PBX**): A PBX is a type of phone system that is typically found in larger organizations.

Public Switched Telephone Network (**PSTN**): This is a telecommunications connectivity provided by a phone company.

Quality of Service (**QoS**): Information contained within Ethernet packet headers that signals network equipment should give packets priority over other packets.

Session Border Controller (**SBC**): This allows SIP calls to traverse network boundaries (firewalls). Because SIP traffic contains IP-specific information, SIP messages need to be modified when they traverse a **NAT**'d (**Network Address Translation**) network connection.

Session Description Protocol (**SDP):** This is a messaging format used to describe streaming media formats. SIP utilizes SDP for setting up sessions.

SIP: This is an **Internet Engineering Task Force** (**IETF**) standard protocol user for conducting interactive communications. SIP can be utilized for many forms of communications sessions including voice, video, and chat. The SIP call signaling is independent from the media sessions it controls.

SIP Gateway: The SIP gateway provides communications system connectivity to the telecommunications providers. A gateway may be a physical device connecting a traditional type phone circuit, discussed earlier, or a software-based gateway providing connectivity to **Internet Telephony Service Providers** (**ITSP**).

SIP Proxy: This can be thought of as a call router. Its job is to direct SIP calls through the system. The proxy itself does not handle any voice traffic (media).

SIP Trunk: This is a term used to describe the method for providing telephone service over the Internet.

Speed Dial: Speed dials are short phone numbers that can be dialed in order to dial a more complicated number. For example a user would dial 752 and the phone system would actually dial 18005555555.

SRV Record or Service Record: This is a type of record found in DNS domains that specifies information about available services.

T1: Similar to an E1 but it is common in North America. T1s are 1.544 Mbps pipes that can carry data or 24 telephone channels. There are no signaling channels on a T1. Also, like an E1, T1s can be channelized and utilized to deliver voice and data.

Unified Messaging System: Unified messaging systems are an extension of voicemail systems that allows users to have a single inbox combining voicemail, email, and faxes. A true unified system will integrate these systems at the server level such that when you open or delete voicemail on a computer it is marked as read or deleted in the voicemail system. A simple version of unified communications involves SMTP forwarding of voicemail to an email or requires setup of client software that handles email integration on the user's computer.

Uninterruptable Power Supply (**UPS**): This is a system that typically employs batteries to maintain power to devices.

Unmanaged Gateway: A SIP gateway that must be manually configured for use with sipXecs.

Unmanaged Phone: A SIP phone that must be manually configured for use with sipXecs.

Virtual Local Area Network (**VLAN**): This is an Ethernet standard that allows multiple virtual networks to be defined within network equipment.

Voicemail System: These systems provide auto attendant functions and the playing and recording of messages. The voicemail system can be thought of as the voice of the phone system.

Wireless Phone: This is a telephone that does not need to be corded to a phone system. These phones connect either via WiFi or by DECT.

Index

A

B

C

D

E

F

G

H

I

N

P

Q

R

S

T

U

V

W

X

Y

Thank you for buying
Building Enterprise Ready Telephony Systems with sipXecs 4.0

Packt Open Source Project Royalties

When we sell a book written on an Open Source project, we pay a royalty directly to that project. Therefore by purchasing Building Enterprise Ready Telephony Systems with sipXecs 4.0, Packt will have given some of the money received to the sipXecs project.

In the long term, we see ourselves and you—customers and readers of our books—as part of the Open Source ecosystem, providing sustainable revenue for the projects we publish on. Our aim at Packt is to establish publishing royalties as an essential part of the service and support a business model that sustains Open Source.

If you're working with an Open Source project that you would like us to publish on, and subsequently pay royalties to, please get in touch with us.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to `author@packtpub.com`. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

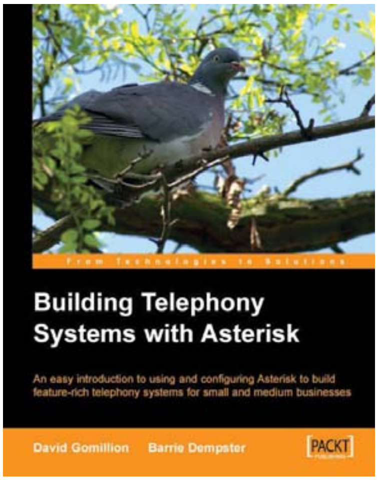
We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

About Packt Publishing

Packt, pronounced 'packed', published its first book "Mastering phpMyAdmin for Effective MySQL Management" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution-based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: `www.PacktPub.com`.



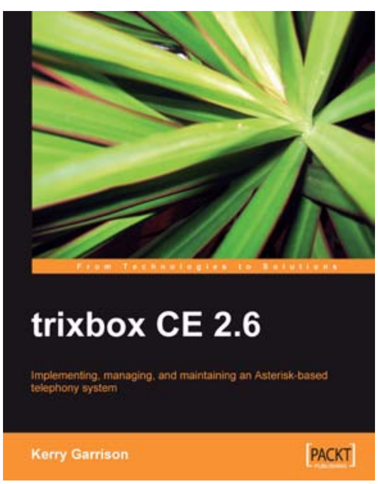
Building Telephony Systems With Asterisk

ISBN: 978-1-904811-15-2 Paperback: 176 pages

An easy introduction to using and configuring Asterisk to build feature-rich telephony systems for small and medium businesses.

1. Install, configure, deploy, secure, and maintain Asterisk
2. Build a fully-featured telephony system and create a dial plan that suits your needs
3. Learn from example configurations for different requirements

---



trixbox CE 2.6

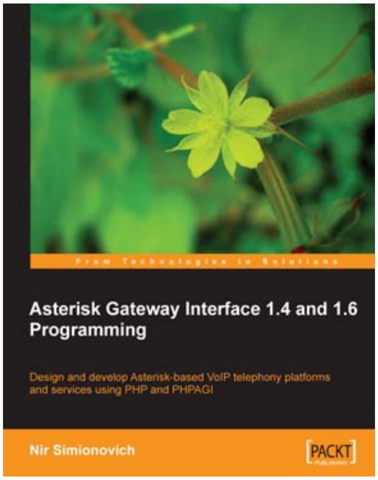
ISBN: 978-1-847192-99-8 Paperback: 344 pages

Implementing, managing, and maintaining an Asterisk-based telephony system

1. Install and configure a complete VoIP and telephonic system of your own; even if this is your first time using trixbox
2. In-depth troubleshooting and maintenance
3. Packed with real-world examples and case studies along with useful screenshots and diagrams
4. Best practices and expert tips straight from the Community Director of trixbox, Kerry Garrison

Please check **www.PacktPub.com** for information on our titles

PACKT PUBLISHING

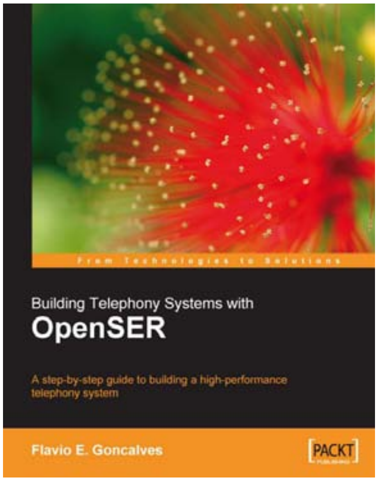


Asterisk Gateway Interface 1.4 and 1.6 Programming

ISBN: 978-1-847194-46-6 Paperback: 220 pages

Design and develop Asterisk-based VoIP telephony platforms and services using PHP and PHPAGI

1. Develop voice-enabled applications utilizing the collective power of Asterisk, PHP, and the PHPAGI class library
2. Learn basic elements of a FastAGI server utilizing PHP and PHPAGI
3. Develop new Voice 2.0 mash ups using the Asterisk Manager



Building Telephony Systems with OpenSER

ISBN: 978-1-847193-73-5 Paperback: 324 pages

A step-by-step guide to building a high performance Telephony System

1. Install, configure, and troubleshoot OpenSER
2. Use OpenSER to build next generation VOIP networks from scratch
3. Learn and understand SIP Protocol and its functionality
4. Integrate MySQL with OpenSER

Please check **www.PacktPub.com** for information on our titles