Denwa
COMMUNIFICATION

Denwa UC&C 4.0.1

User's Manual

Versión: 47

Denwa UC&C 4.0.1 Manual for installation, configuration and use.

Writen by: Nicolás Saravia Vivas
Reviewed by: Nicolás Saravia Vivas
Córdoba, Argentina - Thursday 2nd February, 2023
Páginas Totales: 266
Engineering Department
Denwa Technology Corp.
GlobalThink Technology S.A.

Denwa UC&C 4.0.1

User's Manual

Engineering Department
GlobalThink Technology S.A.
Córdoba, Argentina - Thursday 2nd February, 2023
Version: 47

Créditos

Denwa Technology Corp. reserves the right to make changes without prior notice and shall not be liable for any damages that may be caused by such changes, including typing and grammatical errors

Trademarks

Version

Denwa UC&C 4.0.1 Manual for installation, configuration and use.

Revision: 47
Date: Thursday 2nd February, 2023

Company Information

SALES OFFICE
1000 N.W. 57th Court Suite 1040
Miami, FL 33126 (Blue Lagoon)

I+D Department
Humberto Primo 843 Piso 6
X5000FAQ - Córdoba, Argentina

Argentina: +54 (11) 5129 6905 +54 (351) 571 6300
USA: +1 (305) 433 6166 +1 (305) 5872453
Ecuador: +593 4 390 1463
Chile: +56 (22) 938 1742

Version control

Below is the detail of the changes suffered in each version of this document:

Versión	Detalle
47.0	First engish edition

This page has been intentionally left blank.

CHAPTER 1

DOCUMENT INFORMATION

1.1 Purpose of this document

The purpose of this document is to provide all necessary information for the correct configuration of **Denwa UC&C 4.0.1** .

1.2 Scope

The documentation provided here can be used with any version of the Denwa UC&C system, except for the device called Denwa SOHO, as well as the Telephone Gateways and Soft Switches.

1.3 Symbols

The following symbols shall be used to facilitate understanding of the contents:

- Boxes: They include information regarding the specific functionality that is being developed in the text. It can have different levels of importance. Namely:
  - **Informative**: Grey box.

    Grey box example

    Informative content
  - **Low importance**: Green box. It may affect platform users.

    Green box example

    It may affect platform users.
  - **Medium importance**: Yellow box. It may affect client operation.

    Yellow box example

    It may affect client operation.
  - **High importance**: Red box. It may platform operation.

Red box example

It may platform operation.

- **Transcription**: Between brackets. Transcription of an external document

> Content Content (continued)
>
> ***Name or location of quoted document***

- **System console or file**: In a box with numbered lines

```
View of a system file content or console
```

- Typographies: Specific typographies are used to refer to buttons, text and different elements of the user interface.

Part I

Preparation

CHAPTER 2

INSTALLATION PROCESS

There are currently two (2) ISO files for the installation of Denwa UC&C 4.0.1 , which were designed for completely different environments:

- Regular installation, with direct connection to the Internet.
- Closed environment installation, with local repositories or repositories reachable through the distributor39;s MAN network.

In both environments, the installation process is the same, with the only exception that it will be necessary to declare the server that operates as an Application Proxy or Repository.

However, regardless of the environment in which the installation is to be performed, the installer must have the installation and activation license numbers.

Licenses

Should the installer not know the installation and/or activation license numbers, these can be requested from Denwa Technology Corp. Support Department, by supplying the series number of the equipment in which installation will be performed.

2.1 Available ISO files

At the time of publishing this manual, the released versions of these ISO files are available from the following links:

- **With Internet connection:** `http://dendown.denwaip.com/dendown/downloads/src/DenwaUC-4.0.1.20200212.iso`
- **By Proxy:** `http://dendown.denwaip.com/dendown/downloads/src/DenwaUC-4.0.1.20200903-TECO-p`
  `iso`

2.2 USB Availability

Once the suitable ISO file has been downloaded, it is necessary to have the appropriate software to transfer it to a USB storage device. This may vary depending on the operating system of the computer being used.

2.2.1 Linux

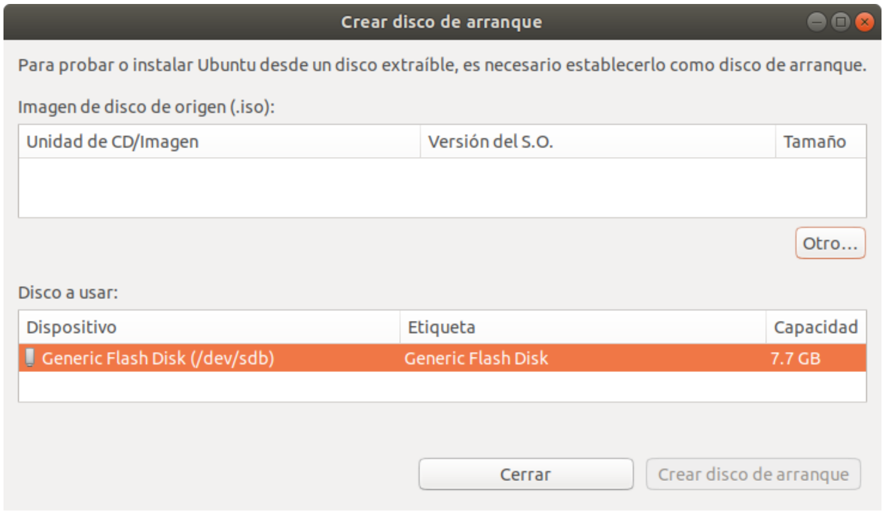
2.2.1.1 GUI Mode

2.2.1.1.1 Debian based In the case of Debian-based operating systems, such as Ubuntu, Deepin, Linux Min, Kali Linux, SteamOS or similar systems, the Startup Disk Creator application can be used. If this application is not in the system, it can be installed from the Terminal using the following command:

```
apt install usb-creator-gtk
```

Once installed, it can be located by typing «Create Startup Disk» in the GNOME activity menu, or in the startup menu of the distribution being used. Once the application is open, you will see that the interface is really simple. In fact, the procedure is practically self-explanatory. It has two sections, one in which you must select the ISO image you want to burn, and another in which the USB device is indicated.

The first thing is to select the ISO image; to do this, under the source disk image box, you must click onthe «Other...», esto abrirá el explorador de archivos y le permitirá localizar y seleccionar el fichero.



Crear disco de arranque

Para probar o instalar Ubuntu desde un disco extraíble, es necesario establecerlo como disco de arranque.

Imagen de disco de origen (.iso):

Unidad de CD/Imagen	Versión del S.O.	Tamaño

Disco a usar:

Dispositivo	Etiqueta	Capacidad
Generic Flash Disk (/dev/sdb)	Generic Flash Disk	7.7 GB

Figure 2.1: Startup Disk Creator Interface

Once you have selected the image to burn, the next step is to select the device to use. There you must select the USB device that you want to serve as the boot disk (it must be connected beforehand).

If you are viewing multiple devices, you must have more than one volume connected to your system through a USB port, so select the appropriate one and you are done. Note that this procedure will erase all the content that was previously on the device.

Once this is done, just click the «Create bootable disk»; button to start the process of burning the image and preparing the volume.

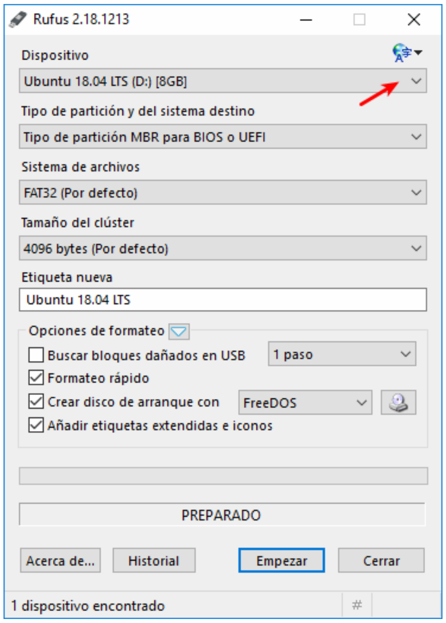
In a matter of minutes (depending on the port speed and the type of USB disk selected) you should have the bootable USB with the Denwa UC&C 4.0.1 installer ready.

2.2.2 Windows

We recommend the use of Rufus for the creation of bootable disks. To download Rufus, you can go to the official website of the project (`https://rufus.ie`)and scroll down to the download section. There you will see that you have two main options: installable or portable.

Using Rufus is really very simple. Once you open the application (if you have downloaded the portable version, you just have to run the downloaded file) you will see a window with several options.

The first step is to select the USB device. A drop-down box will list all USB devices connected to your system. You must be careful which device you choose, since in th process all the data that may be on that device will be erased. In the image below, an 8 GB device has been selected, on which an Ubuntu 18.04 LTS image was previously burned.



Rufus 2.18.1213

Dispositivo
Ubuntu 18.04 LTS (D:) [8GB]

Tipo de partición y del sistema destino
Tipo de partición MBR para BIOS o UEFI

Sistema de archivos
FAT32 (Por defecto)

Tamaño del clúster
4096 bytes (Por defecto)

Etiqueta nueva
Ubuntu 18.04 LTS

Opciones de formateo
□ Buscar bloques dañados en USB 1 paso
☑ Formateo rápido
☑ Crear disco de arranque con FreeDOS
☑ Añadir etiquetas extendidas e iconos

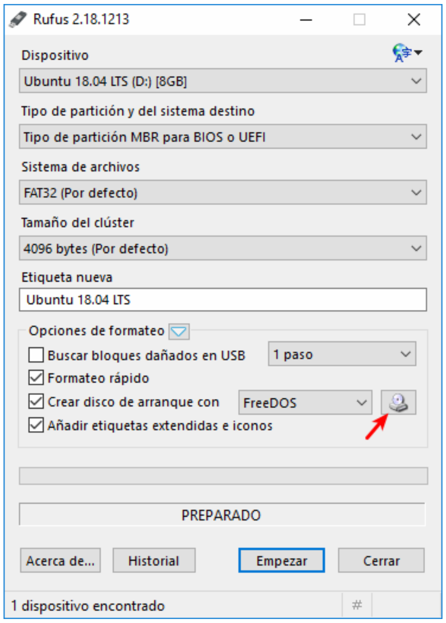
PREPARADO

1 dispositivo encontrado

Figure 2.2: Rufus Interface

It is not necessary to format the selected device beforehand, as Rufus already formats the drive before creating the new boot disk. Notice that the quick format checkbox is checked in the formatting options.

The following step is to select the Denwa UC&C 4.0.1 image (do not forget to check its integrity before), to generate the boot disk. To do this, you have to click on the button indicated in the following image.



Rufus 2.18.1213

Dispositivo: Ubuntu 18.04 LTS (D:) [8GB]

Tipo de partición y del sistema destino: Tipo de partición MBR para BIOS o UEFI

Sistema de archivos: FAT32 (Por defecto)

Tamaño del clúster: 4096 bytes (Por defecto)

Etiqueta nueva: Ubuntu 18.04 LTS

Opciones de formateo

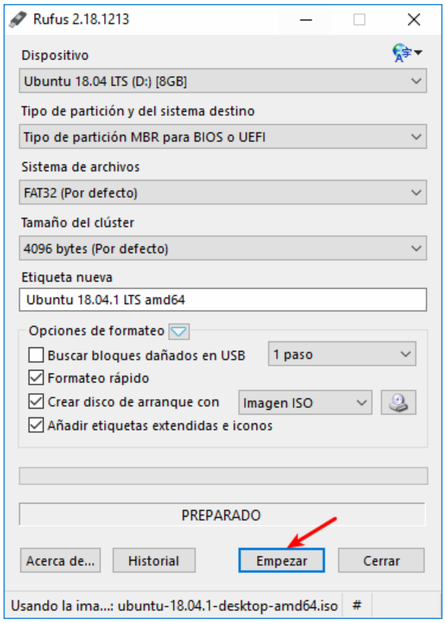
- ☐ Buscar bloques dañados en USB — 1 paso
- ☑ Formateo rápido
- ☑ Crear disco de arranque con — FreeDOS
- ☑ Añadir etiquetas extendidas e iconos

PREPARADO

1 dispositivo encontrado

Figure 2.3: Rufus Interface: ISO selection

When selecting the image, there are several options according to the different settings. You can choose these options, such as the volume label, but it is recommended to use the default options to start the process.



Rufus 2.18.1213

Dispositivo: Ubuntu 18.04 LTS (D:) [8GB]

Tipo de partición y del sistema destino: Tipo de partición MBR para BIOS o UEFI

Sistema de archivos: FAT32 (Por defecto)

Tamaño del clúster: 4096 bytes (Por defecto)

Etiqueta nueva: Ubuntu 18.04.1 LTS amd64

Opciones de formateo

- ☐ Buscar bloques dañados en USB — 1 paso
- ☑ Formateo rápido
- ☑ Crear disco de arranque con — Imagen ISO
- ☑ Añadir etiquetas extendidas e iconos

PREPARADO

Usando la ima...: ubuntu-18.04.1-desktop-amd64.iso

Figure 2.4: Rufus Interface: Burning starts

Once the process is completed, the USB device is ready to be used for the installation of Denwa Denwa UC&C 4.0.1 .

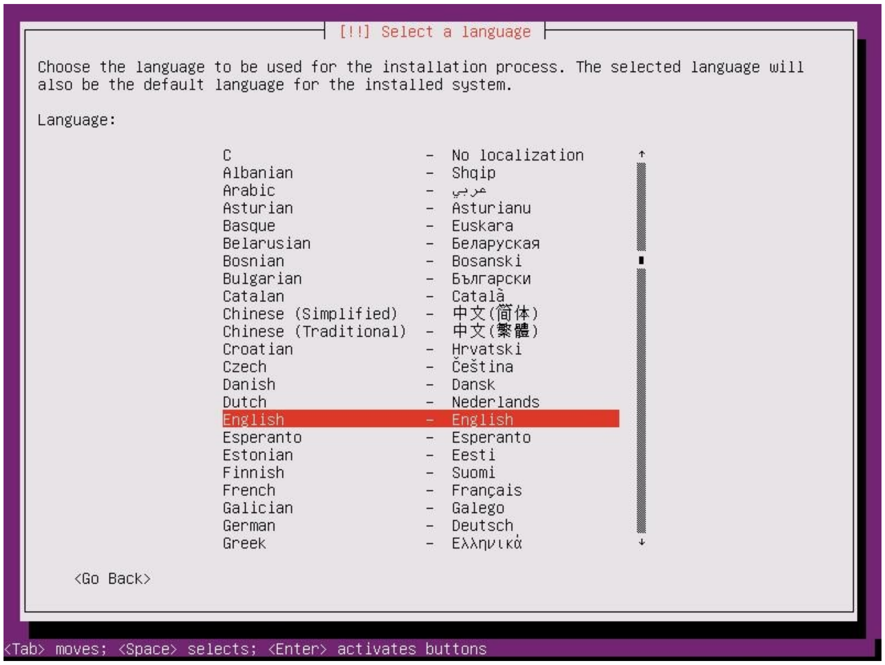
2.3 Base operating system installation

First of all, it is necessary to configure the way in which the computer will boot, for this you must enterthe computer's BIOS and select the USB device mentioned in the previous section as the boot disk. In addition, UEFI must be set as the boot mode..

Boot configuration

Since the Denwa UC&C 4.0.1 system is compatible with equipment of different generations, the way to access the BIOS may be different in each case.

Once the equipment has started with the USB device, a screen will be displayed where you can select the language used for the installation options. We recommend the use of English, as all our reference documentation is in this language.



```
[!!] Select a language

Choose the language to be used for the installation process. The selected language will
also be the default language for the installed system.

Language:

                        C                        -   No localization
                        Albanian                 -   Shqip
                        Arabic                   -   عربي
                        Asturian                 -   Asturianu
                        Basque                   -   Euskara
                        Belarusian               -   Беларуская
                        Bosnian                  -   Bosanski
                        Bulgarian                -   Български
                        Catalan                  -   Català
                        Chinese (Simplified)     -   中文(简体)
                        Chinese (Traditional)    -   中文(繁體)
                        Croatian                 -   Hrvatski
                        Czech                    -   Čeština
                        Danish                   -   Dansk
                        Dutch                    -   Nederlands
                        English                  -   English
                        Esperanto                -   Esperanto
                        Estonian                 -   Eesti
                        Finnish                  -   Suomi
                        French                   -   Français
                        Galician                 -   Galego
                        German                   -   Deutsch
                        Greek                    -   Ελληνικά

     <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 2.5: Operating system installation: selecting installation language

On the next screen you need to select the «Install Denwa UC» option to use automatic partitioning, or «Install Denwa UC Manual Partition» to resize the system partitions differently, and press the «Enter» key.

Manual partitioning

The installation of some modules, CDRs local backup features , massive logs to the system logs, secondary disks or RAID alignments may require the customization of the system partitions.
If in doubt, please contact Denwa Technology Corp. support.

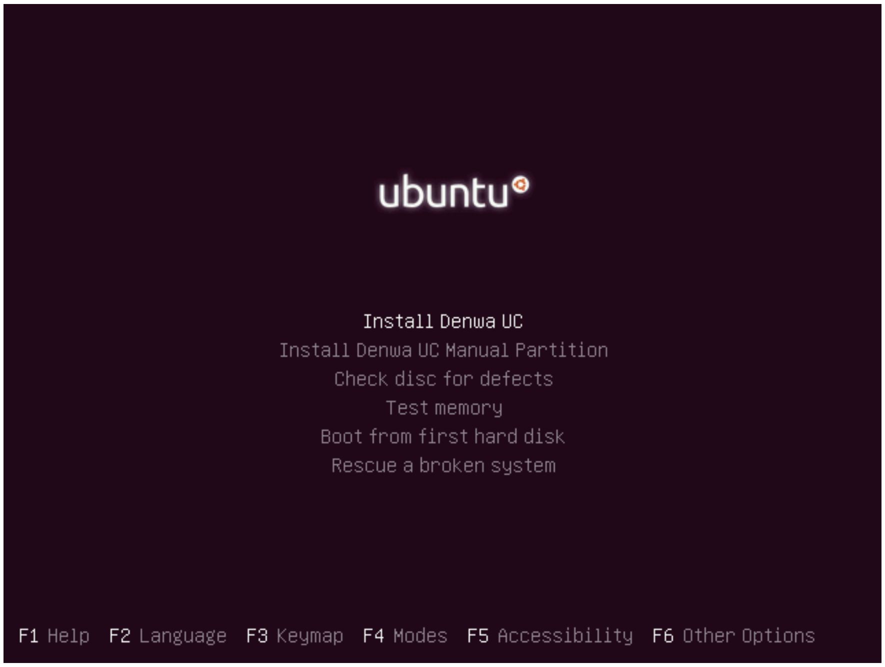
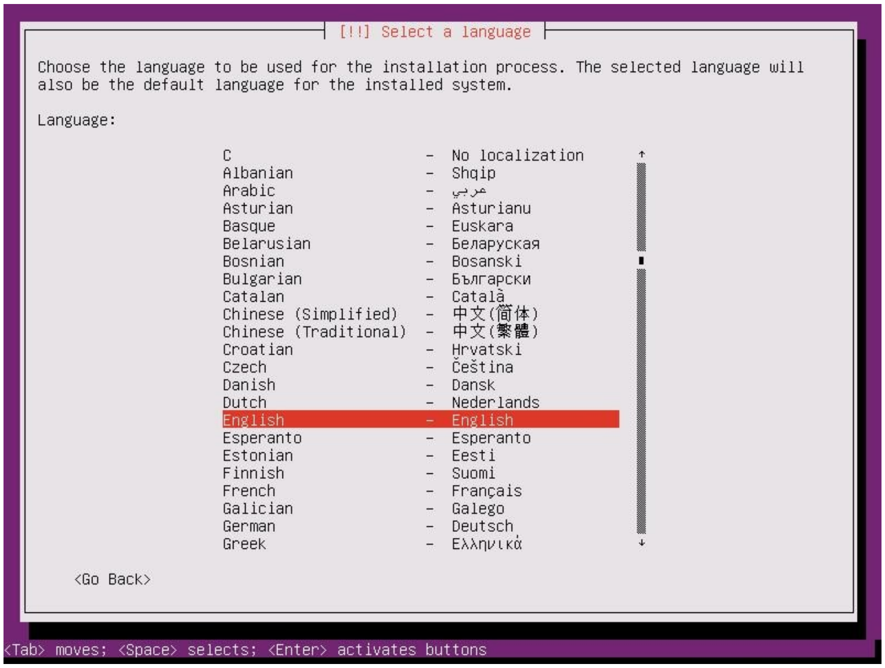

ubuntu
Install Denwa UC
Install Denwa UC Manual Partition
Check disc for defects
Test memory
Boot from first hard disk
Rescue a broken system
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

Figure 2.6: Base operating system installation

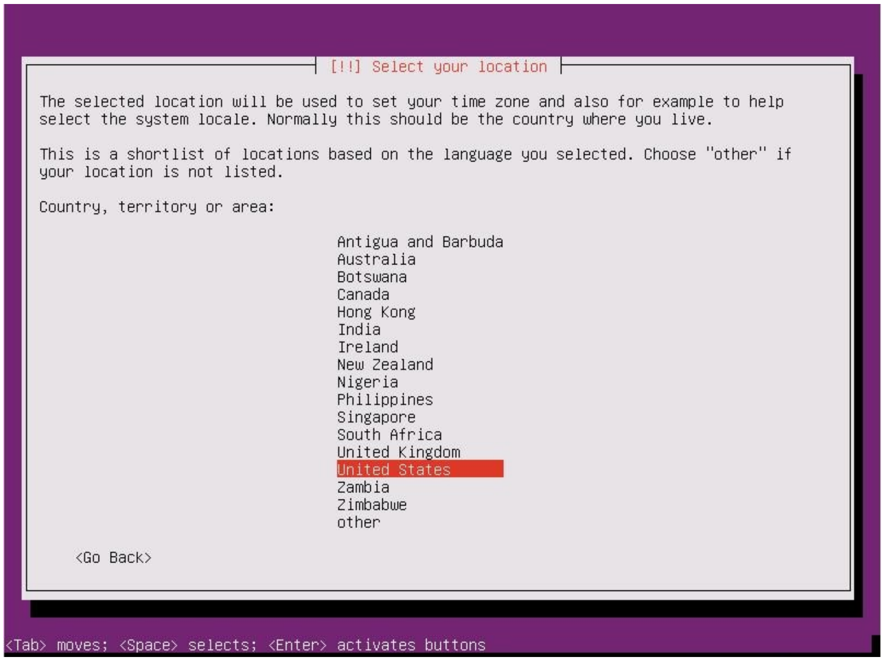
Then you will have to select the installation language of the base operating system; once again, we recommend always using English, because all our reference documentation is in English.



```
[!!] Select a language

Choose the language to be used for the installation process. The selected language will
also be the default language for the installed system.

Language:

                    C                       -  No localization
                    Albanian                -  Shqip
                    Arabic                  -  عربي
                    Asturian                -  Asturianu
                    Basque                  -  Euskara
                    Belarusian              -  Беларуская
                    Bosnian                 -  Bosanski
                    Bulgarian               -  Български
                    Catalan                 -  Català
                    Chinese (Simplified)    -  中文(简体)
                    Chinese (Traditional)   -  中文(繁體)
                    Croatian                -  Hrvatski
                    Czech                   -  Čeština
                    Danish                  -  Dansk
                    Dutch                   -  Nederlands
                    English                 -  English
                    Esperanto               -  Esperanto
                    Estonian                -  Eesti
                    Finnish                 -  Suomi
                    French                  -  Français
                    Galician                -  Galego
                    German                  -  Deutsch
                    Greek                   -  Ελληνικά

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 2.7: Operating system installation: selecting language

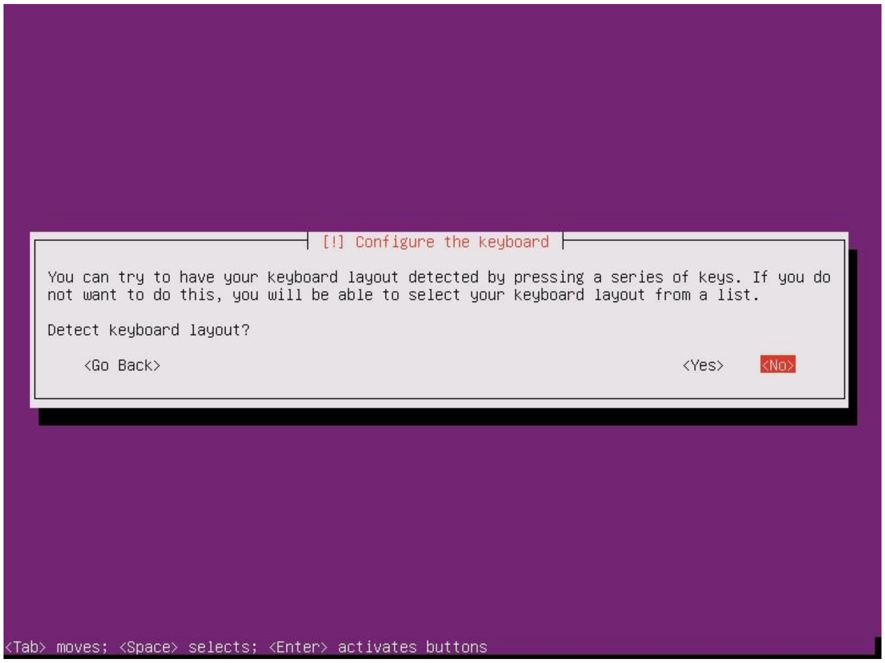
In the next step you will select the location, city, region or country,



```
[!!] Select your location

The selected location will be used to set your time zone and also for example to help
select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if
your location is not listed.

Country, territory or area:

                                  Antigua and Barbuda
                                  Australia
                                  Botswana
                                  Canada
                                  Hong Kong
                                  India
                                  Ireland
                                  New Zealand
                                  Nigeria
                                  Philippines
                                  Singapore
                                  South Africa
                                  United Kingdom
                                  United States
                                  Zambia
                                  Zimbabwe
                                  other

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 2.8: Operating system installation: selecting city, region or country

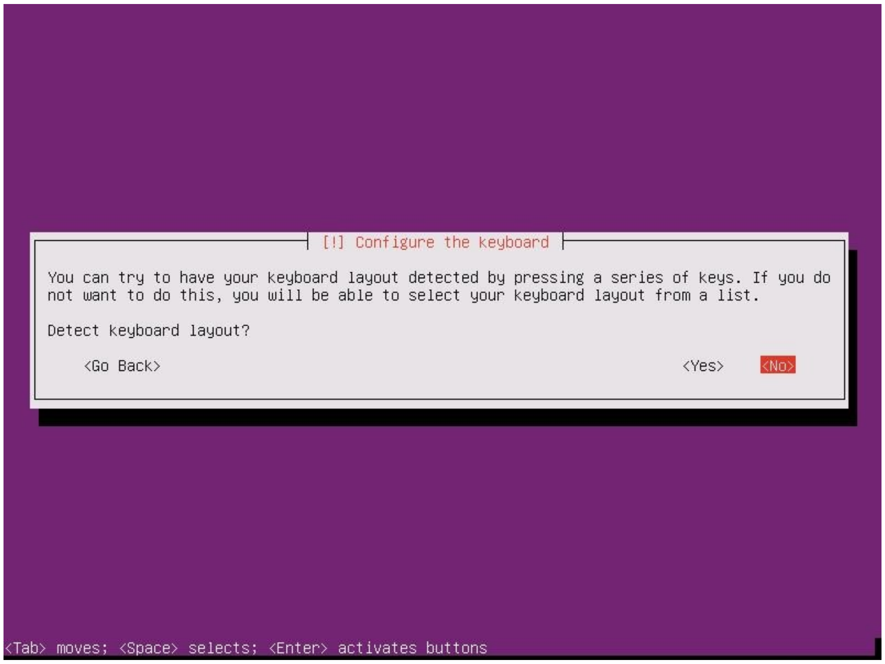
Next you will be asked whether you want to run the keyboard layout wizard. We recommend running it, since it will allow the user to sort out problems by pressing a few keys when entering the computer using the monitor and keyboard.



```
[!] Configure the keyboard

You can try to have your keyboard layout detected by pressing a series of keys. If you do
not want to do this, you will be able to select your keyboard layout from a list.

Detect keyboard layout?

    <Go Back>                                                      <Yes>    <No>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

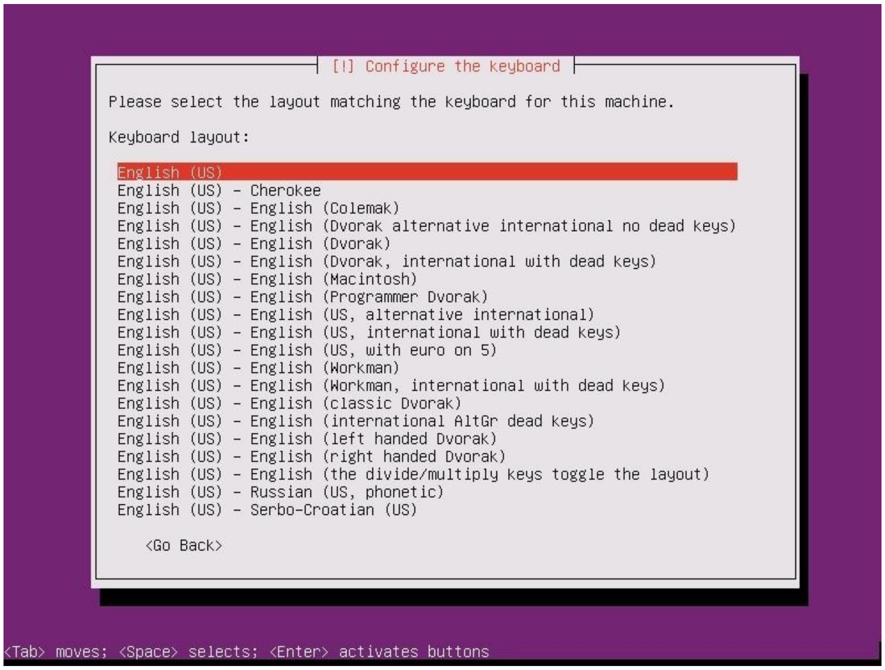
Figure 2.9: Operating system installation: keyboard layout wizzard

Otherwise, you will be presented with a list of all possible keyboard layouts for you to select one from the list. By default, the «English (US)» option is selected



```
[!] Configure the keyboard

You can try to have your keyboard layout detected by pressing a series of keys. If you do
not want to do this, you will be able to select your keyboard layout from a list.

Detect keyboard layout?

    <Go Back>                                                          <Yes>    <No>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

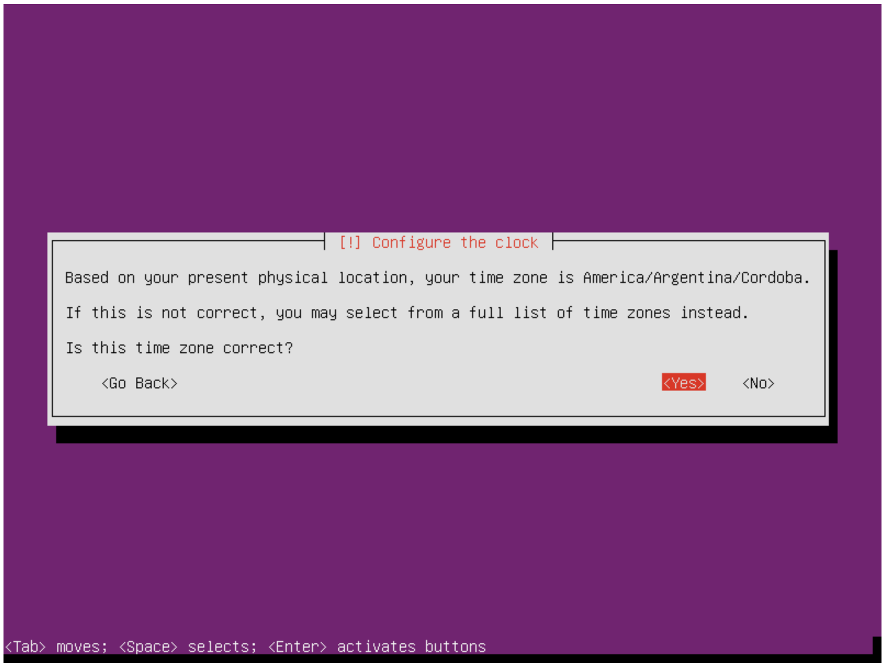
Figure 2.10: Operating system installation: list of languages and countries



```
[!] Configure the keyboard

Please select the layout matching the keyboard for this machine.

Keyboard layout:

 English (US)
 English (US) - Cherokee
 English (US) - English (Colemak)
 English (US) - English (Dvorak alternative international no dead keys)
 English (US) - English (Dvorak)
 English (US) - English (Dvorak, international with dead keys)
 English (US) - English (Macintosh)
 English (US) - English (Programmer Dvorak)
 English (US) - English (US, alternative international)
 English (US) - English (US, international with dead keys)
 English (US) - English (US, with euro on 5)
 English (US) - English (Workman)
 English (US) - English (Workman, international with dead keys)
 English (US) - English (classic Dvorak)
 English (US) - English (international AltGr dead keys)
 English (US) - English (left handed Dvorak)
 English (US) - English (right handed Dvorak)
 English (US) - English (the divide/multiply keys toggle the layout)
 English (US) - Russian (US, phonetic)
 English (US) - Serbo-Croatian (US)

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 2.11: Operating system installation: keyboard distribution list by language and country

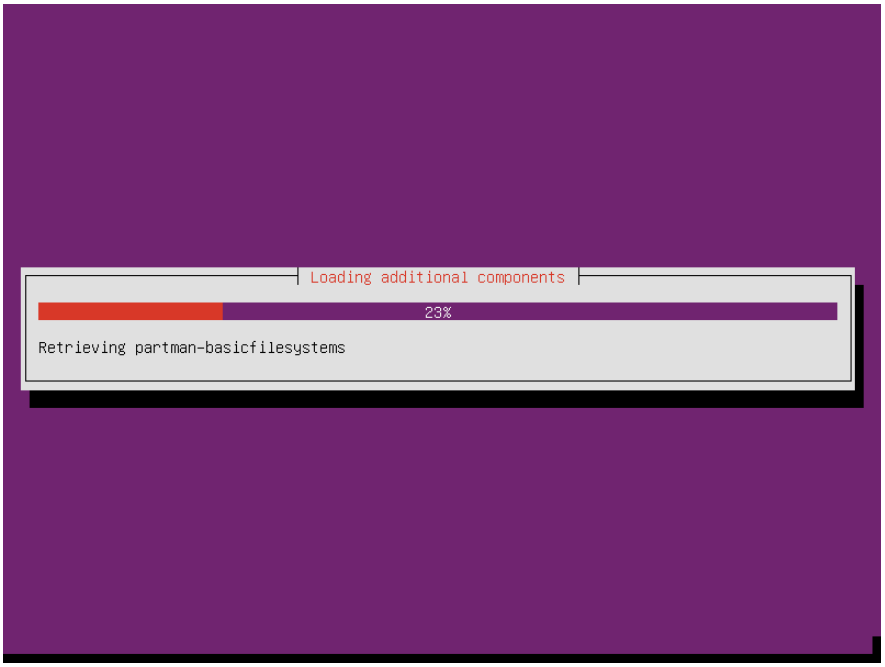
Then, if the equipment has an active internet connection, the time zone in which the installation is being performed will be automatically detected. Presiones «Yes» to validate the detected time zone or «No» to select it from a list.



```
[!] Configure the clock

Based on your present physical location, your time zone is America/Argentina/Cordoba.

If this is not correct, you may select from a full list of time zones instead.

Is this time zone correct?
```

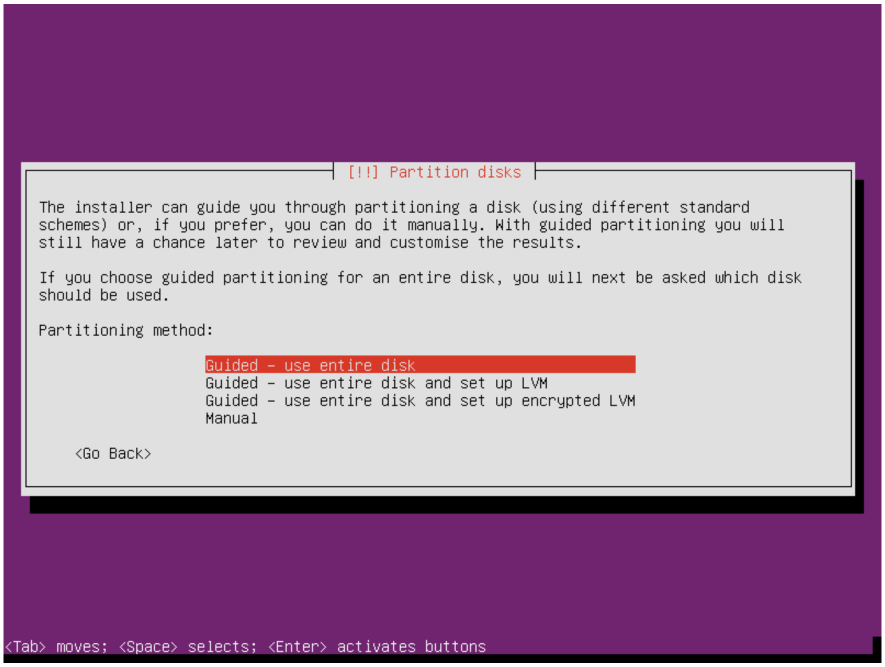
Figure 2.12: Operating system installation: confirming time zone

Once this is done, disk detection and partitioning will start. If you have selected the «Install Denwa UC» option, it will be enough to select the «Guided - use entire disk» option. You will be asked to confirm the disk on which partitioning will be performed.



```
Loading additional components

23%

Retrieving partman-basicfilesystems
```

Figure 2.13: Operating system installation: detecting disks



```
[!!] Partition disks

The installer can guide you through partitioning a disk (using different standard
schemes) or, if you prefer, you can do it manually. With guided partitioning you will
still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk
should be used.

Partitioning method:

                   Guided - use entire disk
                   Guided - use entire disk and set up LVM
                   Guided - use entire disk and set up encrypted LVM
                   Manual

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Figure 2.14: Operating system installation: partitioning method

Customized partitioning

If you have selected the custom partitioning option, the following considerations must be taken into account:

- All partitions, except the «swap» partition, must be of type «ext4»
- At least the following partitions must be created:
  - «\boot» on the solid state disk, for the system boot files.
  - «\\» on the solid state disk, for the base Operating System (20GB minimum, 30 GB recommended), for:
    - Operating System
    - System Logs
    - Operating System user folders («pbxadmin», «Denwa Support»)
    - Module files
  - «**swap**»on the solid state disk, 2GB to 8GB recommended, depending on the equipment (request Denwa Technology Corp. Support)
  - «\denwa» on the solid state disk, for all the processes associated with the telephony engine.
    - Telephony Engine
    - Databases
    - Web interface
    - Recordings to be transferred to the FTP Server (if any)
  - «\persistent» on the mechanical disk (if any) for local storage of call recordings

Now you only need to wait a few minutes for the installation to finish, and it may be possible (in case the installation is done by means of a bootable pen drive) to select the disk where the boot loader will be implemented. We recommend selecting the same device as in the previous step.

This part of the process will end when you are asked to reboot the computer and remove the removable installation media.

2.4 Unified communications system installation

After rebooting, enter the equipment again with the following credentials:

- **User:** pbxadmin
- **Password:** pbxadmin

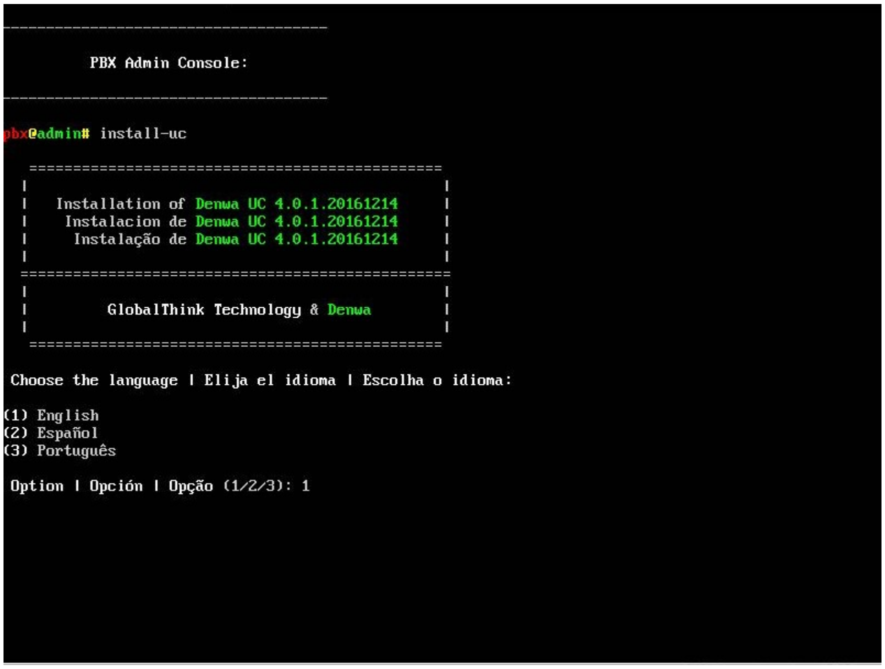
There is no Prompt

If, once the equipment has restarted, there is no system prompt, press Control, Alt and a function key. For example:

```
Ctrl + Alt + F2
```

Once the session has started, a command must be executed to initiate the unified communications system installation process:

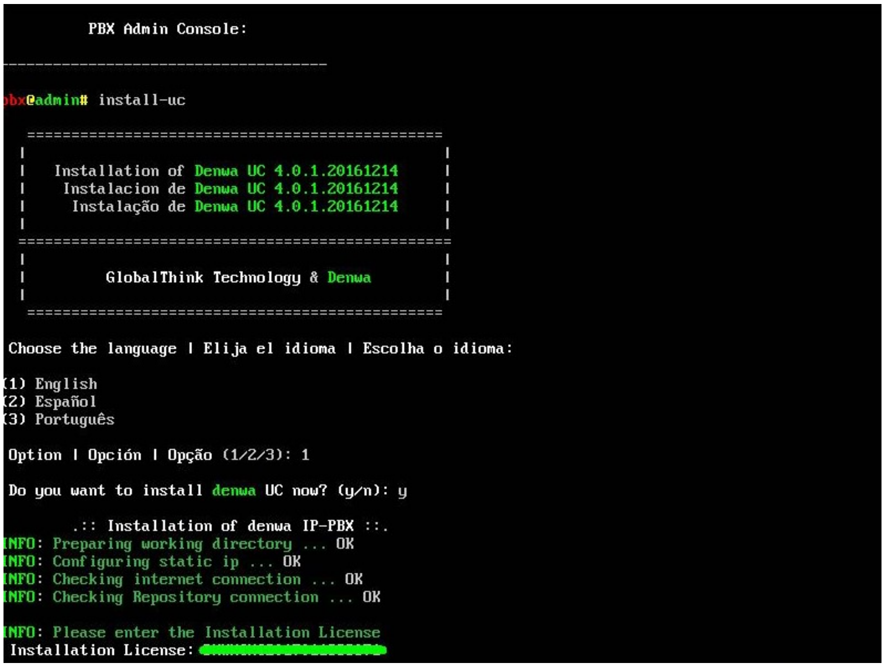
```
all-uc
```



```
-------------------------------------

         PBX Admin Console:

-------------------------------------

pbx@admin# install-uc

   ===============================================
  |                                               |
  |   Installation of Denwa UC 4.0.1.20161214     |
  |    Instalacion de Denwa UC 4.0.1.20161214     |
  |     Instalação de Denwa UC 4.0.1.20161214     |
  |                                               |
  =================================================
  |                                               |
  |         GlobalThink Technology & Denwa        |
  |                                               |
   ===============================================

 Choose the language | Elija el idioma | Escolha o idioma:

(1) English
(2) Español
(3) Português

 Option | Opción | Opção (1/2/3): 1
```

Figure 2.15: Unified communications system installation

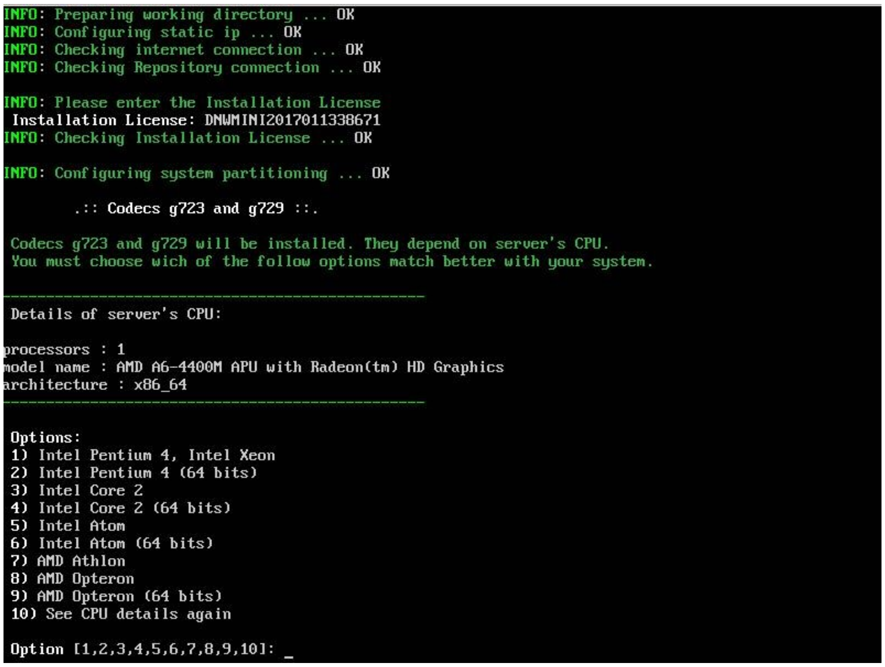
First, you will be asked the installation language of the unified communications system (language to be displayed in the web interface and through SSH access) you prefer, and, after validating the connectivity to the Denwa Technology Corp. repositories (either through the Internet or through the distributor's local repository), the installation license number will be requested.



```
         PBX Admin Console:

-------------------------------------

pbx@admin# install-uc

  ===============================================
 |                                               |
 |   Installation of Denwa UC 4.0.1.20161214     |
 |    Instalacion de Denwa UC 4.0.1.20161214     |
 |     Instalação de Denwa UC 4.0.1.20161214     |
 |                                               |
 =================================================
 |                                               |
 |         GlobalThink Technology & Denwa        |
 |                                               |
  ===============================================

 Choose the language | Elija el idioma | Escolha o idioma:

(1) English
(2) Español
(3) Português

 Option | Opción | Opção (1/2/3): 1

 Do you want to install denwa UC now? (y/n): y

        .:: Installation of denwa IP-PBX ::.
INFO: Preparing working directory ... OK
INFO: Configuring static ip ... OK
INFO: Checking internet connection ... OK
INFO: Checking Repository connection ... OK

INFO: Please enter the Installation License
 Installation License: [redacted]
```

Figure 2.16: Unified communications system installation: installation license

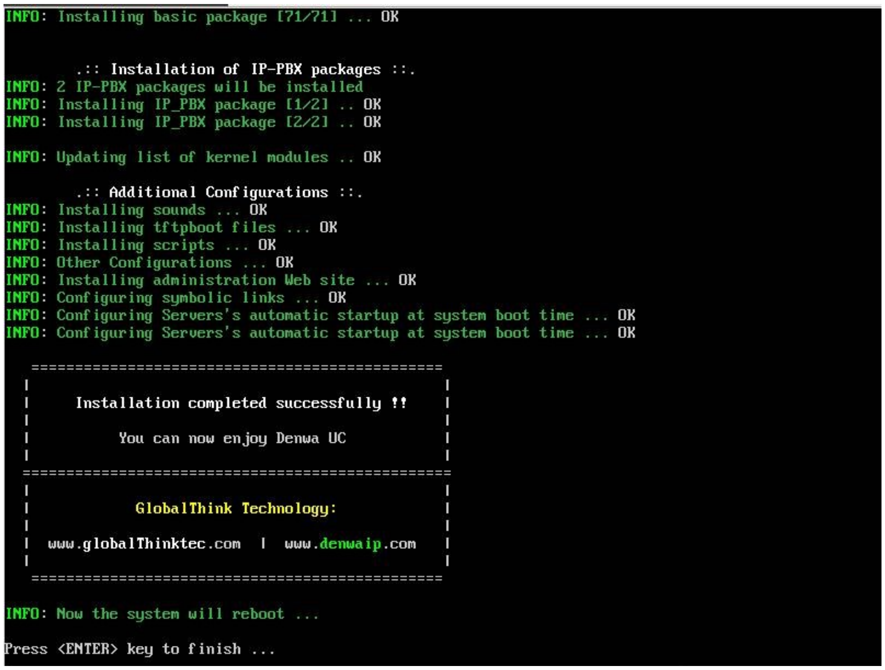
The following step will not be necessary when installing the unified communications system on a physical computer. However, in virtual environments, you will have to provide the processor version or family.



```
INFO: Preparing working directory ... OK
INFO: Configuring static ip ... OK
INFO: Checking internet connection ... OK
INFO: Checking Repository connection ... OK

INFO: Please enter the Installation License
 Installation License: DNWMINI2017011338671
INFO: Checking Installation License ... OK

INFO: Configuring system partitioning ... OK

        .:: Codecs g723 and g729 ::.

 Codecs g723 and g729 will be installed. They depend on server's CPU.
 You must choose wich of the follow options match better with your system.

------------------------------------------------
 Details of server's CPU:

processors : 1
model name : AMD A6-4400M APU with Radeon(tm) HD Graphics
architecture : x86_64
------------------------------------------------

 Options:
 1) Intel Pentium 4, Intel Xeon
 2) Intel Pentium 4 (64 bits)
 3) Intel Core 2
 4) Intel Core 2 (64 bits)
 5) Intel Atom
 6) Intel Atom (64 bits)
 7) AMD Athlon
 8) AMD Opteron
 9) AMD Opteron (64 bits)
 10) See CPU details again

 Option [1,2,3,4,5,6,7,8,9,10]: _
```

Figure 2.17: Unified communications system: processor family

From this point on, you just wait for the download, installation and configuration of the different software packages required for the unified communications system to be completed. Once finished, just press «Enter» and the computer will restart.



```
INFO: Installing basic package [71/71] ... OK

        .:: Installation of IP-PBX packages ::.
INFO: 2 IP-PBX packages will be installed
INFO: Installing IP_PBX package [1/2] .. OK
INFO: Installing IP_PBX package [2/2] .. OK

INFO: Updating list of kernel modules .. OK

        .:: Additional Configurations ::.
INFO: Installing sounds ... OK
INFO: Installing tftpboot files ... OK
INFO: Installing scripts ... OK
INFO: Other Configurations ... OK
INFO: Installing administration Web site ... OK
INFO: Configuring symbolic links ... OK
INFO: Configuring Servers's automatic startup at system boot time ... OK
INFO: Configuring Servers's automatic startup at system boot time ... OK

  ===============================================
  |                                             |
  |     Installation completed successfully !!  |
  |                                             |
  |          You can now enjoy Denwa UC         |
  |                                             |
 =================================================
  |                                             |
  |             GlobalThink Technology:         |
  |                                             |
  |  www.globalThinktec.com  |  www.denwaip.com |
  |                                             |
  ===============================================

INFO: Now the system will reboot ...

Press <ENTER> key to finish ...
```

Figure 2.18: Unified communications system installation: installation finished

2.5 Unified communications system activation

Now, the next step must be executed from the web interface of the unified communications system, so it is necessary to know the IP address of the equipment. Should you not know it (because it was configured by DHCP when installing the base operating system), it is possible to enter using two different methods:

- On the equipment console

  1. Login through the console with the pbxadmin user
  2. Execute the command

     ```
     ifconfig
     ```

  3. Check the IP address assigned to your equipment by the DHCP network server
  4. Using the web browser, enter the IP address obtained.

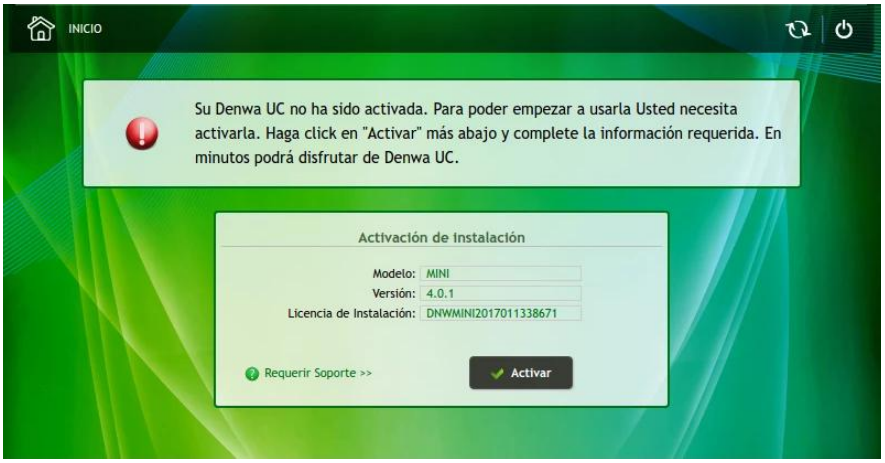
- Using the system predetermined IP

  1. Configure any network IP on your computer 10.10.10.0/24, except the 10.10.10.10
  2. Using the web browser, log into `http://10.10.10.10`

Once the login page has finished loading, log in using the following data:

- **User:** admin
- **Password:** admin
- **Profile:** Administrator

When you log in, you will see this screen



Su Denwa UC no ha sido activada. Para poder empezar a usarla Usted necesita activarla. Haga click en "Activar" más abajo y complete la información requerida. En minutos podrá disfrutar de Denwa UC.

Activación de instalación

Modelo: MINI
Versión: 4.0.1
Licencia de Instalación: DNWMINI2017011338671

Figure 2.19: Unified communications system activation: start screen

You just need to press the only button on the screen to display a form asking for contact information and the activation license. After entering the data, the license status will be validated and activated and any updates available will download.

Part II

Web Access

CHAPTER 3

ADMIN INTERFACE

The way to enter the PBX administration interface is through a web browser, such as: Mozilla Firefox, Google Chrome, Edge, Opera or Internet Explorer. However, our recommendation is to use Google Chrome, version 79 or higher.

3.1 Login Screen

Once the web browser is open, in the address bar you must enter the IP address of the unified communications system and the word «admin», for example: `http://192.168.0.1/admin`. Depending on the latest update installed, the login screen may change.

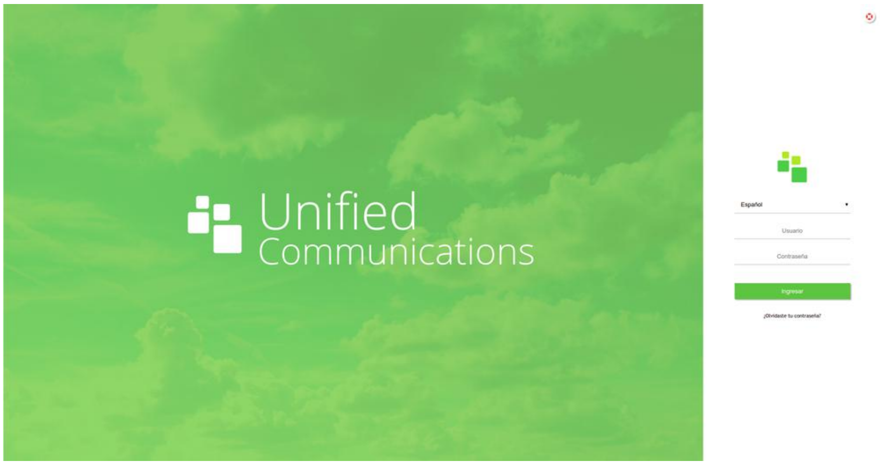
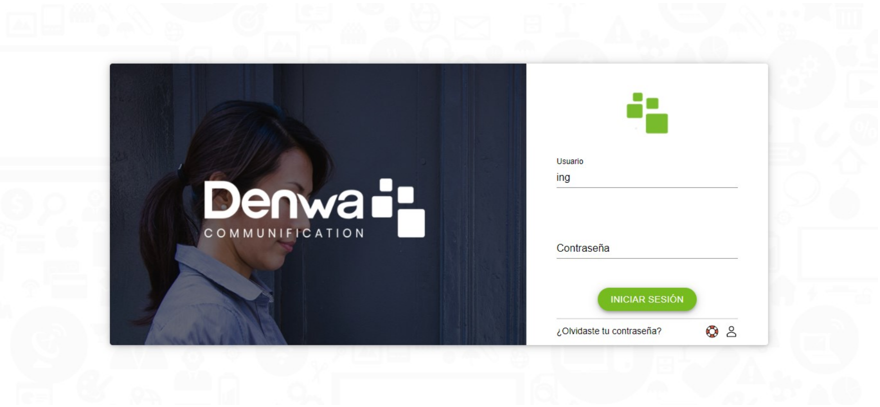


Figure 3.1: Login screen: Updates 001 to 004



Usuario
ing

Figure 3.2: Login screen: Updates 005 onwards

The default credentials are:

- **User**: admin

- **Password**: admin

There is no limit to the number of admin users that can be created and can access simultaneously

Number of administrators It is recommended to have a limited number of administrators and with differentiated access, as can be seen in the Administrators section, on the 102 page.

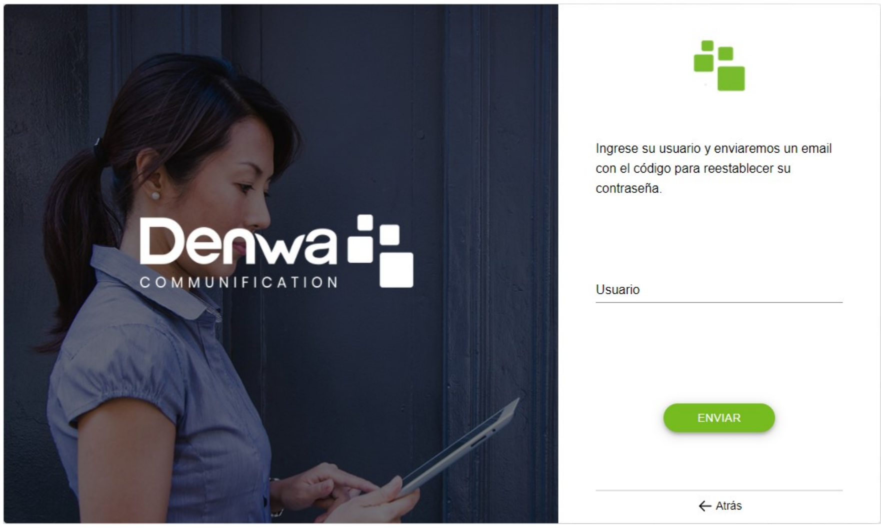
3.1.0.1 Password Recovery

In the event that you have an administrator type user and you have forgotten your password, it is possible to recover it; however, two (2) conditions must be met:

- That the unified communications system has its mail server properly configured (see section Mail Server Tab on the 97 page)

- That the administrator type user (who wants to recover his password) has an associated email address

With both conditions fulfilled, by clicking on the text «Forgot your password?» and entering the administration username, an email will be sent containing the code necessary to recover the password.



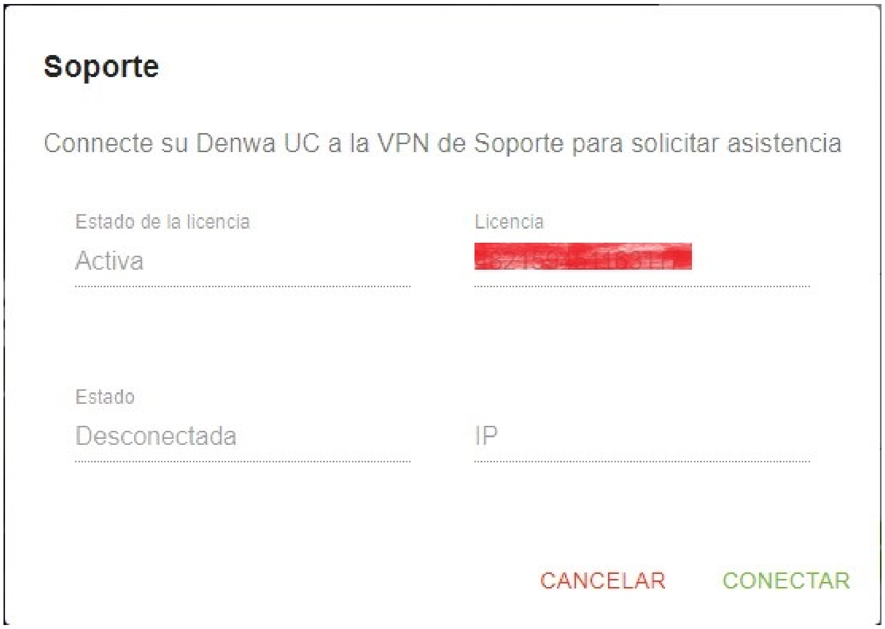
Ingrese su usuario y enviaremos un email con el código para reestablecer su contraseña.

Figure 3.3: Login screen: Password recovery

3.1.0.2 Support VPN Connection

In addition, the possibility of connecting the unified communications system to support has been added without the need for Administrator access, as long as Denwa UC&C 4.0.1 has Internet access.

By clicking on the icon in the shape of a life preserver, located under the login button on the login page, the administrator will open the following window:



Soporte

Connecte su Denwa UC a la VPN de Soporte para solicitar asistencia

Estado de la licencia: Activa

Licencia: [redacted]

Estado: Desconectada

IP

Figure 3.4: Login screen: Connection to Support VPN

In this window it is possible to see relevant information that the Denwa Technology Corp. Support area will request to process your request through the `http://support.denwaip.com` ticket system, namely:

- **License status**: Indicates if the equipment has an active support and updates contract

- **License**: Equipment activation license number
- **Status**: Status of the connection to the Denwa Technology Corp. Support VPN
- **IP**: IP address assigned within the Support VPN

In the event that the field called «Status» indicates that Denwa UC&C 4.0.1 is «Disconnected», you must click on the «Connect» button and wait a few seconds to obtain an IP address to provide to the Support area of Denwa Technology Corp.

3.2 Home Screen

By default, the unified communications system dashboard will be displayed, which will be discussed below.

Options to display

The administrator type user assigned to you may not be able to view all of the menu items described below. If you consider that, due to your functions and abilities, you should have greater privileges, ask your Denwa UC&C 4.0.1 administrator.

3.2.1 Board

Shows relevant system information in card format, indicating:

- **Time**: Parameters of the base operating system used by Denwa UC&C 4.0.1
  - System Date
  - System uptime
- **Update Status**: Shows whether all Denwa UC&C 4.0.1 items are updated to their most recent version; Otherwise, the lower line will be shown in another color, indicating that an action is required on the system.
  - Denwa UC Updates
  - Device firmware updates
- **Active Calls**: Shows a graph representing the number of calls in progress in the last twenty (20) minutes.
- **Classification of incoming calls**: Using a stackable bar graph, it shows the total number of calls in the last eight (8) days, broken down by:
  - Attended
  - not attended
- **Partition status**: Represents the occupancy status in each of the Denwa UC&C 4.0.1 partitions
  - **System**: Normally located on the solid state drive, for the base Operating System, and contains:
    - Operating System
    - System logs
    - Operating System user folders («pbxadmin», «Denwa Support»)
    - Module files

- **Applications**: Usually the solid state disk, for all the processes associated with the telephony engine, that is:
  - Telephony Engine
  - Databases
  - Web interface
  - Recordings to be transferred to the FTP Server (if any)
- **Data**: Only on the mechanical disk (if any) for local storage of call recordings

Availability of partitions

Depending on the computer model and the number of storage devices available, the graphics will be active or inactive.

- **Password security level**: In case of having vulnerable passwords, indicate the number of them.
- **Status of services**
  - Telephony
  - Information DHCP SNMP
  - NTP
  - Messaging
- **Use of storage devices by type of data**: This card summarizes the space used on the disk according to the type of data.
  - Database
  - Logs
  - Backup
  - Recordings
  - Transfers to FTP
  - Voicemail
  - Network Captures
- **State of *Firewall Policies***: Policies are the default response to any connection that does not meet criteria that have been declared as «exceptions».
- **Status of *Firewall services***
  - ***Firewall***: *Firewall* service
  - **Failed attempts**: Service that blocks access from an origin that has failed in its credentials for any type of connection in a defined period of time (see «Firewall», on page pagereffail2ban)
  - **Portscanning**: Service that blocks access from an origin where an attempt to scan ports on Denwa UC&C 4.0.1 has come from (see «Firewall», on page 122)
- **HTTPS enablement status**
- **Number of calls in the last three (3) months**

3.2.2 Users

Shows the list of all Denwa UC&C 4.0.1 users, indicating:

- **General**: Name given to the user
- **Mobile**: User's mobile phone number
- **Extension**: Extension number in Denwa UC&C 4.0.1
- **Mode**:

3.2.3 Advanced Interface

This element is a shortcut to the previous version of the Denwa UC&C 4.0.1 administration web interface. You can see all its content in the Advanced Interface section, starting on the 32 page.

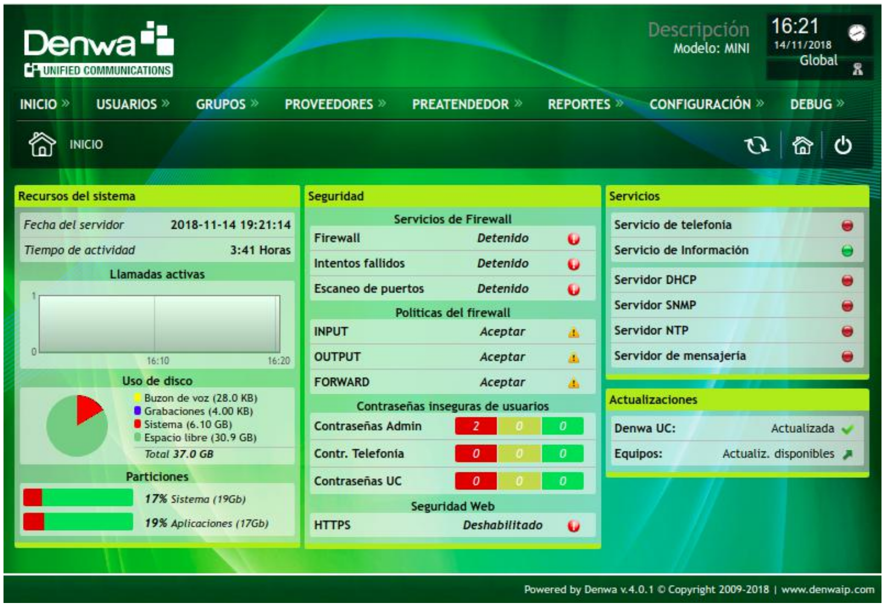
3.2.4 Logout

3.3 Advanced Interface

> **Options to display**
>
> The administrator type user assigned to you may not be able to view all of the menu items described below. If you consider that, due to your functions and abilities, you should have greater privileges, ask your Denwa UC&C 4.0.1 administrator.

3.3.1 Home

When logging in with the Administrator profile, the PBX web interface configuration Home tab is observed. You can find data on server status, information on active services, disk usage statistics and more from Denwa UC&C 4.0.1 .



Recursos del sistema

Fecha del servidor	2018-11-14 19:21:14
Tiempo de actividad	3:41 Horas

Llamadas activas

Uso de disco

- Buzon de voz (28.0 KB)
- Grabaciones (4.00 KB)
- Sistema (6.10 GB)
- Espacio libre (30.9 GB)

Total 37.0 GB

Particiones

- **17%** *Sistema (19Gb)*
- **19%** *Aplicaciones (17Gb)*

Seguridad

Servicios de Firewall		
Firewall	*Detenido*	●
Intentos fallidos	*Detenido*	●
Escaneo de puertos	*Detenido*	●

Politicas del firewall		
INPUT	*Aceptar*	⚠
OUTPUT	*Aceptar*	⚠
FORWARD	*Aceptar*	⚠

Contraseñas inseguras de usuarios			
Contraseñas Admin	2	0	0
Contr. Telefonia	0	0	0
Contraseñas UC	0	0	0

Seguridad Web		
HTTPS	*Deshabilitado*	●

Servicios

Servicio de telefonia	🟥
Servicio de Información	🟩
Servidor DHCP	🟥
Servidor SNMP	🟥
Servidor NTP	🟥
Servidor de mensajeria	🟥

Actualizaciones

Denwa UC:	Actualizada ✓
Equipos:	Actualiz. disponibles ↗

Figure 3.5: Advanced Interface: Home Screen

This page offers the following information expressed in boxes.

- **System Resources**: For more details you can go to Reports > System Resources, or to the System Resources section on the 90 page.
  - **Server Date**: current date and time of the panel.
  - **Activity Time**: Elapsed time since the last time the computer was turned on.
  - **Active calls**: allows you to graphically display the calls made in the last 20 minutes.
  - **Disk Usage**: voicemail, recordings, system, free and total space.
  - **Partitions**: Percentage of use of system partitions.
- **Security**: Indicator and alert of the states in the security schemes at Denwa UC
  - **Firewall Services**: Shows the status of the firewall, failed attempts and port scans.
  - **Firewall Policies**: INPUT, OUTPUT and FORWARD.
  - **Insecure user passwords**: Color-coded status of administrator, telephony, and UC passwords.
  - **Web Security**: Shows the status of HTTPS.
- **Services**: Services status indicator (in green if they are active, and in red if they are deactivated)
  - Telephone service
  - Information Service
  - DHCP server
  - SNMP server
  - NTP Server
  - Messaging server
- Updates
  - **Denwa UC**: indicates if there are updates available for Denwa UC&C 4.0.1 (Settings > Support)
  - **Equipment**: indicates whether there are updates available for approved telephone equipment (Settings > Equipment > Models)

Alerts for disk occupation

When the disk capacity reaches 70%, the system sends an email to the platform administrator-type users, informing that one or more of the system partitions has crossed the threshold (this task is performed once every hour). For these alerts to function correctly, the email server must be previously configured in Configuration > General > Mail Server (see section Mail Server Tab on the 97 page).

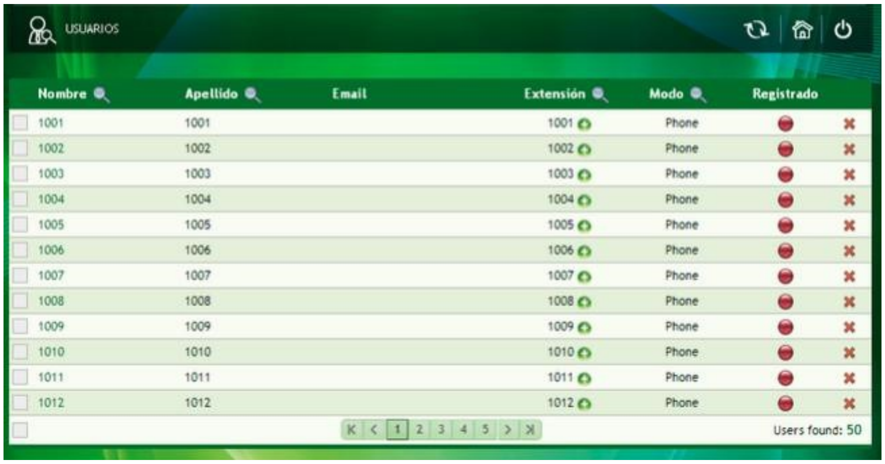
3.3.2 Users

From the Users tab you can select various actions, which will be explained below.

3.3.2.1 View Users

This option allows you to see the complete list of users created, along with their Name, Surname, Email, Extension, Mode and Registration Status. If the extension is registered, placing the mouse over the green circle displays the IP number of the associated telephone.

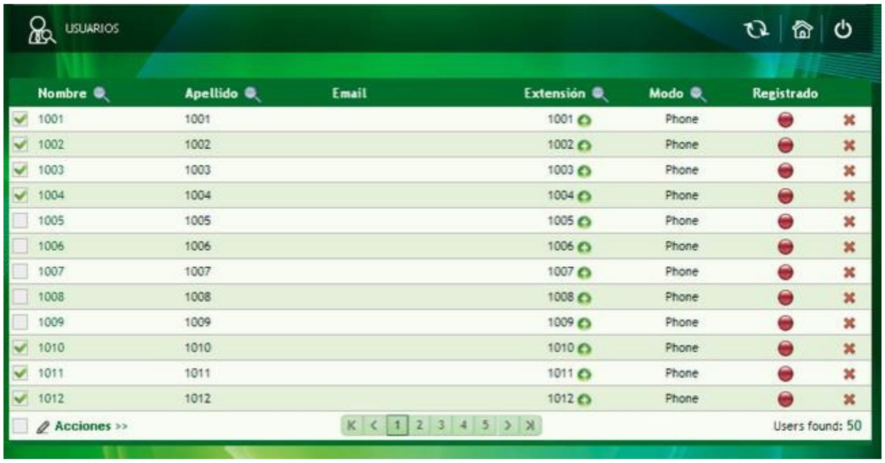
It is also possible to delete and edit users individually directly. To delete a user, it is only necessary to click on the X-shaped icon (✖). While to edit it you must click on the Name of the desired user.



	Nombre	Apellido	Email	Extensión	Modo	Registrado	
□	1001	1001		1001	Phone	●	✖
□	1002	1002		1002	Phone	●	✖
□	1003	1003		1003	Phone	●	✖
□	1004	1004		1004	Phone	●	✖
□	1005	1005		1005	Phone	●	✖
□	1006	1006		1006	Phone	●	✖
□	1007	1007		1007	Phone	●	✖
□	1008	1008		1008	Phone	●	✖
□	1009	1009		1009	Phone	●	✖
□	1010	1010		1010	Phone	●	✖
□	1011	1011		1011	Phone	●	✖
□	1012	1012		1012	Phone	●	✖
□			K < 1 2 3 4 5 > X			Users found: 50	

Figure 3.6: Advanced interface: View users

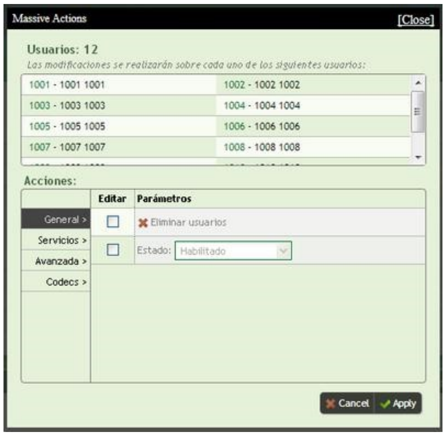
3.3.2.1.1 Multiple edit It is also possible to perform a multiple selection of users. To do this, it is necessary to select at least two users (click on the boxes to the left of the user's name). Then you must access the Actions menu, which is located in the lower left corner of the screen.



	Nombre	Apellido	Email	Extensión	Modo	Registrado	
☑	1001	1001		1001	Phone	●	✖
☑	1002	1002		1002	Phone	●	✖
☑	1003	1003		1003	Phone	●	✖
☑	1004	1004		1004	Phone	●	✖
□	1005	1005		1005	Phone	●	✖
□	1006	1006		1006	Phone	●	✖
□	1007	1007		1007	Phone	●	✖
□	1008	1008		1008	Phone	●	✖
□	1009	1009		1009	Phone	●	✖
☑	1010	1010		1010	Phone	●	✖
☑	1011	1011		1011	Phone	●	✖
☑	1012	1012		1012	Phone	●	✖
□	Acciones >>		K < 1 2 3 4 5 > X			Users found: 50	

Figure 3.7: Advanced interface: View users, multiple selection

In the popup window, the settings of the selected users are displayed, which are a reduced version of what can be found in the New User option.



Usuarios: 12

Las modificaciones se realizarán sobre cada uno de los siguientes usuarios:

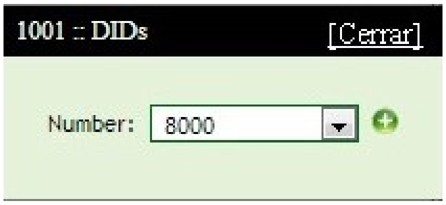
1001 - 1001 1001	1002 - 1002 1002
1003 - 1003 1003	1004 - 1004 1004
1005 - 1005 1005	1006 - 1006 1006
1007 - 1007 1007	1008 - 1008 1008

Acciones:

Editar	Parámetros
□	✖ Eliminar usuarios
□	Estado: Habilitado

Figure 3.8: Advanced interface: View users, multiple editing

3.3.2.1.2 Assignment of accession numbers In addition, DIDs (access numbers) can be assigned to extensions by clicking the plus icon (⊕) to the right of the extension number. This action will display a window like the following:



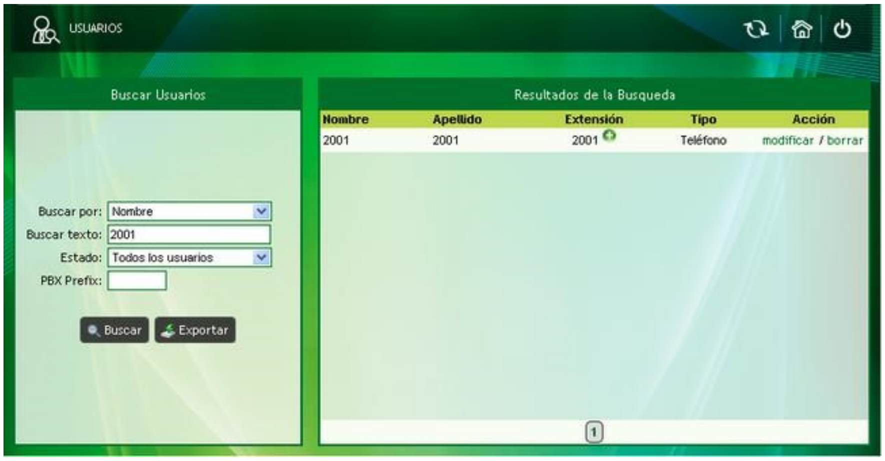
Number: 8000

Figure 3.9: Advanced interface: View users, assigning access numbers

After selecting it, it will be associated to the extension by clicking on the plus icon (⊕). On the other hand, if what you want is to delete the relationship, you must click on the subtraction symbol (−). All changes will be saved by clicking on «[Close]».

3.3.2.2 Search Users

From this option you can search for users by: name, surname, extension, type and DID (access number). Also, it allows you to search for both registered and unregistered users; or by some particular indicative text or prefix. This tool simplifies tasks when you have a large number of inmates.



Buscar por: Nombre
Buscar texto: 2001
Estado: Todos los usuarios
PBX Prefix:

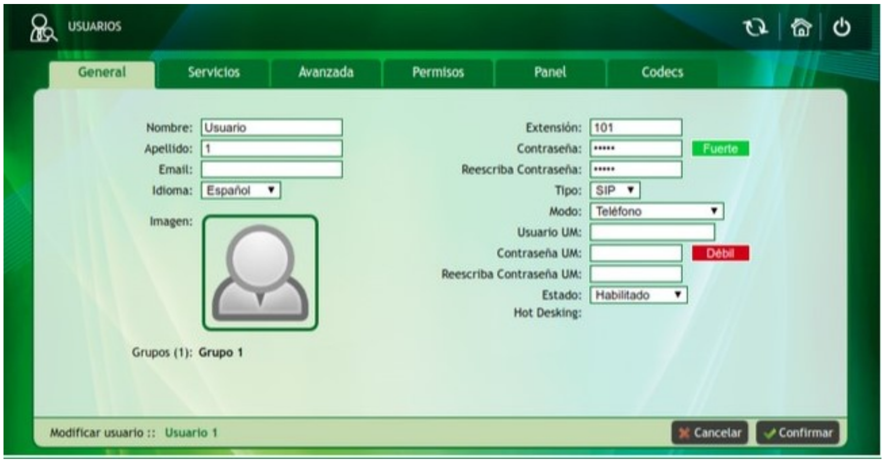
Nombre	Apellido	Extensión	Tipo	Acción
2001	2001	2001	Teléfono	modificar / borrar

Figure 3.10: Advanced interface: Find users

User search Users can also be searched from the screen where all users are listed (see section View Users on page 34), by clicking on the 🔍 icon located in the table header.

The search result is seen in the right pane. From here you can also make user settings, that is, edit, delete and/or add a DID.

3.3.2.2.1 Modify allows you to edit the user's configuration. Clicking on this option displays the Modify User window. This window is identical (except that it already has information) to the user registration window (see section New User on the 36 page). This screen can also be accessed by clicking on the name of the user in the View Users listing on the 34 page.



Nombre: Usuario
Apellido: 1
Email:
Idioma: Español
Imagen:
Grupos (1): Grupo 1
Extensión: 101
Contraseña: •••••
Reescriba Contraseña: •••••
Tipo: SIP
Modo: Teléfono
Usuario UM:
Contraseña UM:
Reescriba Contraseña UM:
Estado: Habilitado
Hot Desking:
Modificar usuario :: Usuario 1

Figure 3.11: Advanced Interface: Modify User

3.3.2.2.2 Delete allows users to be deleted. After clicking on this item, the View Users window is displayed.

3.3.2.3 New User

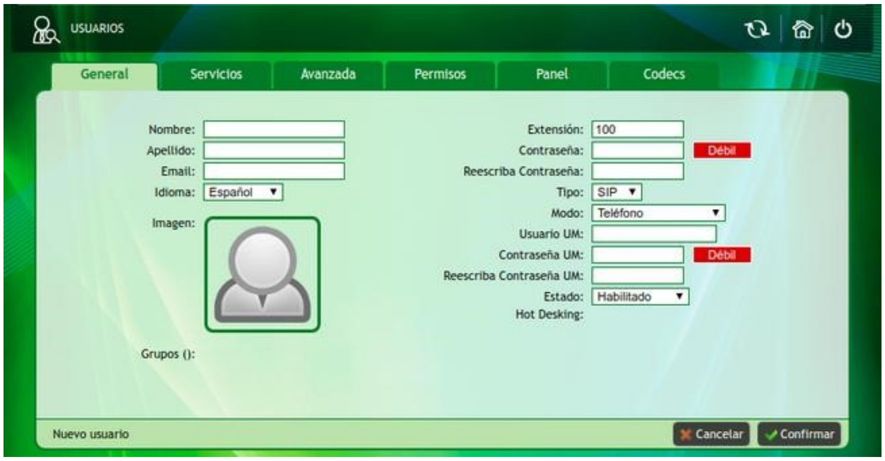
The New User menu allows you to generate a new extension, and make the pertinent configurations.

User limit Although theoretically there is no limit to the number of users, it is our recommendation not to exceed the number indicated in the different Technical Sheets of the products, which have been statistically estimated, considering the relationship between active calls (incoming, outgoing and between internal) and the number of platform users.

If you have any questions, consult the Denwa Technology Corp. Pre-sale area.

3.3.2.3.1 New User General Tab

The window that is displayed allows you to create or modify new users. The data to enter are the following:



Nombre:
Apellido:
Email:
Idioma: Español
Imagen:
Grupos ():

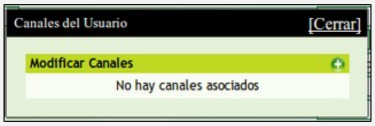
Extensión: 100
Contraseña:
Reescriba Contraseña:
Tipo: SIP
Modo: Teléfono
Usuario UM:
Contraseña UM:
Reescriba Contraseña UM:
Estado: Habilitado
Hot Desking:

Figure 3.12: Advanced interface: New user, general tab

- Personal data of the user
  - **Name**: name of the user assigned to the extension.
  - **LastName**: lastname of the user assigned to the extension.
  - **Email**: email address of the user assigned to the extension. In the event that the extension does not answer the call, the voicemails will be sent there.
  - **Language**: Select the language for the user.
  - **Image**: A profile image can be incorporated from Denwa Desktop.
  - **Group**: Shows the groups to which the user belongs.
- The extension number is defined together with its password and its mode. For a simple extension, phone mode is used; For call center agents, the telephone mode is also used.
  - **Extension**: Define the extension for the user. There is no limit to the number of digits for internal numbering
  - **Password**: the password of the user is defined. It must be strong, so it must be composed of uppercase, lowercase, numbers and special characters.
  - **Retype Password**: The user's password is confirmed.
  - **Type**: Allows you to select the type of extension, the options are SIP, FXS or IAX2.

FXS Extension

If FXS is chosen, the port associated with the extension must be selected. To do this, it is necessary to click on the ⚙icon.



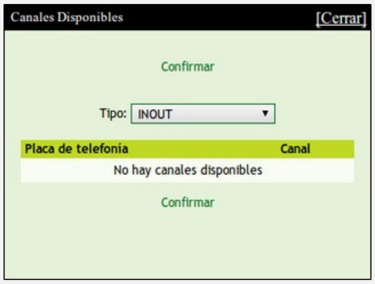
Canales del Usuario [Cerrar]

Modificar Canales ⊕

No hay canales asociados

Figure 3.13: Advanced interface: FXS-like user, user channels

Then, a click on the plus sign (⊕) will suffice to associate the channel.



Canales Disponibles [Cerrar]

Confirmar

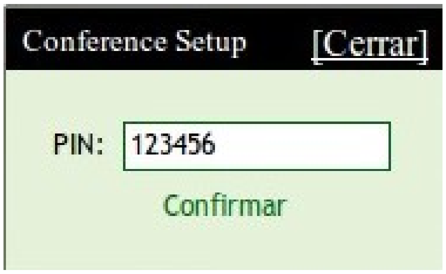
Tipo: INOUT

Placa de telefonia	Canal
No hay canales disponibles	

Confirmar

Figure 3.14: Advanced interface: FXS type user, available channels

- **Mode**:
  - **Phone**: VoIP extension for ATA, Softphone or IPPhone.
  - **Video Phone**: Phone with built-in video screen.
  - **FAX**: VoIP extension for ATA with FAX support.
  - **FAX to Email**: this mode makes it possible to receive FAXs from the Denwa Desktop portal of the associated users or their email boxes. To do this, a user must be created with the FAX to Email mode; its extension is virtual, because it will not be registered (in View User a red circle is displayed in Registered). Then, it is possible to assign users from the New User Advanced Tab. This assignment is what allows the reception of FAXs, in addition to the mailbox of the virtual extension, in that of the assigned users and their Denwa Desktop portals.
  - **Conference**: allows multimedia connection between two or more users. For which it is necessary to create a user with Conference mode; this extension is virtual for this reason it will not be registered (in View User a red circle is displayed in Registered). Once the user is created, the View User option next to the conference mode is displayed. By clicking on this icon the PIN must be defined. After dialing the extension, the user must dial this code to join the conference. There is no limit to creating conference extensions, and the number of users per conference room is limited to the number of concurrent calls.

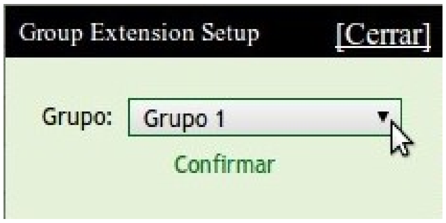


Conference Setup [Cerrar]

PIN: 123456

Figure 3.15: Advanced interface: Conference mode user

- **Group**: allows you to make calls to a group of users gathered in a group according to its configuration, go to View Group. For which a virtual extension must be created (in View User a red circle is displayed in Registered). Once the user is created, the View User option next to the Group mode displays . When executing a click on this icon, you must select the group to which the extension will be assigned and Confirm.



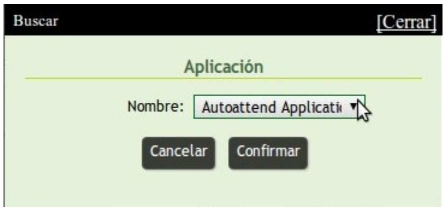
Group Extension Setup [Cerrar]

Grupo: Grupo 1

Figure 3.16: Advanced interface: User Group mode

- **Visitor**: makes it possible for people not belonging to the network to use the equipment registered in the network, that is, it is an extension that is generated to be able to make calls from any equipment. To do this, when creating the user in this mode, it is necessary to establish a security PIN. To make a call, you must validate your identity by calling *65, then enter the security PIN and finally the extension to call.
- **Parking**: Allows you to store incoming calls. When creating a parking user, it is necessary to assign a group of extensions to which the calls that cannot be answered at the moment will be transferred. The number of extensions that are assigned to the mode are the number of calls that can be stored. For this process to be possible, it is necessary to take the incoming call and then transfer it. When the call in progress ends, the PBX calls the user and notifies them in which parking extension the call was stored. To answer the call, you only have to dial the parking extension in which it was saved.
- **Doorphone**: allows you to manage calls to the door where the electric doorphone is located. For this it is necessary to create a new user with Doorman mode and confirm. Then you must enter View Users, click on the intercom extension, in the Services Tab you must configure the telephone extension that will ring when the intercom is called. The equipment provisioning must be done after the extension is created.
- **Intercom**: Allows you to configure an extension with this mode. Then, by checking the Enable Intercom option in the New User Permissions Tab, this functionality is available. This type of extension can receive calls and auto-attend the line with only one audio channel. This path is from the calling extension. It is used to make announcements or locate personnel. It is accessed by dialing *59 + EXT. FROM THE INTERCOM + SEND.
- **Call Center**: allows you to configure an extension to integrate third-party Call Centers. The call center is registered using this type of extension, the traffic of incoming calls will be balanced between the different teams.

  - **Dispatcher**: a dispatcher type extension will be generated and implemented for mass sending of Voice, FAX, Video and SMS messages.
  - **Video Security**: allows you to assign security equipment to an extension. You can also make calls from video phones to these extensions and view the activity in the place by connecting in promiscuous mode or with two-way audio.
  - **Preattender**: Allows you to create an extension that works as a preattendant.
  - **Application**: This mode allows you to call an application for execution. To do this, you must select the ⚙icon. The pop-up screen makes it possible to choose the desired application. Then, you must press Confirm and Close.



Nombre: Autoattend Applicati

Figure 3.17: Advanced interface: User Application mode

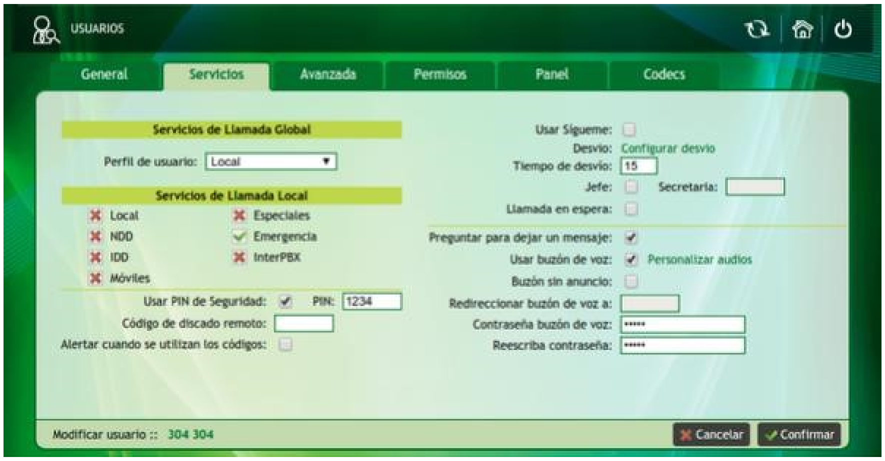
  - **Shared telephone**: an extension is created that can call any extension normally, but when you want to make another type of call (external for example), a remote dialing code is requested. This code is unique for each user. The user who wants to use a shared phone must enter his remote dial code. Configurations are made in the Services Tab (see section New User Services Tab on the 40 page) or from the Denwa Desktop portal (see section User Interface on page 157).
  - **Public Phone**: This option allows you to create an extension that can call normally, but the user is prompted for a remote dialing code. This code is unique for each user. The user who wants to use a public telephone must enter his remote dialing code. Configurations are made in the Services Tab (see section New User Services Tab on the 40 page) or from the Denwa Desktop portal (see section User Interface on page 157).

- Settings for Denwa Desktop (see section User Interface on the 157 page) and status of this extension.

  - **UM User**: UM (Unified Messaging) username.
  - **UM Password**: UM password. It must be strong, so it must be composed of uppercase, lowercase, numbers and special characters.
  - **Retype UM Password**: retype to confirm the UM password.
  - **Status**: a status is assigned to the extension
    - Enabled: calls can be made in and out of Denwa UC&C 4.0.1 .
    - Suspended: calls can only be made within Denwa UC&C 4.0.1 , but allows calls outside of it.
    - Disabled: you cannot make and receive any type of calls regardless of their destination.

3.3.2.3.2 New User Services Tab

From this tab you must determine the call services. Here you can configure the user's line according to the services that you want to enable.



Servicios de Llamada Global

Perfil de usuario: Local ▾

Servicios de Llamada Local

✗ Local
✗ NDD
✗ IDD
✗ Móviles
✗ Especiales
✓ Emergencia
✗ InterPBX

Usar PIN de Seguridad: ☑ PIN: 1234

Código de discado remoto:

Alertar cuando se utilizan los códigos: □

Usar Sigueme: □

Desvio: Configurar desvio

Tiempo de desvío: 15

Jefe: □ Secretaria:

Llamada en espera: □

Preguntar para dejar un mensaje: ☑

Usar buzón de voz: ☑ Personalizar audios

Buzón sin anuncio: □

Redireccionar buzón de voz a:

Contraseña buzón de voz: *****

Reescriba contraseña: *****

Modificar usuario :: 304 304

Figure 3.18: Advanced interface: New user, services tab

The fields that can be managed are the following.

- **Global Call Services**: allows the user to be assigned a profile, that is, a set of characteristics common to several users can be established; these can be configured in User Profiles (see section User Profiles on the 53 page). If there is no profile created, the Local profile is offered by default, that is, calls can be made 7 days a week, 24 hours a day.
- **Local Call Services**: allows you to manage permissions to make various types of calls. They can be enabled or allowed (✔), denied (✖) or protected by the Security Pin (🔒). In the event that you want all call services to be protected by Security PIN, it is recommended to check Use Security PIN. To configure the prefixes that correspond to each type of call, you must access Call Services (see Call service on page 126).
  - Local: local calls
  - NDD: national long distance
  - IDD: international long distance
  - Mobiles: calls to mobiles
  - Specials: calls to special services, such as 0800, 0810 and 0600, for example
  - Emergency: emergency numbers
  - InterPBX: calls to another telephone exchange connected by an intercon trunk

Sip interconn

Interconn-type trunks allow the interconnection of two telephone equipment, allowing their users to communicate with each other as if they were on the same equipment, in addition to sharing their other trunks. For example:
In the event that there are two (2) exchanges 200 and 300 connected through an interconn trunk, the 200 users can make calls to the outside using the 300 trunks, and vice versa.

- **Use Security PIN**: A PIN is used for each of the calls made by the user to request authorization. There are two use cases, for which the user must dial his PIN to make a call:
  1. When placing in the call services, it is not necessary to click on the checkbox corresponding to «Use Security PIN».
  2. It is required to put in each call service and then click on the checkbox «Use Security PIN».

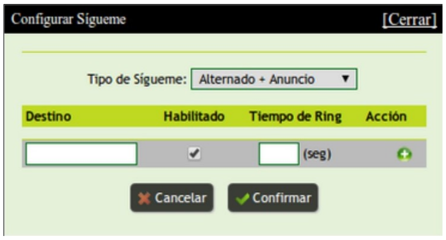
- **PIN (Personal Identification Number)**: This numerical code is chosen by the administrator, which must be entered when requested.

- **Remote Dial Code**: This code is used to make outgoing Denwa UC&C 4.0.1 calls from a shared phone. This code is unique for each user.

- **Alert when codes are used**: an email is sent to the email address that the user has registered in the General New User Tab (see New User General Tab on page 37) when these codes are used.

- **Use follow me**: After creating the user, in this tab it is possible to enable the option to activate Follow me. To do this, you must click on the checkbox, this enables its configuration.

  - Types of follow me:
    - **Toggle + Announce**: a ringing sequence is followed, an attendant allows the caller to announce himself.
    - **Simultaneous + Announcement**: all extensions ring at the same time and an operator allows the caller to announce himself.
    - **Alternate**: describes the way in which the extensions ring, in this case it is following a sequence one at a time.
    - **Simultaneous**: with this option all extensions ring at the same time.
    - **Alternate + Silent**: a ringing sequence is followed and there is no attendant. The call is automatically transferred to the next type of extension.
    - **Simultaneous + Silent**: they ring at the same time and there is no operator.
  - Clicking the button with the plus icon (⊕) adds the follow me rule.
  - In the fields below you can configure the extensions or numbers that are associated with that user. Ring time can also be set. For the action to take place, you must click on the plus icon (⊕).



Configurar Sígueme

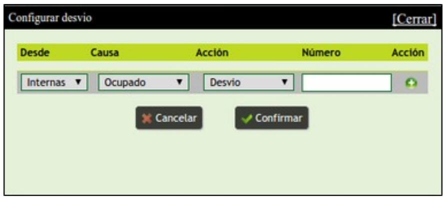
Tipo de Sígueme: Alternado + Anuncio

Destino	Habilitado	Tiempo de Ring	Acción
	☑	(seg)	⊕

Figure 3.19: Advanced interface: User follow me settings

- **Detour**: In this section, it is also possible to configure detours.

  - **From**: allows you to select the origin of the calls that arrive at the extension. The following options are displayed in the drop-down menu: internal, external and all.
  - **Cause**: is the reason that gives rise to the execution of the diversion rule. In this menu you can select among the options: busy, no answer and always.
  - **Action**: here the course that the call will take is indicated, within these you can select: diversion, disconnect and voice mail. Number: this option is activated whenever the disconnect option was not selected in the corresponding action. This is because it is necessary to place the number to which the diversion or voice mail will be made.
  - Clicking the button with the plus icon (⊕) adds the diversion rule.

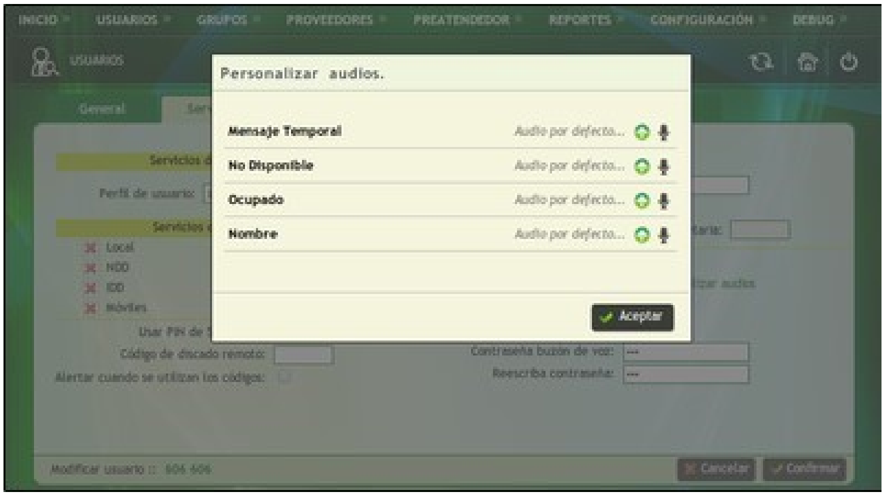


Configurar desvio

Desde	Causa	Acción	Número	Acción
Internas ▾	Ocupado ▾	Desvio ▾		

Figure 3.20: Advanced interface: User forwarding configuration

- **Forward time**: defines the time to wait before forwarding the call.
- **Boss**: All incoming calls to your extension are forced to first be redirected to the Secretary. To do this, you must select the option «Boss» and enter the extension of «Secretary».
- **Call Waiting**: if enabled, if the user is on a phone call and another call enters, it will play a tone alerting the new call, allowing the user to answer the second one, while leaving the pause the first
- **Ask to leave a message**: applies to external calls, that is, when a call is received, which in the first instance is answered with a pre-attendant, this option may be available.
- **Use voicemail**: if you want to use a voicemail on the extension, you only have to check the box corresponding to the mailbox. Once this is done, the possibility of customizing the audio messages is enabled. To do this, it is possible to click on ⬆ and load an audio file or click on 🎙 and record the audio from its extension.



Personalizar audios.

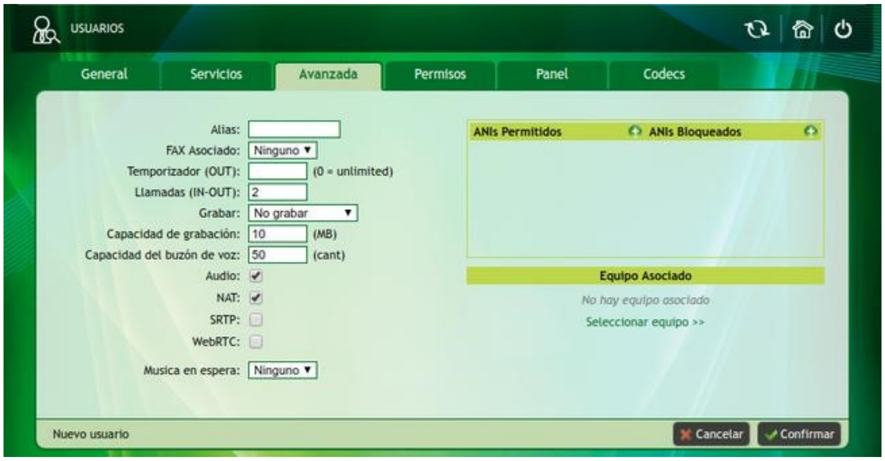
Mensaje Temporal	Audio por defecto...
No Disponible	Audio por defecto...
Ocupado	Audio por defecto...
Nombre	Audio por defecto...

Figure 3.21: Advanced interface: User: Audio customization

- **Mailbox without announcement**: with this option the voicemail announcement is enabled or disabled.
- **Redirect voicemail to**: Voicemail must be disabled in order to use this option. After this, the extension to which the voice mail is redirected is loaded.
- **Voicemail Password**: Set a password to access saved messages from the phone device.
- **Retype Password**: Must match the password, in order to complete the process.

3.3.2.3.3 Advanced New User Tab

From this tab you can configure extra functions for each user.



Alias:
FAX Asociado: Ninguno ▾
Temporizador (OUT): (0 = unlimited)
Llamadas (IN-OUT): 2
Grabar: No grabar ▾
Capacidad de grabación: 10 (MB)
Capacidad del buzón de voz: 50 (cant)
Audio: ☑
NAT: ☑
SRTP: □
WebRTC: □
Musica en espera: Ninguno ▾

No hay equipo asociado

Figure 3.22: Advanced interface: User advanced settings

- **Alias**: allows you to create a number and associate it with the user. With this, incoming calls can dial that number and communicate with the desired extension.
- **Associated FAX**: the possibility of associating a user type FAX, or FAX to Email to the extension is granted, and in this way, messages are received on the Desktop or in the email box.
- **Timer (OUT)**: Allows you to add a timer which limits the duration of outgoing calls.
- **Calls (IN-OUT)**: allows you to determine the number of simultaneous calls that each user can make or receive.
- **Record**: Allows you to record outgoing calls, incoming calls or both, randomly or continuously.
  - **Do not record**: Do not record any calls
  - **All-Continuous**: Record all calls, incoming or outgoing
  - **All-Random**: Record some calls, both incoming and outgoing
  - **In-Continuous**: Record all incoming calls
  - **In-Random**: Record some incoming calls
  - **Out-Continuous**: Record all outgoing calls
  - **Out-Random**: Record some outgoing calls
- **Recording capacity**: the space in MB available for call recording is limited. When the space is exceeded, the oldest recordings will start to be deleted, in case you want to keep them, it will be necessary to configure a backup server from Backup Tab of General (see Backup Tab on page 97) to store those recordings.
- **Voicemail Capacity**: Set the number of voicemails that can be stored locally in Denwa UC&C 4.0.1 . If a backup server is configured from the Backup tab of General (see Backup Tab on the 97 page), excess voicemails will be stored on it; otherwise, they will be deleted.
- **Audio**: This box is checked by default and is required to be able to make recordings; however, unchecking it decreases Denwa UC&C 4.0.1 's processing by only sending signaling packets over it, while *media* packets are sent from host to host.

Mean from point to point

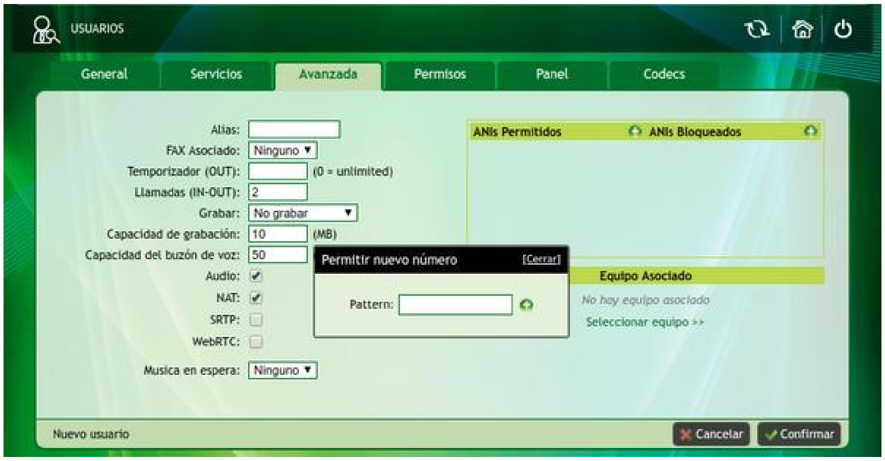
In the event that the audio and/or video are sent end-to-end (without going through Denwa UC&C 4.0.1), it will be necessary for both devices to use the same *Codecs*; Otherwise, the communication will not be established, since the *Transcoding* function is performed by the unified communications system.

- **NAT (*Network Address Translation*)**: is a mechanism used to exchange packets between two networks that assign incompatible addresses. This option is necessary to incorporate equipment that requires it into the network.
- **SRPT (*Secure Real Time Transport Protocol*)**: Defines an RTP profile, providing encryption, message authentication and integrity, and data resend protection in unicast and multicast applications .
- **Music On Hold**: Choose the music on hold for when the user puts a call on hold. To choose, the music must first be loaded in the Configuration > Announcements > Music on Hold section (see section Music on Hold on the 131 page).

Characteristics of audio files for music on hold

Audio files must be WAV with a bit rate of 128Kbps, their audio sample size must be 16 bit, single channel (mono) 8KHz sample rate in PCM format.

- **WebRTC**: Enabling this box provides webRTC protocol support to the extension, that is, it will be able to use SIP credentials through the web.
- **Allowed ANIs**: with this option a list of ANIs (*Automatic Number Identification*) is created from which calls can be received. If there is no ANI in this box, there are no restrictions on incoming calls. If, on the other hand, there are allowed ANIs, you can only receive calls from them. To do this, click on the plus icon (⊕).



Alias:
FAX Asociado: Ninguno ▾
Temporizador (OUT): (0 = unlimited)
Llamadas (IN-OUT): 2
Grabar: No grabar ▾
Capacidad de grabación: 10 (MB)
Capacidad del buzón de voz: 50
Audio: ☑
NAT: ☑
SRTP: ☐
WebRTC: ☐
Musica en espera: Ninguno ▾

Pattern:

No hay equipo asociado
Seleccionar equipo >>

Figure 3.23: Advanced interface: User, whitelist

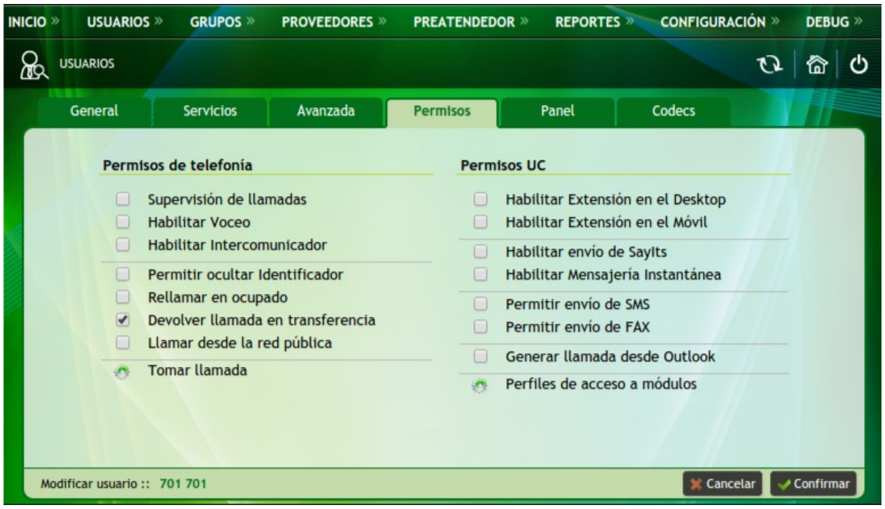
Allowed ANIs in Boss - Secretary configuration

In the event that the Boss-Secretary option is configured in the New User Services Tab, the secretary's extension will be found in this list. In addition, all those ANIs allowed, will be able to communicate directly with the «Boss» without having to go through the «Secretaria».

- **Blocked ANIs**: A list of ANIs from which calls cannot be received is created.

IAX2 users

For some phones that register with the IAX2 protocol, you should not request a token for registration. The option to configure the RCT parameter was added when the internals have the IAX2 protocol configured.



Permisos de telefonía

- □ Supervisión de llamadas
- □ Habilitar Voceo
- □ Habilitar Intercomunicador
- □ Permitir ocultar Identificador
- □ Rellamar en ocupado
- ☑ Devolver llamada en transferencia
- □ Llamar desde la red pública
- Tomar llamada

Permisos UC

- □ Habilitar Extensión en el Desktop
- □ Habilitar Extensión en el Móvil
- □ Habilitar envío de SayIts
- □ Habilitar Mensajería Instantánea
- □ Permitir envío de SMS
- □ Permitir envío de FAX
- □ Generar llamada desde Outlook
- Perfiles de acceso a módulos

Modificar usuario :: 701 701

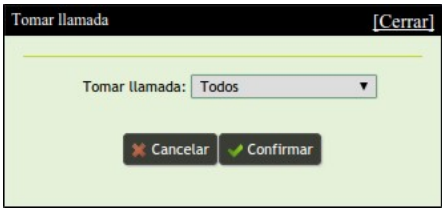
Figure 3.24: Advanced interface: User, new user permissions

3.3.2.3.4 New User Permissions Tab From the permissions tab you can configure the following options:

- **Telephony permissions**
  - **Call supervision**: the user is enabled to intervene calls, dialing *49 + extension number to intervene. There are three ways to perform this action:
    - By pressing number 4 you can listen to the conversation, but without being able to interact with any of the agents.
    - By pressing number 5 you can listen to the conversation, while interacting with the intervened user.
    - By pressing number 6, communication can be carried out normally as in a conference.
  - **Paging Enable**: This is similar to an intercom, only it applies to a group. To make a page to a group, dial *58 + extension number (extension configured as group).
  - **Enable Intercom**: Announcements can be made to an extension without the receiver having to answer. This is accomplished by dialing *59 + extension number.
  - **Hide Identifier**: Allows you to hide the identification of the extension in outgoing calls. To do this, you must dial the code *36 + Number to dial.
  - **Recall when busy**: When the user has this option enabled, and a call is made to another (internal) user who is busy, a notification about this situation is heard and the call ends. When the receiving user becomes free, Denwa UC&C 4.0.1 manages the communication between both users by calling them both.
  - **Return call in transfer**: the destination extension of the unattended transfer is generated to return the call to the transferee in case it is not answered.

   - **Call from public network**: allows the extension to call from an external network to the private network.

- **Take calls**: With this option, *88 (Group take call), *89 (All take call) is enabled or not in each user, which allows calls to be taken. The different options for taking calls are:
   - All
   - My Groups
   - Direct Extension
   - None

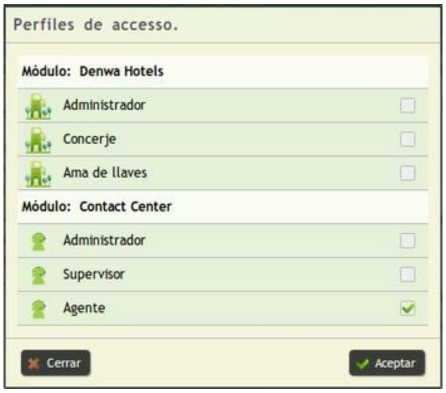


Tomar llamada [Cerrar]

Tomar llamada: Todos

Figure 3.25: Advanced interface: User, take calls

- **UC permissions**
   - **Enable Extension on Desktop**: the option to register the extension on Denwa Desktop is enabled. This is unified communications software that allows access to different services from a single multi-platform interface.
   - **Enable Extension on Mobile**: the option to register the extension on the mobile is enabled. The user must register from his mobile phone through the Denwa Softphone by adding the letter m in front of his extension number (for example, m100). It is necessary to configure from Denwa Desktop the way in which you want to make and receive calls. Options are All, Home, Web, and Mobile.
   - **Enable SayIts delivery**: the user is enabled to write in the Corporate News. This is a service within Denwa Desktop, it is a business social network that drives internal communications and builds a more robust way of sharing news and information.
   - **Enable Instant Messaging**: Allows the extension to use Denwa Desktop's unified messaging. With instant messaging (IM), multi-user messages can be sent and received and online support service.
   - **Allow SMS sending**: the possibility of sending SMS is enabled.
   - **Allow FAX sending**: the possibility of sending FAX is enabled.
   - **Generate call from Outlook**: Allows the use of TAPI SP. This option allows us to monitor the extension from a Windows application such as dialer.exe. The steps are:
      1. Enable the extension to generate the call from Outlook.
      2. Download and install setupDenwaTSP (32 and 64 bit version).
      3. Configure in the application the IP of the central extension and the password of the extension to be monitored (the extension for which we enabled TAPI SP).
      4. Configure dialer.exe, and from that software we will access various functionalities. Call transfer, contacts to be called automatically, etc.
   - **Module access profile**: There are additional modules adapted for Denwa UC&C 4.0.1 , each of these modules allows assigning a profile to each user. In the following example, we see that this Denwa PBX has the Hotels and Contact Center module installed. Therefore, this user is assigned an Agent profile.



Perfiles de accesso.

Módulo: Denwa Hotels

- Administrador □
- Conserje □
- Ama de llaves □

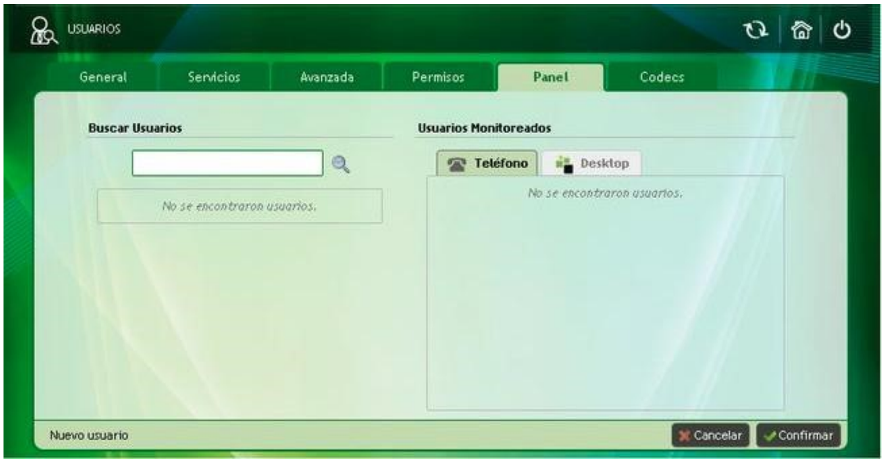
Módulo: Contact Center

- Administrador □
- Supervisor □
- Agente ☑

Figure 3.26: Advanced interface: User, module access permission

3.3.2.3.5 New User Panel Tab

In the Panel tab, users can be assigned to monitor the new user.



No se encontraron usuarios.

No se encontraron usuarios.

Figure 3.27: Advanced interface: User, user panel

To start a search, you must enter some data regarding the user to monitor (name, extension, etc.) and then press the button. In the following image you can see that Juan was entered, the search button was pressed, and with that it was enough to find the user Juan Perez.

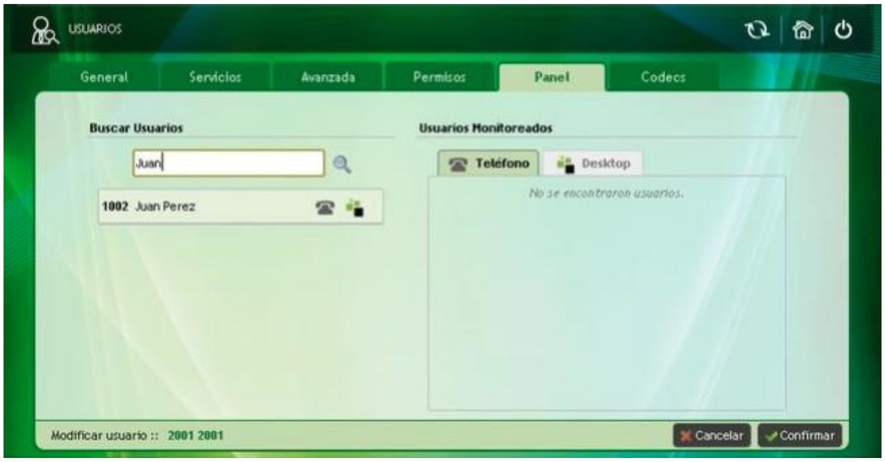


Figure 3.28: Advanced interface: User, user panel (example)

Then, to allow user monitoring, use the ☎ button for the phone's BLF, and the ▪ button for denwa Desktop monitoring to select the desired .

In the right sector of the screen there are two lists of users that will be monitored, in the «☎ Phone» tab there are all the BLFs and in the « Desktop» the list of monitored users on the Denwa Desktop.

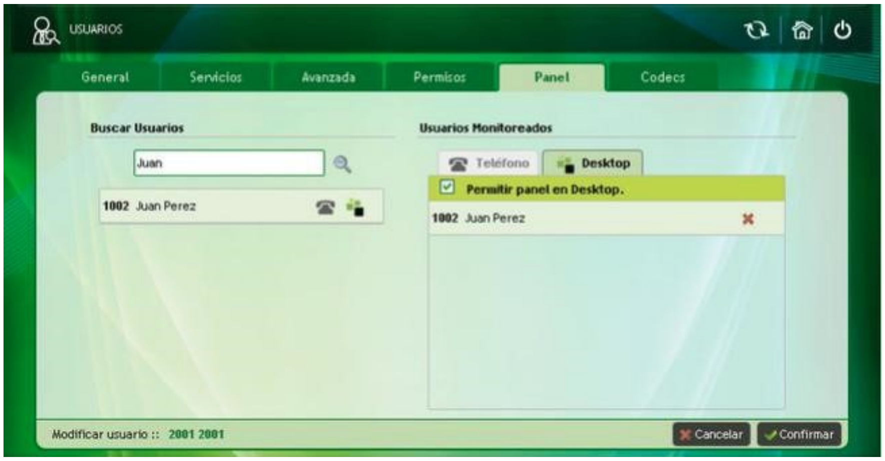


Figure 3.29: Advanced interface: User, user panel: panel activation in Denwa Desktop

It is possible to Allow panel on the Desktop by applying a tick in the corresponding box, which generates a new tab where the monitored users can be observed on the Desktop.

3.3.2.3.6 New User Codecs Tab

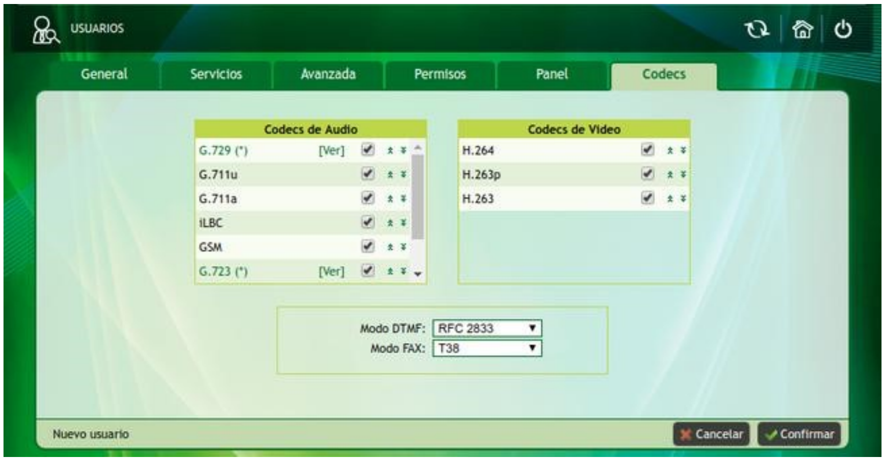
From this tab you can choose the audio and video codecs that will be assigned to the user. Also, it is allowed to select the DTMF mode and the desired FAX mode.

It is convenient that at least the following codecs be selected:

- **G.729**: is an audio data compression algorithm for speech that compresses speech audio into 10-millisecond chunks. Tones such as DTMF or fax cannot be transported reliably with this codec. Therefore, G.711 or out-of-band signaling methods must be used to carry those signals. It is recommended to use it when the communications are outgoing from Denwa UC&C 4.0.1 .

- **G.711**: is an ITU-T standard for audio encoding. The G.711 encoder provides a 64 Kbit/s data stream. For this standard there are two main methods, the µ-law (used in the United States and Japan) and the A-law (used in Europe and the rest of the world). This codec is recommended for communications between extensions belonging to the same Denwa PBX (users connected to the central LAN).

- **H.264**: is a standard that defines a high compression video codec. This standard is capable of providing good image quality at lower bit rates than previous standards.



Codecs de Audio		
G.729 (*)	[Ver]	☑
G.711u		☑
G.711a		☑
iLBC		☑
GSM		☑
G.723 (*)	[Ver]	☑

Codecs de Video	
H.264	☑
H.263p	☑
H.263	☑

Modo DTMF: RFC 2833
Modo FAX: T38

Figure 3.30: Advanced interface: User, codecs

DTMF (*Dual-Tone Multi-Frequency*) modes: are analog signals needed when making phone calls.

- **RFC 2833**: DTMF signals are sent outside of audio. Avoid using it with the G.711 codecs as in this case they will be distorted.

- **IN BAND**: DTMF tones can be sent in band (encoded as audio). It can only be done if the coding used does not use any type of compression, this is the case of G.711.

- **INFO**: it is not recommended for the delivery of DTMF, since it does not allow generating the signaling of the digits in synchrony with the audio, therefore it produces temporary displacements.

FAX modes: are protocols that describe how to send and receive faxes over a data network.

- **T38**: The fax is converted to an image, then needs to be sent to another T38 fax device, and finally converted back to an analog fax signal.

- **T38 Redundancy**: An alternative to T38 is provided to eliminate the effects of packet loss through data redundancy. That is to say, the packets are sent more than once; this increases the bandwidth that is used, but is still less than not using T38.

- **Pass Through**: When an analogue FAX is connected directly to an FXS socket, faxes go in and out automatically, using a series of internal management mechanisms.

3.3.2.4 Import Users

It is possible to import users from a file in .csv format simply by clicking «Select File», selecting the file and clicking «✔ Import».

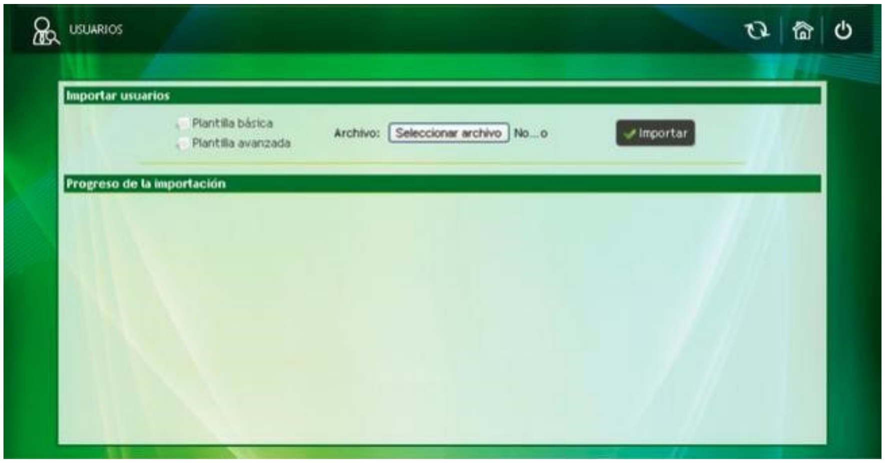


Figure 3.31: Advanced Interface: Import Users

Furthermore, it is possible to generate your own version of the .csv file; To facilitate this task, there is the possibility of downloading some templates (by clicking on «Basic Template» or «Advanced Template»). The difference between them is the possibility of configuration that they present: the basic template requires few data and presents a limited configuration; On the other hand, the advanced template allows access to all the configurations to create a new user.

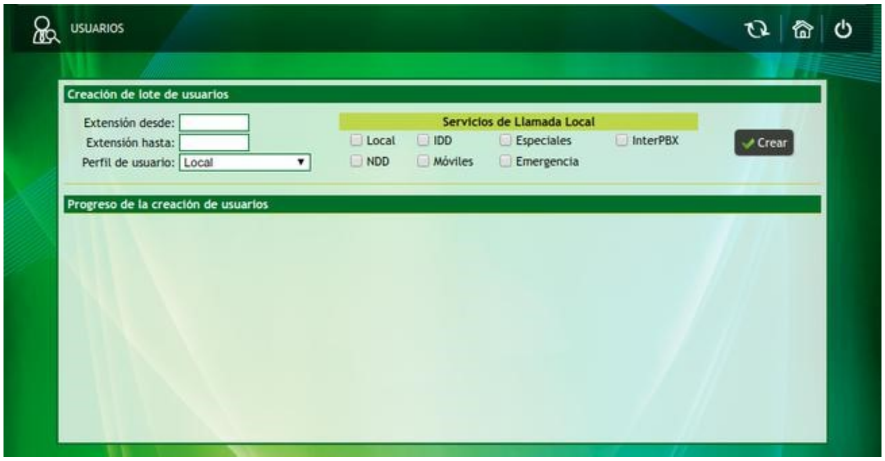
- Basic template users_basic.csv:
    - Extension
    - Password
    - Name
    - Last Name
    - Email
    - number of turnout
    - Deviation time
    - Language
    - Status (0 disable,1 enable, 2 suspend)
    - UM User
    - UM Password
    - Type
    - Mode
    - Local (0 disable,1 enable)
    - NDD (0 disable,1 enable)
    - IDD (0 disable,1 enable)
    - Mobiles (0 disable,1 enable)
    - Specials (0 disable,1 enable)
    - Emergency (0 disable,1 enable)
    - InterPBX (0 disable,1 enable)
- Advanced template users_advanced.csv:
    - Extension

- Password
- Name
- Last Name
- Email
- number of turnout
- Deviation time
- Language
- Status (0 disable,1 enable, 2 suspend)
- UM User
- UM Password
- Type
- Mode
- Local (0 disable,1 enable)
- NDD (0 disable,1 enable)
- IDD (0 disable,1 enable)
- Mobiles (0 disable,1 enable)
- Specials (0 disable,1 enable)
- Emergency (0 disable,1 enable)
- InterPBX (0 disable,1 enable)
- Type of group (simultaneous, alternated or balanced)
- User Profile
- Device
- Timer (OUT)
- Record
- Voice Mail Capacity
- Recording capacity
- Audio
- NAT
- Call from public network
- Aliases
- Use security PIN
- Security PIN
- Use voicemail
- Redirect voicemail to
- Secretary
- Allow SMS sending
- Allow FAX sending
- Audio and Video Codecs
- DTMF mode
- FAX mode

It is recommended to edit the fields of the templates and then verify that the format has not been modified.

3.3.2.5 Generating Users

This functionality allows users to be created in batches, that is, in a single step a certain number of users can be created, with the same profile and local call service options.



Perfil de usuario: Local

Figure 3.32: Advanced Interface: User Generation

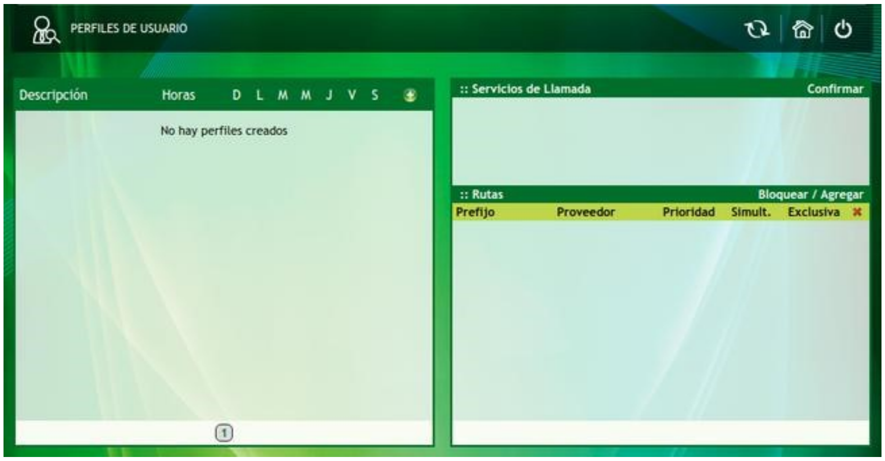
To create a batch of users, you must:

1. Enter the range of extensions (from, to) that you want to generate
2. Select the appropriate profile for users, or local call services (see User Profiles on page User Profiles)
3. Click «✔ Create»

In the lower box: «User creation progress» all users generated.

3.3.2.6 User Profiles

This functionality allows different profiles to be created so that they can then be assigned to extensions. These profiles allow you to limit telephone use by days, hours and assign call services. It is also possible to configure which routes are allowed for each of the profiles.



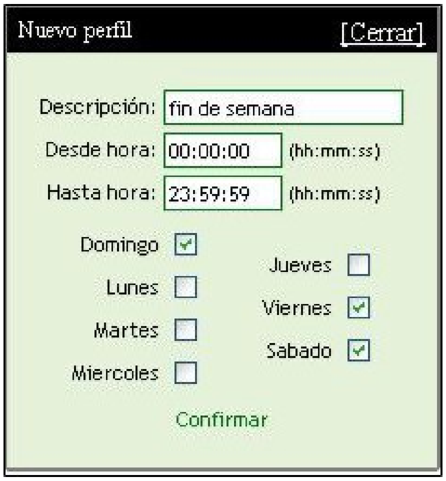
No hay perfiles creados

Figure 3.33: Advanced Interface: User Profiles

3.3.2.6.1 Profile creation

To start with the creation of the profile, you must click on the + sign, this will show a pop-up window.

- **Description**: Descriptive name of the new profile
- **From time**: Time at which the profile will start
- **Until time**: Time in which the profile will end
- **Day of the week**: Select the days of the week on which the previously defined schedule will operate, the corresponding box must be enabled.



Nuevo perfil [Cerrar]

Descripción: fin de semana

Desde hora: 00:00:00 (hh:mm:ss)

Hasta hora: 23:59:59 (hh:mm:ss)

Domingo ☑
Lunes □
Martes □
Miercoles □
Jueves □
Viernes ☑
Sabado ☑

Figure 3.34: Advanced interface: User profiles, new profile

Then you must press «Confirm» to display the new profile in the list.

3.3.2.6.1.1 Modification of the schedule

You can modify the schedule by clicking on the ⚙ icon corresponding to your row, this will display a window similar to the one used to create the profile.

3.3.2.6.1.2 Profile removal

It is possible to delete the profile by clicking on the ✖ icon corresponding to its row.

3.3.2.6.2 Profile modification

Profile modification covers both the editing of existing user profiles and the initial configuration of newly created profiles.

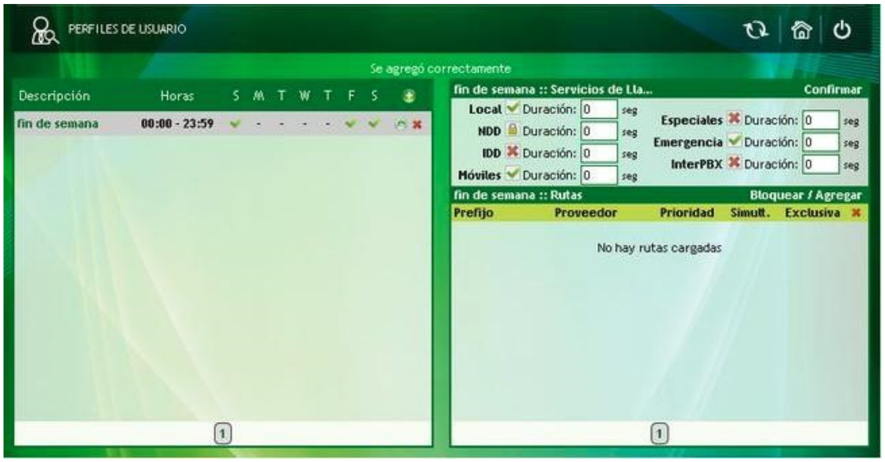
3.3.2.6.2.1 Administration: Call Services

Call services associated with the profile can be set in the upper right box of the screen. Allows you to manage permissions to make various types of calls.

They can be enabled or allowed (✔), denied (✖) or protected by the Security Pin (🔒); It is also possible to indicate the number of seconds allowed for each of the different prefixes. If you want it to be unlimited, the value must be zero (0).

Call Services Configuration

The prefixes that correspond to each type of call must be configured in Call Services (see Call service on page 126).



PERFILES DE USUARIO

Se agregó correctamente

Descripción	Horas	S	M	T	W	T	F	S
fin de semana	00:00 - 23:59	✓	-	-	-	-	✓	✓

fin de semana :: Servicios de Lla... Confirmar

Local ✓ Duración: 0 seg
NDD Duración: 0 seg
IDD ✗ Duración: 0 seg
Móviles ✓ Duración: 0 seg
Especiales ✗ Duración: 0 seg
Emergencia ✓ Duración: 0 seg
InterPBX ✗ Duración: 0 seg

fin de semana :: Rutas Bloquear / Agregar

Prefijo	Proveedor	Prioridad	Simult.	Exclusiva

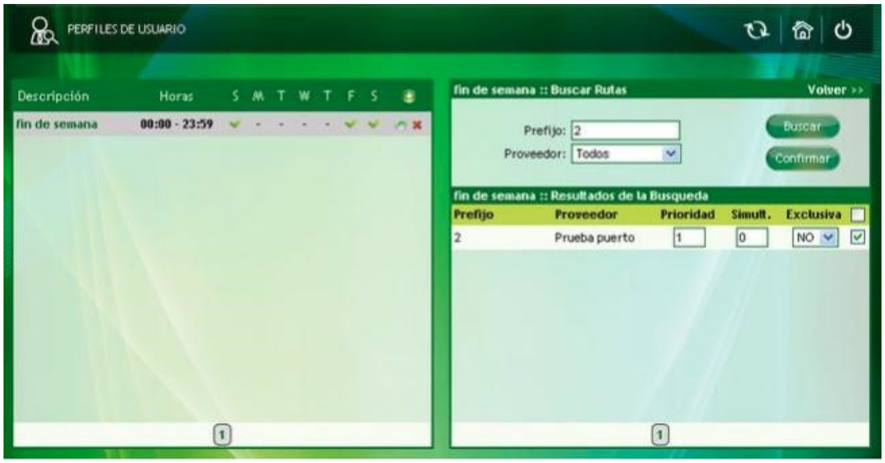
No hay rutas cargadas

Figure 3.35: Advanced interface: User profiles, call services

Once the desired configuration has been made, it is necessary to click on «Confirm».

3.3.2.6.2.2 Administration: Routes It is possible (and necessary) to add routes to the profile, to do this:

- Click on «Add» (located in the Routes box).
- Then a route is searched, this can be done by prefix and/or by providers.
- When the routes are found, they are selected with tildes in the boxes on the right, the priority and number of simultaneous calls are assigned, for it to be of unlimited use a zero (0) must be placed



PERFILES DE USUARIO

Descripción	Horas	S	M	T	W	T	F	S
fin de semana	00:00 - 23:59	✓	-	-	-	-	✓	✓

fin de semana :: Buscar Rutas Volver >>

Prefijo: 2
Proveedor: Todos

fin de semana :: Resultados de la Busqueda

Prefijo	Proveedor	Prioridad	Simult.	Exclusiva	☐
2	Prueba puerto	1	0	NO	☑

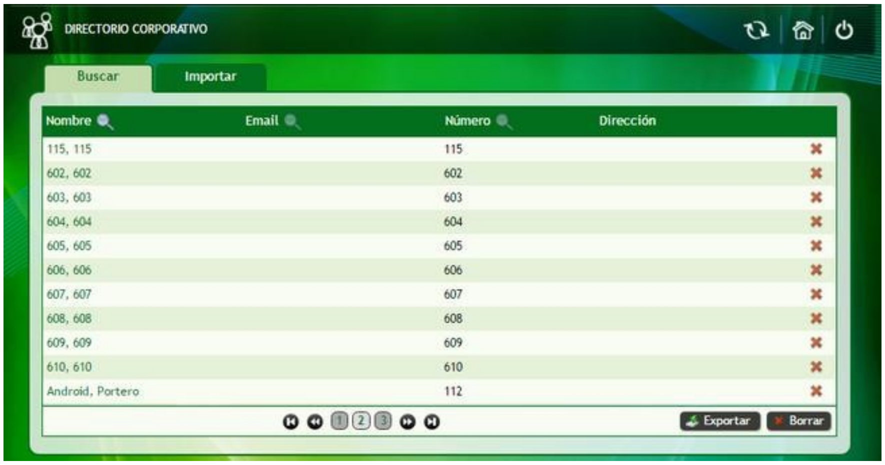
Figure 3.36: Advanced interface: User profiles, paths

Once the routes have been selected and configured, all you have to do is click on the «Confirm» button. If you do not wish to save the changes, you must click on the text «back».

In the same way it is possible to restrict the use of a provider, clicking on «Block» instead of «Add».

3.3.2.7 Corporate Directory

With the corporate directory, contact lists can be uploaded to be used by users who have Denwa Desktop.

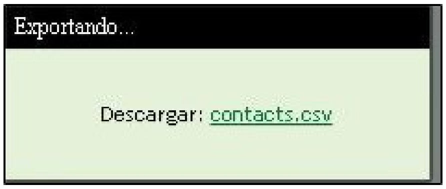


Nombre 🔍	Email 🔍	Número 🔍	Dirección	
115, 115		115		✖
602, 602		602		✖
603, 603		603		✖
604, 604		604		✖
605, 605		605		✖
606, 606		606		✖
607, 607		607		✖
608, 608		608		✖
609, 609		609		✖
610, 610		610		✖
Android, Portero		112		✖

Figure 3.37: Advanced Interface: Corporate Directory

3.3.2.7.1 Search tab In this tab you can see the list of contacts available in the Corporate Directory. The search can be done by Name, Email or Number, by clicking on the 🔍 icon in the header of the table. There is also information regarding your address.

In case you need to work with the list of contacts, you can export the directory with the «⬇ Export» button, which will generate a file in .csv format.

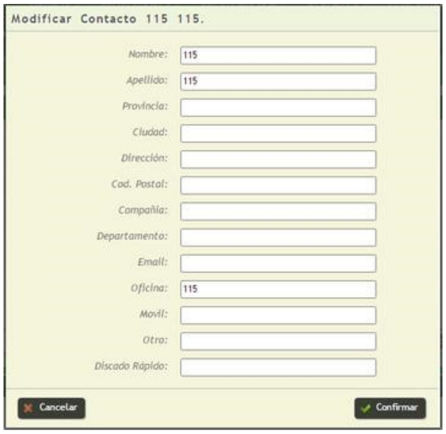


Exportando...

Descargar: contacts.csv

Figure 3.38: Advanced interface: Corporate Directory, CSV download

There is also the possibility of deleting the entire corporate directory by clicking on the «✖ Delete» button; delete a single contact by clicking on the ✖ icon in its corresponding row, or edit a contact by clicking on its name.

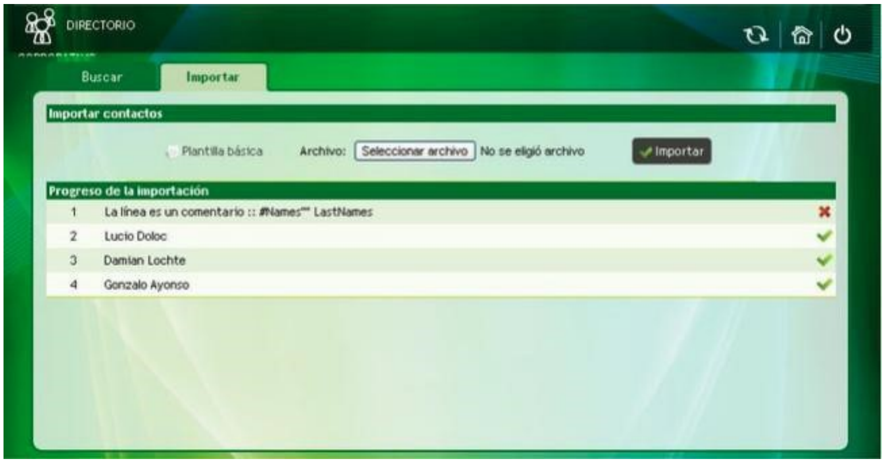


Modificar Contacto 115 115.

Nombre:	115
Apellido:	115
Provincia:	
Ciudad:	
Dirección:	
Cod. Postal:	
Compañía:	
Departamento:	
Email:	
Oficina:	115
Movil:	
Otro:	
Discado Rápido:	

Figure 3.39: Advanced interface: Corporate Directory, contact editing

3.3.2.7.2 Import tab With the Basic Template you can download the contacts_basic.csv file that will serve as a guide when designing the corporate directory contact list. Once the desired contacts have been entered into the spreadsheet, click on the «Select file» button to search for it among the computer's directories and then, pressing the «✔ Import» button will start the import process . If there are problems with any entry in the directory, it will be displayed with a ✖.



Importar contactos

Plantilla básica Archivo: Seleccionar archivo No se eligió archivo ✓ Importar

Progreso de la importación

1	La línea es un comentario :: #Names"" LastNames	✗
2	Lucio Doloc	✓
3	Damian Lochte	✓
4	Gonzalo Ayonso	✓

Figure 3.40: Advanced interface: Corporate Directory, import contacts

3.3.3 Groups

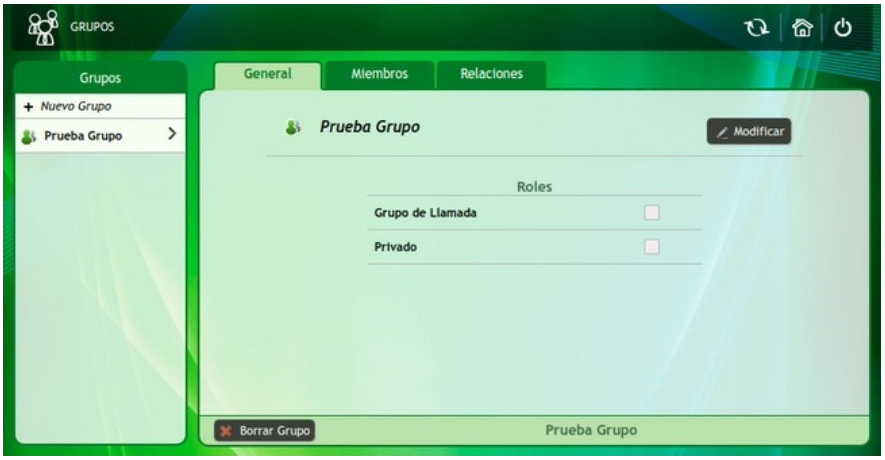
From the Groups tab you can manage and administer them.

User groups can be created that can be used as:

- Call groups.
- Groups to then assign them certain characteristics and relationships with others, even if it is not a group intended to receive calls.

3.3.3.1 View Groups

Allows you to view and edit all the groups created, as well as their characteristics.



Roles

Grupo de Llamada □

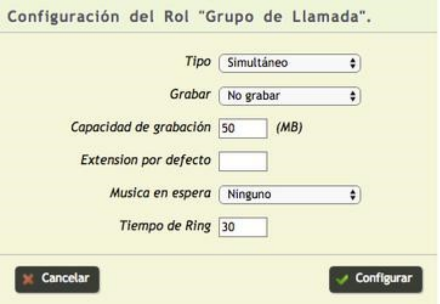
Privado □

Figure 3.41: Advanced Interface: View Groups

The names of all the groups created on the PBX in question appear in the list of groups. By clicking on the name of a group you can make changes in the different tabs

3.3.3.1.1 General Tab

- **Modify**: allows you to make changes to both the name of the group and its icon.
- **Roles**: refer to the behavior that the group calls will have.
  - **Call Group**: only the groups that fulfill this role can be part of the pre-attendant. In addition, it activates calls between users of the same group, also with users who do not belong to it. When checking the checkbox, to opt for this option, the following window is displayed.


Configuración del Rol "Grupo de Llamada".

Tipo: Simultáneo

Grabar: No grabar

Capacidad de grabación: 50 (MB)

Extension por defecto:

Musica en espera: Ninguno

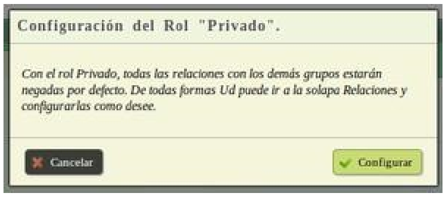
Tiempo de Ring: 30

Figure 3.42: Advanced Interface: Call Group Configuration

- **Type**: indicates the course that each of the incoming calls to the group must follow. The options provided by the dropdown menu are
  - **Simultaneous**: when a call enters the group, all the telephones belonging to it ring; when one of them answers the call, the other phones stop ringing.
  - **Alternate**: this mode uses the group Members list order (see following figure); that is, when entering a call, the telephone of the first member of said list rings, the second call goes to the second member and so on.
  - **Balanced**: like the previous mode, this mode uses the list of Group Members (see the following figure), it is capable of analyzing who has received the least number of calls. To then assign the new incoming call to it.

    - **Record**: allows you to record (or not) incoming and outgoing calls. This dropdown menu provides the following options:
        - **Do not record**: As its name implies, this mode does not record any calls, neither incoming nor outgoing.
        - **ALL - Continuous**: all calls are recorded; that is to say, that of all the members of the group, both incoming and outgoing.
        - **ALL - Random**: Only some calls from any member belonging to the group are recorded.
    - **Recording capacity**: it is the capacity to store the recordings of the calls, by default it is 10MB but it is possible to change this value directly from the box. When this capacity (or quota) reaches its maximum, two things can happen: the first is that the oldest recordings begin to be overwritten with the most recent ones and the second is to have created an FTP (File Transfer Protocol) client to which the they export the recordings once the maximum quota is reached. To configure the FTP client it is necessary to see the General Backup Tab (Settings > General > Backup).
    - **Default extension**: refers to the extension, which does not belong to the group, that rings in case the call has not been answered by the corresponding members of the group.
    - **Music On Hold**: Choose the music on hold that is played when the extensions in the group are ringing. It only applies to the Simultaneous strategy and to choose the music, it must previously be loaded in the Configuration > Announcements > Music on Hold section (see Music on Hold on the 131 page).
    - **Ring Time**: indicates the time the phone rings, the unit used is «seconds».

- **Private**: cuts the relations of the group in question with the rest, clicking on its checkbox opens the window shown below, to accept this role it is necessary to click on Configure

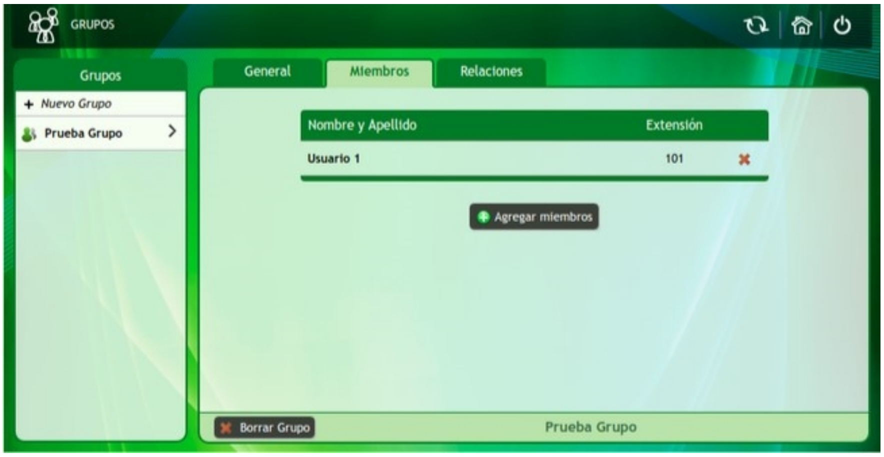


Configuración del Rol "Privado".

Con el rol Privado, todas las relaciones con los demás grupos estarán negadas por defecto. De todas formas Ud puede ir a la solapa Relaciones y configurarlas como desee.

Figure 3.43: Advanced Interface: Private Group Settings

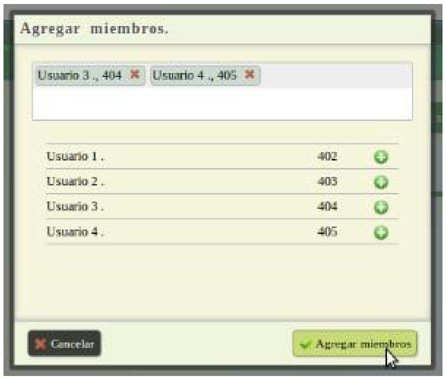
3.3.3.1.2 Members tab The option to remove members from the group is provided by simply clicking on the ✖ icon located to the right of each of them. It is also possible to incorporate users from «⊕ Add members», this opens a window like the following:



Nombre y Apellido	Extensión	
Usuario 1	101	✖

Figure 3.44: Advanced Interface: Member Settings

In it you must write the username in the white box, automatically updating the list at the bottom of the window. They can be added to the group by clicking ✚, user by user. Finally, the changes are saved by clicking on «✔ Add members».



Usuario 1 .	402	✚
Usuario 2 .	403	✚
Usuario 3 .	404	✚
Usuario 4 .	405	✚

Figure 3.45: Advanced interface: Add members

3.3.3.1.3 Relationships tab General and Desktop functions are related between two groups, the group in question with the group that is selected. The arrows that indicate the permissions that one group has for the other, change color (enabling or disabling) just by clicking on them.

- **Instant Messaging**: are those messages that can be sent from one group to another.
- **Calendar**: Allows sharing among groups of calendar activities, such as events, tasks, calls, meetings, anniversary and notes.
- **Conversations**: includes the functions of sending messages, SMS and Fax. The sending of messages reaches both the Desktop and the email address of each member of the group.
- **Monitoring of calls**: enables the opportunity to supervise or not supervise calls from a particular group, for this the permission of Supervision of Calls (New User Permissions Tab) must be activated to all the users of the group that can be perform this action. In this example, the users belonging to group 1 must have user supervision permission and the call monitoring relationship activated to monitor a user belonging to group 2. The action is performed by dialing *49 + Extension number to monitor.

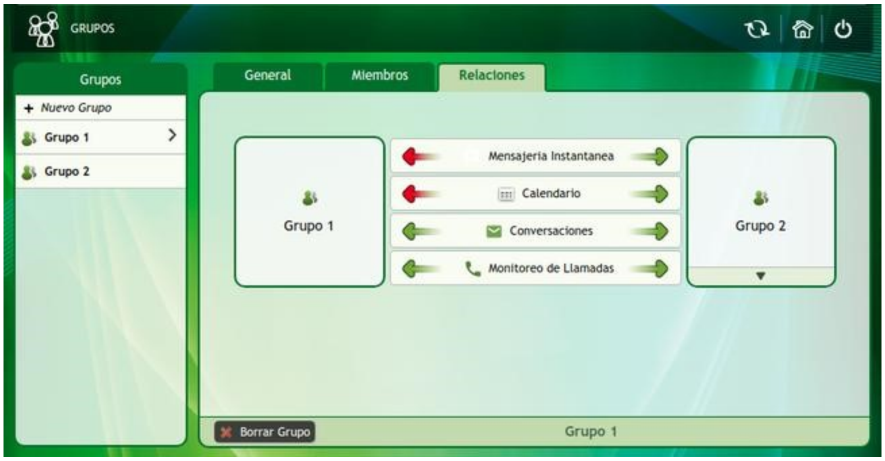


Figure 3.46: Advanced Interface: Group Relations

Once the relationship between both groups is as desired, the changes will be saved by clicking on «✔ Apply changes»; If you wish to restore it to a previous state (if it has not yet been saved), you must click on «↺ Undo changes».

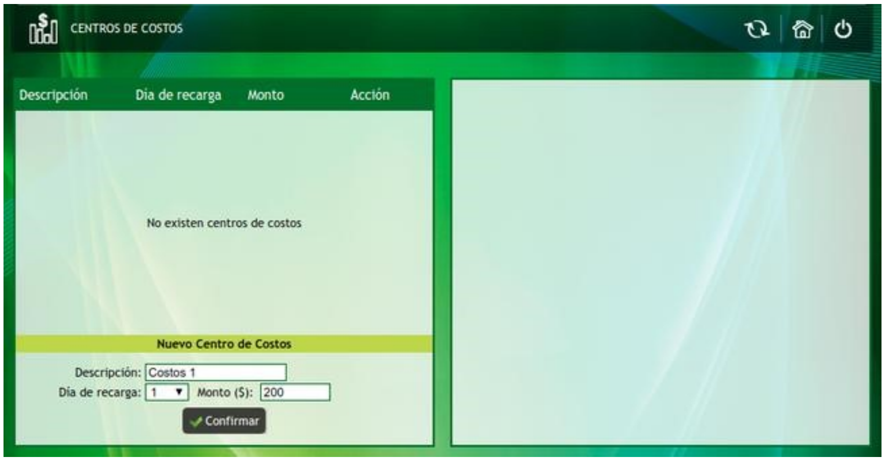
3.3.3.1.4 New group Additionally, clicking on «⊕ New Group» (column on the left of the screen) displays a window requesting the name and icon of the group, as shown in the following figure. To confirm these changes, click on «✔ Create». In this instance, the group has been created, so it is displayed in the Groups column.

3.3.3.2 New Group

This leads to a window requesting the name and icon of the group, as shown in the following figure (Fig. A.). To confirm these changes, click Create. In this instance, the group has been created, so it is displayed in the Groups column.

3.3.3.3 Cost center

The Cost Center option allows assigning costs to calls, discriminating the types of calls, destinations and users.



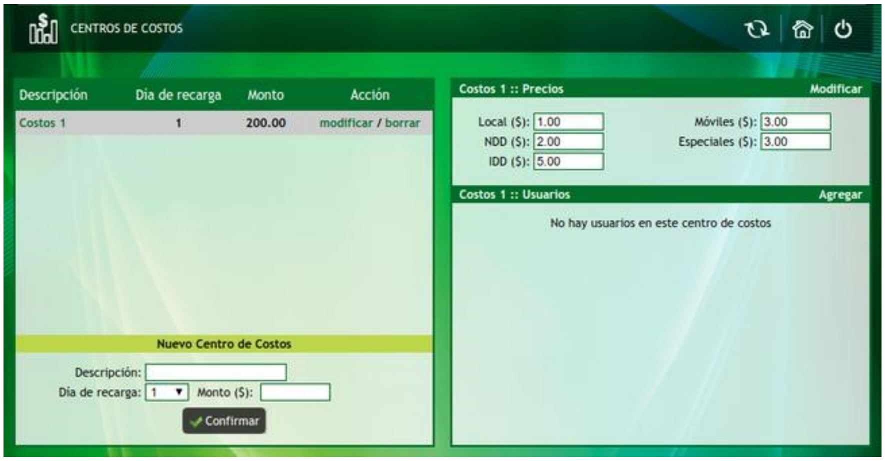
Descripción: Costos 1
Dia de recarga: 1 Monto ($): 200

Figure 3.47: Advanced Interface: Cost Center

In the first instance, a new cost center must be created. For which it is necessary to complete the fields shown below and then click on «✔ Confirm»:

- **Description**: Complete with a brief description or name of this new cost center.
- **Recharge day**: refers to the day of the month on which the charge is made to make calls.
- **Amount**: is the capacity available to make calls, this amount being the number of pesos that are assigned to that account until the new recharge of the following month. The balance is not cumulative with the amount of the new month.

Once the cost center is generated, it is time to assign the amount per minute of the different types of calls (see Call service on page 126)



Descripción	Día de recarga	Monto	Acción
Costos 1	1	200.00	modificar / borrar

Local ($): 1.00
NDD ($): 2.00
IDD ($): 5.00
Móviles ($): 3.00
Especiales ($): 3.00

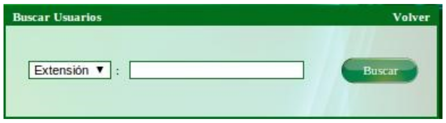
No hay usuarios en este centro de costos

Descripción:
Día de recarga: 1 ▼ Monto ($):

Figure 3.48: Advanced interface: Cost center and call types

Of course you can use the «modify / delete» option to make changes to the cost center or delete it directly.

Now is the time to add users to the cost center, for which it is necessary to click on «Add». Then a window opens presenting a simple drop down menu; which allows you to search for users by extension, first name or last name. If this field is left blank and Search is pressed, it displays a list with all the PBX users and users can be selected to be added to the cost center directly from this list.



Extensión ▼ :

Figure 3.49: Advanced interface: Adding users to the cost center

Cost Center Configuration These procedures must be done for each of the existing cost centers.

3.3.4 Suppliers

The providers are used to create virtual links, through the use of various trunks. In other words, the trunks are used to create connections with other PBX centrals, VoIP operators and with the external PSTN world. Among the different types of trunks are: TDM, SIP, DenwaPBX InterConn, Asterisk InterConn, among others.

Each trunk has defined country and area codes where calls can be sent and/or received; for example: 1786 Miami (USA) or 54351 Córdoba (Argentina), these are called routes.

A trunk can use the registration method to exchange security credentials with the operator, in which case it only allows sending and receiving calls with that operator as long as it is registered.

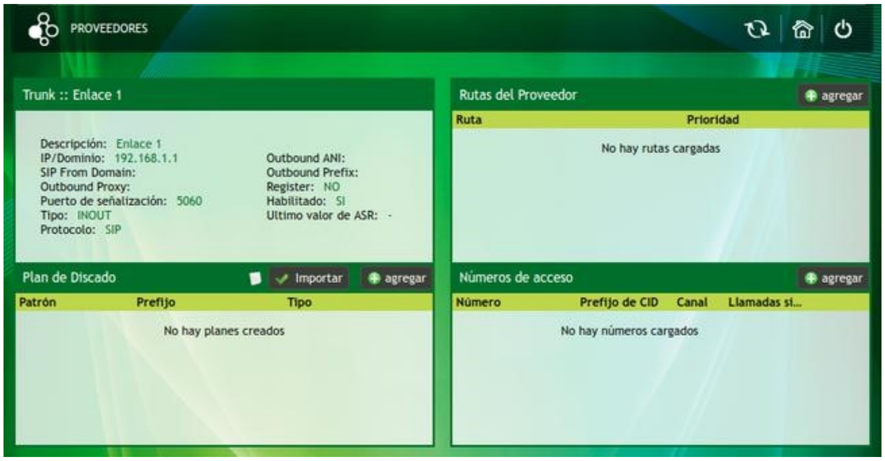
3.3.4.1 View Providers

From this menu you can see the list of providers or trunks (see the following figure), which provides the following information:

- **Description**: simply refers to the name of the trunk.
- **IP**: is the destination IP address of the trunk; For example, there are two exchanges, A and B, when configuring A, the IP address of B is placed and vice versa.
- **Type**: this column details whether the link is:
  - **OUT**: only calls can be made, but there are no incoming calls.
  - **IN**: It is not possible to make calls as there are only incoming calls.
  - **INOUT**: is enabled both to make calls and to receive them.
- **Protocol**: allows you to quickly view the protocol used by the trunk in question (see New Provider General Tab).
- **Registered**: this column exposes if Denwa UC&C 4.0.1 is registered or not as a client of the provider, in case it requests it.
- **Action**: presents the options to directly remove the provider (✖) or to modify it (✎). This last option allows you to edit the options that a new provider has (see New Provider on page 64).

3.3.4.1.1 Provider Configuration

When clicking on the descriptive name that has been selected for the trunk (in the first column) the configuration window is displayed, from it it is possible to define: the routes, the access numbers and dialing plans.



Descripción: Enlace 1
IP/Dominio: 192.168.1.1
SIP From Domain:
Outbound Proxy:
Puerto de señalización: 5060
Tipo: INOUT
Protocolo: SIP

Outbound ANI:
Outbound Prefix:
Register: NO
Habilitado: SI
Ultimo valor de ASR: -

Ruta	Prioridad

No hay rutas cargadas

Patrón	Prefijo	Tipo

No hay planes creados

Número	Prefijo de CID	Canal	Llamadas si...

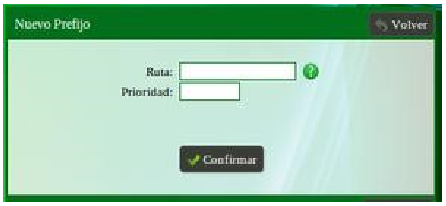
No hay números cargados

Figure 3.50: Advanced Interface: Provider Settings

Four boxes are observed, which are explained below.

- **Trunk**: Allow to check the link details.

- **Provider prefixes**: clicking «⊕ add» displays the following window:



Ruta:
Prioridad:

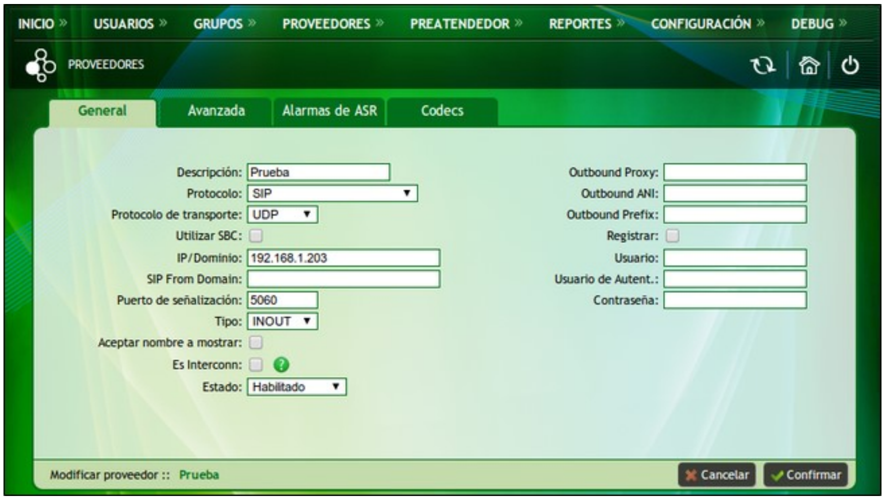
Figure 3.51: Advanced Interface: Vendor Prefixes

  - Route: those digits that are designated as route are the ones that will go out through the trunk in question.
  - Priority: it is possible to assign an order of priorities from 1 to 9, in the case that there are different paths to carry out the call. For example:
    If the route is 4 then it matches all calls that start with 4. If the route is 567, it will carry calls that start with 567. It must be taken into account that the number of digits that follow those that refer to the routes is indistinct.
    When finished, press «✔ Confirm», to save the new route.

Pattern	**Prefix**	**Matches**	multicolumn1c**Is replaced by**
471T or 471*	54351471	471xxxxxx	54351471xxxxxx
471555555	54351478666666	471555555	54351471666666
21.3T or 21_3*	552193	21x3xxxxxx	552193xxxxxx
47.555555 or 47_555555	54351478666666	47x555555	54351478666666

3.3.4.2 New Provider

To generate a new provider or trunk, you must enter the New Provider option and complete the data shown on the screen.



Descripción: Prueba
Protocolo: SIP
Protocolo de transporte: UDP
Utilizar SBC: □
IP/Dominio: 192.168.1.203
SIP From Domain:
Puerto de señalización: 5060
Tipo: INOUT
Aceptar nombre a mostrar: □
Es Interconn: □
Estado: Habilitado

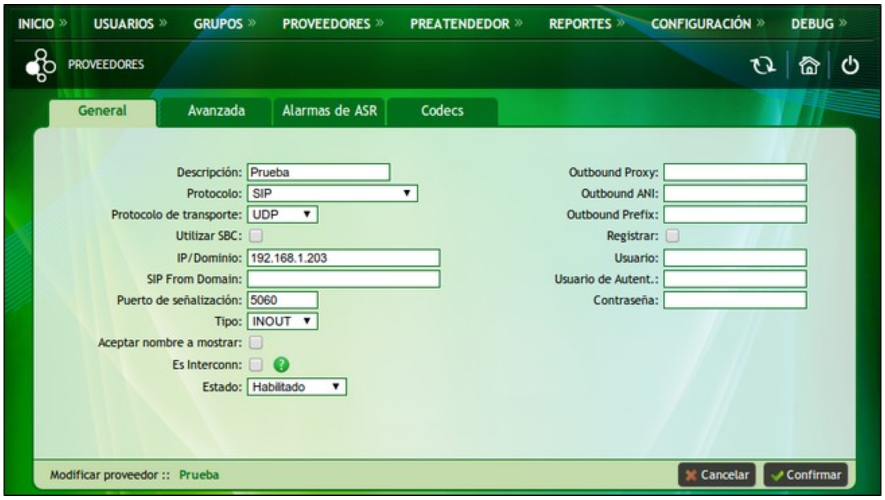
Outbound Proxy:
Outbound ANI:
Outbound Prefix:
Registrar: □
Usuario:
Usuario de Autent.:
Contraseña:

Modificar proveedor :: Prueba

Figure 3.55: Advanced Interface: New Provider

When confirming, you will have four (4) tabs that will be detailed below.

3.3.4.2.1 New Provider General Tab The first tab is General, from here it is possible to carry out the basic configuration of the trunk, filling in the fields that can be seen in the following figure.



Descripción: Prueba
Protocolo: SIP
Protocolo de transporte: UDP
Utilizar SBC: □
IP/Dominio: 192.168.1.203
SIP From Domain:
Puerto de señalización: 5060
Tipo: INOUT
Aceptar nombre a mostrar: □
Es Interconn: □
Estado: Habilitado

Outbound Proxy:
Outbound ANI:
Outbound Prefix:
Registrar: □
Usuario:
Usuario de Autent.:
Contraseña:

Modificar proveedor :: Prueba

Figure 3.56: Advanced Interface: General Provider Settings

- **Description**: refers to the name that is selected for the trunk link.
- **Protocol**: define a protocol for the trunk being created. In the list of protocols it is possible to locate the TDMs; that use both analog and digital boards. In addition, there is TDM Premium which, as the name implies, is included only in the Denwa Premium model. It must be taken into account that all those InterConn protocols are applied to link two PBX exchanges.
  - SIP
  - TDM
  - TDM Khomp
  - DenwaPBX InterConn
  - SIP Microsoft ICS
  - SIP Microsoft Lync
  - SIP Lotus Domino
  - SIP Skype for Business
  - SIP with SMS
  - SIP - Argentina - Metrotel
  - SIP - Costa Rica - ICE
  - SIP - Peru - Globalbackbone
  - SIP - Panama - CableAndWireless
  - SIP - Mexico - Alestra
  - SIP - Mexico - Movistar
  - SIP - Mexico - Izzi
  - SIP - Mexico - Axtel
  - SIP - Mexico - Axtel - Broadsoft
  - Asterisk InterConn

  - TDM InterConn
  - H323.

> **SIP versions**
>
> From the previous item, the most common protocol used for signaling between the connected ends is SIP. The rest of the SIP protocols that are observed in the previous list have been customized for a particular client. Also on this list is Asterisk InterConn which, unlike the rest, uses the IAX (Inter-Asterisk eXchange) protocol.

- **Transport Protocol**: Allows you to choose between TCP or UDP signaling. Of the protocols listed above, only Microsoft Lync SIP uses TCP; while the rest use UDP.
- **Use SBC**: clicking its checkbox enables the SBC (Session Border Controller) on the trunk. This option is only available on the Denwa Premium model.
- **IP/Domain**: refers to the IP address or domain of the equipment connected at the other end of the trunk. In the case of a TDM type trunk, Denwa uses the localhost.
- **SIP From Domain**: used for those operators that request the change in the From field of the SIP packet header.
- **Signaling Port**: indicates the port where the trunk will serve SIP requests; Default is port 5060.
- **Type**: The trunk can be configured to make calls only, receive calls only, or both. For this, there are the OUT, IN and INOUT options, respectively.
- **Accept display name**: by clicking on the corresponding checkbox, when a call is received, the name of the caller (Display Name) is displayed if the provider provides this service.
- **Es interconn**: allows direct calls to extensions configured in DenwaUC without DIDs and using the routes configured in other providers.
- **Status**: this option makes it possible to enable or disable the trunk.
- **Outbound Proxy**: this box must be completed if the provider requires it; as it is automatically placed in the Proxy field of the SIP header. That is, if this option is enabled, all calls are sent to this IP or domain and the trunk IP or domain is only used for registration.
- **Outbound ANI**: if the provider requests it, the ANI (Automatic Number Identification) can always be the same. Completing this box fixes the information in the ANI field of the SIP header.
- **Outbound Prefix**: is the prefix that is placed before each outgoing call. This field is only filled in if the provider requires it to authenticate the call. This option adds the prefix without the need to make a dial plan.
- **Register**: if the corresponding checkbox is checked, the following three fields are enabled.
  - **User**: is the identification that the trunk uses to authenticate itself in the destination server, usually the telephone number assigned to this trunk.
  - **Authentication User**: is for double authentication, in order to provide greater security.

- **Password**: is the key for authentication during registration.

Availability of fields

Depending on the protocol selected, all of the options mentioned above may or may not be available. This variation is due to the characteristics of the protocol. These protocols are defined HERE.

Providers and *Firewall*

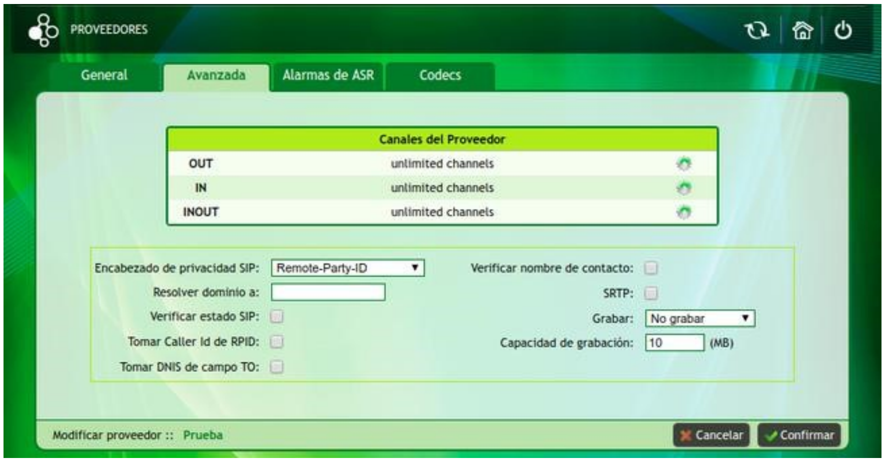
When a trunk is created or its IP is modified, they are added to the high user priority rules in the firewall. This applies to SIP providers, DENWAPBXIC and H323. Two rules per provider will be automatically generated, one for the SIP protocol and the other for RTP.

3.3.4.2.2 Advanced New Provider Tab

After creating the trunk or provider it is necessary to assign channels. This assignment is made depending on the protocol used, as shown below.

3.3.4.2.2.1 SIP and DenwaPBX InterConn

In the case of SIP interconnection it is simply necessary to define the number of channels that can be used. The same is true when using DenwaPBX InterConn trunks.



Canales del Proveedor		
OUT	unlimited channels	⚙
IN	unlimited channels	⚙
INOUT	unlimited channels	⚙

Encabezado de privacidad SIP: Remote-Party-ID ▼
Resolver dominio a:
Verificar estado SIP: □
Tomar Caller Id de RPID: □
Tomar DNIS de campo TO: □
Verificar nombre de contacto: □
SRTP: □
Grabar: No grabar ▼
Capacidad de grabación: 10 (MB)

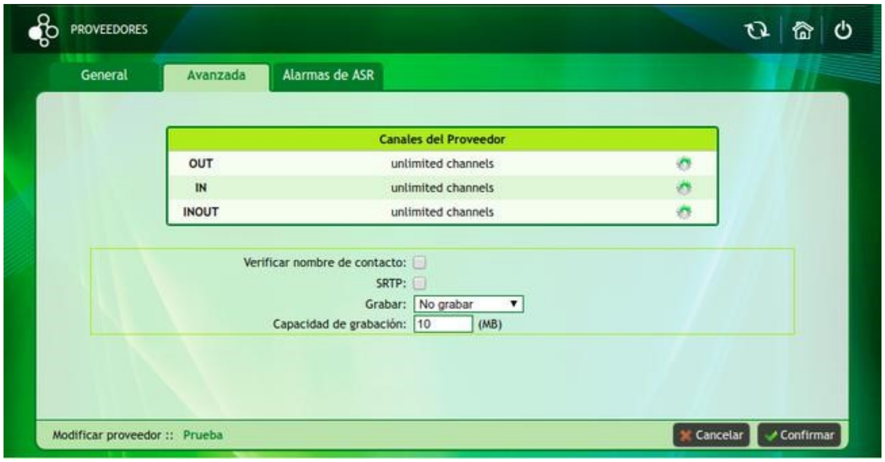
Modificar proveedor :: Prueba

Figure 3.57: Advanced Interface: Advanced Provider Settings

- **Provider Channels**: By simply clicking the ⚙ icon to the right of it you can change the number of channels assigned. Care must be taken with the number of channels that are assigned, because if a number less than the existing one is entered, the SMS channel settings will be lost.
- **Optionals**:
  - **SIP Privacy Header**: these alternatives are for when building the SIP header, they are used to select how the Caller ID is sent to the destination. The options provided by the dropdown menu are Remote-Party-ID and P-Asserted-Identity.
  - **Resolve domain to**: the IP of the provider to resolve the trunk domain is placed in this box (this domain is the one that is completed in Provider > General).

- **Verify SIP status**: if the corresponding checkbox is checked, the connection status of the remote device via SIP is verified.
- **Take Caller Id from RPID**: with this option, the data of the caller (caller id) is taken from the Remote-Party-ID
- **Take DNIS from TO field**: with this option, the data of the caller (DNIS) is taken from the TO field in SIP signaling
- **Verify the contact name**: by checking the checkbox when a call is made or received, the control panel consults for this ID in public databases (Ex: CNAME), in such a way that it displays the name Whose ID does it belong to?
- **SRTP**: With this option, encrypt the RTP audio of outgoing calls on this trunk
- **Record**: allows you to configure the recording of calls by the trunk
- **Recording Capacity**: Allows you to assign a recording quota (disk space) for the recordings of the calls you make through this trunk

3.3.4.2.2.2 Asterisk InterConn This type of trunk offers the same advantages as TDM InterConn, but with the particularity that it uses the IAX2 protocol (Inter-Asterisk eXchange protocol) for signaling.



Canales del Proveedor		
OUT	unlimited channels	⚙
IN	unlimited channels	⚙
INOUT	unlimited channels	⚙

Verificar nombre de contacto: □
SRTP: □
Grabar: No grabar ▾
Capacidad de grabación: 10 (MB)

Modificar proveedor :: Prueba

Figure 3.58: Advanced Interface: Advanced Provider Configuration with Asterisk Interconn

- **Provider Channels**: By simply clicking the ⚙ icon to the right of it you can change the number of channels assigned. Care must be taken with the number of channels that are assigned, because if a number less than the existing one is entered, the SMS channel settings will be lost.
- **Optionals**:
  - **Recording Capacity**: Allows you to assign a recording quota (disk space) for the recordings of the calls made by this trunk.
  - **Record**: Allows you to set the ability to call recordings through the trunk.
  - **Verify contact name**: by checking the checkbox when a call is made, at the receiving end, the name of the person making the call is displayed.
  - **SRTP**: by checking the box, you can encrypt the audio of calls.

In order for this protocol to work correctly, the Asterisk client must be configured at the other end. To do this, the following settings are recommended within the iax.conf file:

- With authentication

```
[USERNAME]
auth=plaintext
secret=PASSWORD
type=friend
permit=DENWAIP
context=default
host=DENWAIP
port=4569
disallow=all
allow=g729
allow=ulaw
allow=alaw
allow=ilbc
allow=gsm
allow=h264
allow=h263p
allow=h263
```

iax.conf file modified for use with authentication

- No authentication

```
[DENWAIP]
type=friend
permit=DENWAIP
context=default
host=DENWAIP
port=4569
disallow=all
allow=g729
allow=ulaw
allow=alaw
allow=ilbc
allow=gsm
allow=h264
allow=h263p
allow=h263
```

iax.conf file modified for use without authentication

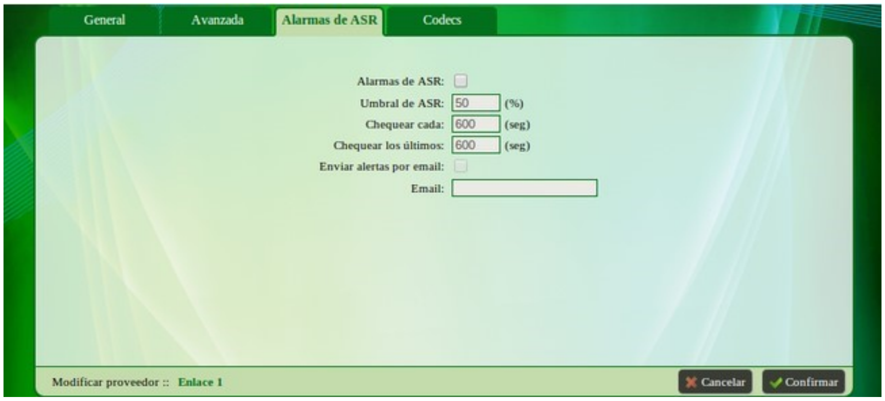
3.3.4.2.3 New Provider ASR Alarms Tab

The ASR (*Answer Seizure Ratio*) is one of the indices that measures the quality of the network and the success rate of calls. It is calculated as the percentage of calls answered with respect to the total volume of calls. ASR alarms can be activated in order to detect problems regarding the number of calls made.

As shown in the previous image, the fields to configure are the following:

- **ASR alarms**: just clicking on the box activates or deactivates them. If this option is checked, the following three option fields are enabled
  - **ASR threshold**: is the limit percentage with which the alarm is activated
  - **Check every**: the time, in seconds, that must wait for the execution of the ASR check is placed
  - **Check the last ones**: in this item you choose the time, in seconds, in which the answered calls and total calls are counted
- **Send alerts by email**: clicking on the corresponding checkbox enables sending reports by email

- **Email**: this field is available only if the previous option has been checked and it allows placing the email address to which the ASR alarm reports are sent



Alarmas de ASR: ☐
Umbral de ASR: 50 (%)
Chequear cada: 600 (seg)
Chequear los últimos: 600 (seg)
Enviar alertas por email: ☐
Email:

Modificar proveedor :: Enlace 1

Figure 3.59: Advanced interface: Provider ASR alarm configuration

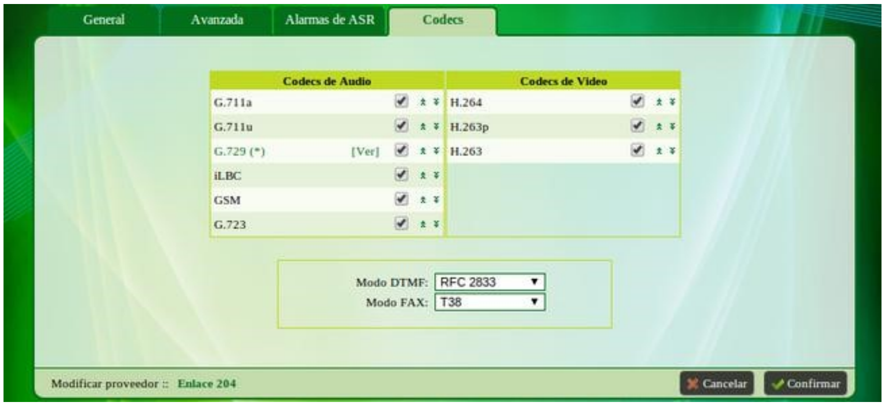
Alert sending condition

For these alerts to function correctly, the email server must be previously configured in Configuration > General > Mail Server (see section Mail Server Tab on the 97 page).

To apply the entered changes, only one click on «✔ Confirm» is needed.

3.3.4.2.4 New Provider Codecs Tab

As expected, in this tab you must select the Codecs, both audio and video, used by the trunk. In addition, the selection of the protocol to be used in DTMF mode and FAX mode is required.



Codecs de Audio		Codecs de Video	
G.711a	☑	H.264	☑
G.711u	☑	H.263p	☑
G.729 (*) [Ver]	☑	H.263	☑
iLBC	☑		
GSM	☑		
G.723	☑		

Modo DTMF: RFC 2833
Modo FAX: T38

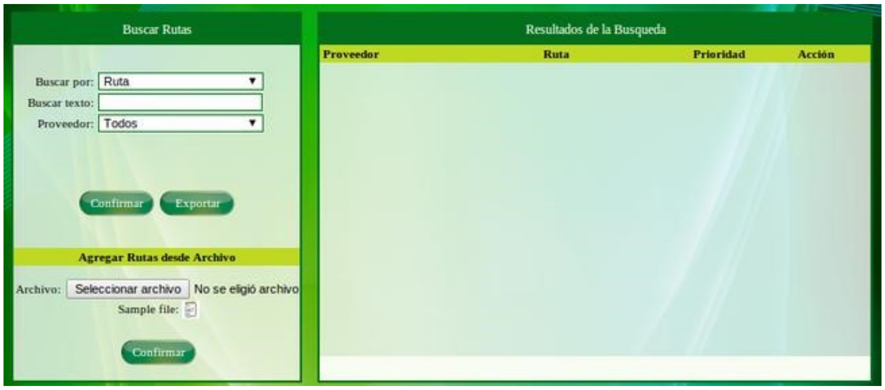
Modificar proveedor :: Enlace 204

Figure 3.60: Advanced interface: Provider codec configuration

For more information about audio and video codecs, see the New User Codecs Tab (see New User Codecs Tab on the 49 page).

3.3.4.3 Routes

The following image shows the Suppliers > Routes window, which provides a search mechanism and makes it faster and more efficient.



Buscar por: Ruta
Buscar texto:
Proveedor: Todos

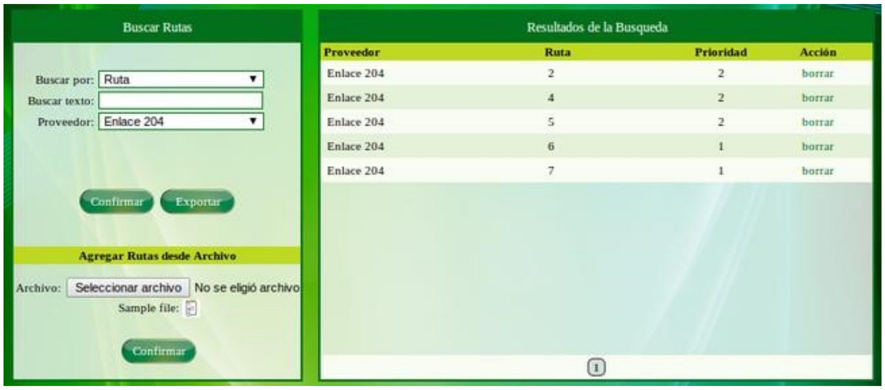
Archivo: Seleccionar archivo No se eligió archivo
Sample file:

Proveedor	Ruta	Prioridad	Acción

Figure 3.61: Advanced interface: Query provider routes

In the box on the left of the screen: «Buscar Rutas», the option of searching for the outgoing route is provided by applying some kind of filter, either through the use of texts or by selecting a provider. No filter can be applied, in this way the complete list of routes of each of the providers is shown. Then there are the options:

- **Confirm**: it is used to apply the search filter and places the results in the right box of the screen, as shown in the following image. The first column shows the name of the provider, the second the output route, the third indicates its priority and the last column offers the possibility of deleting the already created route.
- **Export**: allows you to generate a file containing the routes created and filtered. It is created with the extension «.csv».



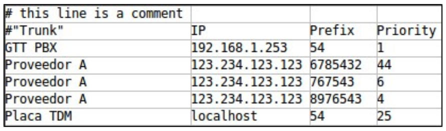
Buscar por: Ruta
Buscar texto:
Proveedor: Enlace 204

Archivo: Seleccionar archivo No se eligió archivo
Sample file:

Proveedor	Ruta	Prioridad	Acción
Enlace 204	2	2	borrar
Enlace 204	4	2	borrar
Enlace 204	5	2	borrar
Enlace 204	6	1	borrar
Enlace 204	7	1	borrar

Figure 3.62: Advanced Interface: Provider Route Query Example

The «Add Routes from File» option makes it possible to add routes in a simple way, by loading a file; To do this, click on «Select file». This file must be in «.csv» format and have the order of the following table (this is the example that can be downloaded by clicking on the 📄 icon next to «Sample file:> >).



# this line is a comment			
#"Trunk"	IP	Prefix	Priority
GTT PBX	192.168.1.253	54	1
Proveedor A	123.234.123.123	6785432	44
Proveedor A	123.234.123.123	767543	6
Proveedor A	123.234.123.123	8976543	4
Placa TDM	localhost	54	25

Figure 3.63: Advanced interface: Example importable file with provider paths

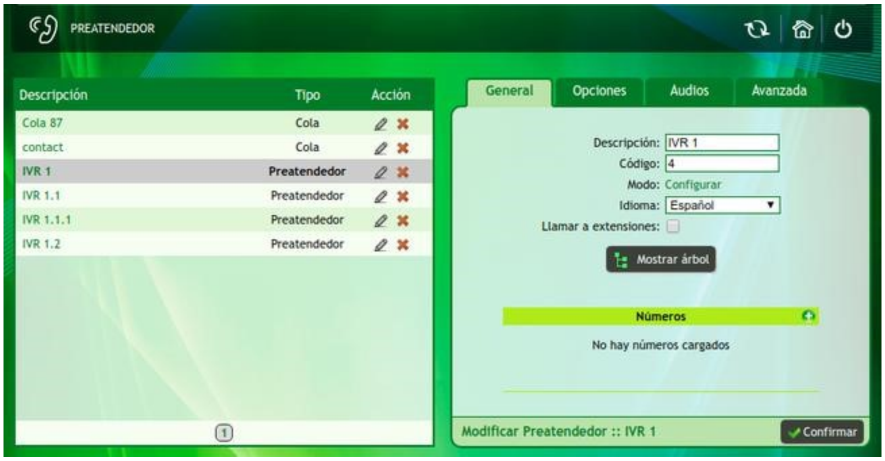
- **Trunk**: the name of the provider is placed in this column.
- **IP**: refers to the IP number that you want to reach.
- **Prefix**: the digits that make up the prefix must be placed in the third column.
- **Priority**: it is necessary to establish the priority order of the routes, for this the fourth column is used.

It is recommended to edit the fields of the templates and then verify that the format has not been modified. Finally, you must click on the «Confirm» button.

3.3.5 Preattendant

The Pre-attendant is in charge of answering a call, and playing an audio that normally explains to the interlocutor what steps he must follow to reach the desired destination. This is why the audios are called IVR (*Interactive Voice Response* or Interactive Voice Response). They allow, in a certain way, to interact with the user. It is also possible to create preattenders with *hung up*, which just play some audio and then cut it off.

In addition, in the Pre-attendant menu, queues can be created to queue calls and have them wait until the Agents associated with them are released and can receive them. Queues do not replace IVRs but complement each other to achieve ACD (*Automatic Call Distributor*) functionality for Call Centers.



Descripción	Tipo	Acción
Cola 87	Cola	✎ ✖
contact	Cola	✎ ✖
IVR 1	Preatendedor	✎ ✖
IVR 1.1	Preatendedor	✎ ✖
IVR 1.1.1	Preatendedor	✎ ✖
IVR 1.2	Preatendedor	✎ ✖

Descripción: IVR 1
Código: 4
Modo: Configurar
Idioma: Español
Llamar a extensiones: □

Números

No hay números cargados

Modificar Preatendedor :: IVR 1

Figure 3.64: Advanced Interface: Preattenders

3.3.5.1 See Preattendant-Queues

From this tab you can see the pre-attenders created. If you click on the ✎ icon under the Action column, you can see in the box on the right all the settings of this preattendant. Four tabs are displayed there, where you can make the settings detailed below.

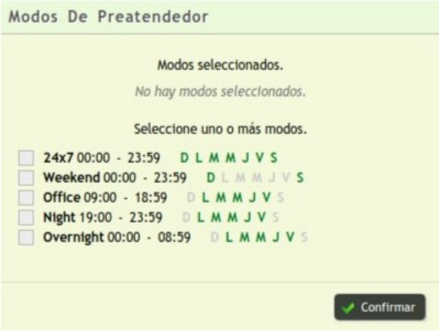
3.3.5.1.1 View Preattendant-Queues General Tab From the General tab you can modify the following fields.

- **Description**: the name or description of the preattendant
- **Language**: select the desired language

- **Call extensions**: allows while listening to the preattendant audio to call the desired extension

- **Code**: number that represents the preattendant within the database

- **Mode**: it is necessary to click on «Configure» which will show a window where you can choose the mode or hours of operation of the pre-attender (for more information you can consult Modes on page 81). To exit this window, click on the button «✔ Confirm»



Modos De Preatendedor

Modos seleccionados.

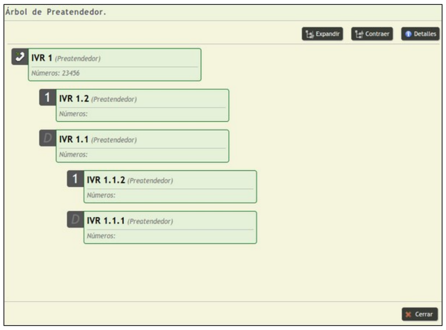
No hay modos seleccionados.

Seleccione uno o más modos.

☐ **24x7** 00:00 - 23:59 D L M M J V S
☐ **Weekend** 00:00 - 23:59 D L M M J V S
☐ **Office** 09:00 - 18:59 D L M M J V S
☐ **Night** 19:00 - 23:59 D L M M J V S
☐ **Overnight** 00:00 - 08:59 D L M M J V S

Figure 3.65: Advanced Interface: Pre-Attendant Modes

- ☰ **Show tree**: By clicking on the icon you can see in the form of a tree diagram, all the pre-attenders in cascade from the selected one. Here is an example:



Árbol de Preatendedor.

IVR 1 *(Preatendedor)*
Números: 23456

1 **IVR 1.2** *(Preatendedor)*
Números:

D **IVR 1.1** *(Preatendedor)*
Números:

1 **IVR 1.1.2** *(Preatendedor)*
Números:

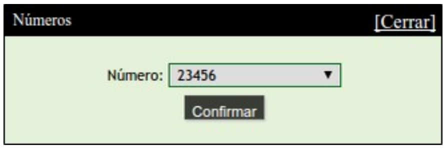
D **IVR 1.1.1** *(Preatendedor)*
Números:

Figure 3.66: Advanced Interface: Pre-Server Tree

The calls enter IVR 1 with the access number 23456, which presents two options. Pressing 1 enters IVR 1.2 and the default option is IVR 1.1. The latter allows you to press the digit 1 to enter the IVR 1.1.2 or the default option 1.1.1.

- **Numbers**:

  - To add access numbers (for more information about access numbers it is recommended to see **??** on page **??**) by clicking on the ✚icon. This will show a pop-up window where it is possible to select the access number to associate, after that, it will be enough to press the button «✔ Confirm»; If you do not wish to save the change, it is recommended to click on «[Close]»



Números [Cerrar]

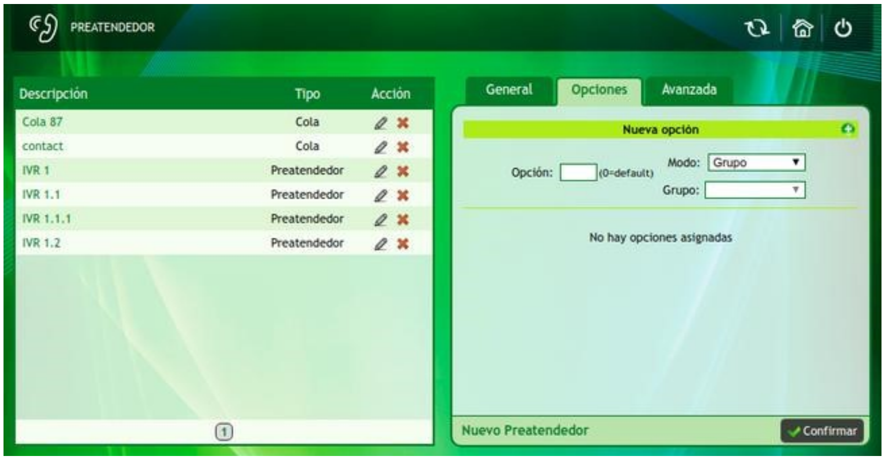
Número: 23456

Figure 3.67: Advanced interface: Assign access number to preattendant

- To delete access numbers, it will only be necessary to click on the − icon located next to the item to be deleted

- ✓ **Confirm**: saves the changes that have been made

3.3.5.1.2 View Preattendant-Queue Options Tab The second configuration tab is Options, from here the association between the preattendant and a particular action is made.



Descripción	Tipo	Acción
Cola 87	Cola	
contact	Cola	
IVR 1	Preatendedor	
IVR 1.1	Preatendedor	
IVR 1.1.1	Preatendedor	
IVR 1.2	Preatendedor	

Opción: (0=default) Modo: Grupo
Grupo:

No hay opciones asignadas

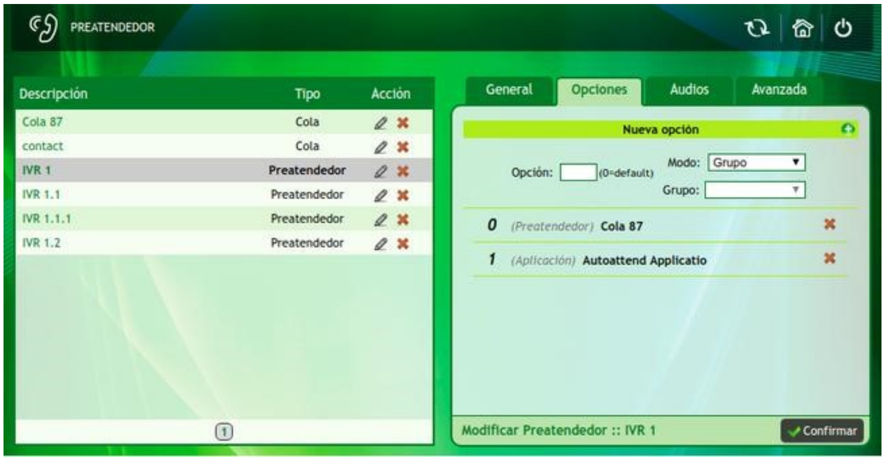
Figure 3.68: Advanced Interface: Pretender Options

It is necessary to complete the fields in the New option box as follows:

- **Option**: number to dial to execute the action. By default the option is zero
- **Mode**: must be chosen among the four possibilities listed below:
  - **Group**: allows the call to be diverted to a group, which will be in charge of answering in the way it is configured (from the Groups menu).
  - **Preattendant**: the call from the preattendant is diverted to another preattendant. With this, a cascading configuration can be carried out (prearranged tree). In this section you can add Queues as an option for the Preattendant.
  - **Application**: If this option is selected, the application you selected is executed.
  - **Extension**: allows marking the extension declared as Preattendant option.

Configuration of preattendant options It is necessary to create a default option, this option is assigned the number 0.

In order to create the options, you must complete the boxes, choose who is assigned to them, and then click on the + icon. As this procedure is followed to create the options, a list like the one shown in the following figure is formed:



PREATENDEDOR

Descripción	Tipo	Acción
Cola 87	Cola	
contact	Cola	
IVR 1	Preatendedor	
IVR 1.1	Preatendedor	
IVR 1.1.1	Preatendedor	
IVR 1.2	Preatendedor	

Opción: (0=default) Modo: Grupo
Grupo:

0 (Preatendedor) Cola 87

1 (Aplicación) Autoattend Applicatio

Modificar Preatendedor :: IVR 1

Figure 3.69: Advanced Interface: Pretender Options Example

!

To save the changes, click on the «✓ Confirm» icon.

3.3.5.1.3 View Preattendant-Queue Audios Tab

3.3.5.1.3.1 Preattender Audios From the Audios tab you can select the audio that will be played in the IVR. To achieve this, the desired pre-attender must be chosen.

Then, in the window located on the right: «New audio», if the audio file is on the computer, the audio file is selected from the ⚙icon.

It is also possible to record the preattendant message through a device registered in the network. To do this, dial *73 and after the tone it is possible to make the recording. Once the audios are added by clicking on the ✓icon.

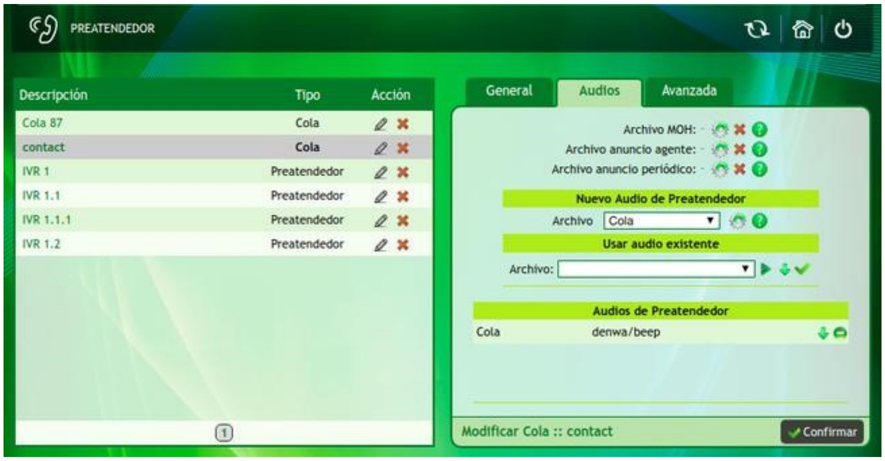
The audios that have been assigned to the pre-attendant (either by loading from the computer or by recording and selecting from the drop-down list) are shown in the form of a list at the bottom, under the heading «Audios»; from where it is possible to download them (↓) or delete them (—).

The files must meet the following parameters to be compatible:

- **File type**: WAV
- **Bit Rate**: 128 kbps
- **Audio Sample Size**: 16 bits
- **Channels**: 1 (mono)
- **Audio Sample Rate**: 8 KHz
- **Audio Format**: PCM

Press «✓ Confirm» to save the changes.

3.3.5.1.3.2 Audio Queue From the Audios tab you can select the audio that will be played in the IVR.



Descripción	Tipo	Acción
Cola 87	Cola	✎ ✖
contact	Cola	✎ ✖
IVR 1	Preatendedor	✎ ✖
IVR 1.1	Preatendedor	✎ ✖
IVR 1.1.1	Preatendedor	✎ ✖
IVR 1.2	Preatendedor	✎ ✖

Archivo MOH: -
Archivo anuncio agente: -
Archivo anuncio periódico: -

Archivo: Cola

Archivo:

Cola	denwa/beep

Modificar Cola :: contact

Figure 3.71: Advanced Interface: Queue Audio

- **MOH file**: music on hold to be configured
- **Agent announcement file**: announcement sent to the agent before receiving the call (usually indicates the name of the pre-attendant option)
- **Periodic announcement file**: announcement that will be given every certain period of time
- **New pre-attender audio**: audio provided before starting music on hold
- **Use existing audio**: file from the recording generated from a telephone terminal

To select the audio file for music on hold, agent announcement, periodic announcement and queue pre-attendant, if the audio file is on the computer, the audio file is searched from the ⚙icon . Instead, to delete the hold music and agent announcement files, press ✖.

It is also possible to record the queue message using a computer registered in the network. To do this, dial *73 and after the tone it is possible to make the recording. Once the audios are added by clicking on the ✔icon.

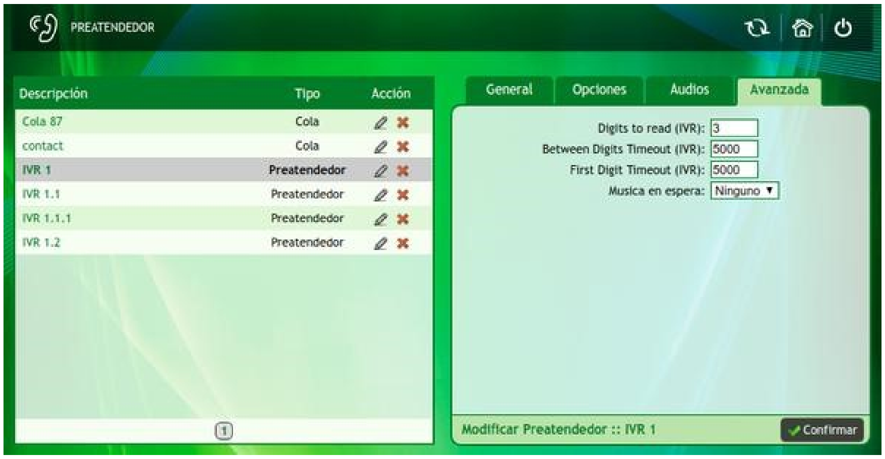
The audios that have been assigned to the queue (either by loading from the computer or by recording and selecting from the drop-down list) are shown in the form of a list at the bottom, under the heading «Audios»; from where it is possible to download them (🡻) or delete them (━).

The files must meet the following parameters to be compatible:

- **File type**: WAV
- **Bit Rate**: 128 kbps
- **Audio Sample Size**: 16 bits
- **Channels**: 1 (mono)
- **Audio Sample Rate**: 8 KHz
- **Audio Format**: PCM

Press «✔ Confirm» to save the changes.

3.3.5.1.4 View Preattender Advanced Tab



Descripción	Tipo	Acción
Cola 87	Cola	✎ ✖
contact	Cola	✎ ✖
IVR 1	Preatendedor	✎ ✖
IVR 1.1	Preatendedor	✎ ✖
IVR 1.1.1	Preatendedor	✎ ✖
IVR 1.2	Preatendedor	✎ ✖

Digits to read (IVR): 3
Between Digits Timeout (IVR): 5000
First Digit Timeout (IVR): 5000
Musica en espera: Ninguno ▼

Modificar Preatendedor :: IVR 1

Figure 3.72: Advanced Interface: Advanced Pretender Settings

3.3.5.1.4.1 Preattendant

- **Digits to read (IVR)**: determine the number of digits that are allowed to be dialed to make the call.
- **Between Digits Timeout (IVR)**: sets the maximum inter-digit timeout to wait.
- **First Digit Timeout (IVR)**: maximum waiting time to dial the first number of the extension.
- **Music on Hold**: When configured, in the call that enters a user from the pre-attendant and is left on hold, this music on hold (MOH) is played. To do this, an audio file must be previously loaded in the Configuration Section > Announcements > Music on hold (see Music on Hold on the 131 page).

3.3.5.2 New Preattendant

To create a new pre-attendant, the following steps must be followed.

- **General**:
  - **Description**: the name or description of the preattendant
  - **Language**: select the desired language
  - **Call extensions**: allows while listening to the preattendant audio to call the desired extension
  - **Code**: number that represents the preattendant within the database
  - **Mode**: it is necessary to click on «Configure» which will show a window where you can choose the mode or hours of operation of the pre-attender (for more information you can consult Modes on page 81). To exit this window, click on the button «✔ Confirm»
  - **Call extensions**: allows while listening to the audio from the preattendant to call the desired extension.

  - ☰ **Show tree**: By clicking on the icon you can see in the form of a tree diagram, all the pre-attenders in cascade from the selected one. However, when registering a new attendant, a pop-up window will be displayed indicating «You must choose a attendant from the list»
  - **Numbers**:
    - To add access numbers (for more information about access numbers it is recommended to see **??** on page **??**) by clicking on the +icon. This will show a pop-up window where it is possible to select the access number to associate, after that, it will be enough to press the button «✓ Confirm»; If you do not wish to save the change, it is recommended to click on «[Close]»
    - To delete access numbers, it will only be necessary to click on the − icon located next to the item to be deleted
  - ✓ **Confirm**: saves the changes that have been made

- **Options**:
  - **Option**: number to dial to execute the action. By default the option is zero
  - **Mode**: must be chosen among the four possibilities listed below:
    - **Group**: allows the call to be diverted to a group, which will be in charge of answering in the way it is configured (from the Groups menu).
    - **Preattendant**: the call from the preattendant is diverted to another preattendant. With this, a cascading configuration can be carried out (prearranged tree). In this section you can add Queues as an option for the Preattendant.
    - **Application**: If this option is selected, the application you selected is executed.
    - **Extension**: allows marking the extension declared as Preattendant option.

  Configuration of preattendant options It is necessary to create a default option, this option is assigned the number 0.

  In order to create the options, you must complete the boxes, choose who is assigned to them, and then click on the +icon. As this procedure is followed to create the options, a list like the one shown in the following figure is formed.

  !

  To finish, click on the «✓ Confirm» button.

3.3.5.3 New Queue

Queue is the name given to a list of elements waiting to be attended, until the automatic call distributor (ACD) distributes the calls according to the defined rules to the respective agents (operators).

A new queue can be created from the preattendant menu, the creation concept, preattendance audio and access numbers are the same as those of a common IVR.

- **General**:
  - **Description**: The name of the new Queue.
  - **Mode**: it is necessary to click on «Configure» which will show a window where you can choose the mode or hours of operation of the pre-attender (for more information you can consult Modes on page 81). To exit this window, click on the button «✓ Confirm»
  - **Language**: Select the language for this queue.

        - **Group**: the name of the extension group to which the task of handling queued calls is assigned.
        - **Strategy**:
            - **Least Recent**: The extension that was idle the longest rings.
            - **Fewest calls**: it is granted to the extension that answered the fewest calls.
            - **Random**: Any extension will ring, randomly.
            - **Round Robin**: cyclically they will ring once each.
            - **Linear**: will follow a linear order. An order of attention is established in the users. When entering a call, it will always do so to agent number one, if he is busy or not there, he will continue with agent two.
            - **Simultaneous**: all extensions in the group ring when a call comes in. The simultaneous ring strategy is not compatible with the use of the Denwa Barra CTI software. When selecting this strategy in a queue, the following confirmation message is displayed:
    - **Ring Time**: the time that the internal ringing will last.
    - **Agent waiting time**: It is the time that the Agent will wait before dispatching another call.
    - **Default extension**: If no agent picks up the call, it will be redirected to an extension that may be the supervisor's or the extension assigned for this reason.
    - **Login required**: If the option is set to YES, agents require a login to be ready to receive calls. Otherwise it is not required and they can always receive calls.
    - **Numbers**:
        - To add access numbers (for more information about access numbers it is recommended to see **??** on page **??**) by clicking on the +icon. This will show a pop-up window where it is possible to select the access number to associate, after that, it will be enough to press the button «✓ Confirm»; If you do not wish to save the change, it is recommended to click on «[Close]»
        - To delete access numbers, it will only be necessary to click on the − icon located next to the item to be deleted
- **Advanced**:
    - **Maximum waiting time**: is the maximum time that the interlocutor will wait before the communication is cut off. Wait without users in queue: allows you to specify whether the call is cut directly or not, in case there are no agents waiting to answer.
    - **Automatic answering**: This option allows that if an agent is logged in the queue and available, the call is transferred to him and answered automatically.
    - **Priority between queues**: Priority setting between queues (1 is the highest priority value).
    - **Recurring Announcement**: Enable the recurring announcement. This ad is loaded in the Queue Audios section
    - **Periodic Announcement Frequency**: Configure the frequency at which the periodic announcement is played.
    - **Position in queue**: Configure the option to give the end user the position in which they are in the queue.
    - **Average Wait Time**: Enable the announcement of average wait time in the queue.
    - **Frequency**: Frequency, in seconds, at which the average wait time is played.
- ✓ **Confirm**: saves the changes that have been made

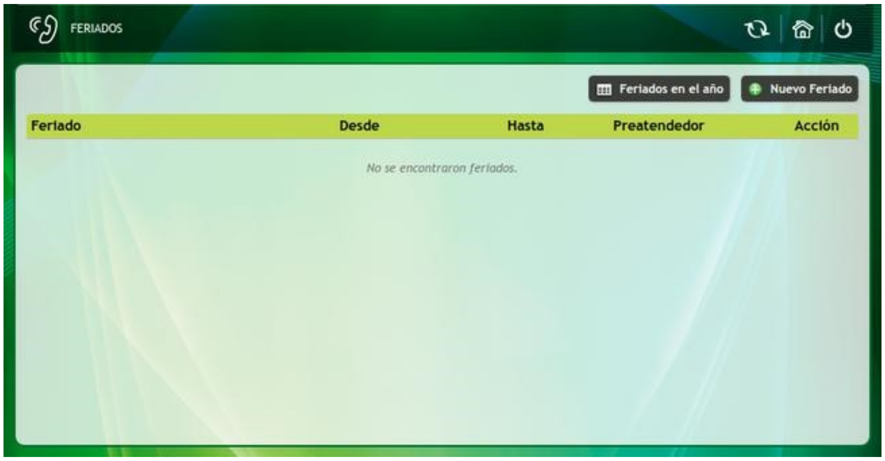
3.3.5.4 Holidays

This section explains the function of the central for forwarding the access numbers of pre-attenders on special dates. On these dates users will not be available in the corresponding areas.

Requirement

In order to use the function, preattendants must have been created with their respective access numbers and options for each one. In addition, one or several pre-attenders with special destinations must have been created to be used on Holidays and partial holidays.

The main view allows you to see the list of holidays that have been configured, under the Action column are the icons ✖ that allows you to delete the holiday and ✎ that allows you to modify the parameters of the holiday, showing a window popup that will allow you to change the same fields used in the registration form of a new holiday.



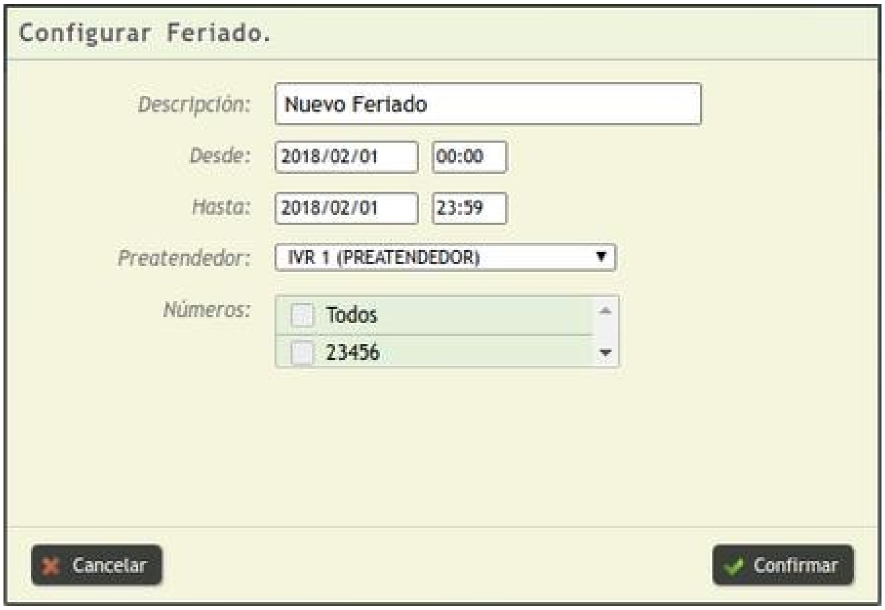
Feriado	Desde	Hasta	Preatendedor	Acción

No se encontraron feriados.

Figure 3.74: Advanced interface: Holidays

3.3.5.4.1 Holiday registration

The registration of holidays can be done from any of the two buttons found on the screen, namely «⊕ New Holiday» and «📅 Holidays in the year», only when clicking on the last one will show (prior to the form) a calendar, where you must double click on the date.



Configurar Feriado.

Descripción: Nuevo Feriado

Desde: 2018/02/01 00:00

Hasta: 2018/02/01 23:59

Preatendedor: IVR 1 (PREATENDEDOR)

Números:
- □ Todos
- □ 23456

Figure 3.75: Advanced Interface: Holiday Settings

The data to complete are:

- **Description**: name of the holiday
- **From**: date and time of the beginning of the configuration of this holiday. If you have selected the date from the calendar, this field will be preconfigured.
- **To**: date and time of the end of the configuration of this holiday. If you have selected the date from the calendar, this field will be preconfigured.
- **Pedestrian**: name of the preattendant where the access numbers are diverted, in general this is a preattendant created with a special audio for the type of holiday or holiday.
- **Numbers**: access numbers that are forwarded to the pre-attendant.

Once this period established for him has ended, the configuration of the access numbers is automatically returned to their respective pre-attendants.

3.3.5.5 Modes

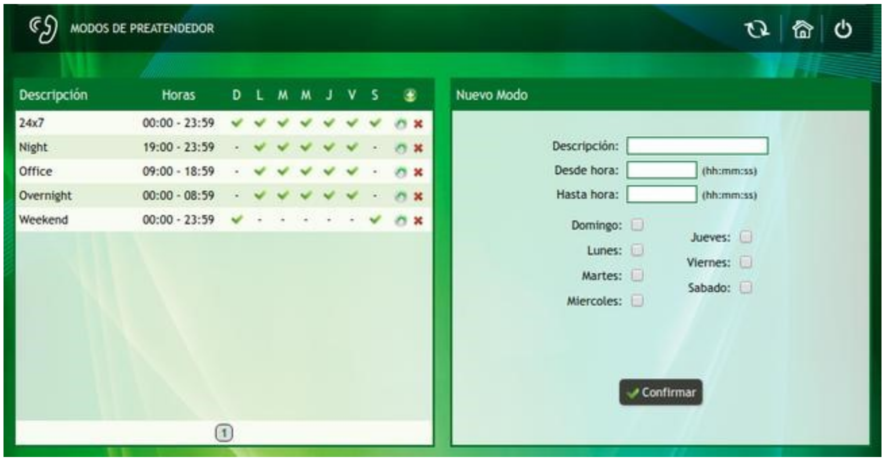
The «Modes» section allows you to make weekly configurations that will later be assigned to pre-attenders and queues. Its main screen is divided into two sections: the left, where all the modes already created are listed, and the right, where it is possible to create new modes.

Existing modes can be deleted (✖) or edited (✎) by clicking on the corresponding icon in the «Actions» column.

3.3.5.5.1 Creating Modes To create a mode it is necessary to complete the form that is on the right of the screen, with the following information:

- **Description**: descriptive name of the mode. This field will be reflected in the list that will be displayed when defining the «Mode» when registering a new queue or a new pre-attendant (see New Preattendant and New Queue in the pages 77 and 78, respectively) so it is necessary that the description be as clear and concise as possible.

- **From time**:mode start time
- **Until time**: mode end time
- **Day of the week**: day of the week on which it will be applied



Descripción	Horas	D	L	M	M	J	V	S	
24x7	00:00 - 23:59	✓	✓	✓	✓	✓	✓	✓	
Night	19:00 - 23:59	-	✓	✓	✓	✓	✓	-	
Office	09:00 - 18:59	-	✓	✓	✓	✓	✓	-	
Overnight	00:00 - 08:59	-	✓	✓	✓	✓	✓	-	
Weekend	00:00 - 23:59	✓	-	-	-	-	-	✓	

Descripción:
Desde hora: (hh:mm:ss)
Hasta hora: (hh:mm:ss)
Domingo: □
Lunes: □
Martes: □
Miercoles: □
Jueves: □
Viernes: □
Sabado: □

Figure 3.76: Advanced Interface: Modes

Day and time

For the correct operation of the Modes it is necessary that the device has its current date and time parameters, this requires the proper configuration of the NTP server (see NTP Server on page 125) and internet connection, unless you are locally.

The process will end by pressing the «✓ Confirm» button.

Association

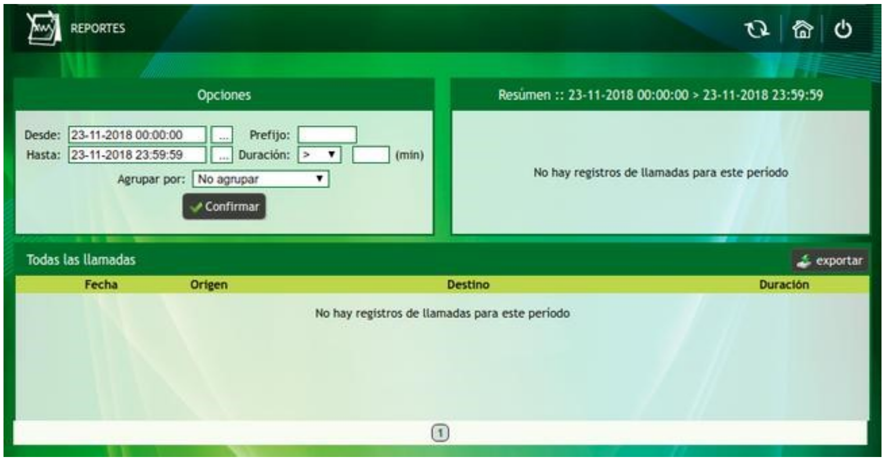
If a mode is associated with a queue or a pre-attendant, it cannot be deleted.

3.3.6 Reports

In this section you can find all the call records, recordings, access numbers, system resources and attendants.

3.3.6.1 Calls

3.3.6.1.1 All calls In this report it is possible to view all calls, whether incoming, outgoing or internal; by default it shows the records of the current day.



Resúmen :: 23-11-2018 00:00:00 > 23-11-2018 23:59:59

Desde: 23-11-2018 00:00:00 ...
Hasta: 23-11-2018 23:59:59 ...
Prefijo:
Duración: > (min)
Agrupar por: No agrupar

No hay registros de llamadas para este periodo

Fecha	Origen	Destino	Duración
No hay registros de llamadas para este periodo			

Figure 3.77: Advanced interface: Report all calls

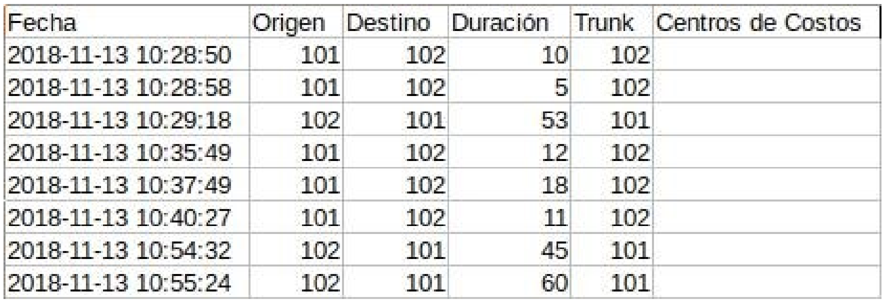
The screen is divided into three boxes:

- **Options**: These options are filters that allow a faster and easier search for whoever has to interpret it.
  - **From**: this field makes it possible to search within a limited period of time (day, month, year and hour). To do this, you must click on «...» and the window of the following image is observed; with calendar and time alternatives.
  - **Until**: this field makes it possible to search within a limited period of time (day, month, year and hour). To do this, you must click on «...» and the window of the following image is observed; with calendar and time alternatives.
  - **Prefix**: This field is optional and enables filtering using the prefix. Only the corresponding digits should be placed in this field.
  - **Duration**: these fields are optional
    - **>**: Indicates that calls that exceed the specified time will be listed
    - **<**: Indicates that those calls that do not exceed the indicated time will be listed
    - **Time**: time to consider for filtering, must be expressed in minutes
  - **Group By**: This field is optional, it allows various actions depending on the selection from the dropdown menu. The options are:
    - Do not group
    - User
    - Group

    If any grouping is executed, the detail of the record is observed in fewer lines.
  - ✓ **Confirm**: this button triggers the search for the corresponding call logs, applying the previously selected filters.
- **Summary**: The information displayed in this box refers to the applied filters. Among them are:
  - **Total calls**: shows the number of calls; thus including those that have been successful and those that have not.
  - **Calls Completed**: This amount refers to the number of calls that have been answered.

  - **Calls not completed**: is the difference between the total calls and the completed calls.
  - **ASR**: shows the percentage value of this ratio, which is calculated taking into account the calls answered with respect to the total volume of calls (see New Provider ASR Alarms Tab)
  - **Total duration**: refers to the sum of the duration of each of the calls.
  - **Average Duration**: This item displays the average duration of calls.
- **All calls**: This box presents the information arranged in columns.
  - **Date**: This column displays the date and time the call was made.
  - **Origin**: Displays the number that initiates the call.
  - **Destination**: Displays the number that is being called.
  - **Duration**: refers to the duration of the call in question.

  On the edge of this box is the «⬇ exportar» button, which allows you to download the entire list in .csv format.



Fecha	Origen	Destino	Duración	Trunk	Centros de Costos
2018-11-13 10:28:50	101	102	10	102	
2018-11-13 10:28:58	101	102	5	102	
2018-11-13 10:29:18	102	101	53	101	
2018-11-13 10:35:49	101	102	12	102	
2018-11-13 10:37:49	101	102	18	102	
2018-11-13 10:40:27	101	102	11	102	
2018-11-13 10:54:32	102	101	45	101	
2018-11-13 10:55:24	102	101	60	101	

Figure 3.78: Advanced interface: Example of the exportable report of all calls

Call log duration

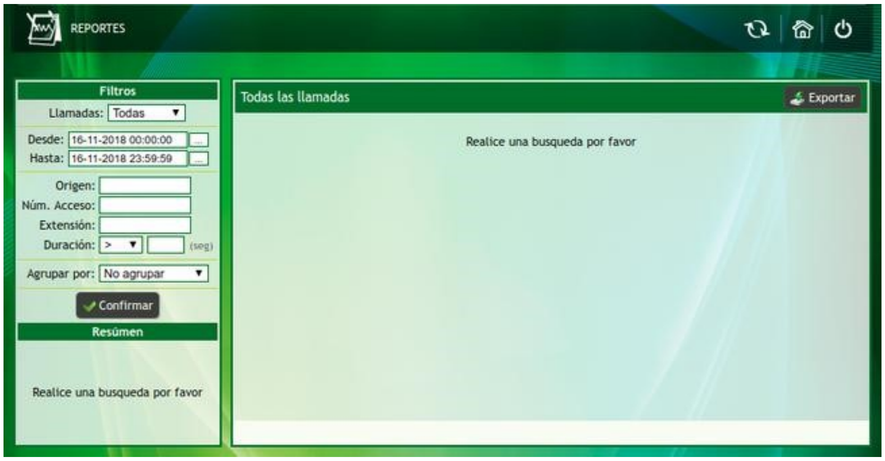
By default, call logs are saved for up to three (3) months of history; however this can be changed in the maintenance configurations section (see Maintenance on page 139).

3.3.6.1.2 Incoming calls This report has the same resources as the previous one (see All calls on page 82), only that it already includes the filter for incoming calls.

3.3.6.1.3 Outgoing calls As with the incoming calls report, it has the same resources as the previous one (see All calls on page 82), only it already has the filter for outgoing calls.

3.3.6.1.4 Internal calls In the same way as with the two (2) previous reports, in addition to having the same alternatives as in «All calls» (see All calls on page 82), filtering is performed for internal calls; that is, within the same Denwa UC&C 4.0.1
.

3.3.6.1.5 Extended This report has the same resources as the «All calls» report (see All calls on page 82); however, it has an aggregate of options that provide deeper detail. The Extended window is displayed in the following figure.



REPORTES

Filtros

Llamadas: Todas

Desde: 16-11-2018 00:00:00 ...
Hasta: 16-11-2018 23:59:59 ...

Origen:
Núm. Acceso:
Extensión:
Duración: > (seg)

Agrupar por: No agrupar

✓ Confirmar

Resúmen

Realice una busqueda por favor

Todas las llamadas

Exportar

Realice una busqueda por favor

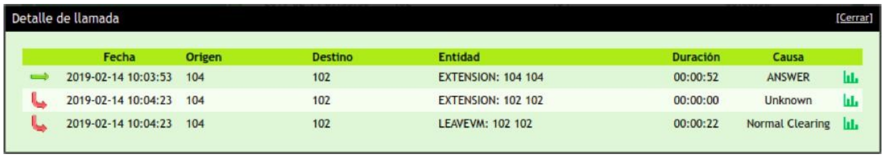
Figure 3.79: Advanced interface: Extended report of all calls

- **Options**: These options are filters that allow a faster and easier search for whoever has to interpret it.
  - **From**: this field makes it possible to search within a limited period of time (day, month, year and hour). To do this, you must click on «...» and the window of the following image is observed; with calendar and time alternatives.
  - **Until**: this field makes it possible to search within a limited period of time (day, month, year and hour). To do this, you must click on «...» and the window of the following image is observed; with calendar and time alternatives.
  - **Prefix**: This field is optional and enables filtering using the prefix. Only the corresponding digits should be placed in this field.
  - **Duration**: these fields are optional
    - **>**: Indicates that calls that exceed the specified time will be listed
    - **<**: Indicates that those calls that do not exceed the indicated time will be listed
    - **Time**: time to consider for filtering, must be expressed in minutes
  - **Group By**: This field is optional, it allows various actions depending on the selection from the dropdown menu. The options are:
    - Do not group
    - User
    - Group

    If any grouping is executed, the detail of the record is observed in fewer lines.
  - ✓ **Confirm**: this button triggers the search for the corresponding call logs, applying the previously selected filters.
- **Summary**: The information displayed in this box refers to the applied filters. Among them are:
  - **Total calls**: shows the number of calls; thus including those that have been successful and those that have not.
  - **Calls Completed**: This amount refers to the number of calls that have been answered.
  - **Calls not completed**: is the difference between the total calls and the completed calls.

- **ASR**: shows the percentage value of this ratio, which is calculated taking into account the calls answered with respect to the total volume of calls (see New Provider ASR Alarms Tab)
- **Total duration**: refers to the sum of the duration of each of the calls.
- **Average Duration**: This item displays the average duration of calls.

- **All calls**: This box presents the information arranged in columns.
  - **Date**: This column displays the date and time the call was made.
  - **Origin**: Displays the number that initiates the call.
  - **Destination**: Displays the number that is being called.
  - **Duration**: refers to the duration of the call in question.
  - **Cause**: Indicates the reason why the call was terminated.
  - **🔍**: By clicking on the icon, a pop-up window is displayed with the details of all the events of the call, namely:

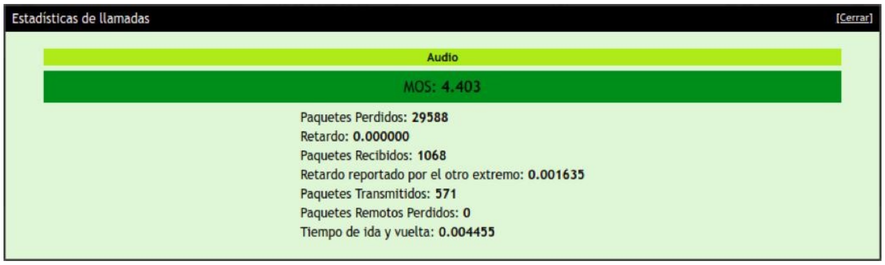


Detalle de llamada [Cerrar]

	Fecha	Origen	Destino	Entidad	Duración	Causa	
→	2019-02-14 10:03:53	104	102	EXTENSION: 104 104	00:00:52	ANSWER	📊
↳	2019-02-14 10:04:23	104	102	EXTENSION: 102 102	00:00:00	Unknown	📊
↳	2019-02-14 10:04:23	104	102	LEAVEVM: 102 102	00:00:22	Normal Clearing	📊

Figure 3.80: Advanced interface: Extended report, call detail

- **Arrows**: There are arrows to represent the different events:
  - →: incoming
  - ←: outgoing
  - ↪: call breakdown
- **Date**: is the timestamp of the event, it is possible that between the first and second row there are a few seconds difference; this is due to the fact that when the source, A, makes a call to B, there is a short delay in the exchange that will carry out the call.
- **Origin**: who originates the call
- **Destination**: to whom the call is directed
- **Entity**: the type of entity from whom the call originates or to whom the call is derived is indicated; for example it can be an extension, a pre-attender or a trunk
- **Duration**: duration of the call at each stage, it is in «hh:mm:ss» format
- **Cause**: cause of disconnection or termination of the call
- **📊**: allows to know the MOS statistics (*Mean Opinion Score*) to evaluate the quality of the call:



Estadísticas de llamadas [Cerrar]

Audio

MOS: 4.403

Paquetes Perdidos: **29588**
Retardo: **0.000000**
Paquetes Recibidos: **1068**
Retardo reportado por el otro extremo: **0.001635**
Paquetes Transmitidos: **571**
Paquetes Remotos Perdidos: **0**
Tiempo de ida y vuelta: **0.004455**

Figure 3.81: Advanced interface: Extended report, call statistics

MOS (*Mean Opinion Score*)

The MOS in VoIP is used to know the audio quality of calls. The calculation is carried out through algorithms/formulas and its result is distributed on a scale from 1 to 5, being:

- 5Excellent
- 4Good
- 3Acceptable
- 2Poor
- 1Bad

On the edge of this box is the «⤓export» button, which allows you to download the entire list in .csv format, said file contains the following information:

- **CallId**: this numbering allows the call to be identified in the different types of records.
- **ConnectTime**: this column refers to the date and time, that is, the connection time.
- **LegType**: here it is indicated how the central office sees the call. For example: when calling from one telephone to another, two events occur: the first is that the control panel sees the originating call as incoming (In); then it sends said call to the destination and observes it as outgoing (Out). PeerType: in this field it is verified what type of entities are those that participate in the call.
- **Peer**: This field corresponds to the previous one, since it shows the name that has been designated, for example, to the participating extension or trunk.
- **ANI**: (*Automatic Number Identification*) allows you to identify the number of the person making the call.
- **Destination**: the data of who is executing the call is provided.
- **Disconnect/Description**: exposes if the call has been answered, canceled or who of the participants has finished it.
- **Duration**: This field verifies the duration, in seconds, of the call.
- **Channel/Protocol**: indicates the channel or protocol used to make the call, this depends on whether or not you have telephone panels.
- **ChannelDescription**: in the first part of the call, that is, from the origin to the exchange, this field shows the origin IP. On the other hand, from the exchange to the destination it shows: the internal if the call is between extensions, the provider IP if the call is external and the channel if it uses TDM.
- **PBXPrefix**: it is used in the case of existing virtual exchanges.
- **CallService**: this column displays the type of call, including national, local, internal, international, special, mobile, among others.

Extended call records duration

By default, extended call logs are saved for up to one (1) month of history; however this can be changed in the maintenance configurations section (see Maintenance on page 139).

3.3.6.1.5.1 New Report

From here it is possible to generate a New Scheduled Report, for which it is necessary to complete the following fields:

- **Description**: the description or name of the scheduled report must be placed.
- **Call type**: select which calls you want the report on, you must choose one of the options from the drop-down menu: incoming, outgoing or internal. The default option is «Outgoing».
- **Group by**: grouping by PBX, user, group, rule or without grouping can be done in the report. The default option is «Do not group».
- **Run every**: it is scheduled how often this report is generated, the drop-down menu options are Hour(s), Day(s) and Month(s). In addition to the default option that is «Do not schedule», that is, the report is not created.
- **Include the last**: includes the last time on which the report is made. The drop-down menu options are Hour(s), Day(s), and Month(s).
- **Send by e-mail to**: enter the e-mail box where you want to receive the report and press the button. More than one email address can be added.
- **Filters**: There is also the possibility of adding filters; clicking on the + icon leads to the following window. Where it is allowed to accommodate the following variables according to our needs.
    - **Filter By**: You can filter by PBX, Group, Duration, Source, Destination, Redirected To, and Rule.
    - **Operator**: this field varies depending on the selection of the previous option. The operator is also associated with the value to be entered from the next field. Depending on the case, the operator can be: is (=), starts with, greater, less or equal.
    - **Value**: according to the selection that has been chosen in Filter by, it will be the value to enter. It can be a PBX, a group, a rule or a numerical value that completes the rule in question. Pressing «**Confirm**» generates the filter rule. You can see a list with the filter rules associated with the report. To delete a rule, press the −button.

  Finally, in order to create the scheduled report, you must click on the Confirm button.

> **Note**
>
> Multiple filter rules can be added. To observe the settings of each programmed report, you must click on the desired description or name (Reports section) and the settings of the same are displayed in the right sector of the screen.

3.3.6.1.5.2 Reports

Here is the list of existing reports. Options are provided to make changes to them, by clicking Modify or by clicking on the name or description of the report. It is allowed to delete them one by one (Delete). To generate a new scheduled report, all you have to do is press the Add button, which enables the right sector of the screen with the fields to complete for the respective creation.

3.3.6.2 Recordings

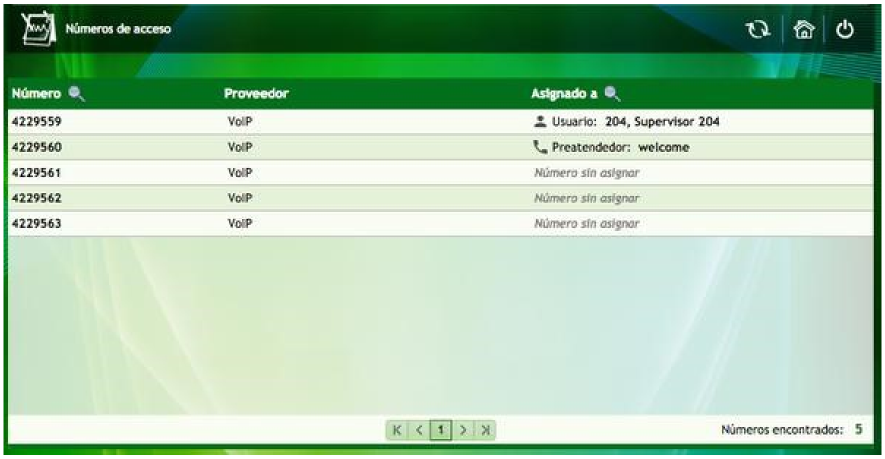
This function allows you to view, listen to and download the recordings of all the calls that are being recorded, either by user (see New User, page 36), trunk (New Provider, page 64) or group (New Group, page 61).

In the previous image two large boxes are displayed, each of them is explained below.

- **Filters**: These options allow a faster and easier search for whoever has to interpret it.
    - **From**: this field makes it possible to search within a limited period of time (day, month, year and hour). To do this, you must click on «...» and the window of the following image is observed; with calendar and time alternatives.
    - **Until**: this field makes it possible to search within a limited period of time (day, month, year and hour). To do this, you must click on «...» and the window of the following image is observed; with calendar and time alternatives.
    - **Provider**: (optional) This field offers the possibility of filtering the calls of the providers, in case they exist.
    - **Preattendant**: (optional) this field offers the possibility of filtering the calls that have been taken by any of the preattenders, if they exist.
    - **Duration**: these fields are optional
        - **>**: Indicates that calls that exceed the specified time will be listed
        - **<**: Indicates that those calls that do not exceed the indicated time will be listed
        - **Time**: time to consider for filtering, must be expressed in minutes
    - 🔍 **Search**: clicking here runs the search considering the selected filters. The results are observed in the Recordings box.
    - ⤓ **Export**: clicking this option exports the recording files; a zip is generated that contains the audios in wav format.
    - ✖ **Delete**: clicking this button applies the search filters and deletes the results obtained.
- **Recordings**: this field presents the search result, ordered in the following columns.
    - **Date**: This column displays the date and time the call was made.
    - **Origin**: Displays the number that initiates the call.
    - **Destination**: Displays the number that is being called.
    - **Size**: This column reports the size of the recording itself.
    - **Action**: grants the possibility of:
        - ▶: play the audio of the recording
        - ⊘: delete the recording

3.3.6.3 Accession numbers

In this section, you can obtain the details of the access numbers (see **??** on page **??**), and to what or to whom they were assigned.



Número	Proveedor	Asignado a
4229559	VoIP	Usuario: 204, Supervisor 204
4229560	VoIP	Preatendedor: welcome
4229561	VoIP	*Número sin asignar*
4229562	VoIP	*Número sin asignar*
4229563	VoIP	*Número sin asignar*

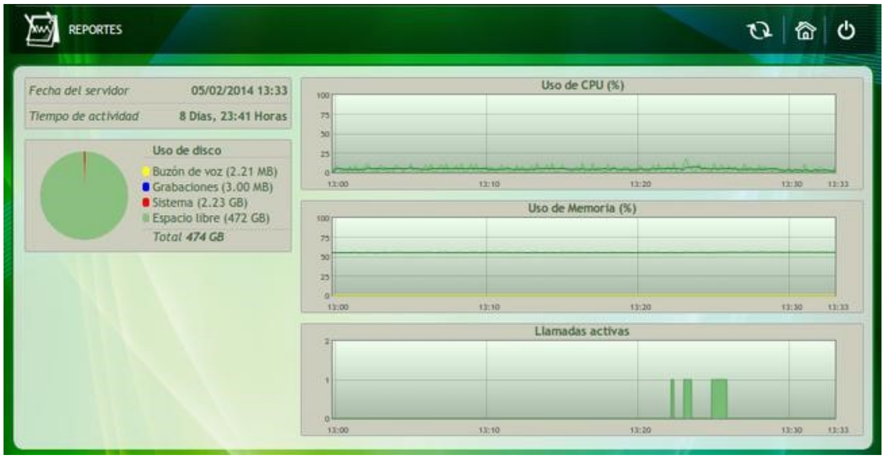
Números encontrados: 5

Figure 3.82: Advanced interface: Report access numbers

3.3.6.4 System Resources

In these options you can see the real-time reports of the various features of the Denwa UC&C 4.0.1 , namely:

- **Server Date**: Show current date and time.
- **Activity time**: indicates the time period that the control panel is working.
- **Disk Usage**: This section displays a pie chart that shows a quick and easy to understand disk usage. In addition, a more detailed list is presented:
  - **Voicemail**: allows you to check how much space voice messages take up on the disk.
  - **Recordings**: refers to the space occupied by telephone recordings.
  - **System**: is the space occupied by the PBX software. Also, backup is contemplated.
  - **Free space**: Allows you to check the space that has not yet been used on the disk.
  - **Total**: contemplates the total capacity of the disk.
- **Activity in the last 33 minutes**:
  - **CPU Usage (%)**: shows both the usage of CPU resources expressed as a percentage, as well as its average.
  - **Memory Usage (%)**: when the PBX's built-in RAM memory is fully used, the default disk space is used. Then, it is necessary to pass the data from the disk to memory, this exchange is called swap. The graphs contained in these axes show memory usage and swap status.
  - **Active Calls**: This graph displays the number of calls being made. If the time is displayed on the lower axis, the duration of each one of them is verified.



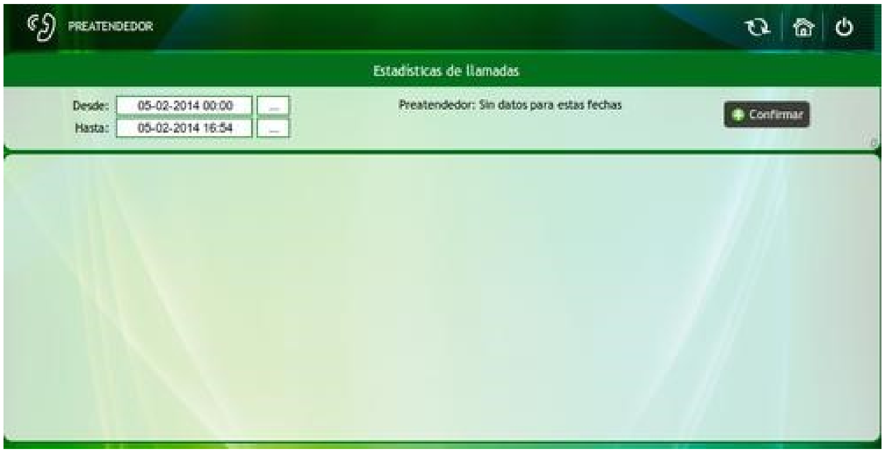
Fecha del servidor 05/02/2014 13:33
Tiempo de actividad 8 Dias, 23:41 Horas

Uso de disco
🟨 Buzón de voz (2.21 MB)
🟦 Grabaciones (3.00 MB)
🟥 Sistema (2.23 GB)
🟩 Espacio libre (472 GB)
Total 474 GB

Figure 3.83: Advanced Interface: System Resources Report

3.3.6.5 Preattenders

Initially, in this section you must select both the time period for which you want to observe the report, as well as the preattendant. Then, click on «✚ Confirm».



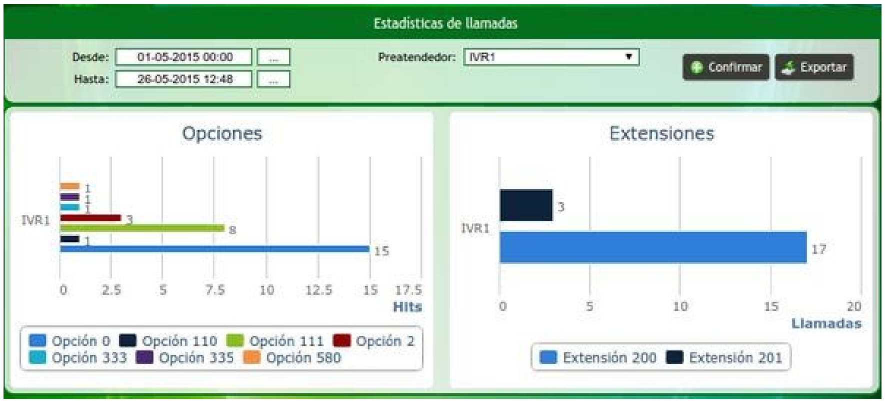
Estadísticas de llamadas

Desde: 05-02-2014 00:00
Hasta: 05-02-2014 16:54

Preatendedor: Sin datos para estas fechas

Figure 3.84: Advanced interface: Pre-attenders report

This displays two graphs. The first shows the options marked by the person who made the call when being attended by the pre-attendant. In addition, it allows you to see how many calls each of the options had. Instead, the second graph shows the extensions that received calls, with the corresponding number.



Estadísticas de llamadas

Desde: 01-05-2015 00:00

Hasta: 26-05-2015 12:48

Preatendedor: IVR1

Figure 3.85: Advanced interface: Pre-attendant report example

After obtaining the graph, the option of exporting a .pdf document («⬇ Export PDF») is provided with the same information of each of the graphs and a table that shows quickly and easily each of the values; or to .csv format («⬇ Export CSV») with the following fields:

- **Date**: date of entry of the call in mm/dd/yyyy format
- **Time**: call entry time in hh:mm:ss format
- **ANI**: telephone number of the caller
- **Access number**: trunk access number through which you entered
- **Access entity**: site through which the call entered
- **Attention Time**: Talk time with an inmate, agent or voicemail in hh:mm:ss format (pink column in diagram)
- **Time in preattendants**: total time found in queues and preattendants in format
- **Total duration**: time elapsed since the call entered until it was cut off
- **Last Option Time**: time you waited after pressing the last option of the chosen pre-attendant before being answered by a voicemail, internal or agent in hh:mm:ss format (yellow column in the diagram)
- **State**: final state of the call
- **IVR**: name of the played preattendant (IVR «A» in the diagram)
- **Destinations**: a column will be displayed for each of the possible branches of the IVR where the user pressed an option:
  - **Option 1**: First option marked on the preattendant (1st Option marked on the diagram)
  - **Option 2**: Second option marked on the preattendant (2nd Option marked on the diagram)
  - **Option 3**: Third option marked on the preattendant (3rd Option marked on the diagram)
  - **Option ...**
  - **Option n-1**
  - **Option n**

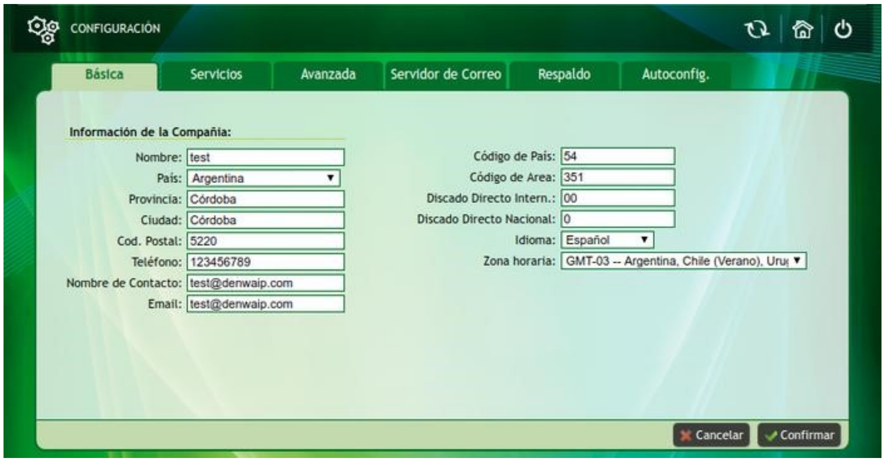
Figure 3.86: Diagram of call steps

3.3.7 Settings

3.3.7.1 General

This functionality allows you to configure the general options of the control panel.

3.3.7.1.1 Basic Tab In the Basic tab, the data shown in the following figure must be entered.



Información de la Compañia:

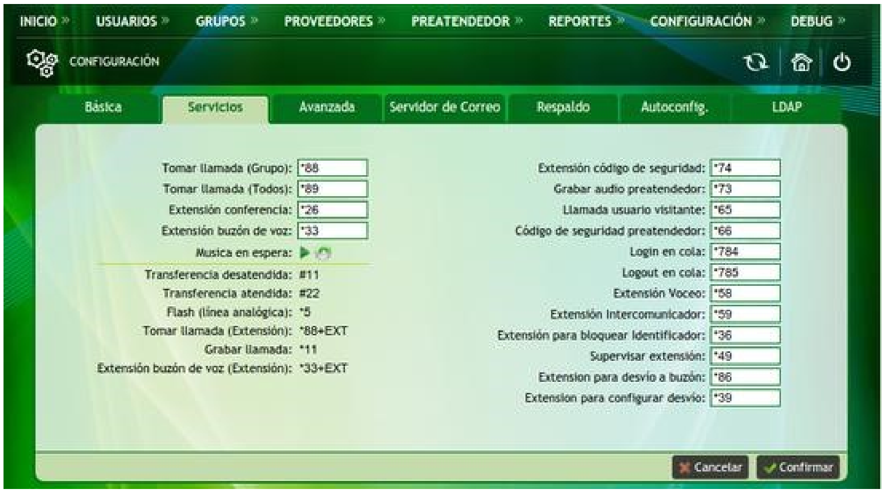
Nombre: test
País: Argentina
Provincia: Córdoba
Ciudad: Córdoba
Cod. Postal: 5220
Teléfono: 123456789
Nombre de Contacto: test@denwaip.com
Email: test@denwaip.com

Código de País: 54
Código de Area: 351
Discado Directo Intern.: 00
Discado Directo Nacional: 0
Idioma: Español
Zona horaria: GMT-03 -- Argentina, Chile (Verano), Uru

Figure 3.87: Advanced interface: Basic system configuration

- **Name**: name of the company.
- **Country**: where Denwa UC&C 4.0.1 is installed
- **Province**: province, region or state where the computer is located
- **City**: city where the team is
- **Postal Code**: postal code of the address
- **Phone**: contact phone number
- **Contact Name**: name of the contact person
- **Email**: contact email
- **Country code**: country code used for international dialing (see `https://es.wikipedia.org/wiki/Anexo:Prefijos_telef%C3%B3nicos_mundiales` for more information)
- **Area Code**: Area code used for domestic long distance dialing
- **International direct dialing**: code used for international exit (usually «00»)
- **National direct dialing**: code used for national dialing
- **Language**:
- **Time zone**:

After loading all the data, you must click on «✔ Confirm», if you do not want to save the changes, just click on the «✖ Cancel» button.



Tomar llamada (Grupo): *88
Tomar llamada (Todos): *89
Extensión conferencia: *26
Extensión buzón de voz: *33
Musica en espera: ▶
Transferencia desatendida: #11
Transferencia atendida: #22
Flash (línea analógica): *5
Tomar llamada (Extensión): *88+EXT
Grabar llamada: *11
Extensión buzón de voz (Extensión): *33+EXT

Extensión código de seguridad: *74
Grabar audio preatendedor: *73
Llamada usuario visitante: *65
Código de seguridad preatendedor: *66
Login en cola: *784
Logout en cola: *785
Extensión Voceo: *58
Extensión Intercomunicador: *59
Extensión para bloquear Identificador: *36
Supervisar extensión: *49
Extension para desvio a buzón: *86
Extension para configurar desvio: *39

Figure 3.88: Advanced Interface: System Services Configuration

3.3.7.1.2 Services Tab

In this tab it is possible to configure the Denwa UC&C 4.0.1 services, they can be used from the telephone terminals, by means of a combination of keys:

- **Take call (Group)**: takes the incoming call to the group where you are located.
- **Take Call (All)**: Pick up the incoming call to all extensions, a function used in small installations.
- **Conference extension**: OnLine and OnDemand conferences, this function allows you to create a conference between people on demand. The user who wants to create a room must dial *26. Users who intend to join said conference must dial *26 + extension of the user who created the room. This must also be done by the user creating the room.
- **Voicemail Extension**: Take messages from voicemail, where the extension number and password are required.
- **Music On Hold**: by clicking ⚙ icon you can add an audio file, such as Denwa UC music on hold, otherwise it can be downloaded or played by clicking ▶icon
.
- **Security Code Extension**: allows you to change the status of the security code, enable or disable.
- **Record pre-attendant audio**: allows recording audio to be used in IVRs or pre-attendants.
- **Visiting user call**: allows you to make calls as a visiting user from any extension, always dialing PIN + DESTINATION NUMBER.
- **Pre-attendant security code**: allows calling a visiting user from any extension by always dialing SECURITY CODE + DESTINATION NUMBER.
- **Queue login**: allows you to login on the queue by dialing the PREFIX + QUEUE NUMBER.
- **Logout in queue**: allows you to log out of the queue by dialing the PREFIX + QUEUE NUMBER.
- **Paging Extension**: allows you to perform paging functions by calling a group type extension. The audio is one way and PREFIX + EXTENSION NUMBER is dialed.
- **Extension Intercom**: Allows you to perform intercom functions by calling an extension. The audio is two-way and PREFIX + EXTENSION NUMBER is dialed.

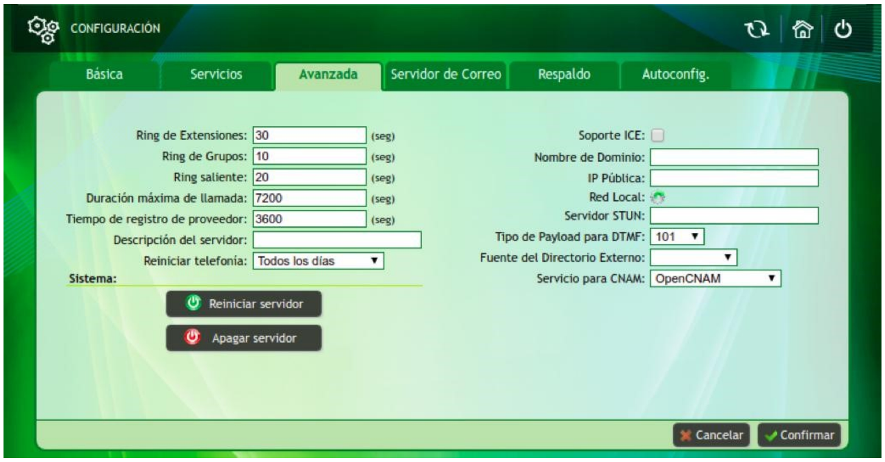
- **Extension to block Identifier**: blocks the ANI.
- **Supervise extension**: allows you to intervene in a communication.
- **Extension for forwarding to mailbox**: redirects calls to voice mail.
- **Extension to configure forwarding**: for the application to work it is necessary to load the audios in My applications > Set Forward Application.

In addition, there are some key combinations that are fixed and cannot be configured:

- **Unattended transfer (#11)**: this functionality transfers the call at the moment of dialing the key combination and cuts the communication with the first user.
- **Attended Transfer (#22)**: This functionality first allows the recipient of the call to speak to the person to whom the transfer is to be made. When the transferor hangs up, the call is transferred to the first caller. Flash (analog line) (*5): allows when the line is busy to enable another line.
- **Call Pickup (Extension) (*88 + EXT)**: This functionality picks up calls from a specific extension, with the combination *88 + EXTNUMBER.
- **Record call (*11)**: allows the recording of the call.

music on hold

If the call enters from the Preattendant to a Group (not a queue) and then to an extension, when putting a call on hold the user's MOH is reproduced; if the user has not configured it, the Group's MOH is reproduced. If the user and the group do not have the MOH configured, the music on hold of the Preattendant is played. If in all cases (user, group and pre-attendant) music on hold is not configured, when leaving a call on hold the MOH of the Denwa UC&C 4.0.1 is played.



Ring de Extensiones: 30 (seg)
Ring de Grupos: 10 (seg)
Ring saliente: 20 (seg)
Duración máxima de llamada: 7200 (seg)
Tiempo de registro de proveedor: 3600 (seg)
Descripción del servidor:
Reiniciar telefonía: Todos los días ▾
Sistema:

Soporte ICE: □
Nombre de Dominio:
IP Pública:
Red Local:
Servidor STUN:
Tipo de Payload para DTMF: 101 ▾
Fuente del Directorio Externo: ▾
Servicio para CNAM: OpenCNAM ▾

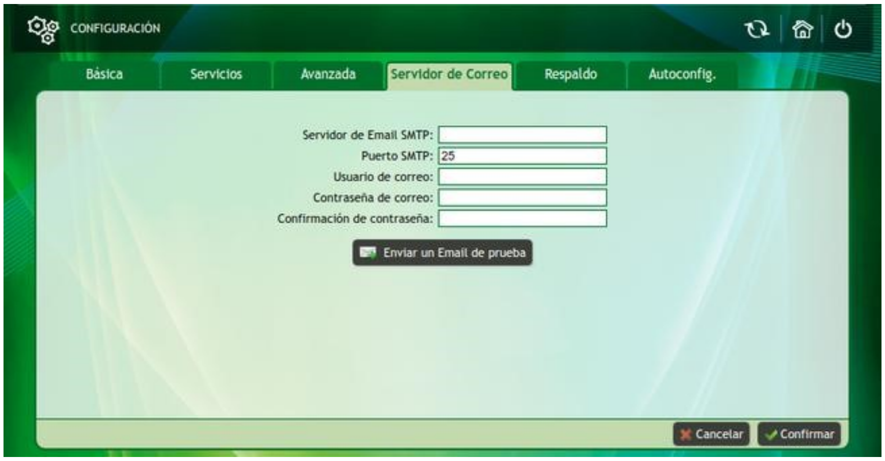
Figure 3.89: Advanced Interface: Advanced System Settings

3.3.7.1.3 Advanced Tab This tab allows you to configure the advanced options of Denwa UC&C 4.0.1 . The fields to configure are the following:

- **Extensions Ring**: is the time in seconds that an extension will ring, after this time the call is cut, sent to voice mail or transferred, this depends on the configured services.

- **Group Ring**: is the time in seconds that a group will ring before moving on to the next group.
- **Outgoing Ring**: is the time in seconds that an outgoing call will ring, after this time, if the call is not answered Denwa UC&C 4.0.1 cuts the call.
- **Maximum call duration**: is the maximum time allowed for an outgoing call, after this time is exceeded the call is cut off. It is necessary to configure this parameter correctly, because when the specified time is reached, the call will be terminated. Keep Recording Information: Allows you to specify the maximum period for which the history of exported recordings will be kept to be included in the reports.
- **Server description**: is the name chosen for DenwaUC. This will appear in the upper right sector of the screen, on the Denwa model.
- **Restart telephony**: allows you to define the period in which the telephony services will be restarted. By default this parameter is configured every day.
- **ICE support**: Option available for control panels where WebRTC technology is used (enabled by default). If you do not have an Internet connection, it is recommended to disable this option, since it directly affects the connection time of a call.
- **Domain Name**: domain name assigned to Denwa UC, it is used in special cases where Denwa UC is in a private network, uses Public IP and dynamic DNS. With this configuration, all SIP messages in this domain are sent to be answered.
- **Public IP**: Public IP assigned to the PBX, it is used in special cases where the PBX is in a private network with a fixed Public IP in a router.
- **Local Network**: is the private network in which the central will be operating. Networks must be added by clicking on ⚙. This will enable a new window, which allows you to add the different networks. The format to add the same in network/mask, both in format of four decimal octets (for example: 192.168.1.0/255.255.255.0). Then you must click on ✚.
- **STUN Server**: this server helps the IP-PBX when there are equipment behind a NAT, it is rarely used in new VoIP installations.
- **Payload type for DTMF**: you can choose between payload types 97 and 101.
- **External Directory Source**: indicates from where the list of contacts can be provisioned. It can be local or external. If it is external, you must press the ⚙button, and enter the URL where the provisioning file is located. Finally «✓ Confirm».
- **Service for CNAM**: it is a service created for the United States that verifies the name of the contact, for this it looks for this name in a database. It is recommended to disable this service in another country.

On this screen it is also possible to shut down or restart the system, for this there are the buttons «⏻ Turn off server» and «⏻ Restart server», respectively



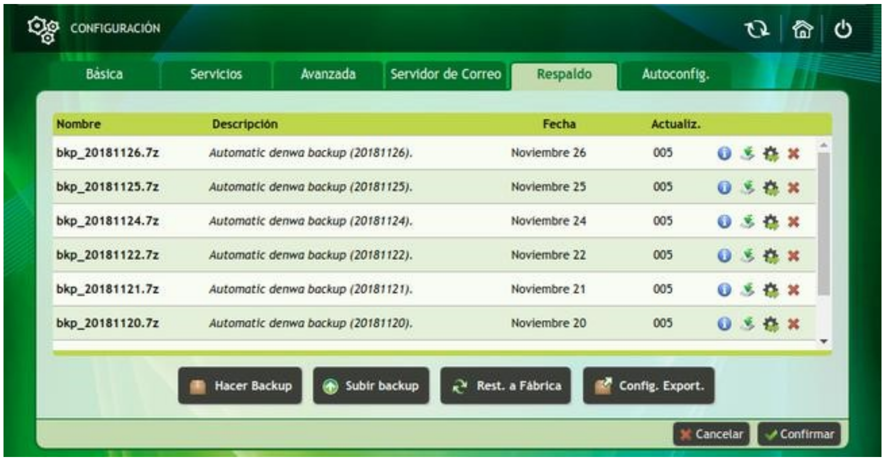
Servidor de Email SMTP:
Puerto SMTP: 25
Usuario de correo:
Contraseña de correo:
Confirmación de contraseña:

Figure 3.90: Advanced Interface: System Mail Server Configuration

3.3.7.1.4 Mail Server Tab This tab allows you to configure a mail server for Denwa UC&C 4.0.1 . Requested: email server, port, username and password.

- **SMTP Email Server**: is a protocol for the simple transfer of email. Here you must write the IP or Domain of the SMTP Server for sending Voice Mail, FAX and Denwa PBX alerts.
- **SMTP Port**: port to be used for the email server, this depends on the server provider. The most used ports are 25, 465 and 587.
- **Mail user**: username for the email account.
- **Email password**: password of the email user.
- **Password Confirmation**

Clicking on the «✉ Send a test email» button will perform a check of the service, this will show a pop-up window where the information from the previous list will be preloaded, being necessary to indicate a destination email address and, if necessary, modify the test message. The «✔ Send» and «✖ Cancel» buttons send the test message or close the window, respectively.



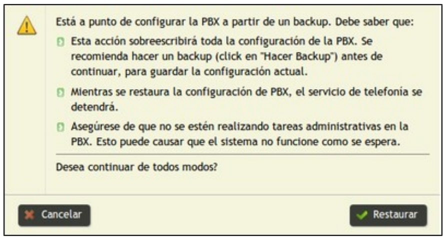
Nombre	Descripción	Fecha	Actualiz.
bkp_20181126.7z	Automatic denwa backup (20181126).	Noviembre 26	005
bkp_20181125.7z	Automatic denwa backup (20181125).	Noviembre 25	005
bkp_20181124.7z	Automatic denwa backup (20181124).	Noviembre 24	005
bkp_20181122.7z	Automatic denwa backup (20181122).	Noviembre 22	005
bkp_20181121.7z	Automatic denwa backup (20181121).	Noviembre 21	005
bkp_20181120.7z	Automatic denwa backup (20181120).	Noviembre 20	005

Figure 3.91: Advanced interface: System backup settings

3.3.7.1.5 Backup Tab

This tab is for all Denwa UC&C 4.0.1 data backup and restore operations. The first thing that is observed is a table where all the Backups made are listed, where it is shown:

- **Name**:
- **Description**:
- **Date**:
- **Update**:
- **Action Icons**:
  - ℹ Shows Backup information.
  - ⤓ Save the Backup file on the computer.
  - ⚙ Allows you to configure Denwa UC&C 4.0.1 from a selected configuration file, clicking on it will display a warning indicating the risks associated with the task.



⚠ Está a punto de configurar la PBX a partir de un backup. Debe saber que:

- Esta acción sobreescribirá toda la configuración de la PBX. Se recomienda hacer un backup (click en "Hacer Backup") antes de continuar, para guardar la configuración actual.
- Mientras se restaura la configuración de PBX, el servicio de telefonia se detendrá.
- Asegúrese de que no se estén realizando tareas administrativas en la PBX. Esto puede causar que el sistema no funcione como se espera.

Desea continuar de todos modos?

Figure 3.92: Advanced interface: Warnings for restoring backups

  - ✖ Delete the Backup.

At the bottom there are four (4) buttons that offer different backup options:

- **Backup**: allows you to create a backup. It is recommended to make the backup when Denwa UC&C 4.0.1 is with little activity.
- **Upload Backup**: this option allows you to restore the configuration from a file saved on the PC.
- **Rest. to Factory**: the panel is restored to the factory settings. Attention! All data will be lost, it is recommended to make a backup beforehand.
- **Config. Export.**: This option allows you to export the backup to an FTP server. The FTP server data must be completed in the window that appears below.
  - **Enable the export of backups**: the export of backups will only work if this field has a tilde (✔) in its box
  - **FTP protocol**:
    - **User**: username to log in to the FTP server
    - **Password**: password of the user used to log in to the FTP server
    - **IP / Domain**: IP address or domain name of the FTP server
    - **Path**: path (within the FTP user's directory) where the files will be stored.

Windows paths

Since in most UNIX-based systems (such as Denwa UC&C 4.0.1) is used as an escape character, and the same is used in Windows systems to define the paths of files and folders; If the FTP server to be used is a Windows computer, it will be necessary to use the «*backslash*» or «backslash» twice, for example:

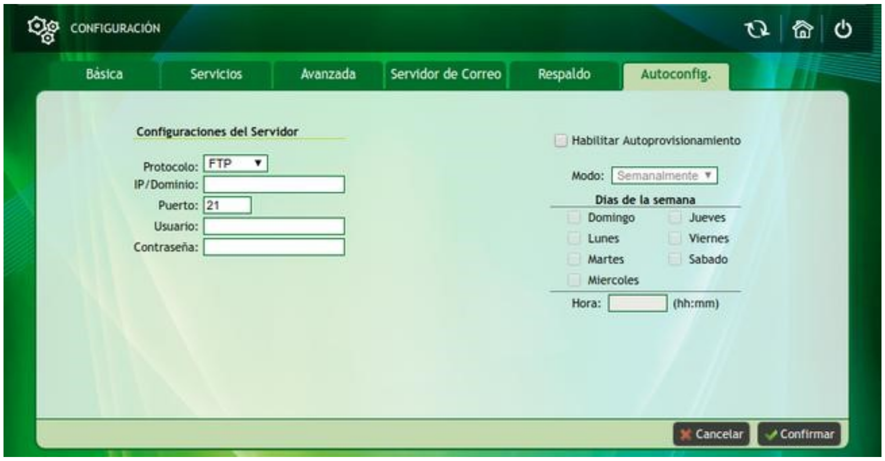
```
C:\\users\\pepito\\FTP\\
```

  - **Name**: distinguished name of the FTP server

- **Buttons**:
  - ✖ **Close** - closes the popup window without saving the changes made
  - ⓘ **Verify connection**: executes a connection test to the FTP server, this test consists of creating a file in the previously defined path, indicating whether the connection was successful or failed
  - ❓ **Help**: displays a help window indicating how each field can be completed
  - ✓ **Configure**: apply and save the applied configuration

Alerts for transfer errors

Denwa UC&C 4.0.1 sends alert emails when connection is lost with the FTP server, or file transfer errors. This functionality is only available if the email server has been configured (see section Mail Server Tab on the 97 page).



Configuraciones del Servidor

Protocolo: FTP
IP/Dominio:
Puerto: 21
Usuario:
Contraseña:

□ Habilitar Autoprovisionamiento

Modo: Semanalmente

Dias de la semana

□ Domingo □ Jueves
□ Lunes □ Viernes
□ Martes □ Sabado
□ Miercoles

Hora: (hh:mm)

Figure 3.93: Advanced Interface: System Autoconfiguration

3.3.7.1.6 Autoconfig tab This tab provides the possibility of obtaining the control panel settings from an FTP, HTTP or HTTPS server (HTTP with security).

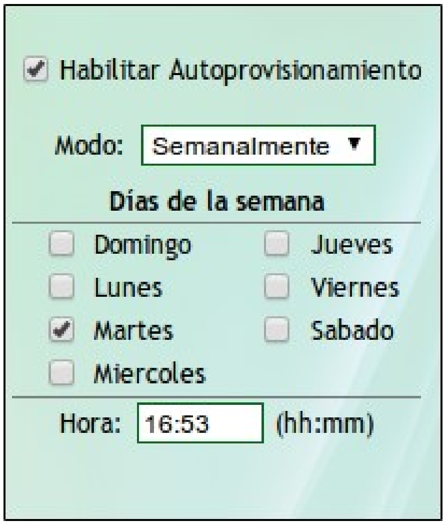
3.3.7.1.6.1 Server Settings Here the server with which the central is going to be provisioned is determined: FTP, HTTP and HTTPS, the options that must be configured are:

- **Protocol**: You must select between FTP, HTTP, HTTPS.

- **IP/Domain**: the server IP is configured.
- **Port**: Sets the port used by the server. By default FTP (port 21) is used, you can also choose HTTP (port 80) or HTTPS (port 443).
- **User**: the server user is determined (if this box is left blank and the password box is blank, the methodology without authentication will be used).
- **Password**: server password.

After configuring the server, you must configure the periodicity with which you want to perform the self-provisioning, for this two options are provided: Weekly or Repeatedly. Their configuration is accessed by clicking on the «■ Enable Auto-provisioning» checkbox.

3.3.7.1.6.2 Weekly Mode This option allows you to configure which days of the week and at what time the self-provisioning of the control panel is carried out. The options are very intuitive, it is enough to select the days of the week and the desired time for the control panel to supply itself.



☑ Habilitar Autoprovisionamiento

Modo: Semanalmente ▼

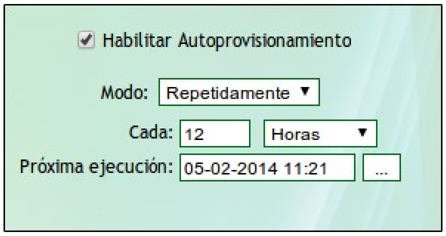
Días de la semana

□ Domingo □ Jueves
□ Lunes □ Viernes
☑ Martes □ Sabado
□ Miercoles

Hora: 16:53 (hh:mm)

Figure 3.94: Advanced interface: Weekly self-provisioning mode

3.3.7.1.6.3 Repeated Mode This option allows you to select how often the control panel supplies itself.



☑ Habilitar Autoprovisionamiento

Modo: Repetidamente ▼

Cada: 12 Horas ▼

Próxima ejecución: 05-02-2014 11:21 ...

Figure 3.95: Advanced interface: Repeated auto-provisioning mode

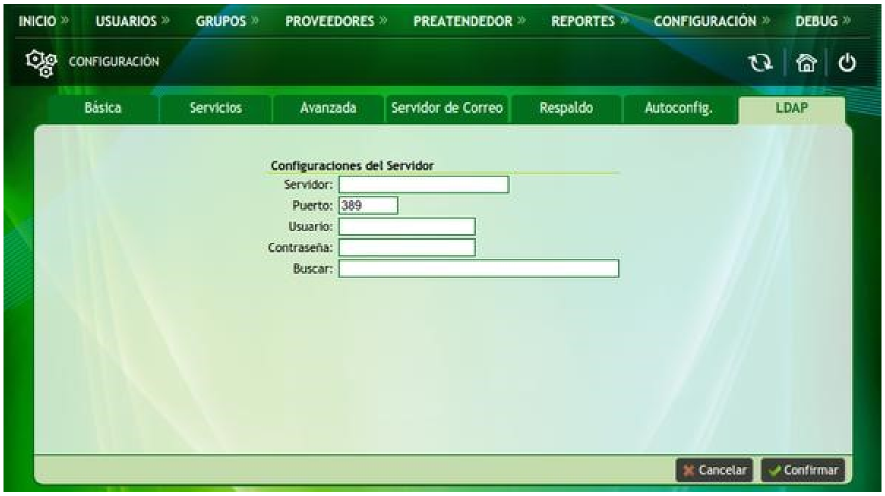
You simply fill in the every field, and then select whether this number represents hours, days, or weeks. Under these options, the day and time of the next execution must be configured, click on you can configure the day and time to execute the first auto-provisioning, then it is repeated according to the period configured in the previous step.

In all cases, after completing the self-provisioning mode, the changes must be confirmed by clicking Confirm.

3.3.7.1.7 LDAP tab This section allows the authentication of operators with the LDAP (Active Directory) system, allowing access with all permissions enabled.

Tab availability

This tab is only available on computers that have the LDAP Auth module installed; Additionally, in case of having the Contact Center module, a greater number of fields can be displayed.



Configuraciones del Servidor

Servidor:

Puerto: 389

Usuario:

Contraseña:

Buscar:

Figure 3.96: Advanced interface: Weekly self-provisioning mode

Below are the server configuration parameters:

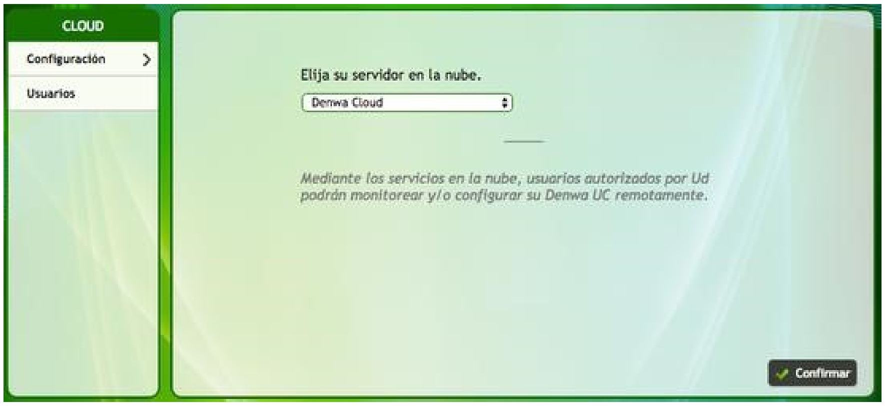
- **Server**: IP address or domain address of the LDAP Server. For example: ldap.mynetwork.loca
- **Port**: refers to the port of the LDAP server where it expects IP connections. For example: 389.
- **User**: DN («Distinguished Name») of the user for access to searches within the Active Directory structure. With this user, the initial connection will be made to search for the user to authenticate, it is necessary that it have the necessary permissions to read the entire group to which the users belong, to which the queries will be made. For example: «cn=user1,ou=people,ou=division1,dc=myorg,dc=es ».
- **Password**: Key used to authenticate the initial connection. For example: «MiClaveLdAp».
- **Search**: DN («Distinguished Name») of the group or organization to which the users who will authenticate, using their LDAP credentials, belong as Denwa UC&C 4.0.1 administrators.

3.3.7.2 Cloud

In this section, you can register, cancel or modify (Monitor or Administrator) the Cloud users (Integrators).

In order for Cloud users to be able to remotely monitor or manage the control panel, the control panels must be associated at cloud.denwaip.com (see Cloud for Integrators document available on the support site).

3.3.7.2.1 Settings In this section you can select the cloud in which the central will be associated:



Elija su servidor en la nube.

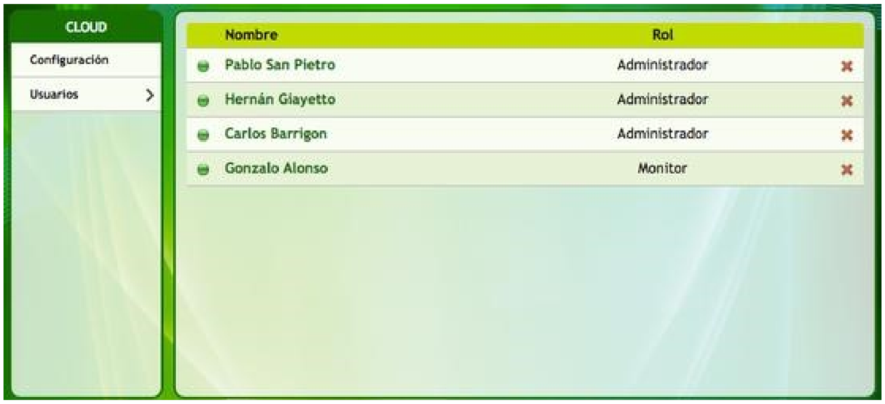
Denwa Cloud

Mediante los servicios en la nube, usuarios autorizados por Ud podrán monitorear y/o configurar su Denwa UC remotamente.

Figure 3.97: Advanced interface: Selection of the cloud from where the equipment will be managed

The control panels can be monitored from the Cloud platform, or from a custom server within the cloud or private network.

3.3.7.2.2 Users In the users section, you can see, modify the role or delete the users who have Administrator or Monitor access to the control panel



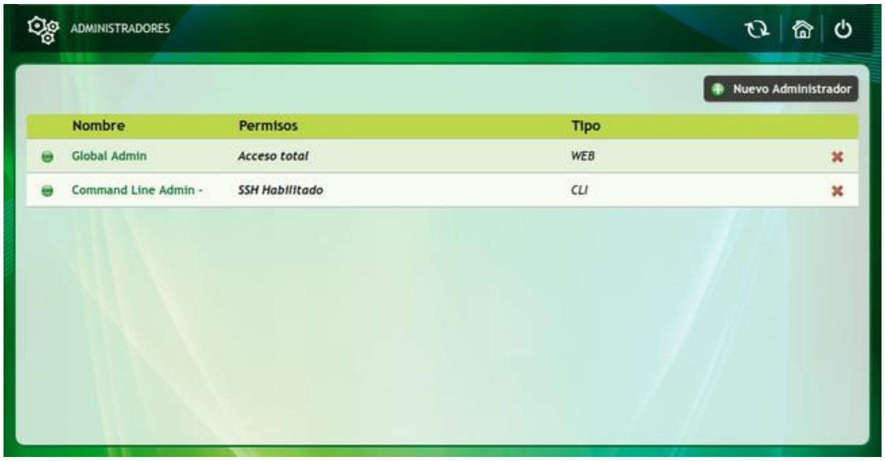
Nombre	Rol
Pablo San Pietro	Administrador
Hernán Glayetto	Administrador
Carlos Barrigon	Administrador
Gonzalo Alonso	Monitor

Figure 3.98: Advanced interface: Configuration of Cloud access users

When entering the user, you can see the data with which the Integrator has registered him in his Cloud account, and it is possible to modify his role: Monitor or Administrator

3.3.7.3 Administrators

This functionality allows you to configure Denwa UC&C 4.0.1 administrators.



	Nombre	Permisos	Tipo	
●	Global Admin	Acceso total	WEB	✖
●	Command Line Admin -	SSH Habilitado	CLI	✖

Figure 3.99: Advanced interface: Denwa UC&C 4.0.1 administrators

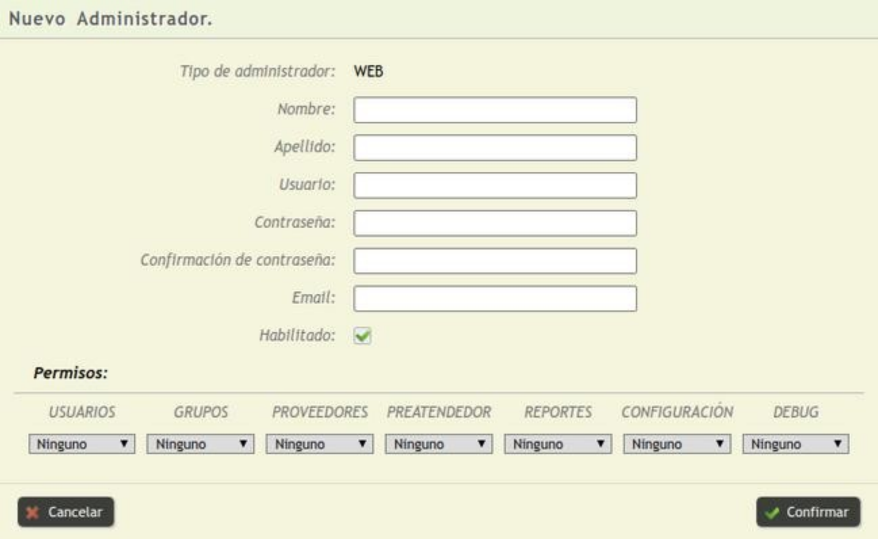
Two types of users are verified:

- **Web**: users with team management via web.
- **CLI**: user with computer management via console or ssh (pbxadmin)

3.3.7.3.1 New Administrator

If you want to create a new administrator, you must click on «✚ New Administrator», this will display a pop-up window requesting the following information:

- **Name**: username
- **LastName**: lastname of the user
- **User**: way to identify yourself when logging into Denwa UC&C 4.0.1
- **Password**: password to use for login
- **Password confirmation**: repetition of the password to be used
- **Email**: email address
- **Enabled**: checkbox to enable (✔) or disable (☐) the user
- **Permissions**: can be read-write, read-only, or none. You must select which menu items you can access, namely:
  - Users (see page 33)
  - Groups (see page 57)
  - Suppliers (see page 62)
  - Preattender (see page 72)
  - Reports (see page 82)
  - Configuration (see page 93)
  - Debug (see page 150)



Nuevo Administrador.

Tipo de administrador: WEB

Nombre:

Apellido:

Usuario:

Contraseña:

Confirmación de contraseña:

Email:

Habilitado: ☑

Permisos:

USUARIOS	GRUPOS	PROVEEDORES	PREATENDEDOR	REPORTES	CONFIGURACIÓN	DEBUG
Ninguno	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno

Figure 3.100: Advanced interface: Web user registration

New administrators It is only possible to generate web administration users

3.3.7.3.2 Administrator Edition

If you want to change any parameter of the existing administrators, you must click on the name of the administrator, which will display the editing window, which has the same fields and characteristics as those mentioned in New Administrator (see page 103). The changes will be stored by clicking on the «✔ Confirm» button, or if you want to discard the modification and close the window, you must click on «✖ Cancel».

3.3.7.3.2.1 CLI user edition

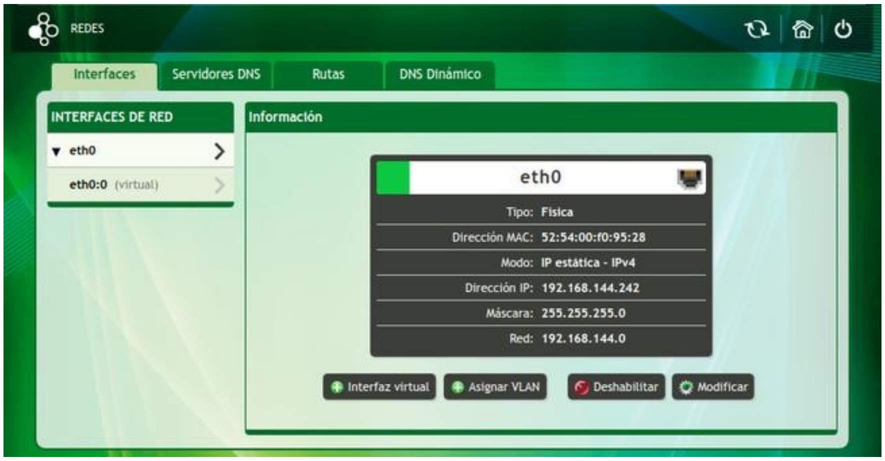
: The editable fields are the password and the possibility of disabling the user in case this management means is not used.

Security Alert It is very important to change the password of the users «admin» and «pbxadmin». For more information, we recommend consulting the **??** section, on the **??** page.

3.3.7.4 Networks

In the «Networks» section, it is possible to configure the way in which Denwa UC&C 4.0.1 relates to existing networks in your environment.

3.3.7.4.1 Network Interfaces



eth0

Tipo: Física

Dirección MAC: 52:54:00:f0:95:28

Modo: IP estática - IPv4

Dirección IP: 192.168.144.242

Máscara: 255.255.255.0

Red: 192.168.144.0

Figure 3.101: Network Interfaces, interfaces tab

3.3.7.4.1.1 Interfaces tab

In the interfaces tab it is possible to register Denwa UC&C 4.0.1 in the different client networks, by assigning IP addresses in the different configurable interfaces, namely:

- **Physical**: associates an IP address to the physical network interface
- **Virtual**: Allows you to assign multiple IP addresses (one for each virtual interface) to a physical network interface
- **VLAN**: allows the VLAN label to be placed on the IP address, it will be assigned to a virtual interface, allowing the use of several IPs from different VLANs on the same physical interface

> **High Availability Exception**
>
> When Denwa UC&C 4.0.1 is part of a High Availability cluster (Active-Passive), the configuration of the Network Interfaces will be blocked by the system, not allowing their editing.

The information is displayed in two main sections:

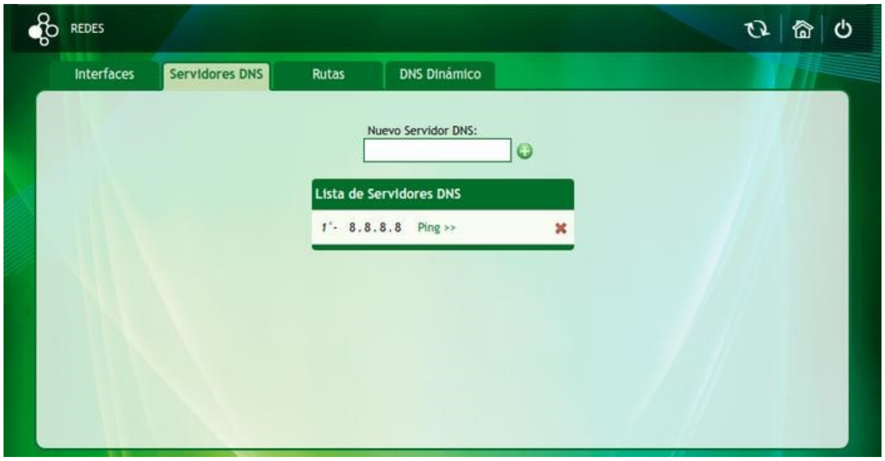
- **Network Interfaces**: Lists all physical interfaces on the platform. Next to the name of each of the interfaces there is the symbol ▶ which, when pressed, will display the list of virtual interfaces (if there are any)
- **Information**: shows the information of the selected interface (active › icon), namely:
  - **Name and link state**: indicates the name of the network interface, as well as the state of its link:
    - **Green**: link established
    - **Red**: no connection
  - **Type**: indicates if the interface is physical or virtual
  - **MAC address**: MAC address of the network card
  - **Mode**: shows if the IP address was configured manually (static) or through a DHCP server, also shows if its configuration is for IPv4 or IPv6 networks
  - **IP Address**: IP address assigned to the board
  - **Mask**: subnet mask
  - **Network**: IP address of the network to which the assigned IP belongs
  - ⊕ **Virtual interface**: allows the creation of a virtual interface on the selected board, pressing this button shows a popup window for its configuration

    - **IP Address**: IP address to configure
    - **Mask**: subnet mask, in case of IPv4 it must be indicated in the decimal format of four (4) octets, however in the case of IPv6 its format is CIDR
    - **Type**: indicates if IPv4 or IPv6 is used
    - ✖ **Cancel**: closes the window without saving changes
    - ✔ **Create**: save the changes and close the window
  - ⊕ **Assign VLAN**: allows the creation of a virtual interface with a VLAN tag, pressing this button displays a popup window for its configuration
    - **VLAN ID**: VLAN number to use
    - **IP Address**: IP address to configure
    - **Mask**: subnet mask, in case of IPv4 it must be indicated in the decimal format of four (4) octets, however in the case of IPv6 its format is CIDR
    - **Type**: indicates if IPv4 or IPv6 is used
    - ✖ **Cancel**: closes the window without saving changes
    - ✔ **Create**: save the changes and close the window

The network interfaces can be configured by following the steps below:

1. The desired interface must be selected, in the case of the image it is eth0. It can be seen that all the data is shown.
2. Below the information, there are four options to configure.
   - Virtual interface: A virtual interface is assigned over eth0. To configure this option, you must enter the IP address and network mask of the new virtual interface. Then you must click on Create.
   - Assign VLAN: A VLAN (Virtual Local Area Network) is generated. With this method, separate logical networks are created within the same physical network. To achieve this you need to enter the VLAN identifier, IP address and netmask.
   - Disable: The network interface is disabled.
   - Modify: you can change the IP address and network mask, choosing the Static or DHCP IP mode and the IPv4 or IPv6 type.

3.3.7.4.1.2 DNS Servers Tab On the DNS Servers tab, the desired domain name server can be configured. To configure the DNS, you must enter an IP or domain of a server in the «>New DNS Server» field, and then press the ⊕button; with this it will be included in the list at the bottom. To remove the servers from the list, click on ✖.



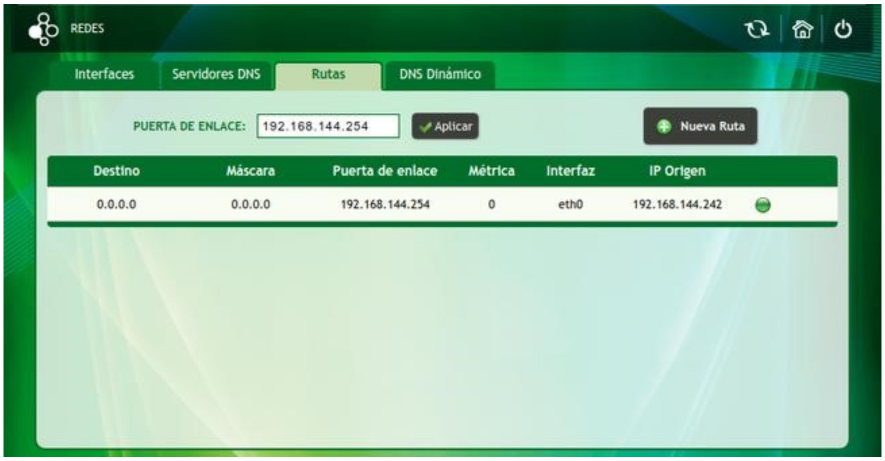
Lista de Servidores DNS

1'- 8.8.8.8 Ping >> ✖

Figure 3.102: Network Interfaces, DNS servers tab

It is possible to check the availability of the server by clicking on the «Ping» text next to its IP address.

3.3.7.4.1.3 Routes tab From this tab you can configure a particular static route for the Denwa UC&C 4.0.1 operation.



PUERTA DE ENLACE: 192.168.144.254

Destino	Máscara	Puerta de enlace	Métrica	Interfaz	IP Origen	
0.0.0.0	0.0.0.0	192.168.144.254	0	eth0	192.168.144.242	●

Figure 3.103: Network Interfaces, Routes tab

The default gateway can be configured by completing the corresponding field next to the legend «Gateway» and clicking the «✔ Apply» button.

If you need to reach destinations through a gateway other than the default, you must click on the «⊕ New Route» button and complete the fields that will be displayed in the displayed form, these fields are:

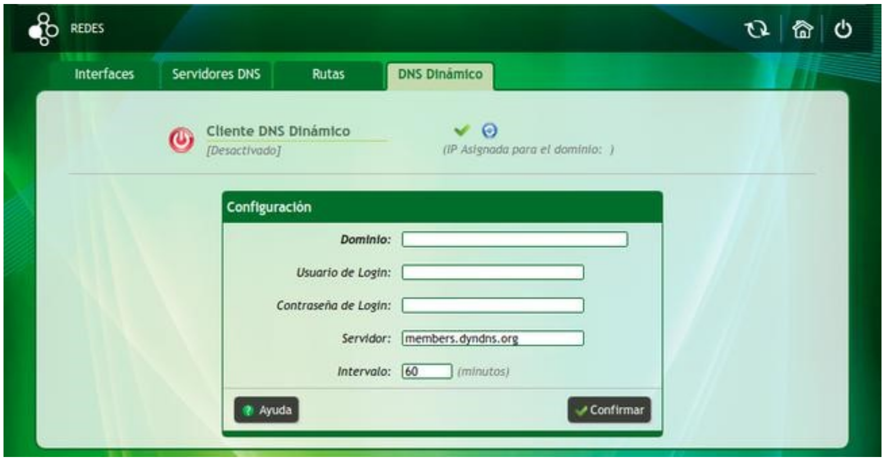
- **Destination**: IP address of the destination host or network, declared in two fields:
  - **IP Address**: IP address of the destination host or network
  - **Mask**: Netmask declared in four (4) decimal octet format
- **Interface**: allows you to select the interface through which the previously declared host or network will be reached, by default it is chosen automatically; in case of wishing to declare a specific interface, it is necessary to remove the ✔from the «Automatic selection» box and select the desired interface.
- **Gateway**: IP address through which the host or network declared above will be reached
- **Metric**: route priority; lower number, higher priority
- **✖ Cancel**: clear the form and close the window
- **❓ Help** - Displays a popup dialog with help text
- **✔ Create**: save the changes and close the window

Path validation The route will only be added if the destination host or network can be reached through the declared gateway

Once the route has been added, it will be displayed in the table at the bottom of the screen, from where the following information can be viewed:

- **Destination**: IP address of the destination host or network
- **Mask**: Netmask declared in four (4) decimal octet format
- **Gateway**: IP address through which the host or network is reached
- **Metric**: route priority; lower number, higher priority

- **Interface**: interface through which the host or network is reached
- **Source IP**: IP address with which the packets are sent to the destination host or network through the declared gateway
- **Status Icon**: can be displayed in two colors:
  - **Green**: the destination host or network can be reached
  - **Red**: the destination host or network cannot be reached
- **Actions**: allows you to delete the route by clicking on the «✖» icon corresponding to its row



Cliente DNS Dinámico
[Desactivado]
(IP Asignada para el dominio:)

Configuración

Dominio:
Usuario de Login:
Contraseña de Login:
Servidor: members.dyndns.org
Intervalo: 60 (minutos)

Figure 3.104: Network Interfaces, Dynamic DNS tab

3.3.7.4.1.4 Dynamic DNS tab It is not always possible to have a static Public IP address, to solve these problems is that there are dynamic DNS servers, they constantly monitor possible changes in the public IP address of Denwa UC&C 4.0.1 and update their records accordingly. that there is always a relationship between the Domain and the assigned public IP address (by PPPoE server, DHCP server, or even static configuration). It can be configured with the following information:

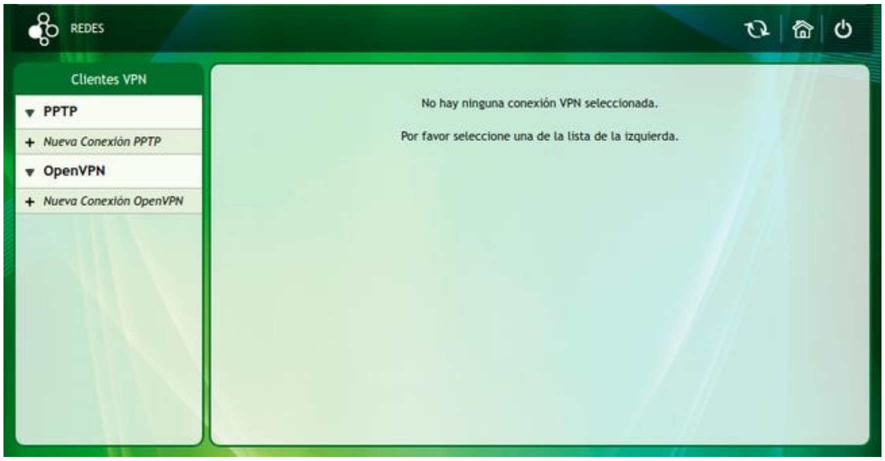
- **Domain**: is the domain registered in the chosen DynDNS server
- **Login User**: user who registers on the server
- **Login Password**: user password
- **Server**: domain or IP address of the server
- **Interval**: fraction of time in which the control panel sends a notification to the DynDNS server to update its IP address, it must be written in minutes
- ❓ **Help**: displays the help dialog, with examples
- ✓ **Confirm** - save changes and turn on the dynamic DNS client

Dynamic DNS servers

The service provided by the dynamic DNS servers is paid and is not included in the licensing and support costs of your Denwa UC&C 4.0.1 license. However, the client (responsible for sending the information to said servers, is available on the platform).

If you have any questions, you can click on Help where examples are shown. The service can be started or stopped by clicking on the ⏻icon. In case you need to send the Public IP address to the dynamic DNS server in advance, you can click on the ↻icon.

3.3.7.4.2 VPN Clients From this tab you can configure a new VPN (Virtual Private Network) connection using the PPTP (Point-To-Point Tunneling Protocol) or the OpenVPN protocol and edit existing connections (if you have one).



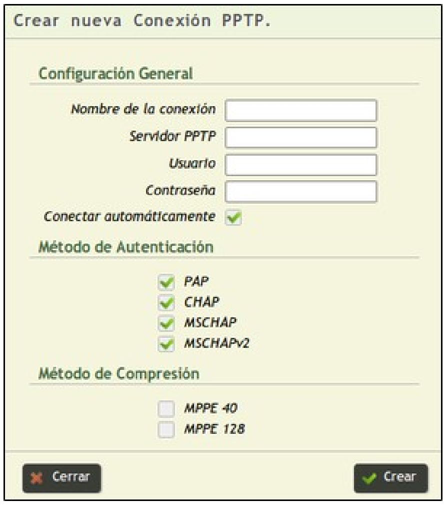
No hay ninguna conexión VPN seleccionada.

Por favor seleccione una de la lista de la izquierda.

Figure 3.105: VPN Clients

VPNs allow a secure extension of the local network over a public network. To do this, a point-to-point virtual connection is made using dedicated and/or encrypted connections. It has the advantage of reducing the bandwidth used and increasing speed. It also provides secure communications on public networks with specific access rights.

3.3.7.4.2.1 PPTP client it connects directly to the destination server creating a virtual network for each remote client, which the administrator can monitor and manage like any other remote access port. To configure this client, click on the New PPTP Connection option.



Crear nueva Conexión PPTP.

Configuración General

Nombre de la conexión
Servidor PPTP
Usuario
Contraseña
Conectar automáticamente ☑

Método de Autenticación

☑ PAP
☑ CHAP
☑ MSCHAP
☑ MSCHAPv2

Método de Compresión

□ MPPE 40
□ MPPE 128

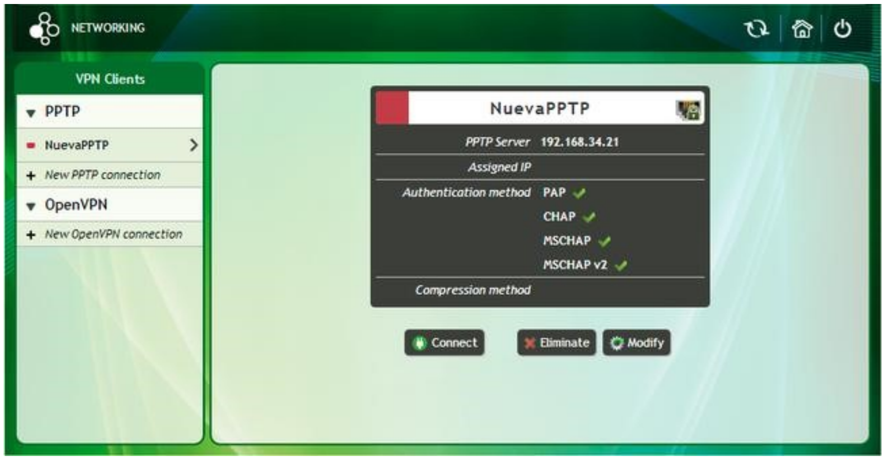
Figure 3.106: VPN Clients, PPTP

Below is the description of the fields:

- General configuration

  - Connection name: name that is assigned to the connection.
  - PPTP Server: IP or domain of the PPTP server.
  - Username: username to access the PPTP server.
  - Password: User password to access the PPTP server.
  - Connect automatically: enable if the connection should always be active
- Authentication Method: the authentication protocol(s) to be used must be selected.
  - PAP (Password Authentication Protocol): is a simple protocol that authenticates a user against a remote access server. Its function is to validate a user to access different resources. For this, PAP transmits passwords in ASCII in the clear, so it should be used as a last resort.
  - CHAP (Challenge Handshake Authentication Protocol): is an authentication protocol by mutual challenge. It periodically verifies the identity of the remote client using an information exchange. With CHAP, the user ID and password are always sent encrypted, making it a more secure protocol than PAP.
  - MSCHAP (Microsoft Challenge Handshake Authentication Protocol): Microsoft challenge handshake authentication protocol. This does not require that both parties know the key in the clear, but a summary (Hash) of it.
  - MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol v2) - Microsoft challenge handshake authentication protocol version 2. Provides high-level security for remote access connections. MS-CHAP v2 resolves some issues with MS-CHAP.
- Compression Method: they are encryption methods, they are only used with the MSCHAP and MSCHAPv2 protocols.
  - MPPE 40 (Microsoft Point-to-Point Encryption): Microsoft 40-bit point-to-point encryption.
  - MPPE 128 (Microsoft Point-to-Point Encryption): Microsoft 128-bit point-to-point encryption.

Then click on Create and the VPN will have been created. Below you can see the generated connection.



NuevaPPTP

PPTP Server 192.168.34.21

Assigned IP

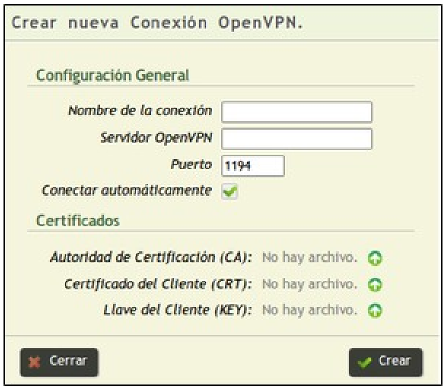
Authentication method PAP ✓ CHAP ✓ MSCHAP ✓ MSCHAP v2 ✓

Compression method

Figure 3.107: VPN clients, PPTP connection configured

Once the new connection is created, it can be Connected, Deleted or Modified from the buttons located in the lower section of the page.

3.3.7.4.2.2 OpenVPN Client is open source virtual private network software, which provides security, stability and encryption mechanisms without introducing complexity. To configure the OpenVPN client, click on the New OpenVPN Connection option.



Crear nueva Conexión OpenVPN.

Configuración General

Nombre de la conexión

Servidor OpenVPN

Puerto 1194

Conectar automáticamente ☑

Certificados

Autoridad de Certificación (CA): No hay archivo.

Certificado del Cliente (CRT): No hay archivo.

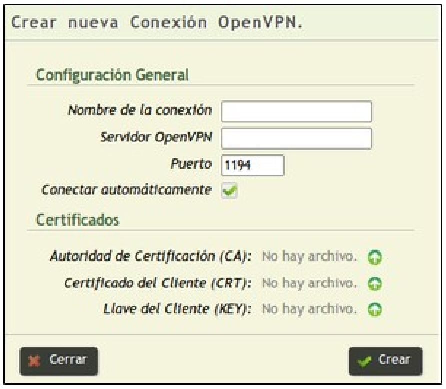
Llave del Cliente (KEY): No hay archivo.

Figure 3.108: VPN clients, OpenVPN settings

Below is the description of the fields:

- General Settings
  - Connection name: name that will be assigned to the connection.
  - OpenVPN Server: IP or domain of the OpenVPN server.
  - Port: port that will be used for the VPN connection.
  - Connect automatically: enable if the connection should always be active.
- Certificates
  - Certification Authority (CA): Allows importing the file.
  - Client Certificate (CRT): Allows importing the file.
  - Customer Key (KEY): Allows importing the file.

These certificates must be granted by the OpenVPN server administrator.



Crear nueva Conexión OpenVPN.

Configuración General

Nombre de la conexión

Servidor OpenVPN

Puerto 1194

Conectar automáticamente ☑

Certificados

Autoridad de Certificación (CA): No hay archivo.

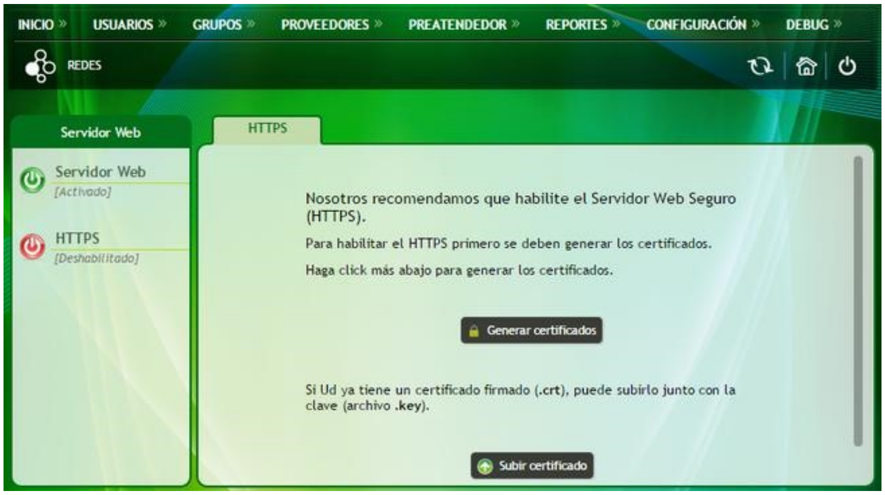
Certificado del Cliente (CRT): No hay archivo.

Llave del Cliente (KEY): No hay archivo.

Figure 3.109: VPN clients, OpenVPN settings

As with PPTP, you can Connect, Delete or Modify the connection from the buttons located in the lower section of the page.

3.3.7.4.3 Web Server By entering this configuration tab, you can activate or deactivate the safe browsing option. It is recommended to activate this option, since the transmitted data is encrypted. Therefore, it generates less probability that the information is intercepted by third parties. To activate secure browsing, you need to click the Enable HTTPS button.



Nosotros recomendamos que habilite el Servidor Web Seguro (HTTPS).

Para habilitar el HTTPS primero se deben generar los certificados.

Haga click más abajo para generar los certificados.

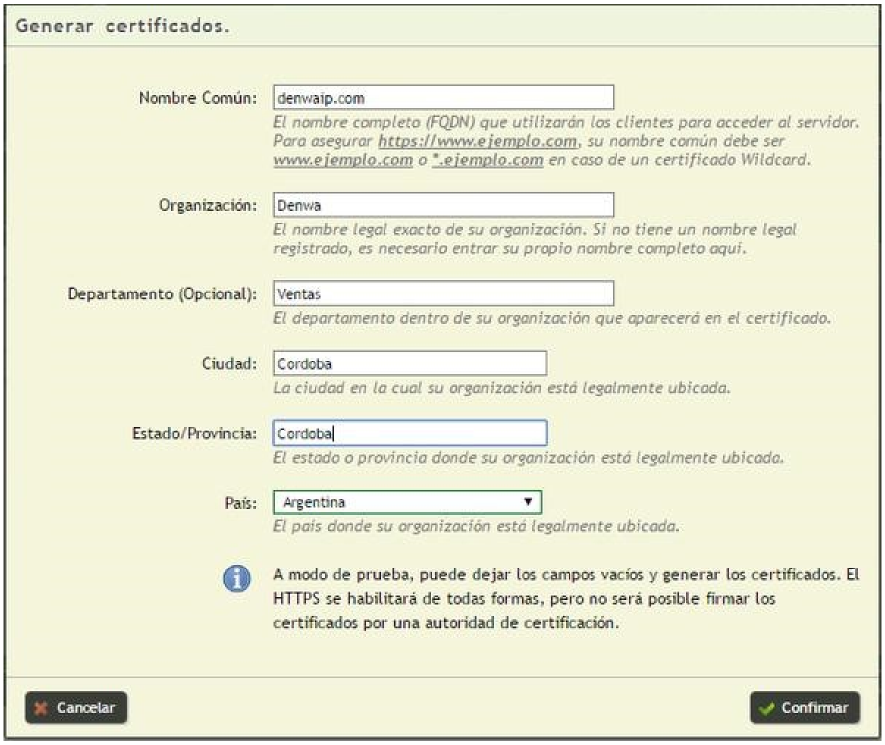
Si Ud ya tiene un certificado firmado (.crt), puede subirlo junto con la clave (archivo .key).

Figure 3.110: Webserver

HTTP Secure

A secure web server ensures that the information travels through the network, protected by the use of some encryption algorithm, ensuring that it is intelligible only by the server and the user who accesses the web.

To enable the secure web server, the generation of the certificate for HTTPs is requested, this is done through the Generate Certificate button. With this, the following page is displayed to complete the certificate data:



Generar certificados.

Nombre Común: denwaip.com
El nombre completo (FQDN) que utilizarán los clientes para acceder al servidor. Para asegurar https://www.ejemplo.com, su nombre común debe ser www.ejemplo.com o *.ejemplo.com en caso de un certificado Wildcard.

Organización: Denwa
El nombre legal exacto de su organización. Si no tiene un nombre legal registrado, es necesario entrar su propio nombre completo aquí.

Departamento (Opcional): Ventas
El departamento dentro de su organización que aparecerá en el certificado.

Ciudad: Cordoba
La ciudad en la cual su organización está legalmente ubicada.

Estado/Provincia: Cordoba
El estado o provincia donde su organización está legalmente ubicada.

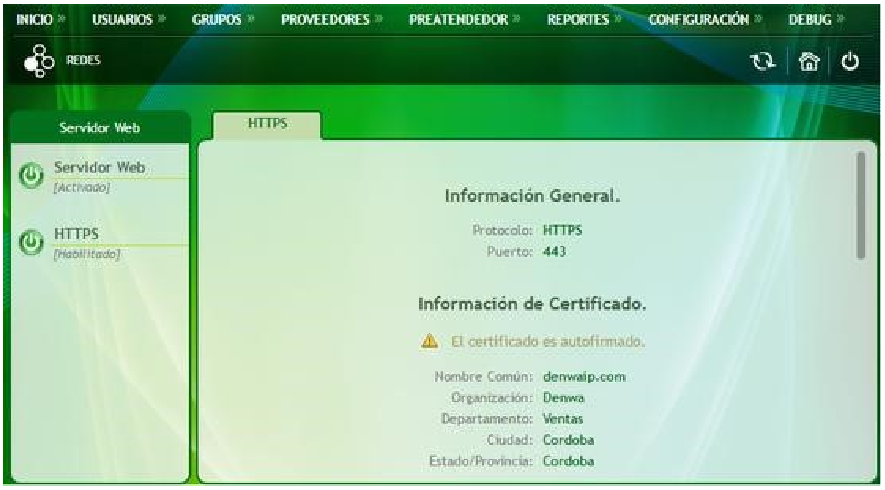
País: Argentina
El país donde su organización está legalmente ubicada.

A modo de prueba, puede dejar los campos vacíos y generar los certificados. El HTTPS se habilitará de todas formas, pero no será posible firmar los certificados por una autoridad de certificación.

Figure 3.111: Web server, certificate upload

With this, the ssl certificate is generated and loaded internally so that the central works with HTTPs, thus showing the service is active. Of course, since the server is now in secure browsing mode, you must log in as administrator again to continue with the DenwaUC configuration.

When entering the web server section again, you can see the HTTPs activated and the information of the Certificate that was generated.



Servidor Web [Activado]

HTTPS [Habilitado]

Información General.

Protocolo: HTTPS
Puerto: 443

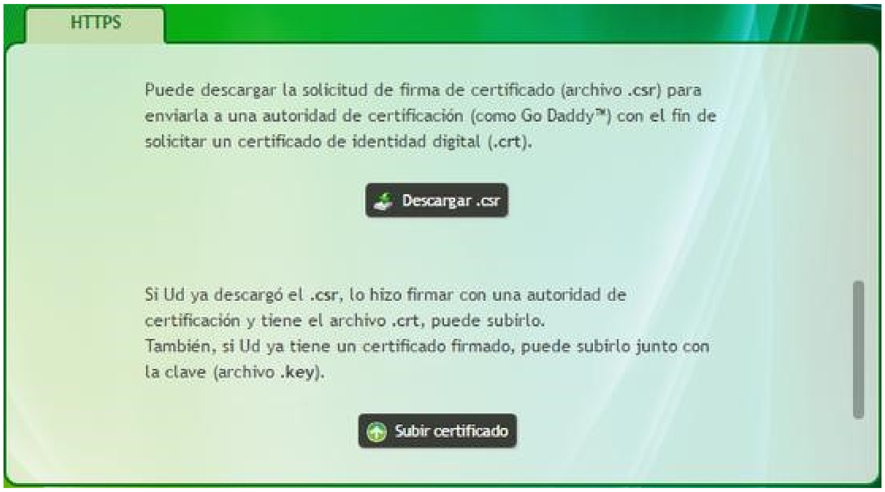
Información de Certificado.

El certificado es autofirmado.

Nombre Común: denwaip.com
Organización: Denwa
Departamento: Ventas
Ciudad: Cordoba
Estado/Provincia: Cordoba

Figure 3.112: Web server, service enabled

Denwa offers the function of downloading the generated Certificate, to be validated by a Certifying Entity. Denwa offers the possibility of validating the ssl certificate and being able to load again so that when entering safe mode, the certificate error does not appear in the browser.

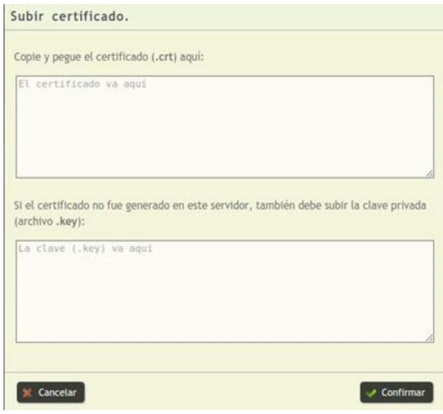


Puede descargar la solicitud de firma de certificado (archivo .csr) para enviarla a una autoridad de certificación (como Go Daddy™) con el fin de solicitar un certificado de identidad digital (.crt).

Si Ud ya descargó el .csr, lo hizo firmar con una autoridad de certificación y tiene el archivo .crt, puede subirlo.
También, si Ud ya tiene un certificado firmado, puede subirlo junto con la clave (archivo .key).

Figure 3.113: Web server, certificate download and import

It is important that, when uploading the certificates, the part corresponding to each one is pasted. In the first field the certificate (.crt), and in the second the private key (.key).



Subir certificado.

Copie y pegue el certificado (.crt) aqui:

El certificado va aqui

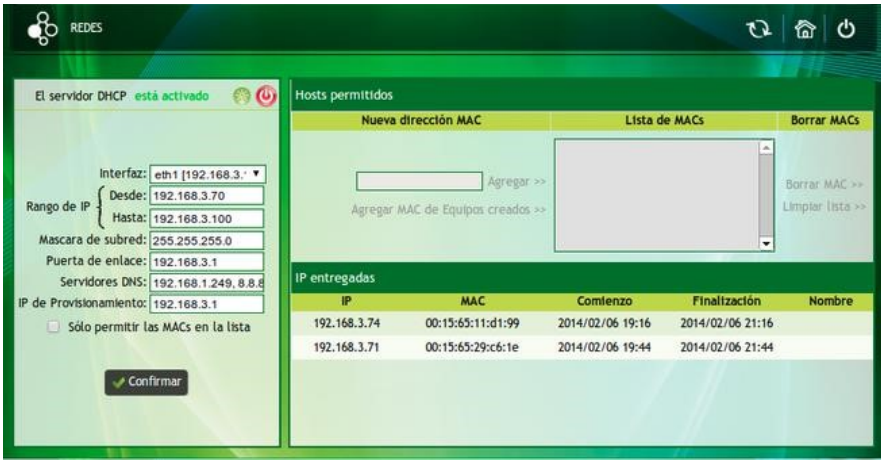
Si el certificado no fue generado en este servidor, también debe subir la clave privada (archivo .key):

La clave (.key) va aqui

Figure 3.114: Web server, certificate upload form

To disable the secure web server, it is necessary to click on the HTTPS button, the system requests confirmation and again you must enter the web as an administrator to continue configuring the options.

3.3.7.4.4 DHCP Server This service allows us to configure a server. DHCP (Dynamic Host Configuration Protocol) is a network protocol that allows clients on an IP network to obtain their configuration parameters automatically. The server is responsible for providing the host with the basic network configuration (IP, netmask, gateway, DNS, provisioning IP).



El servidor DHCP está activado

Interfaz: eth1 [192.168.3.
Rango de IP Desde: 192.168.3.70
Hasta: 192.168.3.100
Mascara de subred: 255.255.255.0
Puerta de enlace: 192.168.3.1
Servidores DNS: 192.168.1.249, 8.8.8
IP de Provisionamiento: 192.168.3.1
□ Sólo permitir las MACs en la lista

Hosts permitidos

Nueva dirección MAC	Lista de MACs	Borrar MACs
Agregar >> Agregar MAC de Equipos creados >>		Borrar MAC >> Limpiar lista >>

IP entregadas

IP	MAC	Comienzo	Finalización	Nombre
192.168.3.74	00:15:65:11:d1:99	2014/02/06 19:16	2014/02/06 21:16	
192.168.3.71	00:15:65:29:c6:1e	2014/02/06 19:44	2014/02/06 21:44	

Figure 3.115: DHCP Server

As seen in the previous figure, the screen is divided into three zones. In the main area, on the left of the screen, you will find the DHCP server settings.

It is necessary to configure the following data for the correct functioning of the server.

- **Interface**: the network interface on which the DHCP server will be used must be selected. Remember that the interface that is configured as the DHCP server must be in the same IP range as the gateway and provisioning IP.
- **IP Range**: is the range of IP addresses that the server will deliver to the different clients (host) that request them.
- **Subnet mask**: combination of bits used to define which part of the IP address is the network number and which part corresponds to the host.
- **Gateway**: is the gateway of the network.
- **DNS Server**: is the address of the DNS server that we will use.
- **Provisioning IP**: It is the IP address that will be used for equipment provisioning. The phone when taking ip by DHCP will also take the address where to look for the configuration file.

The «□ Only allow MACs in the list» field enables MAC filtering according to the list shown on the right of the screen. The MAC can be added manually, writing the address in the corresponding field and pressing «Add»; or adding all the computers added to «My Computers» (see **??** on the **??** page) by clicking on «Add MAC of created Computers»

External DHCP server If you are using an alternative DHCP to Denwa, in order to provision you need to configure DHCP options 66 and 67 by pointing them to `http://ip-denwa/provisioning/general/`

After completing these parameters, confirm the configuration by clicking on «✔ Confirm» and activate the service by clicking on the ⏻icon. If you want to restart it, just click on the ✱button.

In the lower right sector are the computers that are currently connected to the DHCP server, along with the following information:

- **IP**: IP address assigned to the device
- **MAC**: MAC address of the network card that was given the IP address
- **Start**: date and time of IP address grant
- **End**: date and time at which the lease will be renewed
- **Name**: device name

3.3.7.4.5 SNMPv1 Server

Simple Network Management Protocol or SNMP (for its acronym in English) is an application layer protocol that facilitates the exchange of management information between network devices. SNMP allows administrators to monitor network performance, find and resolve problems.

SNMP is based on two main elements, a supervisor and agents. The supervisor is the terminal that allows the network administrator to make management requests and the agents are entities that are at the level of each interface. They connect the managed devices to the network. These devices can be hardware information, configuration parameters, performance statistics, etc. These elements are classified in a database called MIB («Management Information Database»).

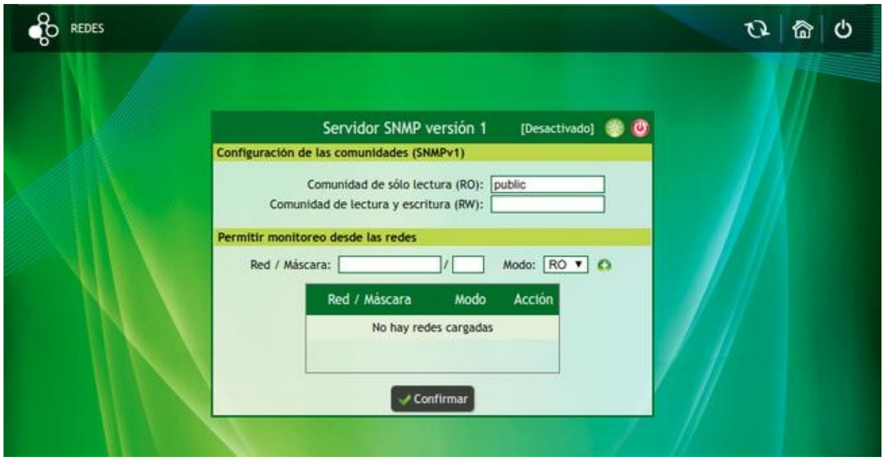
In order to carry out monitoring as an administration, it is necessary to follow the following steps

1. Install the SNMP application on the PC to monitor from the linux console

```
sudo apt-get install snmp
```

SNMP installation

2. Configure the SNMP server in Denwa UC&C 4.0.1 by going to Configuration > Networks > SNMP server



Servidor SNMP versión 1 [Desactivado]

Configuración de las comunidades (SNMPv1)

Comunidad de sólo lectura (RO): public
Comunidad de lectura y escritura (RW):

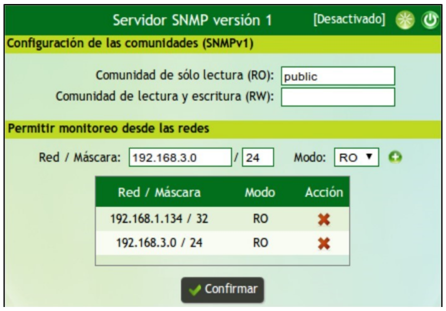
Permitir monitoreo desde las redes

Red / Máscara: / Modo: RO

Red / Máscara	Modo	Acción
No hay redes cargadas		

Figure 3.116: SNMPv1 Server

The first step in configuring is to set the authorized community and the permissions for them. There are different methods to determine the communities: the public option (it is possible to monitor any network), list (certain networks or hosts are established) or the empty box (the permission for the community is not configured).
Then it must be determined which host or networks are allowed to monitor the Denwa. To define a host, you must enter the IP number with mask 32 and for a network, the IP number of the network and its mask. In addition, the permissions are assigned to each one from the Mode checkbox. To complete the process, click on the ⊕sign. All networks are displayed in a list at the bottom of the screen.



Servidor SNMP versión 1 [Desactivado]

Configuración de las comunidades (SNMPv1)

Comunidad de sólo lectura (RO): public

Comunidad de lectura y escritura (RW):

Permitir monitoreo desde las redes

Red / Máscara: 192.168.3.0 / 24 Modo: RO

Red / Máscara	Modo	Acción
192.168.1.134 / 32	RO	✖
192.168.3.0 / 24	RO	✖

✔ Confirmar

Figure 3.117: SNMPv1 server, network addition

Finally, you must click on «✔ Confirm» and enable the SNMP server by clicking on ✱.

3. Monitor Denwa from the LInux console. To do this, you must write the following command.

```
snmpget -v2c -c public 192.168.1.204 .1.3.6.1.4.1.2021.4.5.0
```

Snmp Query Example

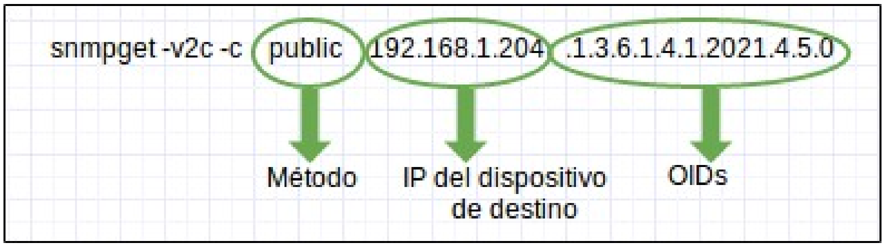

snmpget -v2c -c public 192.168.1.204 .1.3.6.1.4.1.2021.4.5.0
Método
IP del dispositivo de destino
OIDs

Figure 3.118: SNMPv1 server, query structure

Some of the OIDs are described below with the association of the type of information presented by each one.

- **CPU Statistics**
  - **Last minute upload**: .1.3.6.1.4.1.2021.10.1.3.1
  - **Load last 5 minutes**: .1.3.6.1.4.1.2021.10.1.3.2
  - **Load last 15 minutes**: .1.3.6.1.4.1.2021.10.1.3.3
- **CPU**
  - **CPU time percentage per user**: .1.3.6.1.4.1.2021.11.9.0
  - **System CPU time**: .1.3.6.1.4.1.2021.11.10.0
  - **CPU free time percentage**: .1.3.6.1.4.1.2021.11.11.0
- **Memory Statistics**
  - **Total Swap Size**: .1.3.6.1.4.1.2021.4.3.0
  - **Available swap space**: .1.3.6.1.4.1.2021.4.4.0
  - **Total RAM**: .1.3.6.1.4.1.2021.4.5.0
  - **Used RAM**: .1.3.6.1.4.1.2021.4.6.0
  - **Free RAM**: .1.3.6.1.4.1.2021.4.11.0
  - **Shared RAM**: .1.3.6.1.4.1.2021.4.13.0
  - **RAM Buffered**: .1.3.6.1.4.1.2021.4.14.0
  - **Total memory cached**: .1.3.6.1.4.1.2021.4.15.0

- **Disk Statistics**
  - **Path where the disk is mounted**: .1.3.6.1.4.1.2021.9.1.2.1
  - **Path to the computer partition**: .1.3.6.1.4.1.2021.9.1.3.1
  - **Total disk/partition size(kBytes)**: .1.3.6.1.4.1.2021.9.1.6.1
  - **Available disk space**: .1.3.6.1.4.1.2021.9.1.7.1
  - **Used disk space**: .1.3.6.1.4.1.2021.9.1.8.1
  - **Percentage of disk used**: .1.3.6.1.4.1.2021.9.1.9.1
  - **Percentage of inodes used**: .1.3.6.1.4.1.2021.9.1.10.1

3.3.7.4.5.1 RAM Query Example

To monitor the total RAM memory available to Denwa UC&C 4.0.1 , it is entered in a console client.

```
get -v2c -c public 192.168.1.139 .1.3.6.1.4.1.2021.4.5.0
```

Snmp RAM Query Example

The answer is:

```
3.6.1.4.1.2021.4.5.0 = INTEGER: 1016600
```

Sample response to RAM query by snmp

Where 1016600 is the size in megabytes of RAM.

3.3.7.4.5.2 Temperature query example

Performing a snmp query to the equipment can obtain the desired information, however it must be correlated. The community is configured from the web interface of the PBX (SNMPv1 Server Network Configuration) and the IP corresponds to the IP of the equipment that you wish to consult.

```
walk -v 2c -c 1.3.6.1.4.1.2021.13.16
```

Snmp Temperature Query Example

The following is an example of the data you'll get from this query:

```
3.6.1.4.1.2021.13.16.2.1.1.1 = INTEGER: 1
3.6.1.4.1.2021.13.16.2.1.1.2 = INTEGER: 2
3.6.1.4.1.2021.13.16.2.1.1.3 = INTEGER: 3
3.6.1.4.1.2021.13.16.2.1.1.4 = INTEGER: 4
3.6.1.4.1.2021.13.16.2.1.1.5 = INTEGER: 5
3.6.1.4.1.2021.13.16.2.1.1.6 = INTEGER: 6
3.6.1.4.1.2021.13.16.2.1.1.7 = INTEGER: 7
3.6.1.4.1.2021.13.16.2.1.1.8 = INTEGER: 8
3.6.1.4.1.2021.13.16.2.1.1.9 = INTEGER: 9
3.6.1.4.1.2021.13.16.2.1.1.10 = INTEGER: 10
3.6.1.4.1.2021.13.16.2.1.1.11 = INTEGER: 11
3.6.1.4.1.2021.13.16.2.1.2.1 = STRING: “loc1"
3.6.1.4.1.2021.13.16.2.1.2.2 = STRING: “Physical id 0"
3.6.1.4.1.2021.13.16.2.1.2.3 = STRING: “Core 0"
3.6.1.4.1.2021.13.16.2.1.2.4 = STRING: “Core 1"
3.6.1.4.1.2021.13.16.2.1.2.5 = STRING: “Core 2"
3.6.1.4.1.2021.13.16.2.1.2.6 = STRING: “Core 3"
3.6.1.4.1.2021.13.16.2.1.2.7 = STRING: “Core 4"
3.6.1.4.1.2021.13.16.2.1.2.8 = STRING: “Core 5"
3.6.1.4.1.2021.13.16.2.1.2.9 = STRING: “Core 6"
3.6.1.4.1.2021.13.16.2.1.2.10 = STRING: “Core 7"
3.6.1.4.1.2021.13.16.2.1.2.11 = STRING: “Physical id 1"
3.6.1.4.1.2021.13.16.2.1.3.1 = Gauge32: 47000
```

```
3.6.1.4.1.2021.13.16.2.1.3.2 = Gauge32: 33000
3.6.1.4.1.2021.13.16.2.1.3.3 = Gauge32: 29000
3.6.1.4.1.2021.13.16.2.1.3.4 = Gauge32: 29000
3.6.1.4.1.2021.13.16.2.1.3.5 = Gauge32: 28000
3.6.1.4.1.2021.13.16.2.1.3.6 = Gauge32: 28000
3.6.1.4.1.2021.13.16.2.1.3.7 = Gauge32: 28000
3.6.1.4.1.2021.13.16.2.1.3.8 = Gauge32: 27000
3.6.1.4.1.2021.13.16.2.1.3.9 = Gauge32: 27000
3.6.1.4.1.2021.13.16.2.1.3.10 = Gauge32: 27000
3.6.1.4.1.2021.13.16.2.1.3.11 = Gauge32: 34000
```

Example of response to the snmp temperature query

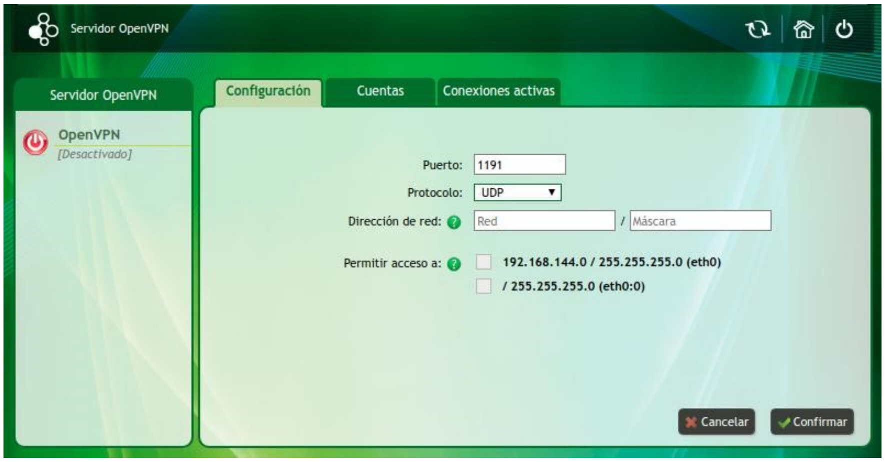
The information must be related by sensor number, this being the last number of the query string (in iso.3.6.1.4.1.2021.13.16.2.1.3.11 the sensor number would be 11), and the results of the the following way:

1	loc1	47000
2	Physical id 0	33000
3	Core 0	29000
4	Core 1	29000
5	Core 2	28000
6	Core 3	28000
7	Core 4	28000
8	Core 5	27000
9	Core 6	27000
10	Core 7	27000
11	Physical id 1	34000

The value is in Centigrade milligrades, that is, it must be divided into a thousand to be read in Centigrade degrees; that is to say:

1	loc1	47,000 °C
2	Physical id 0	33,000 °C
3	Core 0	29,000°C
4	Core 1	29,000°C
5	Core 2	28,000°C
6	Core 3	28,000°C
7	Core 4	28,000°C
8	Core 5	27,000°C
9	Core 6	27,000°C
10	Core 7	27,000°C
11	Physical id 1	34,000 °C

3.3.7.4.6 OpenVPN Server In this section, the OpenVPN service will be configured to have secure connections for users outside the network. When entering the server you can see a screen like the following:



OpenVPN
[Desactivado]

Puerto: 1191
Protocolo: UDP
Dirección de red: Red / Máscara
Permitir acceso a: □ 192.168.144.0 / 255.255.255.0 (eth0)
□ / 255.255.255.0 (eth0:0)

Figure 3.119: OpenVPN Server

In the left column it is possible to start or stop the OpenVPN Server service by clicking on the ⏻icon.

3.3.7.4.6.1 Settings Tab In the previous image you can see that the server is disabled and that there is no pre-loaded configuration. Below is the detail of the parameters to be configured:

- **Port**: port to use for the OpenVPN service
- **Protocol**: protocol used by the server
- **Network Address/Mask**: network from which IP addresses will be given to clients
- **Allow Access**: Networks to which you want to give clients access.

3.3.7.4.6.2 Accounts Tab In this tab it is possible to register accounts for remote access to the unified communications platform and/or to the networks selected in the configuration tab.

Figure 3.120: OpenVPN server, access accounts

To make a new account we simply click on Create Account, and fill in the username; with this the account has been created and it is possible to download its certificates.

Figure 3.121: OpenVPN server, login account creation

To use the OpenVPN server it is necessary to have the certificates on the computers that will connect to it, so they must be downloaded from the accounts tab. Once on the local computer, it is necessary to have the OpenVPN «client» software and, from a basic text editor, generate an .ovpn file like the one shown below:

```
###########################################
nVPN Client
###########################################
```

```
nt
tun
ocol PROTOCOL
te SERVER_IP SERVER_PORT
lv-retry infinite
nd
-lzo
 3
rtificate files
CERTIFICATE_PATH/ca.crt"“
 CERTIFICATE_PATH/CERTIFICATE_NAME.crt"“
CERTIFICATE_PATH/CERTIFICATE_NAME.key"
###########################################
```

You must replace where it says «PROTOCOL», «IP_OF_SERVER», «PORT_OF_SERVER», «PATH_OF_CERTIFICATE», «NAME_CERTIFICATE» according to the configurations made on the server, as well as the downloaded certificates.

3.3.7.4.6.3 Logs Tab

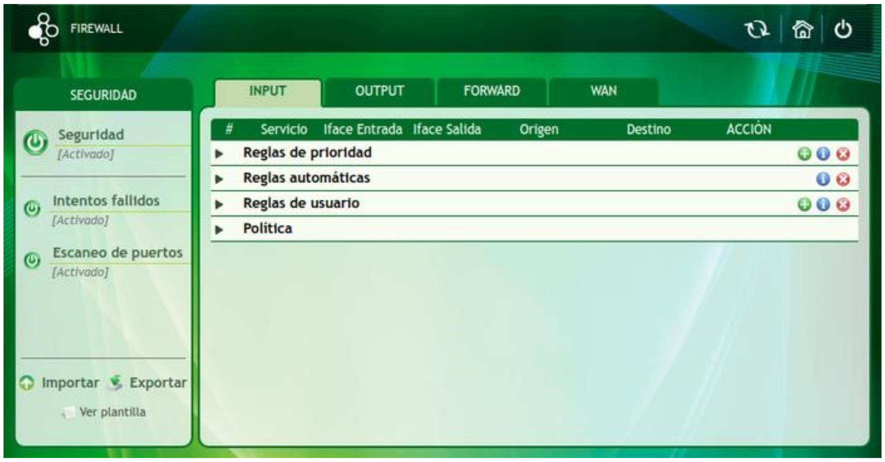
This tab will show the list of all active connections («clients» connected) to the OpenVPN service.

3.3.7.4.7 Firewall

This service allows you to set up a firewall, which is intended to help prevent hackers or malicious software from gaining access to your computer over a network or the Internet. It is responsible for creating a barrier between the Internet and the computer, just like the physical barrier that would constitute a brick wall.

The firewall acts as a filter controlling all the communications that pass from one network to another and based on this it allows or denies the passage, for this it examines the type of service to which it corresponds. It also inspects if the communication is incoming or outgoing and depending on its address it can allow it or not.

When entering the Firewall configuration, there is a panel with three buttons that enable and disable various options, detailed below.



Seguridad [Activado]

Intentos fallidos [Activado]

Escaneo de puertos [Activado]

#	Servicio	Iface Entrada	Iface Salida	Origen	Destino	ACCIÓN
▶	Reglas de prioridad					
▶	Reglas automáticas					
▶	Reglas de usuario					
▶	Política					

Figure 3.122: Firewall

From the ⏻ button you can enable or disable Denwa UC&C 4.0.1 security. With the firewall activated, the ports are opened dynamically, only during the time required to allow access to the desired services.

Failed attempts : If the system detects more than five failed attempts to register the computers, it automatically blocks access from the IP address, as it takes this as an attempted attack. The only way for this rule to be removed from the firewall is for an authorized administrator to remove it manually.

Port scanning : allows you to block attacks of this type automatically, Denwa UC&C 4.0.1 is constantly checking for possible port scans on the computer, when detecting this the system automatically blocks the IP address it is trying to perform this possible attack by creating a new rule in the Firewall. The only way for this rule to be removed from the firewall is for an authorized administrator to remove it manually.

Denwa also allows you to create new rules, these depend on what you want. The new rules can be entry, exit or forward.

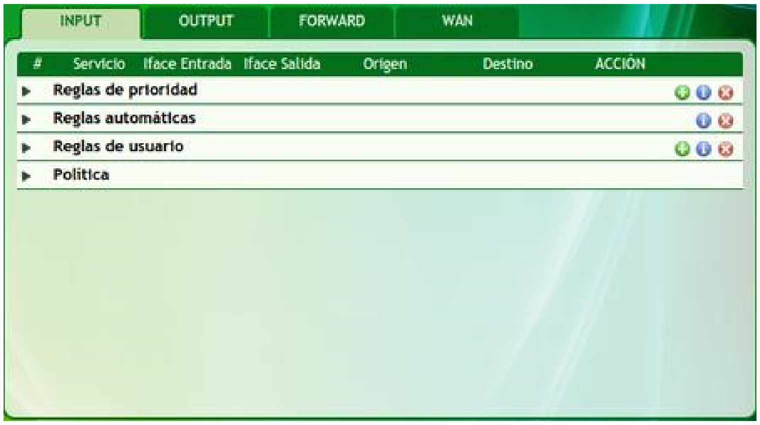
These rules can be imported by clicking on the «⬆ Import» icon or exported from the «⬇ Export» icon using a .csv file. For the import, it is recommended to download a template by clicking on the «🗋 View Template» icon and editing each row with the rule you want to add. It is suggested to verify that the format has not been modified.

Firewall Policy

Denwa UC&C 4.0.1 determines a general firewall policy. This can be Accept or Drop, if the **Accept** policy is set, all the rules created must be **Drop**, that is, exceptions to the policy.

3.3.7.4.7.1 INPUT, OUTPUT and FORWARD tabs

From the INPUT, OUTPUT and FORWARD tabs you can manage incoming, outgoing and redirected connections, respectively.



#	Servicio	Iface Entrada	Iface Salida	Origen	Destino	ACCIÓN
▸	Reglas de prioridad					⊕ ⓘ ⊗
▸	Reglas automáticas					ⓘ ⊗
▸	Reglas de usuario					⊕ ⓘ ⊗
▸	Politica					

Figure 3.123: Firewall, string configuration

There are three (3) types of rules:

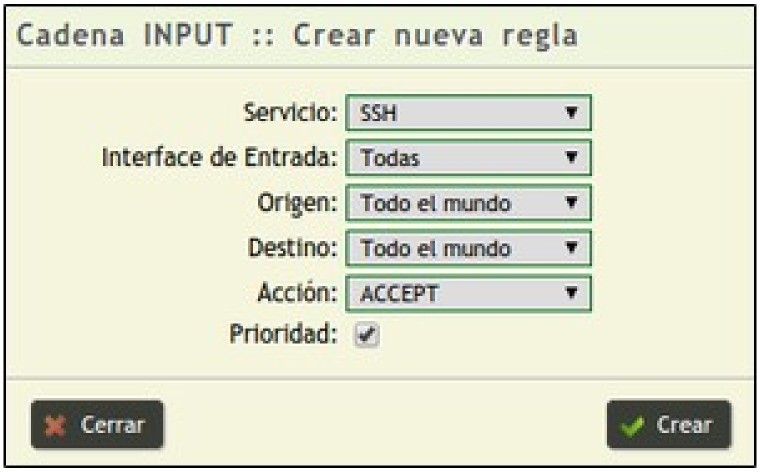
- **Priority Rules**: These are high-priority rules created by the Denwa UC administrator and have higher priority than rules added by auto-blocking services. It has the buttons ⊕ (add rule), ⓘ (help) and ⊗ (delete all rules).

High Availability Exception

When Denwa UC&C 4.0.1 is part of a High Availability cluster (Active-Passive), the priority rules will be blocked by the system, not allowing their editing.

- **Automatic Rules**: These rules are not generated by administrators, but are generated automatically by port scanning services and failed attempts. It has the buttons ⓘ (help) and ⊗ (clear all rules).
- **User rules**: These are rules created by the administrator. It has the buttons ⊕ (add rule), ⓘ (help) and ⊗ (delete all rules).

Both in priority rules and in user rules, when adding a rule the following window is displayed:



Cadena INPUT :: Crear nueva regla

Servicio: SSH

Interface de Entrada: Todas

Origen: Todo el mundo

Destino: Todo el mundo

Acción: ACCEPT

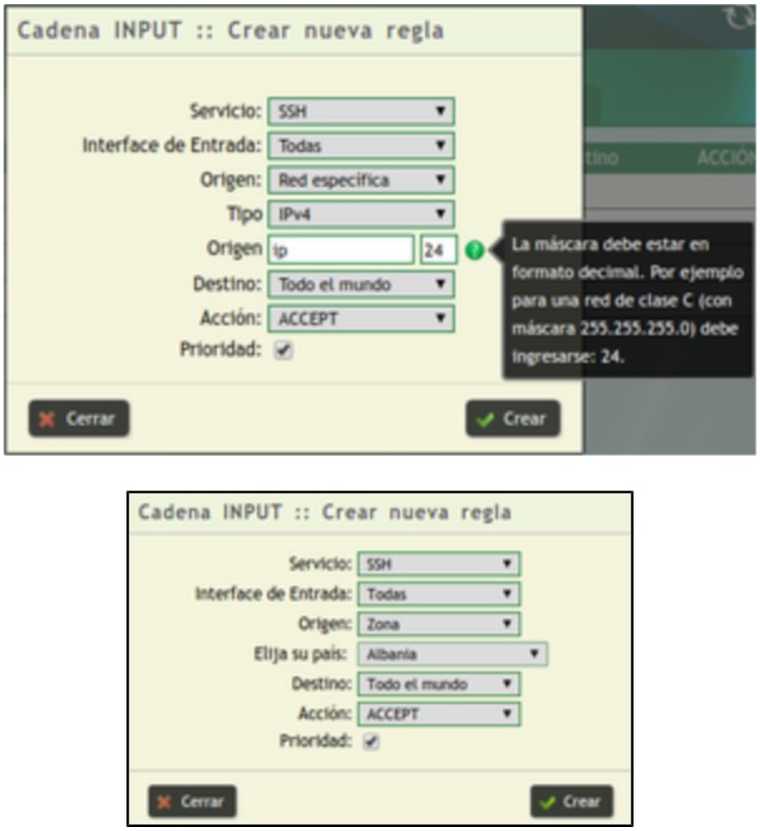
Prioridad: ☑

Figure 3.124: Firewall, add rule

- **Service**: select the service to manage from a drop-down list. Services can be:
  - SSH
  - PING
  - RTP
  - SIP
  - HTTP
  - HTTPS
  - TFTP
  - FTP
  - DNS
  - XMPP
  - VPN
  - All
  - Or by protocol and port

  In the latter case, the window will change to be able to locate the protocol (TCP or UDP) and the corresponding port number.
- **Input Interface**: choose the interface to which the rule applies.
- **Origin**: determines who the rule is set to, it can be Everybody, Specific Host, Specific Network or Zone. In the case of a specific network, the IP or Domain

must also be assigned; in the case of a zone, a country must be selected; and for the specific Host and specific Network cases, the type must be selected.



Cadena INPUT :: Crear nueva regla

Servicio: SSH
Interface de Entrada: Todas
Origen: Red especifica
Tipo IPv4
Origen ip 24
Destino: Todo el mundo
Acción: ACCEPT
Prioridad: ☑

La máscara debe estar en formato decimal. Por ejemplo para una red de clase C (con máscara 255.255.255.0) debe ingresarse: 24.

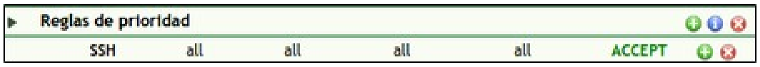
Cadena INPUT :: Crear nueva regla

Servicio: SSH
Interface de Entrada: Todas
Origen: Zona
Elija su país: Albania
Destino: Todo el mundo
Acción: ACCEPT
Prioridad: ☑

Figure 3.125: Chain configuration, network specific

- **Destination**: can be Worldwide, Host specific, or Network specific. In these last cases, the IP or Domain and the type must also be assigned.
- **Action**: The options will be ACCEPT, REJECT, and DROP. These actions determine what type of rule is created.
- **Priority:** ☐: This field indicates that the rule created is of high priority.

Once the rule is created, it is displayed as follows:



▸ Reglas de prioridad

SSH	all	all	all	all	ACCEPT

Figure 3.126: Chain configuration, created rule

From the symbols ⊕ ⊗ it is possible to add a new rule or delete the existing one, respectively. In the first case, adding a new rule, provides the options of:

- Insert Top
- Insert Below

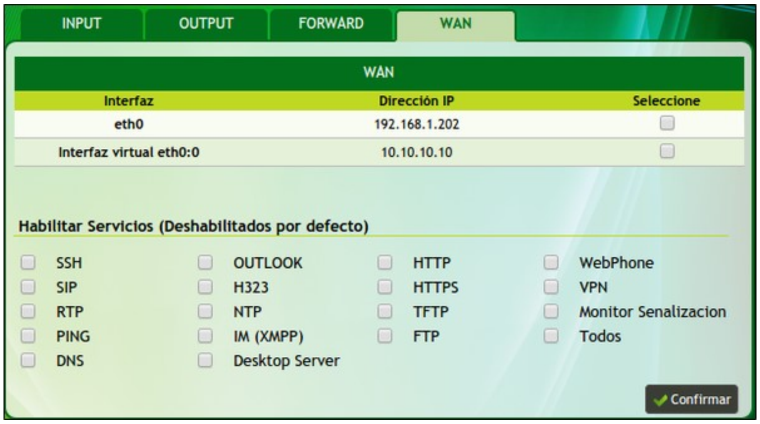
In addition to the usual options, it is possible to select whether the new rule will be placed above or below the existing one.

Policy The default rule is established that any packet that does not match any of the created rules will be accepted/rejected, as selected from the drop-down menu; By default the policy is accepted.

Order and priority It must always be kept in mind that the firewall is 'sequential', therefore priority will be given to those rules that are found over the others. The sequence used by said firewall is the following: Priority Rules, Automatic Rules, User Rules, Services (WAN) and Policy.

3.3.7.4.7.2 WAN tab

In this section it is possible to configure the security of WAN services, that is, it only applies to incoming traffic. A simple management is provided for the administrator through a window like the one shown in the following image:



WAN

Interfaz	Dirección IP	Seleccione
eth0	192.168.1.202	□
Interfaz virtual eth0:0	10.10.10.10	□

Habilitar Servicios (Deshabilitados por defecto)

- □ SSH
- □ SIP
- □ RTP
- □ PING
- □ DNS
- □ OUTLOOK
- □ H323
- □ NTP
- □ IM (XMPP)
- □ Desktop Server
- □ HTTP
- □ HTTPS
- □ TFTP
- □ FTP
- □ WebPhone
- □ VPN
- □ Monitor Senalizacion
- □ Todos

Figure 3.127: Firewall, WAN settings

The list above shows the network interfaces that Denwa UC&C 4.0.1 has configured, in the last column you must select the interface that will be used as WAN.

Since all the default services are disabled to raise the level of security; Only those that you want to allow from the WAN should be enabled.

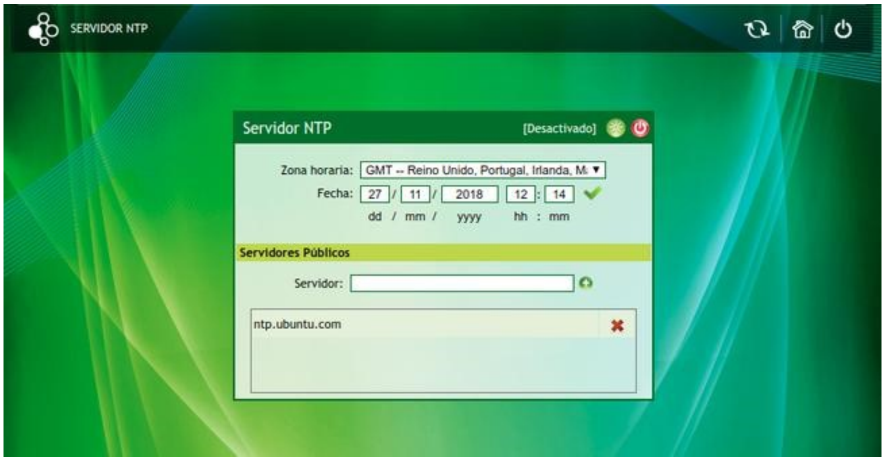
Order and priority It must always be kept in mind that the firewall is 'sequential', therefore priority will be given to those rules that are found over the others. The sequence used by said firewall is the following: Priority Rules, Automatic Rules, User Rules, Services (WAN) and Policy.

3.3.7.4.8 NTP Server

NTP (*Network Time Protocol*) is a protocol for synchronizing clocks in network equipment based on a client-server system. This functionality is important because it allows network devices to have the correct time settings at all times (even when internet connection is lost).

With this server clients are provided *offset*, *round-trip delay* and hash reference. The *offset* specifies the difference between the local system time and the external clock reference. *Round-trip delay* specifies the time latencies measured during packet transfers within the network. The time spread reference specifies the maximum number of errors associated with time information received from an external clock.

For the configuration of the server within Denwa UC&C 4.0.1 the following steps must be carried out



Servidor NTP [Desactivado]

Zona horaria: GMT -- Reino Unido, Portugal, Irlanda, M. ▾
Fecha: 27 / 11 / 2018 12 : 14 ✓
dd / mm / yyyy hh : mm

Servidores Públicos

Servidor:

ntp.ubuntu.com ✖

Figure 3.128: NTP, configuration

The time zone and date parameters can be modified. The time zone must be chosen from the drop-down menu, while the current date must be filled in in the *textbox* with the format «dd/mm/yyyy», while the time in the «hh :mm». To accept the changes it is necessary to click on the ✓icon.

In case you want to disable the service, it can be turned off using the ⏻button.

By default, Denwa UC&C 4.0.1 checks its own time settings with an external server, this is the default server `ntp.ubuntu.com`, it is possible to add or use a server other than the one configured by factory by completing the server domain and clicking ⊕.

Once the NTP server is configured, Denwa UC&C 4.0.1 will proceed to:

- Configure all the computers on the network with the changes previously made.
- Periodically check that your time settings are correct using the servers that were configured earlier (default: ntp.ubuntu.com).
- If the connection to these servers is lost, the computers on the network will be synchronized against Denwa UC&C 4.0.1 and will not lose their configuration.

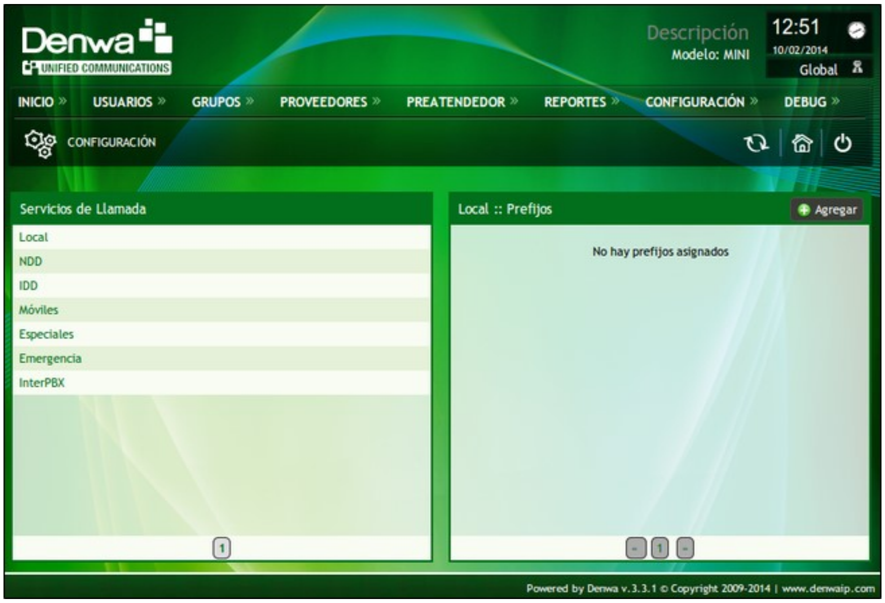
3.3.7.4.9 Messaging server

The messaging server allows you to activate and deactivate instant messaging for users created in Denwa.

To activate the server you must click on ✱ and to deactivate it on ⏻.

3.3.7.5 Call service

From the Call Services menu you can create and manage the definition of the numbering plan that is used in the Denwa PBX.



Servicios de Llamada

- Local
- NDD
- IDD
- Móviles
- Especiales
- Emergencia
- InterPBX

Local :: Prefijos

No hay prefijos asignados

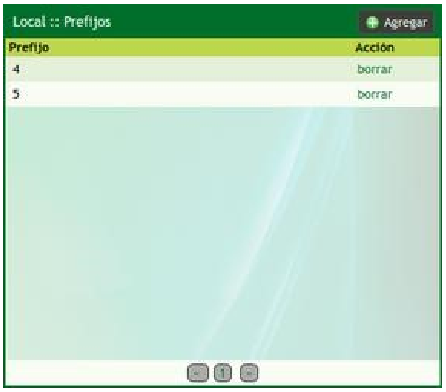
Powered by Denwa v.3.3.1 © Copyright 2009-2014 | www.denwaip.com

Figure 3.129: Call service

The different services are the following:

- **Local**: are the dialed numbers that the system will identify as local calls. To add a local prefix you must:
  1. Select «Local» in the list on the left
  2. Press the «✚ Add» button in the box called «Local :: Prefixes»
  3. Add the new prefix for local calls
  4. Click on the button «✚ Confirm»

  These steps can be repeated as many times as necessary, leaving the list as follows:



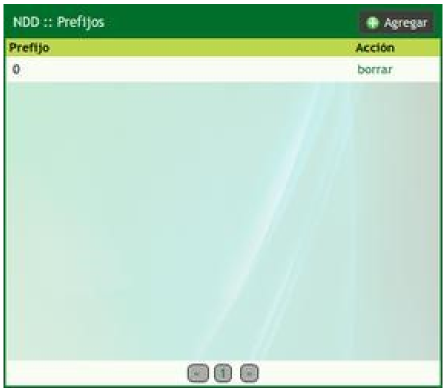
Local :: Prefijos

Prefijo	Acción
4	borrar
5	borrar

Figure 3.130: Call service, local call prefixes

- **NDD**: are dialed numbers that the system will identify as national calls. To add an NDD prefix you must:
  1. Select «NDD» in the list on the left
  2. Press the «✚ Add» button in the box called «NDD :: Prefixes»
  3. Add the new prefix for direct dial national calls
  4. Click on the button «✚ Confirm»

These steps can be repeated as many times as necessary, leaving the list as follows:



NDD :: Prefijos

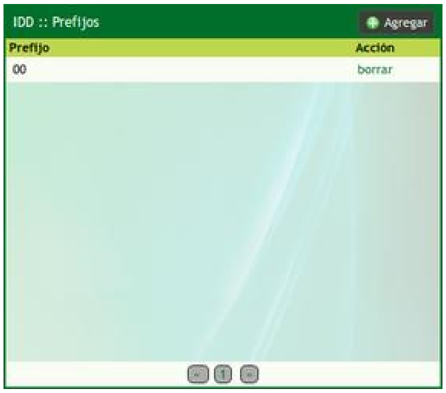
Prefijo	Acción
0	borrar

Figure 3.131: Call service, direct dial national call prefixes

In this case, for Argentina, the national direct dialing is 0.

- **IDD**: These are dialed numbers that the system will identify as International calls. To add an IDD prefix you must:
  1. Select «IDD» in the list on the left
  2. Press the «✚ Add» button in the box called «IDD :: Prefixes»
  3. Add the new prefix for direct dial international calls
  4. Click on the button «✚ Confirm»

  These steps can be repeated as many times as necessary, leaving the list as follows:



IDD :: Prefijos

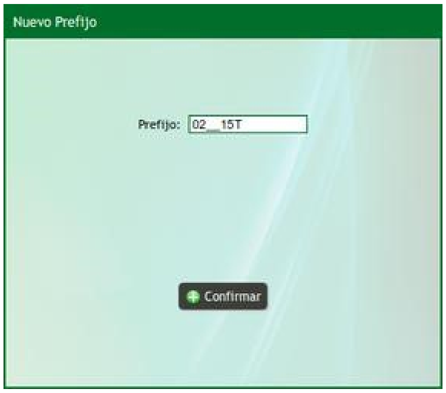
Prefijo	Acción
00	borrar

Figure 3.132: Call service, direct dial international call prefixes

In this case, for Argentina, the international direct dialing is 00.

- **Mobiles**: are dialed numbers that the system will identify as calls to mobiles. To add a Mobile prefix you must:
  1. Select «Mobiles» in the list on the left
  2. Press the «✚ Add» button in the box called «Mobile Phones:: Prefixes»
  3. Add the new prefix for mobile calls
  4. Click on the button «✚ Confirm»

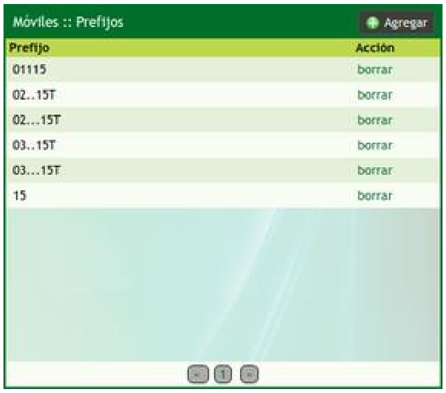
  These steps can be repeated as many times as necessary. In the case of Argentina, calls to mobiles begin with 15, but it must be taken into account that non-local mobiles must precede the area code. For example, for calls to mobiles outside the local area, they must be charged as follows:



Prefijo: 02__15T

Figure 3.133: Call service, call prefix to mobile outside the local area

The list is formed as follows:



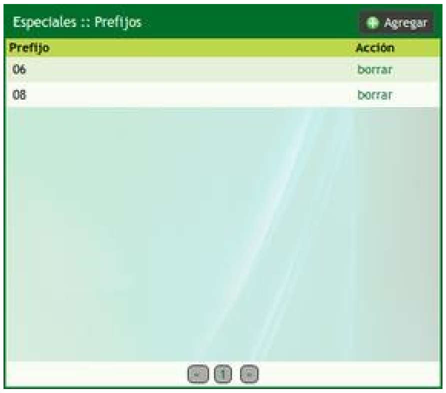
Prefijo	Acción
01115	borrar
02..15T	borrar
02...15T	borrar
03..15T	borrar
03...15T	borrar
15	borrar

Figure 3.134: Call service, mobile call prefixes

- **Special**: are dialed numbers that the system will identify as calls to special numbers such as 0800, 0610, 0600, etc. To add a special prefix you must:

  1. Select «Specials» in the list on the left
  2. Press the «✚ Add» button in the box called «Special :: Prefixes»
  3. Add the new prefix for calls to special numbers
  4. Click on the button «✚ Confirm»

  These steps can be repeated as many times as necessary, leaving the list as follows:



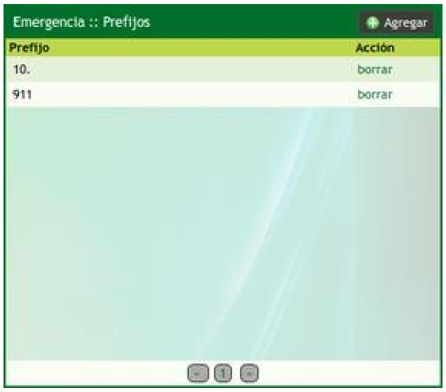
Especiales :: Prefijos

Prefijo	Acción
06	borrar
08	borrar

Figure 3.135: Call service, call prefixes to special numbers

- **Emergency**: are dialed numbers that the system will identify as calls to emergency numbers such as 911, 101, 100. To add an emergency prefix you must:
  1. Select «Emergency» in the list on the left
  2. Press the «⊕ Add» button in the box called «Emergencya:: Prefixes»
  3. Add the new prefix for calls to Emergencies
  4. Click on the button «⊕ Confirm»

  These steps can be repeated as many times as necessary, leaving the list as follows:



Emergencia :: Prefijos

Prefijo	Acción
10.	borrar
911	borrar

Figure 3.136: Call service, emergency call prefixes

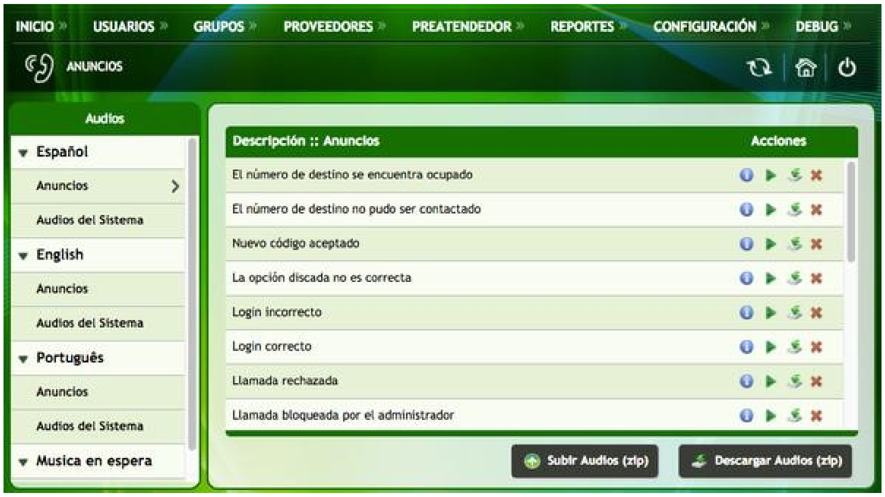
- **InterPBX**: are the numbers dialed for calls between PBXs.

To delete the prefixes from the list, click on «delete».

3.3.7.6 Ads

From the Announcements tab, you can customize announcements or voice messages associated with different Denwa UC&C 4.0.1 events. These messages are predefined by Denwa, but the administrator can customize them according to his convenience. These announcements are available in four (4) languages, namely:

- Spanish
- English
- Portuguese
- Hebrew



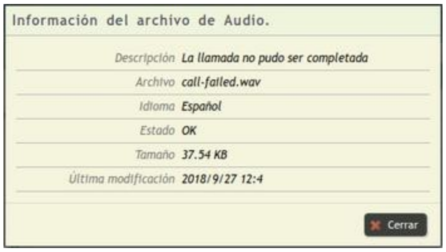
Descripción :: Anuncios	Acciones
El número de destino se encuentra ocupado	ℹ ▶ ⤓ ✖
El número de destino no pudo ser contactado	ℹ ▶ ⤓ ✖
Nuevo código aceptado	ℹ ▶ ⤓ ✖
La opción discada no es correcta	ℹ ▶ ⤓ ✖
Login incorrecto	ℹ ▶ ⤓ ✖
Login correcto	ℹ ▶ ⤓ ✖
Llamada rechazada	ℹ ▶ ⤓ ✖
Llamada bloqueada por el administrador	ℹ ▶ ⤓ ✖

Figure 3.137: Ads

3.3.7.6.1 Ads by Language To display the list of audios corresponding to each language (or music on hold), click on the name of the language, which will change the ▸ icon to ▾. The › icon will be displayed next to the displayed option.

Each and every one of the listed audios has the following options:

- ℹ: Information about the properties of the audio file.



Información del archivo de Audio.

Descripción	La llamada no pudo ser completada
Archivo	call-failed.wav
Idioma	Español
Estado	OK
Tamaño	37.54 KB
Última modificación	2018/9/27 12:4

Figure 3.138: Ads, audio file properties

- ▶: Play
- ⤓: Download
- ✖: Delete

To upload a new announcement, you must first delete the audio file to be replaced and then enter the new one. It also allows you to upload and download files in zip format, using the buttons «⬆ Upload Audios (zip)» and «⤓ Download Audios (zip)»

3.3.7.6.2 Music on Hold This section adds the option to configure music on hold in trunks, groups, users, etc. For which the administrator:

- Must define name and description
- Upload an audio file

In addition, the administrator can download, listen and update each of the lists. Once loaded, they can be selected in the advanced User section, in Groups and Preatttenders.

3.3.7.7 Equipment

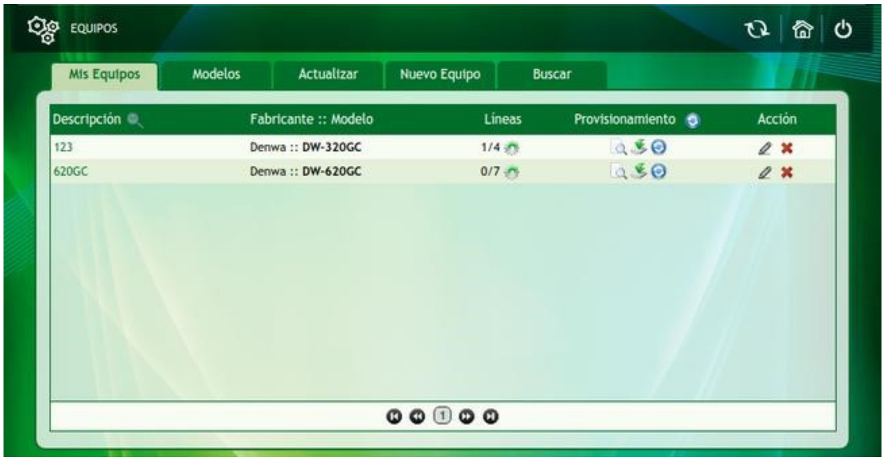
This Denwa UC&C 4.0.1 functionality allows you to search for and incorporate computers in the local network and then associate them with each of the users created.

Requirements The Denwa UC&C 4.0.1 DHCP server must be configured correctly. Within the DHCP server configuration, the provisioning IP must be the Denwa UC&C 4.0.1 IP for optimal operation.

The equipment to be incorporated must have the factory configuration, this is achieved from the equipment administration page or from its menu. The steps to perform depend on the make and model.

external DHCP Computers that did not receive an IP from Denwa UC&C 4.0.1 's DHCP will not be provisioned automatically, so it must be done manually.

3.3.7.7.1 My Computers tab In the My Teams tab, you can find out the status of the teams already configured within Denwa UC&C 4.0.1 .



Descripción 🔍	Fabricante :: Modelo	Lineas	Provisionamiento ⚙	Acción
123	Denwa :: DW-320GC	1/4 ⚙	🔍 ⤓ ⟳	✎ ✖
620GC	Denwa :: DW-620GC	0/7 ⚙	🔍 ⤓ ⟳	✎ ✖

Figure 3.139: Teams, My Teams

In the previous figure you can see a list of the configured equipment, it is possible to filter according to the Description by clicking on 🔍.

To know the information about the provisioned equipment, click on its name, which appears under the «Description» column, with which data related to the device and its manufacturer are displayed, as well as information associated with the network.

By clicking on the ⚙icon, it is possible to manage the SIP accounts of the equipment, and it is possible to disassociate a port by clicking on the X-shaped icon (✖) on the desired port.

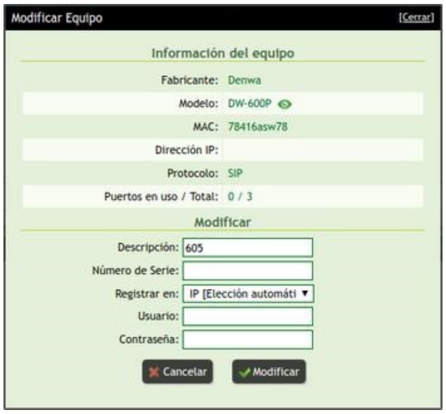
In the «Provisioning» column, there are three options:

- 🗎: View provisioning file.
- ⤓: Download provisioning file.
- ⟳: Regenerate provisioning file, normally used when a change has been generated.

The Action column presents two options:

- ✎: Provides information about the computer and allows you to vary the options, such as:

- **Description**: is a descriptive name of the equipment.
- **Serial number**: equipment serial number.
- **Register in**: interface to register the device
- **User**: computer user name for access.
- **Password**: access key to the equipment for user access



Modificar Equipo [Cerrar]

Información del equipo

Fabricante:	Denwa
Modelo:	DW-600P
MAC:	78416asw78
Dirección IP:	
Protocolo:	SIP
Puertos en uso / Total:	0 / 3

Modificar

Descripción:	605
Número de Serie:	
Registrar en:	IP [Elección automáti ▾
Usuario:	
Contraseña:	

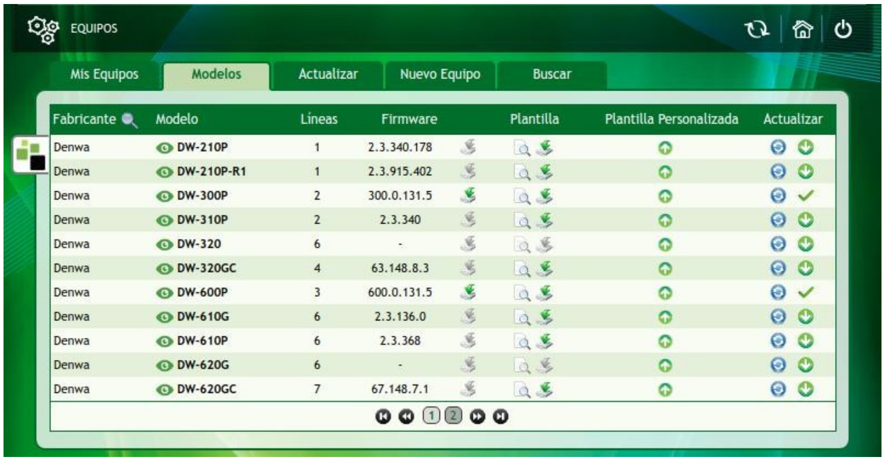
Figure 3.140: Equipment, modification of my equipment

After making the changes, it is necessary to regenerate the provisioning file for the changes to take effect.

- ✖: remove the computer from the Denwa network.

3.3.7.7.2 Models tab

This tab presents a drop-down with brands and models of equipment. With a click on the name of the manufacturer, the list of equipment that has been approved for provisioning from Denwa UC&C 4.0.1 will be displayed.



Fabricante	Modelo	Líneas	Firmware	Plantilla	Plantilla Personalizada	Actualizar
Denwa	DW-210P	1	2.3.340.178			
Denwa	DW-210P-R1	1	2.3.915.402			
Denwa	DW-300P	2	300.0.131.5			✓
Denwa	DW-310P	2	2.3.340			
Denwa	DW-320	6	-			
Denwa	DW-320GC	4	63.148.8.3			
Denwa	DW-600P	3	600.0.131.5			✓
Denwa	DW-610G	6	2.3.136.0			
Denwa	DW-610P	6	2.3.368			
Denwa	DW-620G	6	-			
Denwa	DW-620GC	7	67.148.7.1			

Figure 3.141: Equipment, models

The observed data is:

- **Manufacturer**: name of the manufacturer
- **Model**: shows the model of the device, it is also possible to see a photo of it by clicking on 👁

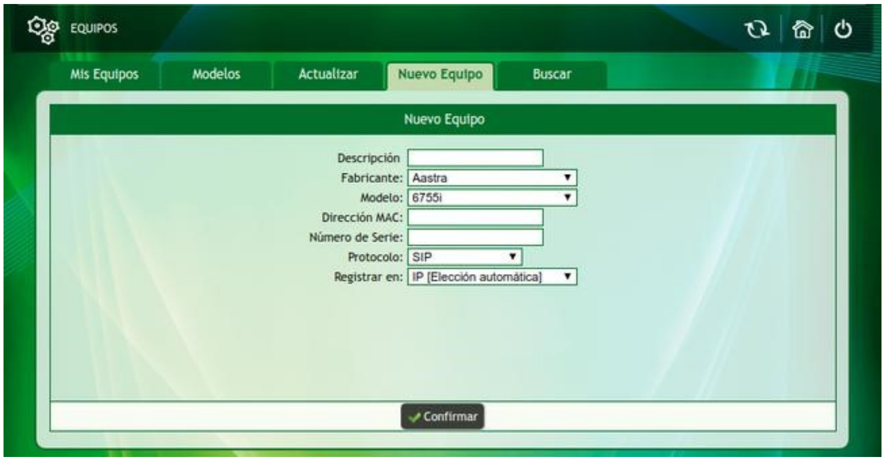
- **Lines**: indicates the number of SIP lines that can be configured
- **Firmware**: it is the firmware version used for the homologation of the equipment, it is necessary to use the same or higher version.

  > **Firmware version**
  >
  > It is possible to check the update option on this same screen to verify that the model has the latest approved firmware version.

  To the right of this option is the icon used to download the approved firmware (⬇).
- **Template**: You can view the template by clicking on 📄 or download it by clicking on ⬇. In both cases, a text file is observed that contains global information of the modules.
- **Custom Template**: Allows you to upload a custom template for the team by clicking on ⬆.
- **Update**: The option has two sections:
  - ⟳: allows you to update all the provisioning templates of the devices corresponding to this model
  - **Update Status**:
    - ✓: the Denwa UC&C 4.0.1 has the most recent version of firmware and approved templates
    - ⬇: Denwa Technology Corp. has released a more recent version of firmware and certified templates, which can be downloaded by clicking on the icon.

3.3.7.7.3 Update Tab It is similar to the previous one (Models tab, page 133), with the exception that only those devices that have an update pending download are shown.

3.3.7.7.4 New Team Tab Through this tab it is possible to manually upload a team to Denwa UC&C 4.0.1 .



Nuevo Equipo

Descripción:
Fabricante: Aastra
Modelo: 6755i
Dirección MAC:
Número de Serie:
Protocolo: SIP
Registrar en: IP [Elección automática]

Figure 3.142: Teams, new team

The fields to complete are the following.

- **Description**: is a descriptive name given to the equipment.

- **Manufacturer**: the list is based on equipment approved for Denwa UC&C 4.0.1 and its provisioning.
- **Model**: Shows a drop-down list with the models approved by this manufacturer for provisioning with the Denwa UC&C 4.0.1 .
- **MAC address**: Important information since it is the unique identifier of the equipment.
- **Serial Number**: equipment serial number.
- **Protocol**: can be SIP or MGCP.
- **Log in**: Allows you to select the interface in which the device will register.

After completing the fields, you must confirm by clicking on «✔ Confirm».

3.3.7.7.5 Search tab This section explains the steps to follow to search for equipment and their provisioning. It is assumed that the prerequisites (see warning in **??** on the **??** page) were configured correctly.

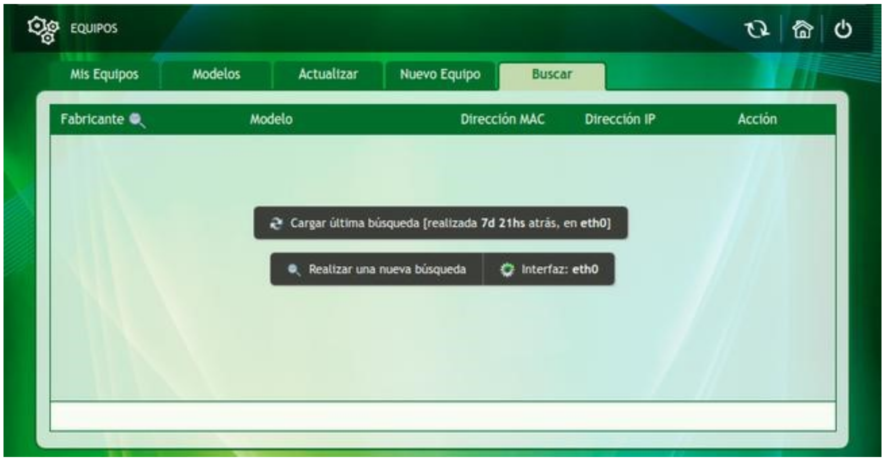
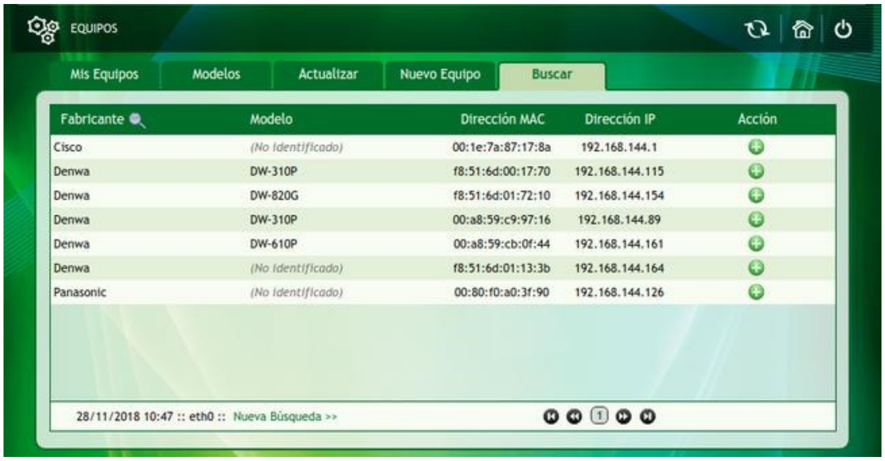


Figure 3.143: Teams, search for teams

Device lookup is based on ARP tables and identifies discovered devices based on their MAC address. The screen shows us two (2) different search options:

- **Load Last Search**: Allows you to rerun the last search performed with the search options used.
- **Perform a new search**: allows you to search the local network for existing computers, the steps to follow are very simple.
  1. Select the interface by clicking on Interface and select the interface in which you want to search for devices from the drop-down list.
  2. Click on Perform a new search.

Once the search is done, the following screen is displayed:



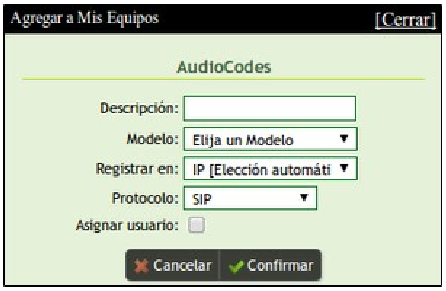
Fabricante	Modelo	Dirección MAC	Dirección IP	Acción
Cisco	*(No identificado)*	00:1e:7a:87:17:8a	192.168.144.1	⊕
Denwa	DW-310P	f8:51:6d:00:17:70	192.168.144.115	⊕
Denwa	DW-820G	f8:51:6d:01:72:10	192.168.144.154	⊕
Denwa	DW-310P	00:a8:59:c9:97:16	192.168.144.89	⊕
Denwa	DW-610P	00:a8:59:cb:0f:44	192.168.144.161	⊕
Denwa	*(No identificado)*	f8:51:6d:01:13:3b	192.168.144.164	⊕
Panasonic	*(No identificado)*	00:80:f0:a0:3f:90	192.168.144.126	⊕

28/11/2018 10:47 :: eth0 :: Nueva Búsqueda >>

Figure 3.144: Teams, team search result

The displayed list contains the devices discovered in the network to which the selected interface belongs. Includes:

- **Manufacturer**: allows filtering by clicking on 🔍
- **Model**
- **MAC address**
- **IP address**
- **Action**: depending on the provisioning status of the equipment, it can display two (2) different icons
  - ℹ: Displayed only next to provisioned computers, allows you to view device information.
  - ⊕: displayed only next to unprovisioned computers, clicking on it displays a popup window to start the provisioning process.



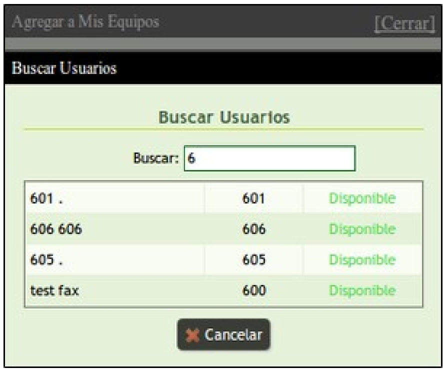
AudioCodes

Descripción:
Modelo: Elija un Modelo
Registrar en: IP [Elección automáti
Protocolo: SIP
Asignar usuario: □

Figure 3.145: Find equipment, add equipment

Its fields are:

- **Description of the equipment**: is a descriptive name of the equipment.
- **Model**:
- **Register in**: select the interface where the device will be registered.
- **Protocol**: Select the protocol, SIP or MGCP.
- **Assign to user:** □: allows assigning the equipment to a user previously created in Denwa UC&C 4.0.1 , clicking on the checkbox opens a window where users can be searched, selecting one is necessary to press «✔ Confirm»



Buscar: 6

601 .	601	Disponible
606 606	606	Disponible
605 .	605	Disponible
test fax	600	Disponible

Figure 3.146: Find equipment, add equipment

Reboot for provisioning

After provisioning, it is necessary to restart the provisioned phone so that it takes the provisioning data. Denwa models support the automatic restart option.

3.3.7.8 My Apps

Denwa allows applications to be used for particular purposes, which can be designed by the administrator on the DTI (Denwa Telephony Interface) module. They also allow assigning them to Preattenders and/or Users.

3.3.7.8.1 My Apps tab When entering this tab, five columns are observed.

- **Name**: The name of the application. When clicking on the name, the following window appears.
- **Description**: small review about the application.
- **Type**: on which the application is based.
- **Audios**: allows you to listen to the audios. Clicking on the following screen is displayed.
  Here you can load an audio from and get information by clicking on . Once the file is loaded it can be played from, downloaded or deleted.
- **Action**: modify or delete the applications.

3.3.7.8.2 New Application Tab To create a new application, you must choose the desired application type, enter a name and a description. Then to finish, click on Confirm.

3.3.7.8.2.1 Boss-Secretary Application In a Boss - Secretary scenario, when the secretary gets up from her post, she can, through the use of her phone, temporarily disable the function. From that moment the calls begin to come directly to the boss. When you resume your position, you can restore the function, and that you return to be a secretary.

This is similar to checking and unchecking the option from the web administration, only that the management is done from the secretary's phone through an application.

To create the application, in the Settings> My applications section, we register the application «Set Boss-Secretary Application» and fill in the Name and Description.

It will then appear in the My Apps list. The audios must be loaded for the application to work, you can customize the audios by clicking on the icon and load according to the function, or click to load the default audios of the application.

When registering the audios, they will appear in the list and the application will be ready to work.

To be able to call the application, it is necessary to create an application type extension and associate it

Only extensions declared as secretaries will be able to call the application type extension.

Procedure

For the configuration example, extension 300 is the Chief Secretary application. In the following image we will see that inmate 107 has inmate 108 configured as Chief-Secretary

With which inmate 108 can call the application (300) to deactivate and activate the Chief-Secretary

3.3.7.8.2.2 IVR Application Backup Mode

This application allows you to derive all the access numbers from the central to a pre-attendant created for Backup mode

To create the application, in the Configuration section > My applications, we register the application «Set Ivr Backup Application», and fill in the Name and Description

It will then appear in the My Apps list. The audios must be loaded for the application to work, you can customize the audios by clicking on the icon and load according to the function, or click to load the default audios of the application.

When registering the audios, they will appear in the list and the application will be ready to work.

To be able to call the application, it is necessary to create an application type extension and associate it

Procedure

To run the application, in the configuration example the application was associated with extension 301.

Once the pre-server is created, this pre-server is identified with the code (for the following example the code is 7)

When extension 301 is called, the pre-attendant code is requested (in this case 7) and the options of activating or deactivating the backup mode are provided. The first time it is activated, all access numbers are derived for a period of 24 hours. If you try to activate again before 24 hours, it indicates that it is active but the first expiration period of the application is respected.

Once the execution time has finished or the application has been deactivated, the access numbers continue to operate in the time modes of the corresponding pre-attendants.

3.3.7.8.2.3 Remote Dialing Code Application

Among the applications that the central unit brings by default, we find the Remote Dialing code application. This application allows you to take a line and make calls through the Preattendant (IVR). This operation is known in telephony as the DISA function.

To use this application, a hidden option is programmed in the Preattendant. For the following example we see that option 9 is in Application mode and has Remote Dialing code selected. This option is not played on the Preattendant audio.

In the user, the Remote dialing code must be set

When calling the access number of the preattendant and pressing the hidden option, the control panel requests to authenticate the user with his remote dialing code. The central identifies the user and the user's permissions to make calls according to what is authorized.

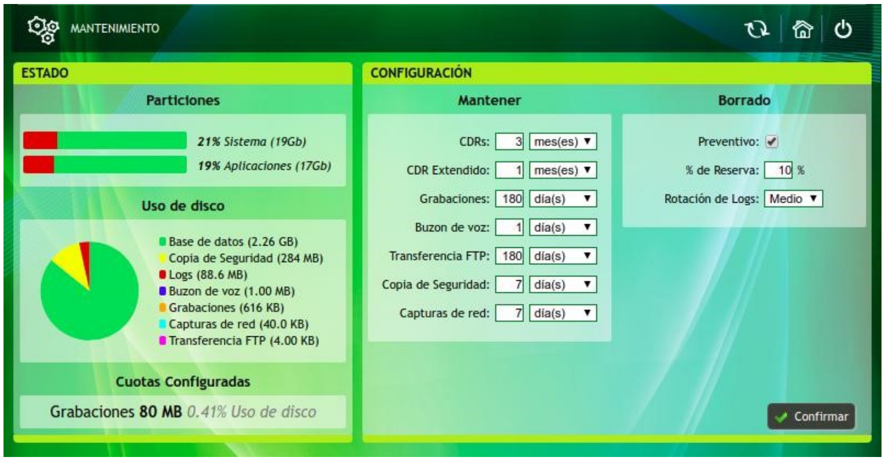
Once the user is identified, the control panel provides a dial tone, allowing the user to make calls as if they were from their extension, that is, being able to call voicemail (*¨33), to another extension, or make outgoing calls using the trunks of the center according to permissions.

3.3.7.8.3 Telephony Interfaces

Denwa version 4.0.1 does not support Telephone Plates. This tab was inherited from Denwa UC&C 4.0.1 3.3.1, which is why it is still enabled.

3.3.7.9 Maintenance

On this page you can see two sectors: Status and Configuration.



21% Sistema (19Gb)
19% Aplicaciones (17Gb)

🟩 Base de datos (2.26 GB)
🟨 Copia de Seguridad (284 MB)
🟥 Logs (88.6 MB)
🟦 Buzon de voz (1.00 MB)
🟧 Grabaciones (616 KB)
🟦 Capturas de red (40.0 KB)
🟪 Transferencia FTP (4.00 KB)

Grabaciones 80 MB 0.41% Uso de disco

CDRs: 3 mes(es)
CDR Extendido: 1 mes(es)
Grabaciones: 180 día(s)
Buzon de voz: 1 día(s)
Transferencia FTP: 180 día(s)
Copia de Seguridad: 7 día(s)
Capturas de red: 7 día(s)

Preventivo: ☑
% de Reserva: 10 %
Rotación de Logs: Medio

Figure 3.147: Maintenance

The left corresponds to the State. It displays information about the use of system partitions, disk usage, and configured quotas.

- **Partitions:** Percentage of system partition usage.
- **Disk Usage:** This section displays a pie chart that shows a quick and easy to understand disk usage. In addition, a more detailed list is presented:
  - **Database**: Refers to the disk space occupied by the information in the database.
  - **Backup:** Allows you to check the space that has been used by the data backup.
  - **Logs:** Refers to the disk space occupied by the platform logs.
  - **Voicemail:** Lets you check how much space voicemails take up on disk.
  - **Recordings:** Refers to the space occupied by telephone recordings.

  - **Network Captures:** Refers to the space occupied by network packet captures.
  - **FTP Transfer:** It refers to the directory where the files pending transfer to the external FTP server are stored.

disk usage graph

The graph summarizes the information across all available storage devices, without discriminating by partition or disk

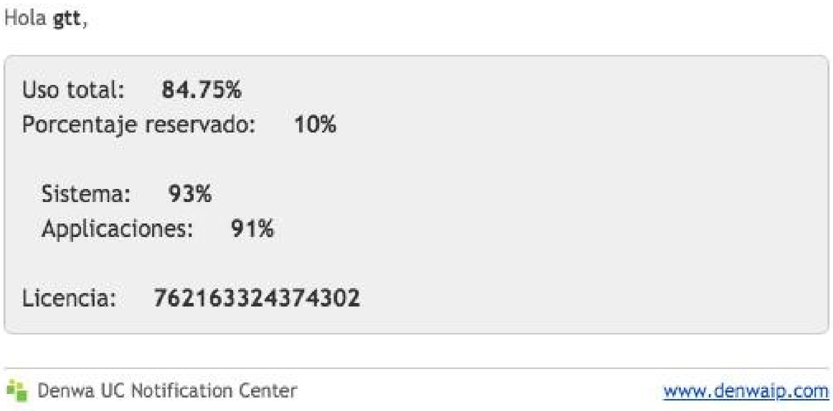
- **Configured Quotas:** is the sum of recording quotas configured for Users, Groups, Trunks, etc. The information is also contrasted with the available space.

The sector on the right corresponds to Settings and is divided into two sections: Keep: In this section you configure the time for which the data will be stored.

- **CDR's:** Refers to call records.
- **CDR's Extended:** Refers to extended call records.
- **Recordings:** It refers to the recordings of the calls.
- **Voicemail:** Refers to the messages stored in the voicemail.
- **FTP Transfer:** refers to the directory where files pending transfer to external FTP are stored.
- **Backup:** Corresponds to the configuration backup files.
- **Network Traps:** capture files (.cap).
- **Delete:** This section allows you to enable the automatic deletion of files when the percentage of disk usage in any of the partitions exceeds the configured disk reserve percentage.
- **Preventive:** enable preventive wipe.
- **% Reserve:** percentage that must remain free.
- **Log Rotation:** mode of deletion of log files, corresponds to the duration of the logs in the system, and accepted size:
  - **Strong:** retains the last 2 days of logs when it is at the threshold corresponding to % Reserve.
  - **Medium:** keeps the last 4 days of logs when it is at the threshold corresponding to % Reserve.
  - **Smooth:** retains the last 6 days of logs when it is at the threshold corresponding to % Reserve.

In the event that the occupancy of Disks reaches 70%, Denwa UC sends one (1) alert per day to the emails of the Administrators. In case the disk usage exceeds 90%, it sends one (1) every hour.

The notification that arrives by mail contains a percentage of the total use of the Disk, and of the partitions together with the license of the center from which the Alert is issued.



Hola **gtt**,

Uso total: **84.75%**
Porcentaje reservado: **10%**

Sistema: **93%**
Applicaciones: **91%**

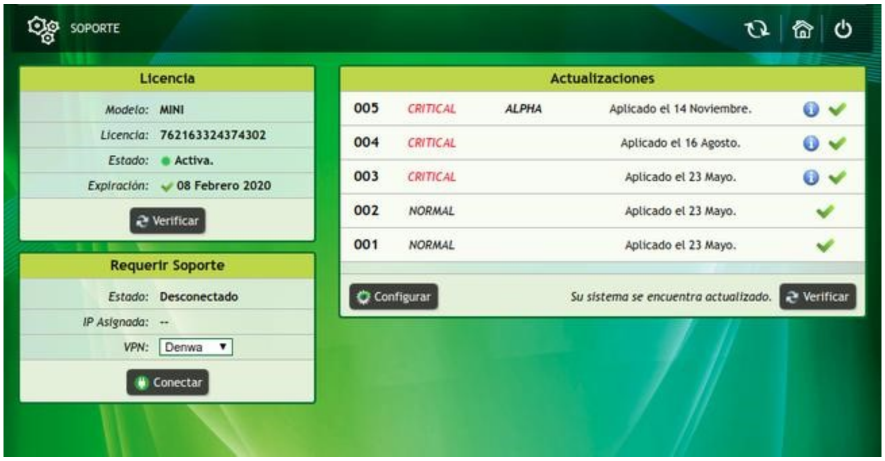
Licencia: **762163324374302**

Denwa UC Notification Center — www.denwaip.com

Figure 3.148: Email alert for partition occupation

3.3.7.10 Support

From this menu, you can request remote support and manage updates to the Denwa PBX.



Licencia

Modelo: MINI
Licencia: 762163324374302
Estado: ● Activa.
Expiración: ✓ 08 Febrero 2020

Requerir Soporte

Estado: Desconectado
IP Asignada: --
VPN: Denwa ▼

Actualizaciones

005	CRITICAL	ALPHA	Aplicado el 14 Noviembre.	✓
004	CRITICAL		Aplicado el 16 Agosto.	✓
003	CRITICAL		Aplicado el 23 Mayo.	✓
002	NORMAL		Aplicado el 23 Mayo.	✓
001	NORMAL		Aplicado el 23 Mayo.	✓

Su sistema se encuentra actualizado.

Figure 3.149: Support

3.3.7.10.1 License

In this section you can view our license and support status, along with the expiration date.

3.3.7.10.2 Require Support

this option allows you to connect the Denwa UC&C 4.0.1 to the secure technical support network for troubleshooting, taking screenshots or configuring the control panel. The Status field shows us if you are connected to support or not, and the IP Address field shows the IP delivered by Denwa's secure support network.

If you require first-level support, you can choose to connect the control panel to the Distributor's support, where a prompt response is provided to the most frequent queries, generally associated with configurations of the control panel or the network associated with it. Below is a list of the available VPNs and their relationship with the different distributors:

- **Denwa**: VPN by default, delivers IP addresses on the 192.168.155.0/24 network
- **VPN 001**: VPN for Basilvox (Brazil) and Telssa (Nicaragua), delivers IP addresses on the 192.168.202.0/24 network
- **VPN 002**: VPN for Calltech (Colombia), delivers IP addresses on the 192.168.206.0/24 network
- **VPN 003**: VPN for Portenntum (Mexico), delivers IP addresses on the 192.168.207.0/24 network
- **VPN 004**: VPN for Provetel (Argentina), delivers IP addresses in the 192.168.204.0/24 network
- **VPN 005**: VPN for Sistek (Chile) and ProNet (Panama), delivers IP addresses in the 192.168.208.0/24 network
- **VPN 006**: VPN for Sumtec (Peru), delivers IP addresses on the 192.168.205.0/24 network
- **VPN 007**: VPN for Telered (Ecuador), delivers IP addresses on the 192.168.203.0/24 network
- **VPN 008**: VPN for SignalSoft (Chile) and Ericnet (Argentina), delivers IP addresses on the 192.168.197.0/24 network
- **VPN 009**: VPN for Retracom (Bolivia), delivers IP addresses on the 192.168.198.0/24 network
- **VPN 010**: VPN for Technology Bureau (Argentina), delivers IP addresses in the 192.168.199.0/24 network

Access to support The fact that the equipment can connect to any of the Support VPNs does not imply that it has a current service contract either by the Integrators, Distributors or the Factory.

3.3.7.10.3 PBX Updates allows you to enable the option to Apply updates automatically, these are done at 07:00 UTC. By disabling this option, the administrator can perform updates manually when required.

The code of the last applied update in Denwa UC&C 4.0.1 is also shown.

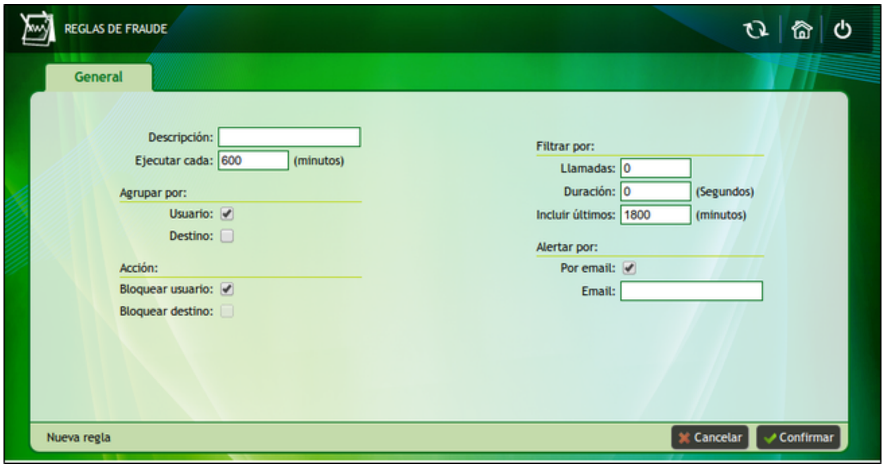
3.3.7.11 Fraud Control

This section analyzes one of the most important aspects regarding the security of the Denwa Unified Communications Center.

Fraud control is used to prevent misuse of the PBX due to abuse of calls from an extension.

With fraud control, limits can be established according to the use of inmates, in which possible abuses are automatically limited; At the same time, DoS attacks (*«Denial of Service»*, in Spanish «Denial of Service») are avoided on digital trunks, by automatically rejecting incoming calls from certain prefixes.

All this is established through rules.



Descripción:
Ejecutar cada: 600 (minutos)

Agrupar por:
Usuario: ☑
Destino: ☐

Acción:
Bloquear usuario: ☑
Bloquear destino: ☐

Filtrar por:
Llamadas: 0
Duración: 0 (Segundos)
Incluir últimos: 1800 (minutos)

Alertar por:
Por email: ☑
Email:

Figure 3.150: Fraud Control, new rule

3.3.7.11.1 New Rule The parameters for the creation of the new rules are detailed below.

- Description: name assigned to the rule. For example, «Control 1».
- Execute every: time in which it is evaluated if any of the stipulated rules are fulfilled.
- Group By
  - User: When creating the rules that will block the calls, they can be applied to the internals of the users.
  - Destination: when creating the rules that will block the calls, they can be applied to the destinations.
- Action
  - Block user: if the rule is met, the fraud control is executed, placing the user in Suspended mode (can receive but not make calls).
  - Block destination: if the rule is met, fraud control is executed, blocking calls to said destinations.
- Filter by
  - Calls: number of calls to be made in the monitored time interval.
  - Duration: duration of calls in the monitored time interval.
  - Include last: although it is determined how often the control rules are to be evaluated, this parameter specifies how far back it is taken into account.
- Alert
  - By email: activate or deactivate the notification function via email
  - Email: email address to which notifications arrive each time fraud control executes a block.

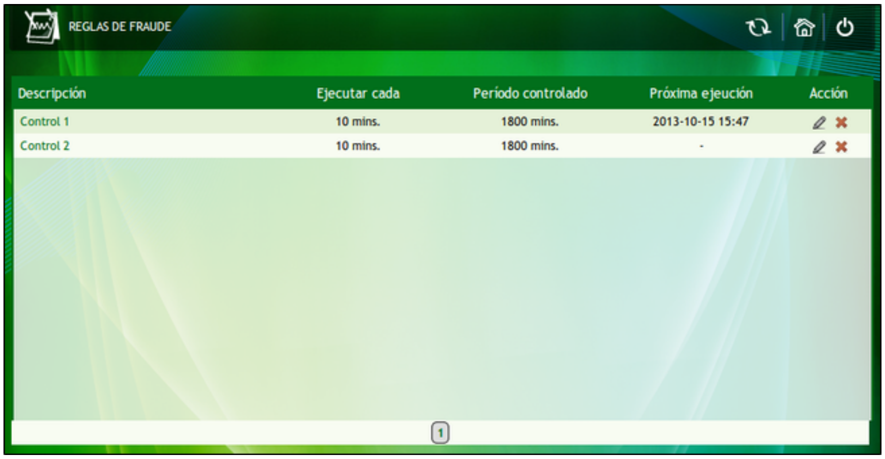
Simply click on the «✔ Confirm» button to save the new rule, or on «✖ Cancel» to reject the configuration made and return to the previous screen.

Execution conditions

In order for a fraud control block to be executed, both rules, by calls and by duration, must be fulfilled at the same time, that is, that the number of calls is exceeded in the configured time and that the sum of the duration of these exceeds the maximum duration time.

3.3.7.11.2 Fraud Rules

In this section, the created rules are observed, and the moment in which said rules will be executed again.

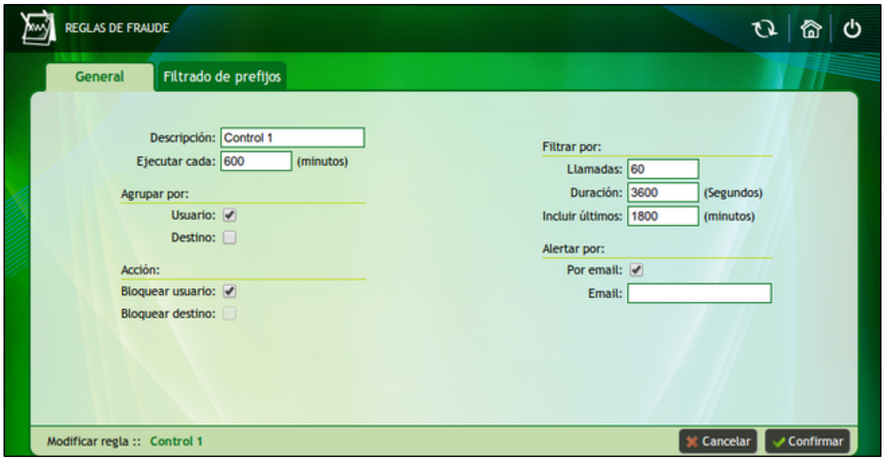


Descripción	Ejecutar cada	Periodo controlado	Próxima ejeución	Acción
Control 1	10 mins.	1800 mins.	2013-10-15 15:47	✎ ✖
Control 2	10 mins.	1800 mins.	-	✎ ✖

Figure 3.151: Fraud Control, fraud rules created

These rules are displayed in list form. The Action column of this tab provides the possibility to edit the rule by clicking on «✎», or delete it by clicking on the «✖» icon.

When you want to edit the rule and click on the corresponding icon, a new window with two tabs appears. The first of these is the general configuration of the rule (see New Rule on page 143) and the second presents the blocked prefixes (see Incoming Prefixes Blocked on page 144).



Descripción: Control 1
Ejecutar cada: 600 (minutos)

Agrupar por:
Usuario: ☑
Destino: □

Acción:
Bloquear usuario: ☑
Bloquear destino: □

Filtrar por:
Llamadas: 60
Duración: 3600 (Segundos)
Incluir últimos: 1800 (minutos)

Alertar por:
Por email: ☑
Email:

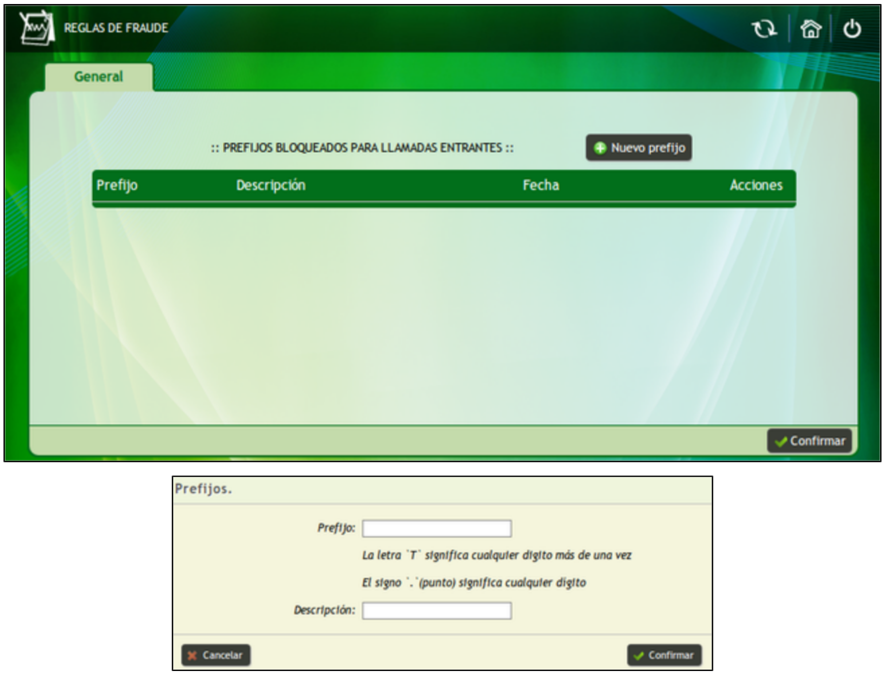
Modificar regla :: Control 1

Figure 3.152: Fraud Control, editing the previously created fraud rule

To finish, click on «✓ Confirm» and the changes are saved.

3.3.7.11.3 Incoming Prefixes Blocked

Another feature of Denwa is the blocking of prefix calls from specific addresses. This is useful to avoid a DDoS attack and in the case of trunks to the Denwa UC&C 4.0.1 , to prevent calls from being issued from those trunks.



:: PREFIJOS BLOQUEADOS PARA LLAMADAS ENTRANTES ::

Prefijo	Descripción	Fecha	Acciones

Prefijos.

Prefijo:

La letra `T` significa cualquier digito más de una vez

El signo `.`(punto) significa cualquier digito

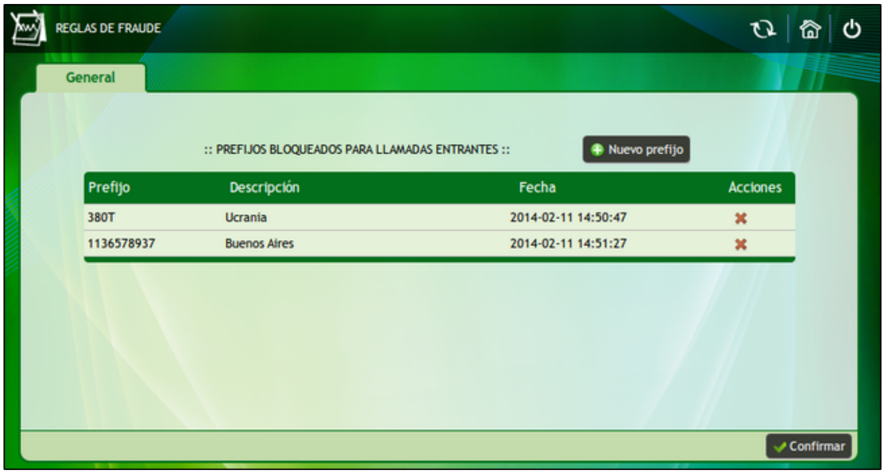
Descripción:

Figure 3.153: Fraud Control, prefixes blocked for incoming calls

In this section the incoming prefix blocking rules are observed, and it is allowed to create new rules with a click on .

- Prefix: you can enter the first digits to be blocked, followed by any of the following characters:
  - «.» indicates a single (1) digit, can be repeated as many times as necessary
  - «T» implies an indeterminate number of digits
- Description: A reference (naming) is added for this rule.

The following image shows two examples of blocking incoming prefixes.



:: PREFIJOS BLOQUEADOS PARA LLAMADAS ENTRANTES ::

Prefijo	Descripción	Fecha	Acciones
380T	Ucrania	2014-02-11 14:50:47	✖
1136578937	Buenos Aires	2014-02-11 14:51:27	✖

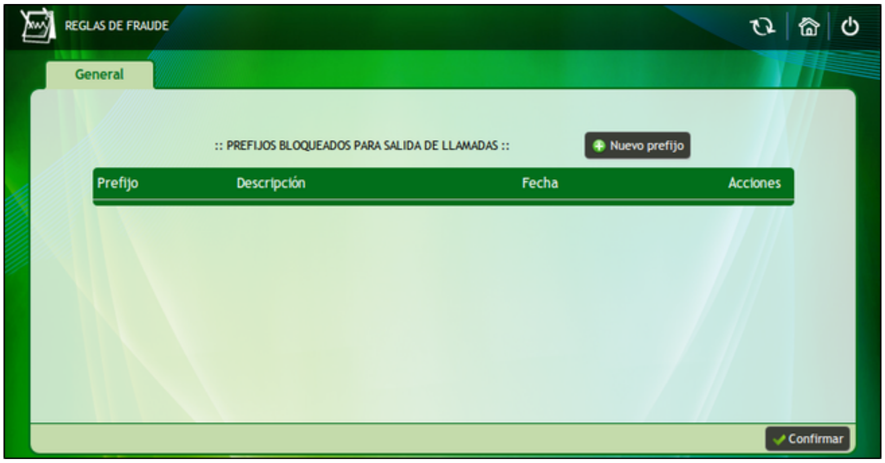
Figure 3.154: Fraud Control, example of blocked incoming prefixes

In the first item, any number starting with 380 is blocked, in the second item calls from the number 1136578937 are blocked.
To delete any of the created rules, press «✖».

3.3.7.11.4 Blocked Destinations

To see and create blocking of outgoing calls, it is done from Blocked Destinations

Destinations that comply with fraud control and are blocked can be seen in this section. In addition, locks can be added by clicking «⊕ New Prefix».

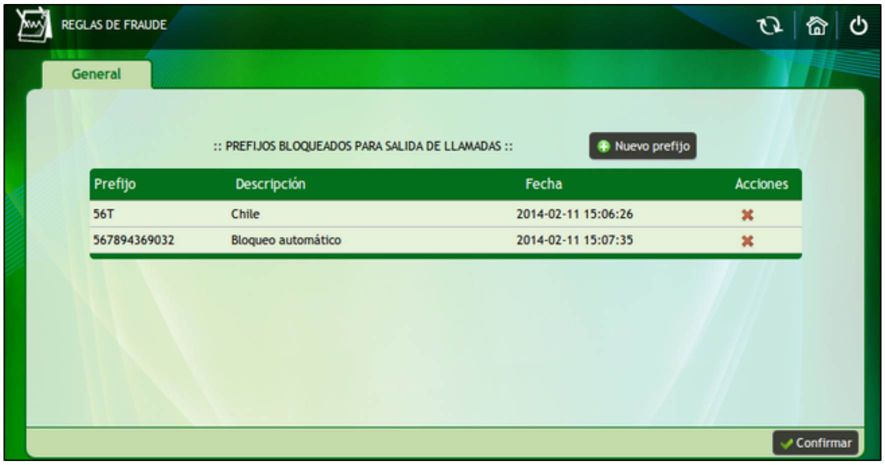


Prefijo	Descripción	Fecha	Acciones

Figure 3.155: Fraud Control, prefixes blocked for outgoing calls

- Prefix: you can enter the first digits to be blocked, followed by T (which means any digit or digits).
- Description: A reference (naming) is added for this rule.

Two examples are shown below.



Prefijo	Descripción	Fecha	Acciones
56T	Chile	2014-02-11 15:06:26	✖
567894369032	Bloqueo automático	2014-02-11 15:07:35	✖

Figure 3.156: Fraud Control, example of prefixes blocked for outgoing calls

In the first item, all outgoing calls to Chile are blocked, while in the second item, outgoing calls to the number 567896369032 are blocked.

To delete any of the created rules, click on .

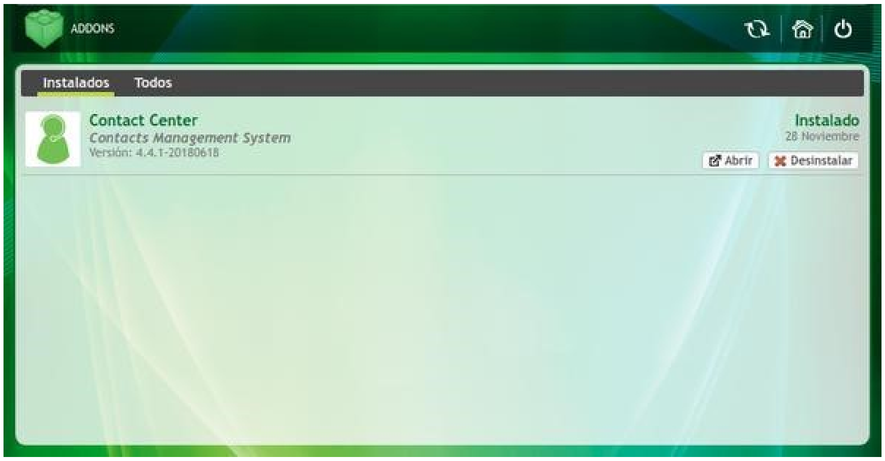
3.3.7.12 Denwa Store

The Denwa Store option allows the incorporation of new applications, called modules for Denwa PBX. These modules are developed according to the needs of the user. Initially you must have a module, and then install it and enjoy its advantages.

It has two tabs: «Installed» and «All»

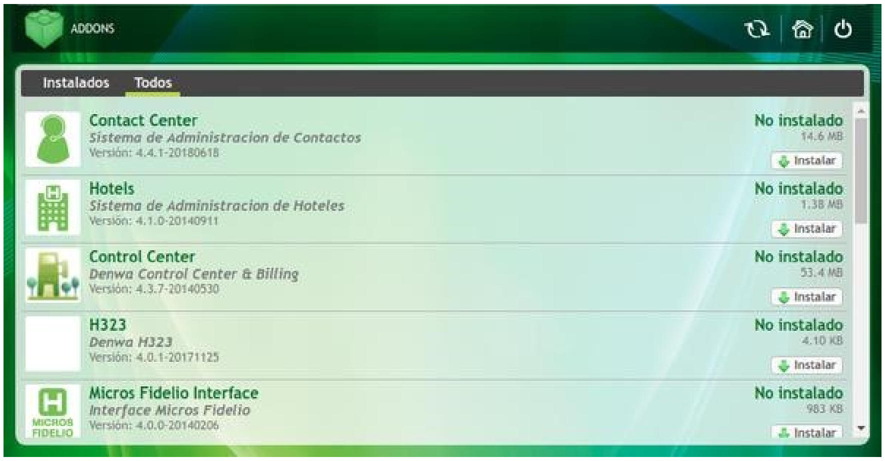
3.3.7.12.1 Installed

In this tab you can see the modules installed for our Denwa PBX. In this case the Contact Center module has been installed.



Contact Center
Contacts Management System
Versión: 4.4.1-20180618
Instalado
28 Noviembre

Figure 3.157: Denwa Store, installed modules



Contact Center
Sistema de Administracion de Contactos
Versión: 4.4.1-20180618
No instalado
14.6 MB

Hotels
Sistema de Administracion de Hoteles
Versión: 4.1.0-20140911
No instalado
1.38 MB

Control Center
Denwa Control Center & Billing
Versión: 4.3.7-20140530
No instalado
53.4 MB

H323
Denwa H323
Versión: 4.0.1-20171125
No instalado
4.10 KB

Micros Fidelio Interface
Interface Micros Fidelio
Versión: 4.0.0-20140206
No instalado
983 KB

Figure 3.158: Denwa Store, all modules

3.3.7.12.2 All

The list in the previous figure shows the information in two columns. In the first, the available modules are displayed, with a brief description and corresponding version. Among the existing modules are the following:

- **Control Center**: is a utility that allows monitoring, cost allocation and billing of calls in a Denwa PBX or in a group of them.
- **Contact Center**: this module is oriented as a tool for Call Centers. Generally, it is used for inbound and outbound calling campaigns.
- **H323** – Grants the ability to configure a provider using the H323 protocol.

- **High Availability**: this application allows a Denwa PBX to function as a backup for another Denwa PBX; that is why the data is updated between them. Participating Denwa PBXs need to be of the same model. When installing this module in the control panels, one must be configured in master mode and the other in slave mode.

- **Hotels**: this module facilitates hotel management procedures. Because it assigns each room an extension, this allows you to generate a quick report on the status of the rooms and a detailed report for each one of them. The detail of the calls is delivered to the central via Telnet, which makes it possible to be in real time. In other words, interaction with the billing system or PMS (Property Management System) is allowed online; which brings dynamism.

- **Denwa Audits**: it is a functionality that allows the monitoring of Denwa UC&C 4.0.1 , you can obtain information corresponding to the latest activities and statistics. The last activities are shown in three columns, the first shows the date and time in which the activity took place, the second verifies the user who performed it, and the third column shows which of the options in the menu provided by Denwa UC&C 4.0.1 some action is executed. Statistics provide a summary of activities for the day, the last ten days, and the last month. This module requires a control panel updated to version 84.

- **UPS Management**: Allows you to monitor and manage the UPS. The main functionality of this module lies in the possibility of executing various actions according to a certain condition. Several UPSs can be monitored with this module and to obtain information about their status, every 30 seconds it performs a check. Which is done through SNMP, pinging and pertinent queries to obtain information on voltage status, power outages, battery capacity, estimated remaining battery time, among others.

- **LDAP**: allows the authentication of operators with the LDAP system (Active Directory) allowing access with all permissions enabled.

Installing modules

Module installation is only possible on a computer whose license has a current support plan for Denwa Technology Corp. . Check with your implementer for the status and support level of your license.

In the second column, it is possible to corroborate the installation status with its respective characteristics:

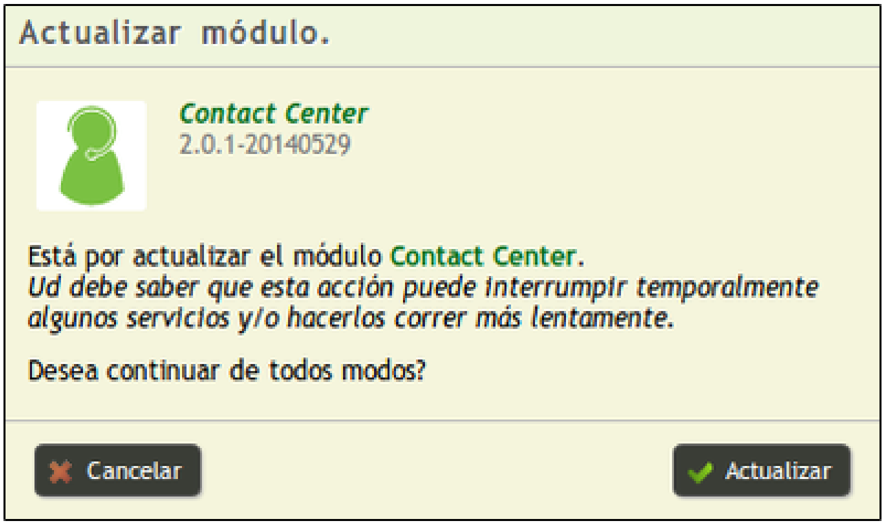
- Not installed, module size and option to install it.

- Installed and not updated, date of last installation and the options open, update and uninstall.

- Installed, installation date, and the open and uninstall options.

You can also update the modules from this tab, from the «✔ Update» button.

When you click Update, a new window appears, in it you must click the «✔ Update» button to continue with the process, or «✖ Cancel» to cancel it.



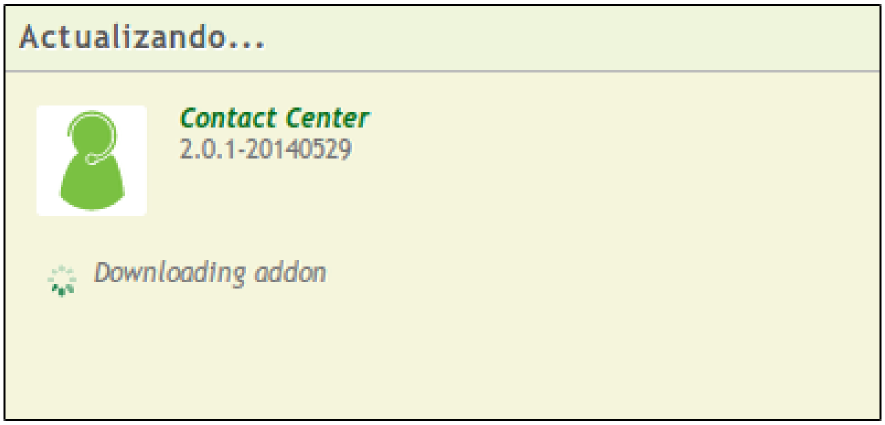
Actualizar módulo.

Contact Center
2.0.1-20140529

Está por actualizar el módulo Contact Center.
Ud debe saber que esta acción puede interrumpir temporalmente algunos servicios y/o hacerlos correr más lentamente.

Desea continuar de todos modos?

Figure 3.159: Denwa Store, module update window



Actualizando...

Contact Center
2.0.1-20140529

Downloading addon

Figure 3.160: Denwa Store, module being updated

Module Update Since the release of a module can be due both to adding new features, as well as to fixing bugs, the automatic process that is executed internally during the update consists of five steps:

1. Update package download
2. Creation of a backup copy of the information contained in the module to be updated
3. Uninstalling the current version of the module
4. Installing the updated version of the module
5. Restoring the information contained in the backup made in step 2

!

3.3.7.13 Licenses

In this interface you can manage the license of the Desktop Web Phone provided by Denwa UC for free and request Simultaneous SBC Premium sections.

The first of the licenses is loaded only once and is used for the Desktop phone of all users associated with the Denwa UC in question; while the second indicates the number of SBC sections enabled, the Denwa UC Premium includes 12 built-in sections, but it is possible to add packages of 5 sections.

The image above shows the information contained in columns. Among which are description, status, enablement and expiration (they show the respective dates).

- **Description**: Brief description of the application.
- **Status**: Allows you to see if the license is enabled and the number of sections available.
- **Enabling**: Shows the date on which the license is enabled.
- **Expiration**: Currently it does not have a valid function, since the licenses of «IP Phone for WEB» are granted free of charge by Denwa Technology Corp. , while the additional ones for the SBC sessions of the Denwa Premium team are associated with the number equipment serial.
- **Action**: There are three options:
  - ✉: this button is used to request a license. For web licenses, the process involves sending an email to the Denwa staff, then receiving the response with the corresponding file. For SBC sections it is necessary to load the code of the purchased package in the following window.
    Licenses requested are not transferable. This means that once You require SBC Licenses, they are activated only for this device and it will not be possible to use them on another. Once the licenses have been activated (through this requirement) it is not possible to reverse the process. The activation process can take around 3-5 business days.
  - 🔑– Clicking this icon should load the file that was obtained from the license request
  - ℹ: SBC licenses currently loaded on Denwa UC Premium are displayed.

Considerations for license application

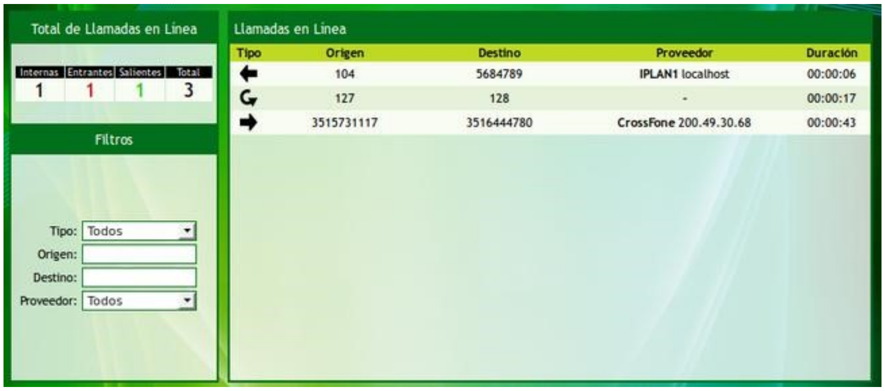
1. The reply email with the license information is received at the email address declared in **Settings > General > Tab: Basic**
2. It is necessary to have an Internet connection
3. Static IP configuration should be considered

3.3.8 Debug

This section presents a very powerful tool that is capable of showing in detail the packets that participate in each communication. Which allows finding outages or important failures that affect the service in some way.

3.3.8.1 Call Monitor

This section presents the events in real time that occur in the control panel. The window that is observed is the one in the following image.



Total de Llamadas en Linea

Internas	Entrantes	Salientes	Total
1	1	1	3

Filtros

Tipo: Todos
Origen:
Destino:
Proveedor: Todos

Llamadas en Linea

Tipo	Origen	Destino	Proveedor	Duración
←	104	5684789	IPLAN1 localhost	00:00:06
↻	127	128	-	00:00:17
→	3515731117	3516444780	CrossFone 200.49.30.68	00:00:43

Figure 3.162: Debug, monitor calls

3.3.8.1.1 Total Online Calls

This section displays both the number of internal, external and outgoing calls in real time, as well as the sum of them.

3.3.8.1.2 Filters

A variety of conditions are presented; when applying them, only those that comply with them are allowed to be displayed. By default, it shows all calls from all providers.

- **Type**: you have the possibility to observe all the calls, using the option All; You can also see only the internal, external or salient ones.
- **Origin**: supports filtering based on the number that initiates the call.
- **Destination**: Allows you to select the number that receives the call as the filter pattern.
- **Provider**: in this case the possibility of choosing a provider to see your calls online is provided.

3.3.8.1.3 Online Calls

Only those calls that are occurring in real time are displayed, under the previously selected filtering conditions.

- **Type**: This information is provided through the use of icons:
  - ←: incoming call.
  - ↻: call between internals.
  - →: outgoing call.
- **Origin**: shows the number of the person making the call.
- **Destination**: allows you to see the receiving number of the call in question.
- **Provider**: enables the option to view through which exchange provider the call is made, if necessary.
- **Duration**: reveals the duration of the call, which does not imply that it has been answered; because ring time is included in this period.

3.3.8.2 Signaling Monitor

This section allows you to view the events that occur within the Denwa UC&C 4.0.1 telephony engine. It has multiple buttons and filters.

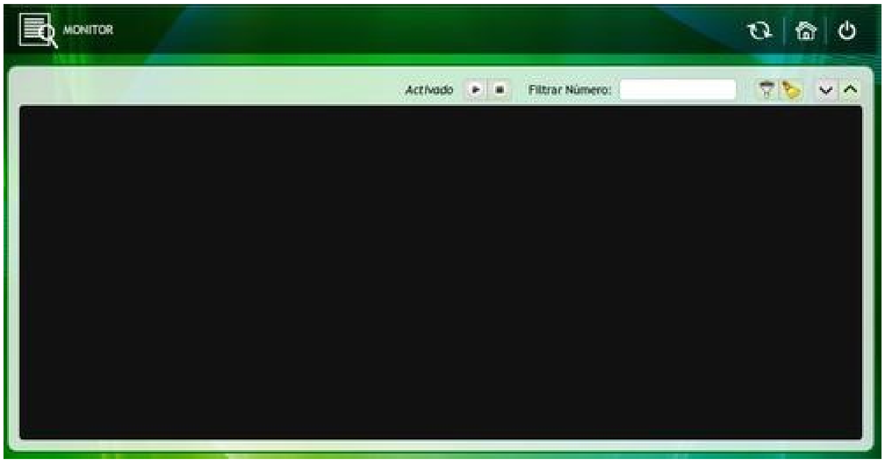
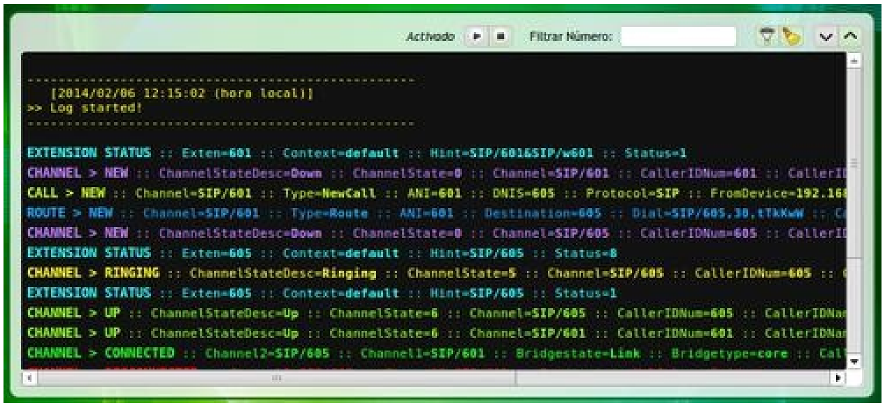


Figure 3.163: Debug, beacon monitor

- ⦿ ⦾: to start monitoring you must click on the button whose icon is a triangle («*Play*») and to stop it you only need to click on the button that contains a square («*Stop*»).

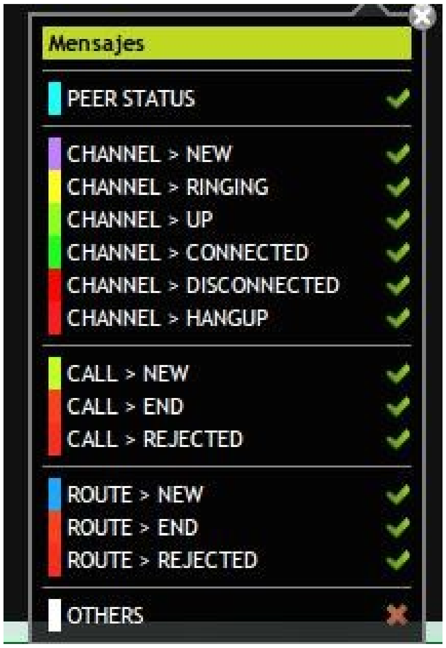


```
------------------------------------------------------------
   [2014/02/06 12:15:02 (hora local)]
>> Log started!
------------------------------------------------------------

EXTENSION STATUS :: Exten=601 :: Context=default :: Hint=SIP/601&SIP/w601 :: Status=1
CHANNEL > NEW :: ChannelStateDesc=Down :: ChannelState=0 :: Channel=SIP/601 :: CallerIDNum=601 :: CallerII
CALL > NEW :: Channel=SIP/601 :: Type=NewCall :: ANI=601 :: DNIS=605 :: Protocol=SIP :: FromDevice=192.168
ROUTE > NEW :: Channel=SIP/601 :: Type=Route :: ANI=601 :: Destination=605 :: Dial=SIP/605,30,tTkKwW :: Ca
CHANNEL > NEW :: ChannelStateDesc=Down :: ChannelState=0 :: Channel=SIP/605 :: CallerIDNum=605 :: CallerII
EXTENSION STATUS :: Exten=605 :: Context=default :: Hint=SIP/605 :: Status=8
CHANNEL > RINGING :: ChannelStateDesc=Ringing :: ChannelState=5 :: Channel=SIP/605 :: CallerIDNum=605 :: C
EXTENSION STATUS :: Exten=605 :: Context=default :: Hint=SIP/605 :: Status=1
CHANNEL > UP :: ChannelStateDesc=Up :: ChannelState=6 :: Channel=SIP/605 :: CallerIDNum=605 :: CallerIDNa
CHANNEL > UP :: ChannelStateDesc=Up :: ChannelState=6 :: Channel=SIP/601 :: CallerIDNum=601 :: CallerIDNa
CHANNEL > CONNECTED :: Channel2=SIP/605 :: Channel1=SIP/601 :: Bridgestate=Link :: Bridgetype=core :: Cal
```

Figure 3.164: Debug, beacon monitor: result of starting the monitor

- **Filter number**: Used to monitor calls from a particular number.

- ▼: it is used to carry out a specific filtering. Clicking on this icon displays a list, which contains the color with which the messages will be displayed and the type of message. Finally, there are the options of the tilde and the cross; that allow or not to capture these messages during the establishment and closing of the call.



Mensajes

PEER STATUS ✓

CHANNEL > NEW ✓
CHANNEL > RINGING ✓
CHANNEL > UP ✓
CHANNEL > CONNECTED ✓
CHANNEL > DISCONNECTED ✓
CHANNEL > HANGUP ✓

CALL > NEW ✓
CALL > END ✓
CALL > REJECTED ✓

ROUTE > NEW ✓
ROUTE > END ✓
ROUTE > REJECTED ✓

OTHERS ✗

Figure 3.165: Debug, beacon monitor: available filters

- **Peer Status**: Provides information on the periodic registration of extensions in Denwa UC&C 4.0.1 .
- **Channel - New**: A channel is established for communication via the specified protocol.
- **Channel - Ringing**: ringing tone at the destination.
- **Channel - Up**: Establishes the link between the originator of the call and Denwa UC&C 4.0.1 .
- **Channel - Connected**: in this case the complete link is established in two sections. The first, spans from the originator of the call to Denwa UC&C 4.0.1 . Instead, the second involves from Denwa UC&C 4.0.1 to the receiving end of the call.
- **Channel - Disconnected**: indicates the end of the connection.
- **Channel - Hangup**: the call is terminated and the channel is released.
- **Call - New**: Signals that Denwa UC&C 4.0.1 internally starts handling the call.
- **Call - End**: shows that the PBX ends the call, as an internal process.
- **Call - Rejected**: this message shows that the call never reaches its destination. So it only uses the link between source and Denwa UC&C 4.0.1 .
- **Route - New**: sets the second link on every call.
- **Route - End**: At the end of the call, the second link ends.
- **Route - Rejected**: in this case only one of the links is used.
- **Others**: shows even more details of the internal processes that the PBX handles to establish and close the call.

- 🖌: clicking on this icon opens the window in the following figure. Which offers the possibility of showing only the last 100, 500, 1000 or 2000 messages, since these options are the ones presented by the drop-down menu. In addition, you can delete all the messages, for which you need to click on «Delete all messages now»

- **⌄⌃**: these buttons are used to maximize and minimize the monitor screen, respectively.

3.3.8.3 Network Tools

In this section you will find the tools for solving problems in networks (troubleshooting), thus allowing a quick and better analysis of the network.

The available tools are: PING, TRACEROUTE, ARP, ETH-TOOL, NSLOOKUP and My-Traceroute.

3.3.8.3.1 Ping Allows a certain number of ICMP queries to be sent to a certain destination, this is used to determine if the DenwaUC can reach this destination.

The results of this function allow us to determine the percentage of packets lost, what is the average time between the query and the response, and the variation of the time between the query and response.

3.3.8.3.2 Traceroute Allows you to send ICMP queries with incremental TTL (starting at 1), to determine the number of hops or hosts a query must traverse to reach the destination.

The results of this function allow to determine if the traffic sent to the destination is sent by the previously determined route.

3.3.8.3.3 ARP The ARP Scan Tool is a very fast ARP packet scanner that displays all active devices on the subnet. Since ARP is not routable, this type of scan only works on the local LAN (local subnet or network segment).

ARP scan tool shows all active devices even if they have firewalls. Devices cannot hide from ARP packets like they can hide from Ping. It can be used with the following parameters:

- **-a**: show information obtained through all network interfaces
- **-i**: display information obtained via a particular interface
- **-n**: display the information in a numerical format

3.3.8.3.4 NSLOOKUP The main use of nslookup is to identify DNS related problems.

3.3.8.3.5 ETH-TOOL Displays configuration information for network interfaces. Being able to be used:

- **no parameters** - displays Ethernet card properties such as speed, wakeup, duplex, and link detection status
- **-i**: display driver version, firmware version, and bus details
- **-S**: show transmit and receive statistics

3.3.8.3.6 My-TraceRoute This tool is a mix of two (2) mentioned above: Ping and TraceRoute. uses:

- checkbox for each of the possible fields to display in the output (-o LDRSNBAWVGJMXI), according to the following list:
  - L Loss ratio
  - D Dropped packets

    - R Received packets
    - S Sent Packets
    - N Newest RTT(ms)
    - B Min/Best RTT(ms)
    - A Average RTT(ms)
    - W Max/Worst RTT(ms)
    - V Standard Deviation
    - G Geometric Mean
    - J Current Jitter
    - M Jitter Mean/Avg.
    - X Worst Jitter
    - I Interarrival Jitter
  - text field for IPs or domain names
  - checkbox to show only the IP of the jump (-n)
  - checkbox to show the IP and domain name of the jump (-b)
  - integer field for the number of packets to send (-c)
  - integer field for maximum hops (-m)
  - integer field for the time interval between each packet sending (-i)
  - integer field for the destination port to query (-P)
  - integer field for source port (-L)
  - integer field for packet size (-s)
  - checkbox to select if you want the report to be exportable (-r) and enable the text field to place the name of the file to be exported. If this option is selected, the generated reports will be listed in the table located at the bottom of the screen

3.3.8.4 Digital Line Monitor

Denwa version 4.0.1 does not support Telephone Plates. This tab was inherited from Denwa UC&C 4.0.1 3.3.1, which is why it is still enabled.

3.3.8.5 Packet Capture

This option allows capturing network frames by using a sniffer. This tool provides very detailed and ordered information. It has three (3) boxes that are described below:

1. **SNIFFER: : New capture**: here you must select the conditions under which the capture is performed.
    - **Cap Name**: here the name of the file to be generated is indicated.
    - **Interface**: refers to the interface on which you want to perform the packet capture.
    - **Min Packet Size**: assigns the minimum size of the packets to be captured. It is recommended to use the default value (1500).
    - **Maximum Duration**: in the event that the capture is not finished manually, once this time period expires it ends automatically.
    - **Services**: you can choose all (ALL) or select only those protocols you want to capture.
    - **▶■**: These buttons start and end the capture, respectively.
2. **Captures**: in this section you can view the captures made.

   - **Cap Name**: refers to the name with which the capture was saved.
   - **Captured services**: allows you to see which services were captured.
   - **Iface**: This column shows the interfaces on which the capture was executed.
   - **Date Time**: indicates the data at the time the capture began.
   - **Size**: displays the size of the file (KB).
   - **Action**: This column presents three options.
     - ✂: with this icon it is possible to activate the advanced filter option, which appears at the bottom.
     - ⤓: it is possible to use this icon to export the file, to later open it using the sniffer.
     - ✖: This alternative provides the option to delete the captured capture.

3. **Advanced Filter**: allows you to simplify the analysis, since it allows you to limit the capture.
   - **Split Capture**:
     - **Divide by**: this option makes it possible to divide the capture, through a drop-down menu that supports division by packets and by time.
     - **Packages**: Striping the file based on the number of files it contains is supported.
   - **Advanced Filter**: from the existing capture file, it allows to generate new files that contain only the data that is going to be filtered again. The great advantage of this possibility is that the files are considerably smaller in size.
     - **Cap name**: Here you must select the name of the new capture file.
     - **Filter**: clicking on create opens a window like the following, which allows you to establish specific conditions on the new filter rule. You can choose a protocol or expression from the drop down menu. Also, the possibility of configuring rules is provided. Clicking on Add and then Confirm is required to apply the filter in question.

CHAPTER 4

USER INTERFACE

4.1 Monitoring Dashboard

4.2 Introduction

Denwa Desktop is the new portal for user management in the Denwa Unified Communications and Collaboration platform. It is aimed at improving the user experience in Unified Communications, it provides a web interface with great visual appeal that unifies all the resources under the same environment, from where the user can control all the services in real time with just a simple click. .

Designed with the robustness and simplicity that characterize our products, it provides a «user-friendly» scenario to interact with the different communication services that surround us, among which are:

- Instant Messaging
- Presence
- Telephony
- Video conference
- Voice Mail
- Private social network
- Application Launcher
- Fax and SMS (sending and receiving)
- Collaboration

In addition to these services, there are other functionalities that will allow you to take full advantage of the integration benefits, such as:

- Favorites
- Contact management
- Phone Finder
- Call log
- Agenda
- Calendar

Additionally, Denwa Desktop can be accessed from a mobile, tablet or laptop from anywhere in the world in the same way as when you are inside your office.

4.3 Requirements

In order to run Denwa Desktop, we need to meet the following requirements.

- Browser (minimum version):
  - Internet Explorer 9
  - Opera 10
  - Mozilla Firefox 31 Apple Safari 5
  - Google Chrome 35
- Operating system:
  WindowsLinux Mac OS
- Ports:
  - INTERNET EXPLORER >9: UDP 5060, UDP 10000-20000
  - MOZILLA FIREFOX >31: TCP 10060, TCP 10062, UDP 10000-20000
  - GOOGLE CHROME >35: TCP 10060, TCP 10062, UDP 10000-20000

4.4 Access

To access the Desktop system, we must enter the IP address of the unified communications center (`http://IP_Denwa`) through the web browser.

Once this link is accessed, you must enter the UC username and password and click on «Login session». This will display a screen similar to the one shown below.

4.4.1 Elements

In the upper right corner of the screen we can see the icons of:

- Shortcuts (see ⊕Add Launcher, page 158)
- Notifications
- Date and time
- Configuration
- Exit

When there is a new notification, a white number on a red background will appear on the corresponding icon alerting about the new notification. The icons are as follows.

4.4.1.1 ⊕Add Launcher

We can add a launcher or a shortcut to the Desktop, that is, a link to a specific web page. To do this, it is necessary to click on ⊕, enter the URL and a description, press the ⊞sign; If you want to remove any launcher, you must click on the ⊟icon.

The launchers will be presented next to the notification icons, in order to have faster access to the pages most visited by the user. In the following image we can see a launcher to www.denwaip.com and www.google.com.

4.4.1.2 🗺 Social Map

By clicking on this icon, we can enter the map to see the locations of our contacts, as can be seen in the following image. By clicking on each user we will see a text with its location.

4.4.1.3 👥Groups

Missing information Information is missing

4.4.1.4 ✉Messages

This icon notifies how many new messages there are. Among these messages we can find voicemails or offline messages.

In case of offline message, it will be displayed as below.

4.4.1.5 ☎Telephone

By clicking on the phone icon (☎), it is possible to access the webphone.

WebRTC Requirements For the proper functioning of WebRTC, as well as the webphone, it is necessary for Denwa UC&C 4.0.1 to have the HTTPS protocol enabled (see «Web Server» on the 111 page).

To start the session, click on the arrow located at the end of the box. From here it is possible to receive and make calls.

When receiving a call, the phone will start blinking on the top bar. By clicking on this icon, a new window is displayed from which you can answer or reject the call.

To make calls we must write the destination number and then press on the phone.

It is also possible to make call transfers, conference calls and the option to enable the keyboard.

Calls in transfer: To do this, when the call is in progress, you must press on . This displays a new section at the bottom. There we must enter the destination number to which the call will be transferred and press on

Conference calls: you must click on the icon, in this way the destination is sent to the conference room.

Then the screen to make a new call is enabled. When it is answered, we click on the same icon and we send the destination to the conference room. The number of participants in a conference room will depend on the number of simultaneous calls that the central can make, that is, it is determined by the PBX model. Finally, to join the conference you must click on the following image.

Keyboard option: the icon displays the keyboard in the left sector of the screen.

INTERNET EXPLORER browser > 9 On the Internet it is possible to choose between two Webphones, by default we have Webphone Webrtc or change to the Webphone with video.

In order to use the webphone we must follow the following steps:

1. As an administrator in Configuration>Licenses, request a license, the response will arrive at the email configured in General Configuration.
2. When obtaining the license, as an administrator we load the license in Configuration>Licenses.
3. We enter the Desktop as a user and access the configuration, in the third tab ”Telephone” we remove the tick in the checkbox that says ”Use New WebPhone”.
4. We must refresh the page to load the new webphone, click on ”Exit this page”.
5. When loading the Desktop again, instructions will appear to install the necessary plugin to finish the installation.

If we click on the phone, we will access the webphone. To start the session we must press the Connect button. Then, every time we click on the corresponding icon, the phone window will appear. To use the webphone you must request its activation from the Configuration / Licenses menu in the administrator environment.

By default, the keyboard is hidden, but we can easily display it. From here we can make and receive calls. To transfer a call, we must click on the icon and then enter the extension using the numeric keypad, followed by the # key. We can also activate the function (Do Not Disturb).

If you receive a call, a notice will appear in the notification area. We can answer or reject it with a click of the mouse, or answer from our physical extension if it is properly configured.

If we are using the Microsoft Windows operating system, in addition to the functionalities detailed above, we will have the possibility of opting for video calls and conferences. We will find that the Denwa WebPhone presents the following aspect.

To make a video call, we just have to click on , mark and press the button.

To make a video conference we repeat the procedure for a video call, but on several lines, with the possibility of up to four lines. Once the desired calls have been established, we must press the Conference button. We can also put a call on hold with the button.

To mute the microphone, we must click on , to block the sending of video, and to control the volume of the call.

When establishing a video call we can see the following image.

4.4.1.6 Instant Messaging

Presents a notice when a new instant message arrives. Clicking on the notification icon will open the messaging window, where we can see the new message, and communicate in real time with the user who sent it.

Below the user's name, we can see his personal message, and three icons. One shows the user's status (connected, busy, absent or disconnected), the next one allows you to make a direct call from the softphone or the physical IP phone according to how it is configured, and finally the camera icon allows you to make a video call, as shown in the following image (GOOGLE CHROME Browser>35 AND MOZILLA FIREFOX >31). In the lower bar of the messaging window, we can find the tab indicator of each user with whom we are communicating, and switch between the messengers with a single mouse click.

Screen Sharing Introduction Screen Sharing is another function associated with the desktop (such as call and video chat) that provides an advanced interaction between two users, offering, in addition to a video call, the possibility of sharing your work desktop where you can see in real time the operations performed by the user. Since this feature is built into the desktop, no installer is needed and it runs under any operating system with Google Chorme browser (version 28.0 onwards) under https.

NOTE: If your PBX uses http, the Screen Sharing icon will not appear on the desktop

Previous steps To run this function we simply need to be connected to our user on the desktop. The first thing that appears to us is a message like the following, in which it indicates the steps we must take to enable the necessary permissions from Google Chrome.

When entering the Google Chorme configuration page, we add the extension. Then the browser must be restarted to take the configuration.

Start up For the user who receives the Screen Sharing, there will be a request for a video call,

When you accept, the following will appear:

The user who wants to share the desktop when clicking on the icon will be able to select the window to share.

Once the window is selected, the button will be enabled and will be observed as follows by both users.

This feature is very useful for how-tos, showing settings, sharing information, etc.

IM Contacts Notify when we receive a request for a new instant messaging contact. To accept the request, we must click on the icon and then allow.

4.4.1.7 ⚙Configuration

From here we can access the profile edition. We can see that we have three tabs, General, IM and Phone, Notifications and Google Sync.

4.4.1.7.1 Personal Data In the first we will find the following personal data fields.

- Name
- Last Name
- Birthday
- Email
- Country
- State/Province
- City
- Address
- ZIP Code
- Company
- Department
- Position
- Desktop User (username to access the Desktop from the web browser)
- Key Desktop
- Confirm Password
- Language

4.4.1.7.2 IM In the IM tab we find

- Automatic Login: If we enable it, we will access the Desktop with the messaging session started
- Status: Determines the status of the automatic login. Online, Away and Busy
- Notifications for new messages. Only for Google Chrome
  - With IM Window Closed: Defines the method of notifying a new conversation when the IM window is closed. The options to select are Sound, External Popups, Sound + External Popups, or None. Supported in Chrome
  - First Message: Defines the notification method of the first message of a conversation. The options to select are Sound, External Popups, Sound + External PopUps, or None. Supported in Chrome
  - Each Message: Defines the notification method for each message in a conversation. The options to select are Sound, External Popups, Sound + External Popups, or None. Supported in Chrome

4.4.1.7.3 Phone In the third tab, Phone, we can find the following options.

- Office Tel.: The number of the extension connected to the PBX
- Other Numbers: We can add extra numbers to provide information to the rest of the users
- Voice Mail Password: From here we can choose the new password to check the voice mail
- Confirm Password: Confirm to validate the voicemail password
- Use Security PIN: Check to activate
- Security PIN: Enter the PIN
- Remote Dial Code: Enter the desired code to dial in order to use a shared phone.
- Use follow-me?: Activate the follow me option. We will be able to choose the forwarding time and the ringing method we will use.

  item+announcement: The designated numbers will ring alternately, the user who originated the call must announce his name following the instructions, then he will be informed of the transfer of the call to the next extensionsimultaneous+announcement: The designated numbers will ring simultaneously, the user who originated the call must announce his name following the instructions alternating+silence: The designated numbers will ring alternately, without making any report to the users simultaneous+silence: The designated numbers will ring simultaneously, without making any information to the users
- Diversion Number: We can assign a diversion number to redirect the call there.
- Deviation Time: The time to wait before making the diversion.
- Speed Dial: We can assign the numbers that are convenient to make calls to other phones. For example, assign the number 1 to the phone 23566437.
- Receive Calls On: Simultaneously receive calls on the telephones: All, Main and Web.
- Make Calls From: Enable make calls from the Main phone and Web.

4.4.1.7.4 Notifications In the fourth tab, Notifications, it is possible to configure which events, in addition to showing them on the desktop, send us an email notification.

If we want to change the image to be displayed, we just have to click on it. The desktop will request that we choose a new file, after doing so, we must select the segment of the image that we want to establish as a photo, and press Save.

To finish editing the configuration, press Confirm.

4.4.1.7.5 Google Sync In this last tab, we can synchronize our contacts from a Google account directly to the Desktop contact directory:

To synchronize our contacts, we tick in the tab contacts and we confirm. At this point, a page will open that allows us to authorize the synchronization of contacts. We already have a session with a Google account in the browser, we directly click on Authorize.

On the other hand, if we do not have an open session, a window will open to access our Google account.

Once we get to this point, we agree to the terms and conditions for Denwa Unified Communications to manage our Google account contacts.

Once we have authorized, we will see that the synchronization of contacts begins.

Once the synchronization is achieved, we can see the contacts being added in our Desktop directory

In the Desktop directory, we can search for a contact and we will see the following logo in the contacts that were added from the Google account

4.4.1.8 ➜ Sign Out

Log off.

4.4.2 Left Panel

4.4.2.1 Personal data

Although the administrator is in charge of creating the users and assigning them permissions, each user will be able to edit their personal data when accessing the Desktop.

The configuration window can be accessed from the Configuration button or clicking on the pencil that appears next to the user's name will open the profile editing window.

The personal message can also be edited by clicking on it; After changing it, we must click on the pencil to save the changes.

We can also indicate our state. It can vary between:

- Absent
- Connected
- in call
- in meeting
- Busy
- Offline

4.4.2.2 Favorites

In the favorites tab we can see the users that we have added as favorites, as well as their status (indicated by the color under their photo).

If we move the mouse near the name, the option to Remove from Favorites will appear. We can find buttons with actions to the right of the user. If we click on the plus sign, the following options will be displayed:

- Info: Shows the information of the selected user.
- Mail: If we have a default mail client, clicking here will open the corresponding window to compose an e-mail to this user.
- Call: Make a call from the softphone.
- IM: Starts the Instant Messaging window with the selected user.

4.4.2.3 Connected

In this tab we will be able to observe the users that are connected (both those available, as well as those who are busy or absent).

If we move the mouse near one of the names, the option to Remove from IM Contacts will appear (in case it has already been added to IM contacts). We have the same options to display information, send an email, call and start instant messaging as in the Favorites tab. If we click on a user, we can see their personal data as shown below.

Within the personal data, we can execute three actions, Remove from Favorites, Remove from IM Contacts, and Show on map (this last option shows the user's location on the map).

4.4.2.4 Dashboard

The Dashboard tab must be authorized by the administrator. If the user does not have the certain permissions, he will not be able to observe it. This tab presents a list of monitored users, also enabled by the administrator. You can see the status of each of the monitored users, if the phone icon is red, it means that the user is on a call, yellow indicates that the phone is off the hook, green indicates that the line is on idle, and gray that the phone did not register with the IP-PBX.

Of course, by clicking on the phone icon we can make a call, being able to choose (if the user has more than one phone number) the extension to call. Let's look at the following figure.

In the central section we will find the registration area. These records can be call, message, or voice mail.

4.4.2.5 Contact Finder

From here we will be able to search for scheduled users, at the Company level (all company members use the same telephone directory), Personal (it only searches its own directory) and National (country level).

The results will be displayed in a dropdown list. From it, we will be able to access the profile of each user, add them to our Favorites and Messaging contacts.

If what we want is to add a new contact to the directory, we must click on the plus sign. When doing so, we will see a new tab like the following.

After completing all the required data, we can check the option Public contact? to allow any member of the company to access this contact.

4.4.3 Middle Panel

4.4.3.1 Messages

We will find in this sector the messages we have received. They can be voice mails, or fax files or offline messages. In the following image we can see a received fax.

Offline messages are shown below, offline messages can be sent to a group of users.

And you can continue the conversation from the message sector.

Next we can see two voice mails, with the lower one playing, after having clicked on the message.

We can find in the previous image the lower message bar. From here we can check the blank box to select all the messages, and then download or delete them. We can also search for a particular message from the search engine (if we change the tab to Calls, the search engine also works), and if we click on the plus sign, we can send offline messages, SMS or Fax.

When we send a Fax, the file to be sent must have the extension pdf, jpg, png, or gif.

4.4.3.2 Calls

We will be able to observe all the events related to the calls. In the following image we see the report of two received calls, one missed call and one made. We can make a call again, by clicking on the phone that is to the right of the call record.

4.4.4 Right panel

4.4.4.1 Calendar

In the calendar we can see the days with their respective date, and if we click on a certain day a window will appear offering the possibility of filtering the events (All, Messages, Calls, Agenda, or News) that we want to observe on that particular date .

4.4.4.2 Schedule

The calendar is used to schedule Events, Tasks, Calls, Meetings, Anniversaries and Notes. These programming can be done by clicking on the plus sign that appears next to each item.

In the Agenda tab you can see the list of all scheduled items. By clicking on each one they can be modified. In the lower sector, we can filter the list of items, and add new ones from the button with the plus sign.

4.4.4.3 News

In the news section we can see the corporate chat, that is, any of the Desktop users can express themselves through this chat, which will be updated in real time and will show the latest messages.

To write in the news, we must use Say it!. We will need permission from the administrator to be able to do this.

4.5 Services

Service	Code
Pick up call (Group):	*88
Pick up call (Extension):	*88+ext
Pick up call (All):	*89
Conference extension:	*26
Voicemail extension:	*33
Voicemail Extension (Extension):	
Security code extension:	*74
Record pre-attend audio:	*73
Visiting user call:	*65
Pre-attendant security code:	*66
Queue login:	*784
Queued logout:	*785
Page Extension:	*58
Intercom Extension:	*59
Extension to block Identifier:	*36

Continued from previous page

Service	Code
Monitor extension:	*49
Extension for forwarding to mailbox:	*86
Extension to configure forwarding:	*39
Record call:	*11
Flash (analog line):	*5
Unattended transfer:	#11
Transfer attended:	#22

Part III

Step-by-step guides

CHAPTER 5

SECURITY ABOUT DENWA UC&C

Since VoIP protocols operate over IP networks, the integrity of the former depends to a large extent on the latter; Therefore, the complement of a high-level security system is necessary to face potential threats that may exist in this new technology.

To carry out an attack on the system, there must be at least one vulnerability in it. Since the IP network is susceptible to security problems, the system must be composed of several applications in the different parts that make up the solution, so that the network is: secure, reliable and provides protection to all its members.

Highlights

Any computer exposed to the network without any protection is vulnerable and a candidate for attack.

Our main recommendation is: **DO NOT** expose the Denwa UC&C platform to the internet by placing a public IP on it; unless it is not strictly necessary and there are (minimally) security means such as: SBC and Firewall.

This document provides a configuration guide for the unified communications system focused on network security. Although the topic addressed is very broad, explanations and configurations (step-by-step) necessary to perform an optimal configuration are provided.

Important

The Denwa UC&C platform should only be accessible from known and authorized networks and IP addresses, usually LAN networks. For this, it is recommended to configure a management port (network interface or VLAN) that is only used by authorized personnel.
In case of enabling access to networks and IP addresses outside the LAN (for example MAN or WAN), it is recommended to allow access, from the Firewall tool, only to specific ports and protocols.

5.1 DenwaUC

5.1.1 General outline

The following image shows us all the blocks that an attacker has to go through from the moment he tries to attack Denwa until he manages to make an illegal call. Likewise , it will be explained later how to configure all these blocks so that the attacker does not achieve his goal in any way.

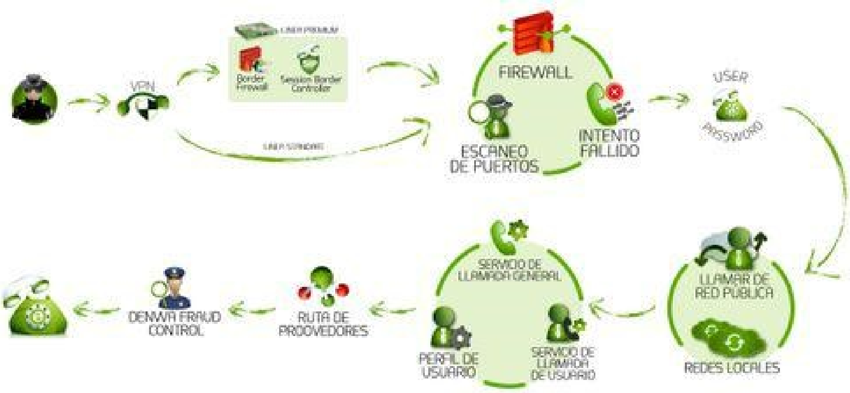


Figure 5.1: General Block Scheme

5.2 Preliminary steps

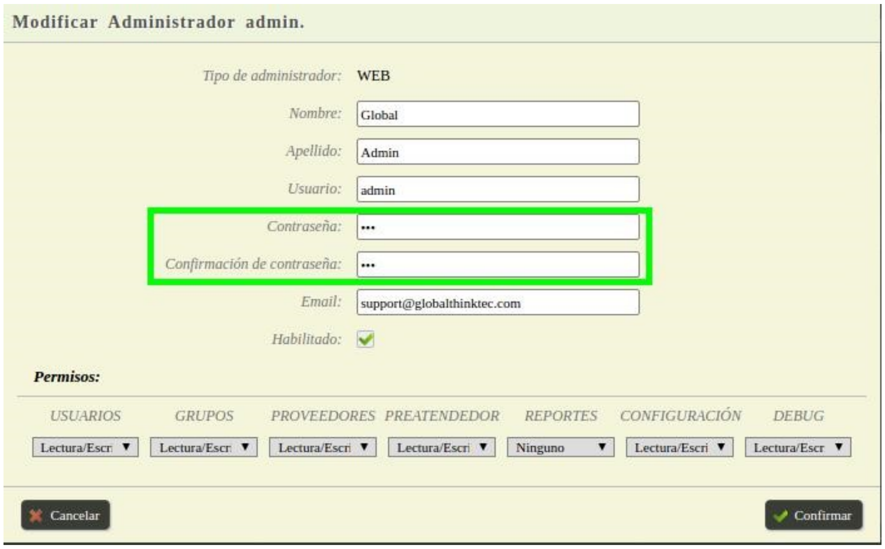
Before addressing the review of each of the items described in the previous image, it is necessary to clarify some minimum security considerations for access to the Denwa UC&C platform.

5.2.1 Changing Default Passwords

To facilitate the installation and initial configuration process, the platform has two (2) default accesses, one of them allowed entry after the installation of the base operating system (from the ISO); while the other one gave the necessary access to be able to activate the license of the equipment. Therefore, these ”generic” passwords should be changed as soon as possible.

5.2.1.1 User admin

To change the password of the user **admin**, you must enter the web administration interface and go to the menu: Configuration > Administrators. Once there, you will be able to view the list of all administrator-type users of the platform. All you have to do is click on the admin user to display a pop-up window, where you can change your password (you must re-enter it in the ”Password confirmation” field).



Modificar Administrador admin.

Tipo de administrador: WEB

Nombre: Global

Apellido: Admin

Usuario: admin

Contraseña: •••

Confirmación de contraseña: •••

Email: support@globalthinktec.com

Habilitado: ☑

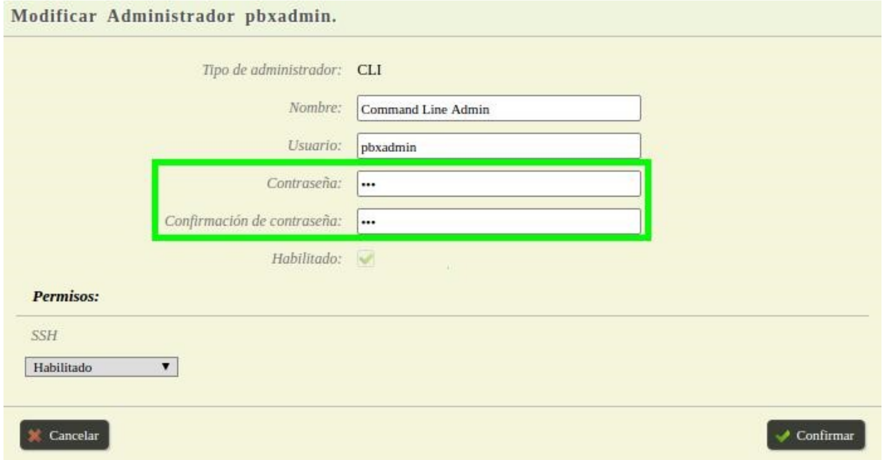
Permisos:

USUARIOS	GRUPOS	PROVEEDORES	PREATENDEDOR	REPORTES	CONFIGURACIÓN	DEBUG
Lectura/Escr ▼	Lectura/Escr ▼	Lectura/Escri ▼	Lectura/Escri ▼	Ninguno ▼	Lectura/Escri ▼	Lectura/Escr ▼

Figure 5.2: Password change of admin user

5.2.1.2 User pbxadmin

The case of the user **pbxadmin** is the same as the previous one, you must enter the web administration interface and go to the menu: Configuration > Administrators and edit the user of the command line interface (*CLI* for your acronym in English).



Modificar Administrador pbxadmin.

Tipo de administrador: CLI

Nombre: Command Line Admin

Usuario: pbxadmin

Contraseña: •••

Confirmación de contraseña: •••

Habilitado: ☑

Permisos:

SSH

Habilitado ▼

Figure 5.3: Change password of user pbxadmin

However, if you consider that it is not necessary, it is recommended to disable it from this same section.

5.2.2 Using HTTPS

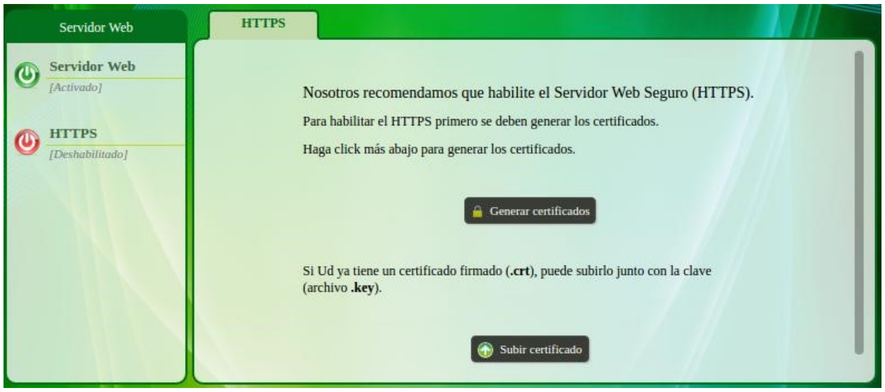
HTTPS is an Internet communication protocol that protects the integrity and confidentiality of user data between their computers and the website. Sending data over HTTPS is protected by the Transport Layer Security (*TLS*) protocol, which provides these three main security layers:

- **Encryption**: Data exchanged is encrypted to keep it safe from prying eyes. This means that when a user is browsing a website, no one can "listen" to their conversations, track their activities across different pages, or steal information from them.

- **Data Integrity**: Data cannot be changed or corrupted during transfers, intentionally or otherwise, without detection.

- **Authentication**: Prove that your users are communicating with the intended website. It provides protection against man-in-the-middle attacks and builds user trust, which translates into other business benefits.

To configure the use of HTTPS, it is necessary to enter the web administration interface and go to the menu: Configuration > Networks > Web server. It is possible to generate self-signed certificates on the computer itself, or import certificates from your domain.



Nosotros recomendamos que habilite el Servidor Web Seguro (HTTPS).

Para habilitar el HTTPS primero se deben generar los certificados.

Haga click más abajo para generar los certificados.

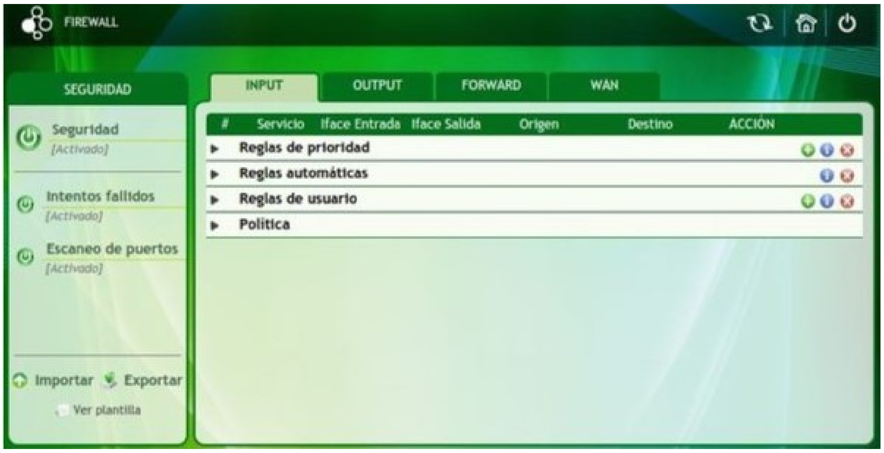
Si Ud ya tiene un certificado firmado (**.crt**), puede subirlo junto con la clave (archivo **.key**).

Figure 5.4: Enabling the HTTPS protocol

5.2.3 Firewall

In order to protect the platform against other types of attacks, in addition to being able to carry out a general security scheme and rules for the different equipment and traffic in our network, there is a fundamental tool available when carrying out a new configuration: the Firewall. This tool can be configured in a graphic, intuitive and simple way.

It is possible to configure specific rules for filtering, accepting, denying or discarding incoming, outgoing or passing traffic through the platform. It does this by specifying: services, protocols, ports and/or source or destination IP addresses. Only administrators can do this type of configuration.



Seguridad [Activado]
Intentos fallidos [Activado]
Escaneo de puertos [Activado]

#	Servicio	Iface Entrada	Iface Salida	Origen	Destino	ACCIÓN
▶	Reglas de prioridad					
▶	Reglas automáticas					
▶	Reglas de usuario					
▶	Política					

Figure 5.5: Firewall Settings

The correct configuration of this tool is essential.

Firewall and High Availability In the case of equipment configured in a High Availability scheme, the Firewall priority rules cannot be configured, instead they must be loaded in the user rules section.

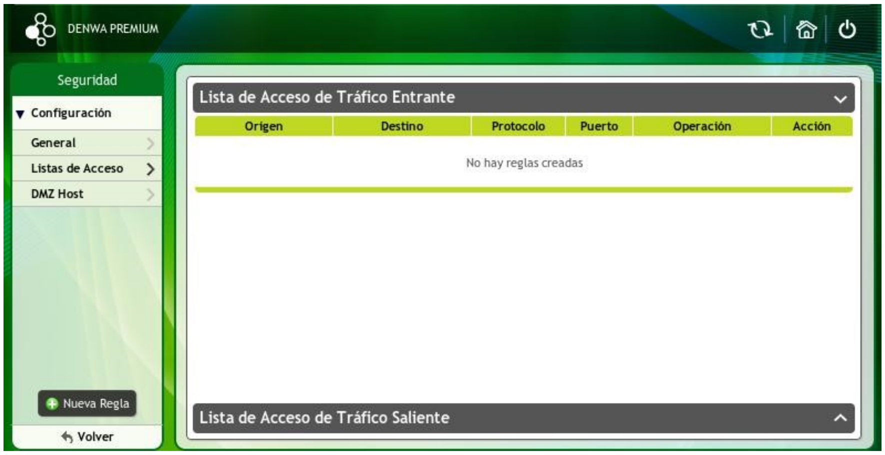
5.2.3.1 Additional Premium Tools

Denwa Premium

The tools mentioned for Premium are only available in version 3.3.1 of the Denwa UC&C system

The Denwa Premium team has, in addition to the additional tools to those mentioned above, two (2) extra functionalities: Border Firewall and SBC (session border controller).

5.2.3.1.1 Edge Firewall The Denwa Premium equipment has the same router functionalities; For this reason, it has a firewall prior to the Denwa UC firewall. This firewall allows you to configure access lists to allow and deny the traffic that is required, both incoming and outgoing. It can be configured from the web administration interface, entering the menu: Configuration > Denwa Premium > Security (access lists).



Lista de Acceso de Tráfico Entrante

Origen	Destino	Protocolo	Puerto	Operación	Acción

No hay reglas creadas

Lista de Acceso de Tráfico Saliente

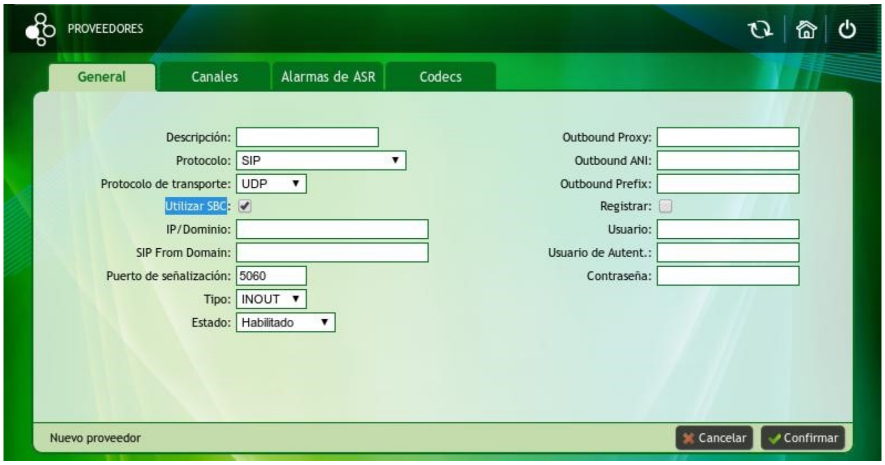
Figure 5.6: Border Firewall Configuration

The correct configuration of this tool is essential

5.2.3.1.2 SBC This tool is perhaps the best aspect of SIP security and normalization that a telephony team can have among its features. The SBC, as its name indicates, allows us to carry out exhaustive control of the SIP sessions that are carried out in the equipment.

It is very helpful when it comes to improving security since the SBC itself discards traffic that does not comply with the basic rules of the SIP protocol (malformed traffic). In the case of Denwa, the SBC will only allow traffic to port 5060 of those providers (or users) that have been expressly declared on the equipment. In addition, it can modify the headers of the SIP packets "masking" the IP of the telephone exchange and it is capable of controlling all kinds of external SIP records.

It is recommended to use the SBC in suppliers; To do this, it is enough to activate the corresponding box in the provider configuration tab, as shown in the following image:



Descripción:
Protocolo: SIP
Protocolo de transporte: UDP
Utilizar SBC: ☑
IP/Dominio:
SIP From Domain:
Puerto de señalización: 5060
Tipo: INOUT
Estado: Habilitado

Outbound Proxy:
Outbound ANI:
Outbound Prefix:
Registrar: □
Usuario:
Usuario de Autent.:
Contraseña:

Nuevo proveedor

Figure 5.7: Configuring the SBC in providers

5.3 Step-by-step of an attack

Until now, everything indicated that can be considered as: general recommendation; however , it is necessary to know the way in which attacks usually occur, as well as the tools that the platform has to repel them.

5.3.1 Step One: Snooping

The attacker will first try to capture as much traffic as possible on the network to try to obtain information that he can use in his attack.

Denwa allows you to use virtual private networks (*VPN*) for your connection to the outside world. This topic will be expanded upon in the VPN section on the 176 page.

5.3.2 Step Two: Scan

Now you need to know as accurately as possible the services that the attacked computer has, to later be able to find vulnerabilities in them, and thus use them.

Denwa counters this with a port scanning detection tool, being able to block this type of attack. This topic will be covered in the **??** section on the **??** page.

5.3.3 Third step: access

The attacker, after having found port 5060 open on the attacked computer, can assume with a high degree of certainty that the computer provides telephony services. Therefore, to advance with its attack, it will proceed to try to gain an account within the team (valid username and password). Usually this type of attack is carried out by brute force, trying to register users using random passwords, until an effective one is found.

Denwa has a tool that detects failed registration and login attempts, with which the IP address of origin of the request is added to a blacklist after making several wrong passwords. This topic will be covered in sections Failed attempts (page 181) and Users password (page 182).

5.3.4 Step Four: Generate Traffic

Trying to make calls at no cost to the attacker, this is what a phone system attacker is looking for. For this, and already registered with the username and password that it was able to capture from its attack, it makes calls to different destinations.

Denwa has a series of tools to control which user can and cannot make certain types of calls; between them:

- Local networks (see page 182)
- Call from the public network (see page 183)
- Call Services (see page 183)
- User Call Service (see page 184)
- **??** (see page **??**)
- Fraud Control (see page 185)

5.4 Denwa UC&C Resources

It is extremely important to know the tools that are available in the unified communications platform, since the security of the platform depends on its correct configuration.

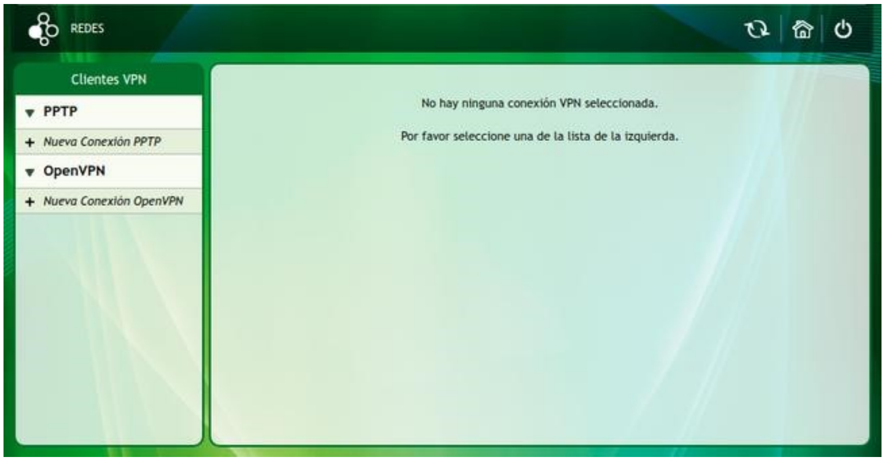
5.4.1 VPN

It is possible to configure the Denwa UC&C system both as a client and as a server for different types of VPN

5.4.1.1 As a VPN client

The configuration of this functionality is recommended in the scenarios that allow it, it can be done in the administration web interface, from the menu: Configuration > Networks > VPN Clients.

From this tab you can configure a new VPN (Virtual Private Network) connection using the PPTP (Point-To-Point Tunneling Protocol) or the OpenVPN protocol and edit existing connections (if you have one).



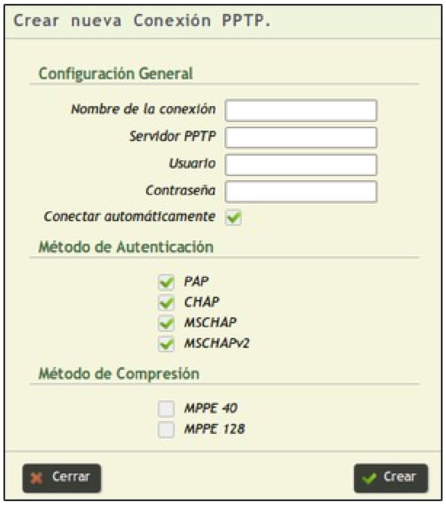
No hay ninguna conexión VPN seleccionada.

Por favor seleccione una de la lista de la izquierda.

Figure 5.8: VPN Clients

VPNs allow a secure extension of the local network over a public network. To do this, a point-to-point virtual connection is made using dedicated and/or encrypted connections. It has the advantage of reducing the bandwidth used and increasing speed. It also provides secure communications on public networks with specific access rights.

5.4.1.1.1 PPTP Client it connects directly to the destination server creating a virtual network for each remote client, which the administrator can monitor and manage like any other remote access port. To configure this client, click on the New PPTP Connection option.



Crear nueva Conexión PPTP.

Configuración General

Nombre de la conexión

Servidor PPTP

Usuario

Contraseña

Conectar automáticamente ☑

Método de Autenticación

☑ PAP
☑ CHAP
☑ MSCHAP
☑ MSCHAPv2

Método de Compresión

☐ MPPE 40
☐ MPPE 128

Figure 5.9: VPN Clients, PPTP

Below is the description of the fields:

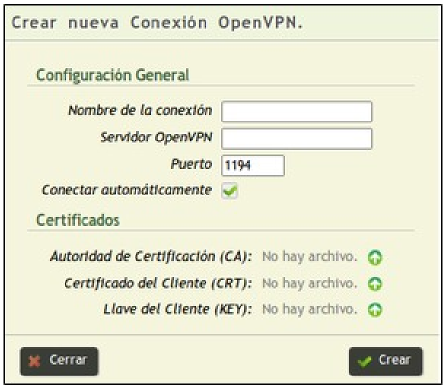
- **General Settings**
  - **Connection name**: name that is assigned to the connection.
  - **PPTP Server**: IP or domain of the PPTP server.
  - **Username**: username to access the PPTP server.
  - **Password**: User password to access the PPTP server.
  - **Connect automatically**: enable in case the connection should always be active
- **Authentication Method**: the authentication protocol(s) to be used must be selected.
  - **PAP** (Password Authentication Protocol): is a simple protocol that authenticates a user against a remote access server. Its function is to validate a user to access different resources. For this, PAP transmits passwords in ASCII in the clear, so it should be used as a last resort.
  - **CHAP** (Challenge Handshake Authentication Protocol): is a challenge handshake authentication protocol. It periodically verifies the identity of the remote client using an information exchange. With CHAP, the user ID and password are always sent encrypted, making it a more secure protocol than PAP.
  - **MSCHAP** (Microsoft Challenge Handshake Authentication Protocol): Microsoft challenge handshake authentication protocol. This does not require that both parties know the key in the clear, but a summary (Hash) of it.
  - **MSCHAPv2** (Microsoft Challenge Handshake Authentication Protocol v2) - Microsoft challenge handshake authentication protocol version 2. Provides high-level security for remote access connections. MS-CHAP v2 resolves some issues with MS-CHAP.
- **Compression Method**: are encryption methods, only used with the MSCHAP and MSCHAPv2 protocols.
  - **MPPE 40** (Microsoft Point-to-Point Encryption): Microsoft 40-bit point-to-point encryption.
  - **MPPE 128** (Microsoft Point-to-Point Encryption): Microsoft 128-bit point-to-point encryption.

Then click on «✔Create» and the VPN will have been created. Below you can see the generated connection.

Figure 5.10: VPN clients, PPTP connection configured

Once the new connection is created, it can be Connected, Deleted or Modified from the buttons located in the lower section of the page.

5.4.1.1.2 OpenVPN Client is open source virtual private network software, which provides security, stability and encryption mechanisms without introducing complexity. To configure the OpenVPN client, click on the New OpenVPN Connection option.



Crear nueva Conexión OpenVPN.

Configuración General

Nombre de la conexión

Servidor OpenVPN

Puerto 1194

Conectar automáticamente ☑

Certificados

Autoridad de Certificación (CA): No hay archivo.

Certificado del Cliente (CRT): No hay archivo.

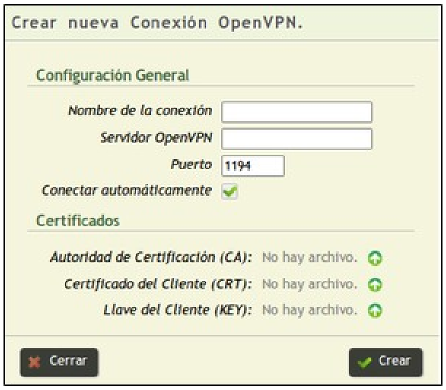
Llave del Cliente (KEY): No hay archivo.

Figure 5.11: VPN clients, OpenVPN configuration

Below is the description of the fields:

- **General Settings**
  - **Connection name**: name to be assigned to the connection.
  - **OpenVPN Server**: IP or domain of the OpenVPN server.
  - **Port**: port to be used for the VPN connection.
  - **Connect automatically**: enable in case the connection should always be active.
- **Certificates**
  - **Certification Authority (CA)**: Allows importing the file.
  - **Client Certificate (CRT)**: Allows importing the file.
  - **Customer Key (KEY)**: Allows importing the file.

These certificates must be granted by the OpenVPN server administrator.



Crear nueva Conexión OpenVPN.

Configuración General

Nombre de la conexión	
Servidor OpenVPN	
Puerto	1194
Conectar automáticamente	☑

Certificados

Autoridad de Certificación (CA):	No hay archivo.
Certificado del Cliente (CRT):	No hay archivo.
Llave del Cliente (KEY):	No hay archivo.

Figure 5.12: VPN clients, OpenVPN configuration

Then, by clicking on the «✓Create» button, the VPN will have been registered in the system. As with PPTP, you can Connect, Delete or Modify the connection from the buttons located in the lower section of the page.

5.4.1.2 As a VPN server

On the other hand, in case of not having a VPN server, the unified communications platform can be configured to fulfill said function.

5.4.1.2.1 OpenVPN Server In this section, the OpenVPN service will be configured to have secure connections for users outside the network. When entering the server you can see a screen like the following:

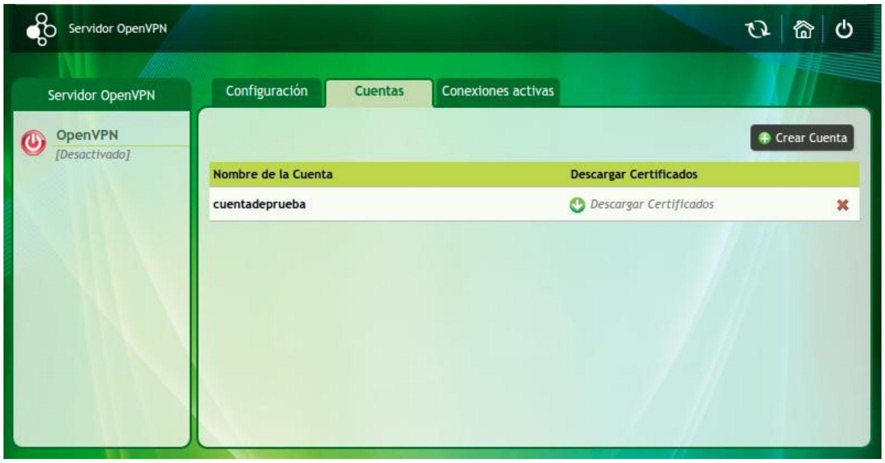
Figure 5.13: OpenVPN Server

In the left column it is possible to start or stop the OpenVPN Server service by clicking on the ⏻icon.

5.4.1.2.1.1 Settings Tab In the previous image you can see that the server is disabled and that there is no pre-loaded configuration. Below is the detail of the parameters to be configured:

- **Port**: port to use for the OpenVPN service
- **Protocol**: protocol used by the server
- **Network Address/Mask**: network from which IP addresses will be given to clients
- **Allow Access**: networks to which you want to give clients access.

5.4.1.2.1.2 Accounts Tab In this tab it is possible to register accounts for remote access to the unified communications platform and/or to the networks selected in the configuration tab.



Nombre de la Cuenta	Descargar Certificados
cuentadeprueba	Descargar Certificados

Figure 5.14: OpenVPN server, access accounts

To create a new account, we simply click on Create Account, and fill in the username; with this the account has been created and it is possible to download its certificates.

Figure 5.15: OpenVPN server, login account creation

To use the OpenVPN server it is necessary to have the certificates on the computers that will connect to it, so they must be downloaded from the accounts tab. Once on the local computer, it is necessary to have the OpenVPN «client» software and, from a basic text editor, generate an .ovpn file like the one shown below:

```
###########################################
nVPN Client
###########################################
nt
tun
ocol PROTOCOL
te SERVER_IP SERVER_PORT
lv-retry infinite
nd
-lzo
 3
rtificate files
CERTIFICATE_PATH/ca.crt"
 "CERTIFICATE_PATH/CERTIFICATE_NAME.crt"
"CERTIFICATE_PATH/CERTIFICATE_NAME.key"
###########################################
```

Example of .ovpn file content

You must replace where it says «PROTOCOL», «IP_OF_SERVER», «PORT_OF_SERVER», «PATH_OF_CERTIFICATE», «NAME_CERTIFICATE» according to the configurations made on the server, as well as the downloaded certificates.

5.4.1.2.1.3 Records Tab This tab will show the list of all active connections («clients» connected) to the OpenVPN service.

5.4.2 Port Scan

The «Port Scan» tool allows you to automatically block attacks of this type, because the system constantly checks for possible port scans on the computer and, when detecting this, automatically blocks the IP address from where the is carrying out the possible attack, creating a new rule in the *Firewall*.

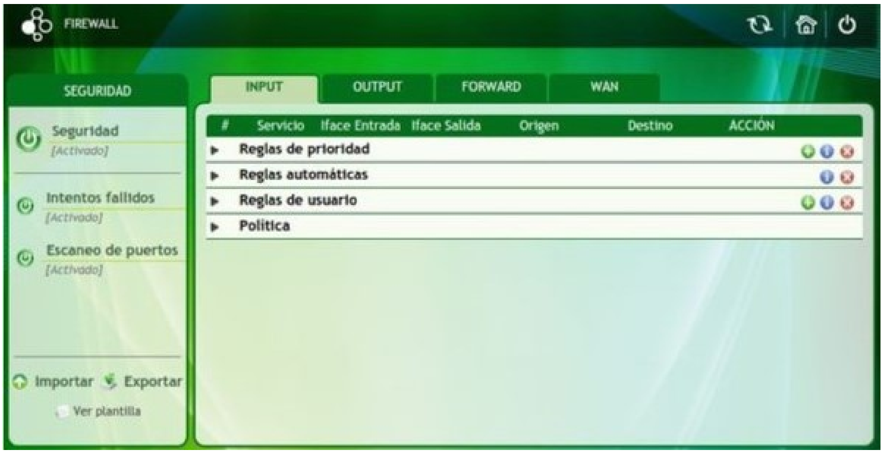
Only administrator type users can modify the Firewall to remove the blocking of an IP address, in case it is considered to have been blocked by mistake.

Port Scan

It is essential to use this tool

Automatic rules

IP address blocks created automatically by the failed attempts and port scanning processes are created in the Automatic Rules Section.



Seguridad [Activado]

Intentos fallidos [Activado]

Escaneo de puertos [Activado]

#	Servicio	Iface Entrada	Iface Salida	Origen	Destino	ACCIÓN
▶	Reglas de prioridad					⊕ ⓘ ⊗
▶	Reglas automáticas					ⓘ ⊗
▶	Reglas de usuario					⊕ ⓘ ⊗
▶	Politica					

Figure 5.16: Port Scanning and Failed Attempts Enabled

5.4.3 Failed attempts

The «Failed Attempts» tool offers the possibility to block «brute force» attacks automatically. The system constantly reviews and saves the list of registration attempts, as well as the IP address from which the attempt was made; If it finds five (5) failed registration attempts from the same IP, it automatically generates a new rule in the Firewall to deny any packet that has the same origin.

Only administrator type users can modify the *Firewall* to unblock an IP address, in case it is considered to have been blocked by mistake.

Failed attempts

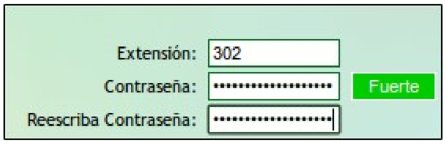
It is essential to use this tool

Automatic rules

IP address blocks created automatically by the failed attempts and port scanning processes are created in the Automatic Rules Section.

5.4.4 Users password

The best way to complement the «Failed Attempts» tool is through the use of strong passwords, so it is important to thoroughly control the complexity level of all users' passwords and ensure their complexity is high . This also applies to administrator-type users.



Extensión: 302
Contraseña: •••••••••••••••••••
Reescriba Contraseña: •••••••••••••••••••

Figure 5.17: Password strength

In the face of a «brute force» attack, the complexity of the passwords decreases the probability that they are easily discovered, in turn increasing the probability that the attacker's IP address will be automatically blocked by the Firewall using the « <Unsuccessful attempts». This applies equally to Denwa Desktop passwords.

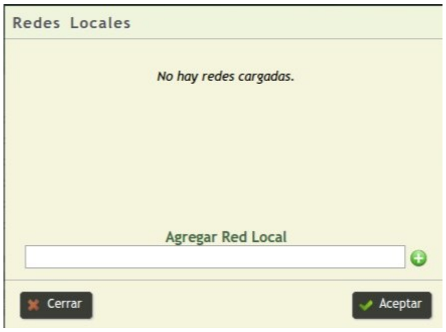
It is possible to know the overall password complexity status of all system users from the home screen in the web management interface.

5.4.5 Local networks

Denwa needs to know in some way the network scheme where it is installed, so it is necessary to indicate the networks that it should interpret as «local»; any network that does not belong to the local networks will be interpreted as an external network.

This is very important during the configuration of the users and their permissions, since it is possible to configure that the user cannot make calls if he has not registered from a local network. Another very useful tool in the case of users who do not have to register from outside the network.

Networks must be added from the administration web interface, in the menu: Configuration > General > Advanced by clicking on the ⚙icon next to «Local Network». This will enable a new window, which allows you to add the different networks.

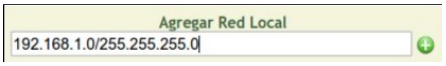


Redes Locales

No hay redes cargadas.

Figure 5.18: Local Networks

By clicking on the ✚icon, a window will be displayed where it is possible to declare the local networks one by one. The format to add the same in network/mask (both in four decimal octets).



Agregar Red Local

192.168.1.0/255.255.255.0

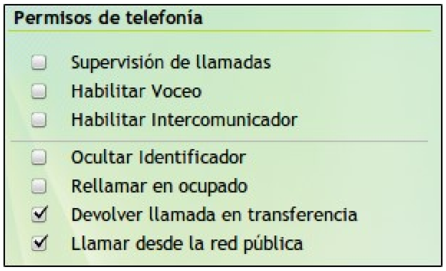
Figure 5.19: Local networks, add a local network

Clicking on the +icon will return to the previous window, being able to repeat the process as many times as there are local networks. Then, all you have to do is click on the «✔Accept» button to finish the task.

5.4.6 Call from the public network

This option enables the user to be able to make calls when registered on a network that does not belong to the local networks configured in the previous step.

It is recommended that only users who actually use this functionality have this option enabled in the advanced user settings.



Permisos de telefonía

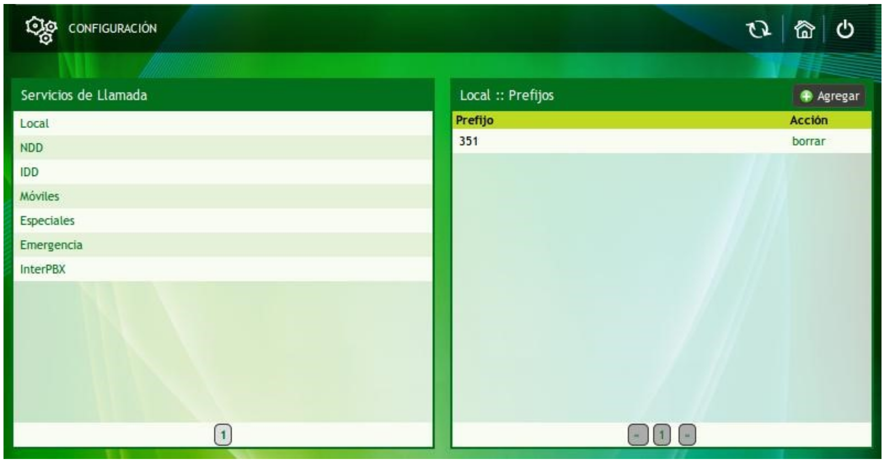
- ☐ Supervisión de llamadas
- ☐ Habilitar Voceo
- ☐ Habilitar Intercomunicador
- ☐ Ocultar Identificador
- ☐ Rellamar en ocupado
- ☑ Devolver llamada en transferencia
- ☑ Llamar desde la red pública

Figure 5.20: Advanced user settings, call from public network

5.4.7 Call Services

In this place, all the call prefixes are configured for each of the types of calls that could be made (Local, National, International, etc.). For example, in the case of International calls the prefix would be «00».

By defining the prefixes in this section, each Denwa user will be allowed to enable or deny the different types of calls. It can be configured from the web administration interface, in the menu: Configuration > Call services.



Servicios de Llamada

- Local
- NDD
- IDD
- Móviles
- Especiales
- Emergencia
- InterPBX

Local :: Prefijos

Prefijo	Acción
351	borrar

Figure 5.21: Call Services

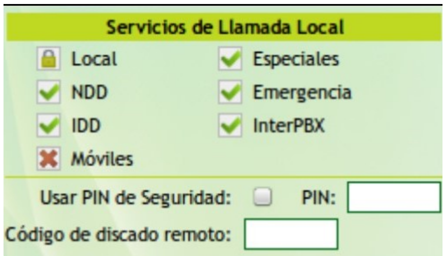
Call Blocking

It is essential to configure the call services correctly, since the call services of the user profiles depend on them.
If it is not configured, all calls will be made regardless of their destination.

5.4.8 User Call Service

Only if User Call Service has been configured, the user's local profile will be valid. The configuration of the users' call services, allows the administrator user to enable or deny, to each user individually, the course of a call according to their prefix.

It can be configured from the web administration interface, in the menu: Users > View users > «User_Name» > Services.



Servicios de Llamada Local

🔒 Local	✓ Especiales
✓ NDD	✓ Emergencia
✓ IDD	✓ InterPBX
✗ Móviles	

Usar PIN de Seguridad: □ PIN:

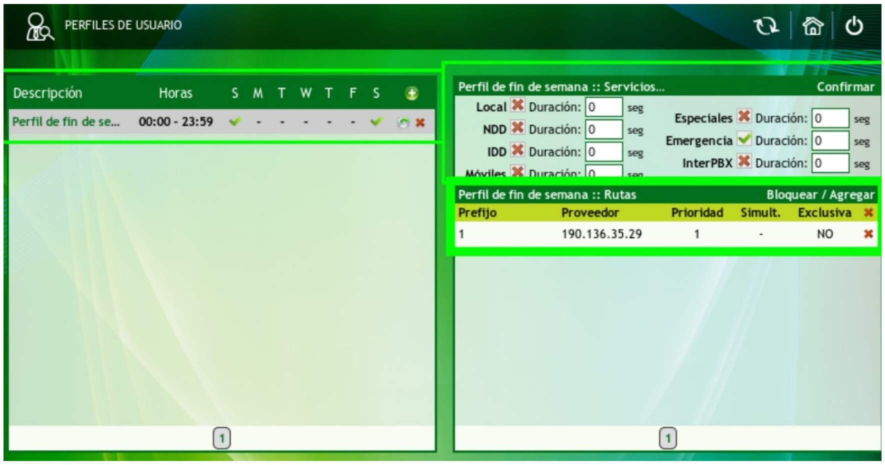
Código de discado remoto:

Figure 5.22: User Call Services

It is recommended to configure the services of each user making a previous study of what function it performs within the structure of the company.

5.4.9 User Profiles

Only if User Call Service has been configured, the profile to be configured for the users will be valid. The user profiles in Denwa allow the enabling or denying of the course of calls to different destinations according to their prefix, based on criteria such as: day of the week, time and provider to use. This adds greater control of the calls, since it is possible to define: who (user to whom the profile has been applied), how (according to the call prefix), where (according to the defined provider) and when (according to the day and time) you can make calls.



Descripción	Horas	S	M	T	W	T	F	S
Perfil de fin de se...	00:00 - 23:59	✓	-	-	-	-	-	✓

Perfil de fin de semana :: Servicios... Confirmar

Local ✗	Duración: 0	seg		Especiales ✗	Duración: 0	seg
NDD ✗	Duración: 0	seg		Emergencia ✓	Duración: 0	seg
IDD ✗	Duración: 0	seg		InterPBX ✗	Duración: 0	seg
Móviles ✗	Duración: 0	seg				

Perfil de fin de semana :: Rutas Bloquear / Agregar

Prefijo	Proveedor	Prioridad	Simult.	Exclusiva	✗
1	190.136.35.29	1	-	NO	✗

Figure 5.23: User Profiles

It can be configured from the web administration interface, in the menu: Users > User profiles.

Routes

In the event that a profile does not have defined routes, the user who has that profile assigned will not be able to make calls to the outside.

User Profiles

The use of this tool is recommended.

5.4.10 Provider Path

It is important to correctly configure the different routes of each of the providers within Denwa. These routes are the ones that enable calls to be made by one or another provider, according to the number dialed. They must be configured in the most specific way possible so that only calls that have been correctly dialed are sent. Here is an example:

In case calls that begin with the number 0 and have a length of 7 digits (including 0) need to be made by a certain provider, two (2) possible configurations can be presented:

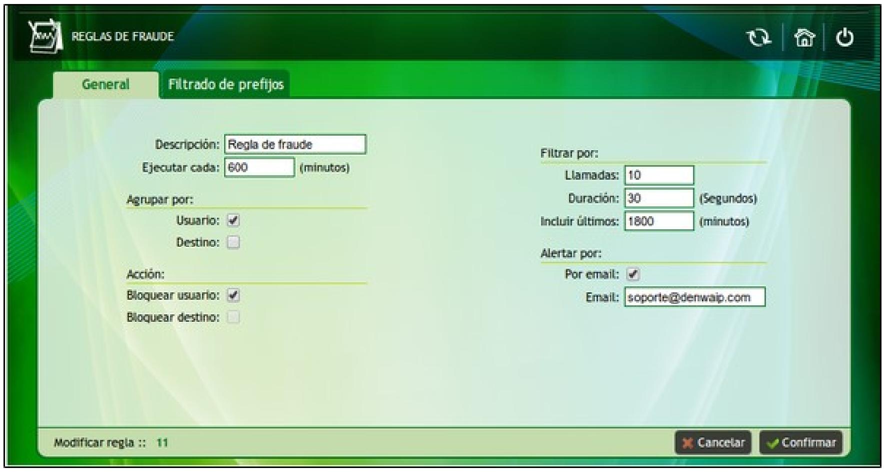
- **Configuration correct** (✔): The path configuration should be "0______" (one zero and six _)
- **Incorrect configuration** (✖): route simply with 0 and priority 1 allows any call beginning with 0 to be routed by this provider

Provider path

Careful configuration of provider routes is recommended.

5.4.11 Fraud Control

As if that were not enough, the Denwa system has a last line of protection against attacks, the «Fraud Control» tool. This tool allows you to analyze the behavior of each user of the platform, being able to block those calls that seem suspicious. For example: if an extension generates 10 calls in 5 minutes, it is possibly a «boot» that is trying to generate calls with the aim of doing damage. In such a case the user or the destination can be blocked, at the same time an email notice is sent to alert the situation.



Descripción: Regla de fraude
Ejecutar cada: 600 (minutos)

Agrupar por:
Usuario: ☑
Destino: □

Acción:
Bloquear usuario: ☑
Bloquear destino: □

Filtrar por:
Llamadas: 10
Duración: 30 (Segundos)
Incluir últimos: 1800 (minutos)

Alertar por:
Por email: ☑
Email: soporte@denwaip.com

Modificar regla :: 11

Figure 5.24: Fraud Control

It can be configured from the web administration interface, in the menu: Configuration > Fraud control.

Email Alert

Email alerts will only be sent if your mail server is properly configured (Settings > General > Mail Server)

5.5 End of configurations about Denwa UC&C

These are the tools that make Denwa an extremely secure solution on all your computers. Bottom line: An attacker requires all of these tools to be misconfigured to make unauthorized calls through our unified communications platform.

In the following sections, general recommendations will be added about devices outside the unified communications platform, but that do to the security of the VoIP system and the correct implementation of the network structure.

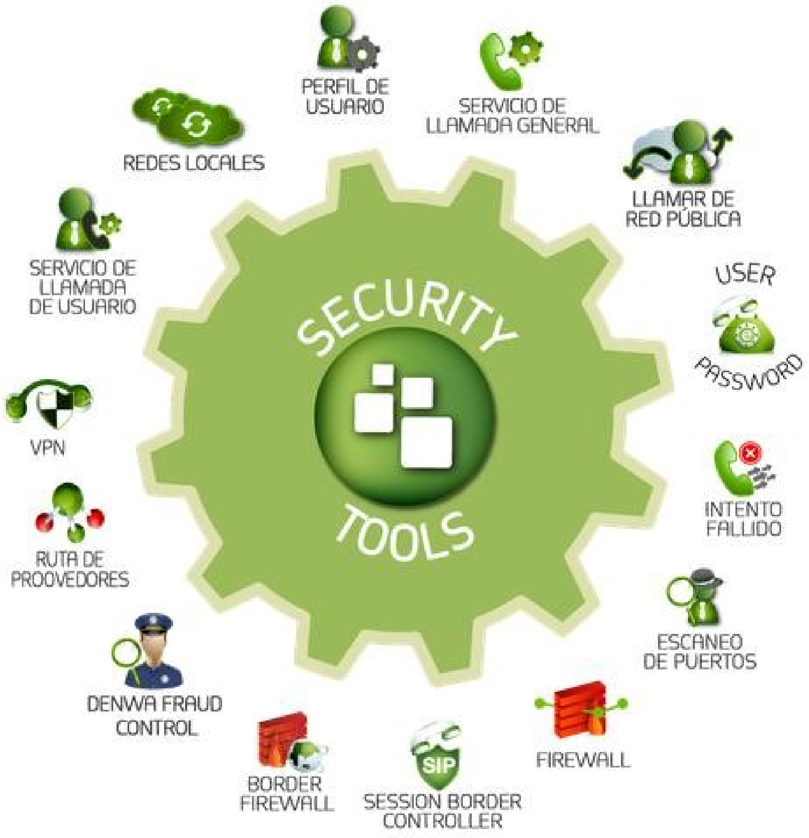


Figure 5.25: Denwa Security Tools

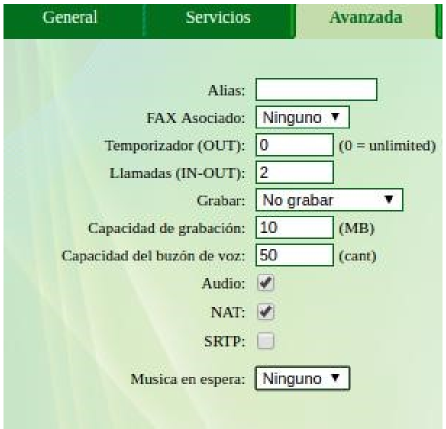
This page has been intentionally left blank.

CHAPTER 6

SECURITY ON TELEPHONE TERMINALS

Here are our recommendations for the security of telephone terminals:

1. Change the administration password of the telephone terminals.
2. Configure the internal firewall of the Denwa phones so that they can only be accessible from the IP address of the unified communications platform and from the range of IP addresses of its administrator-type users.
3. Enable SRTP in order to have voice encryption. In case of provisioning the terminals from the Denwa UC&C platform, it will suffice to enable it in the user configuration (Users > View users > «User_Name» > Advanced)



Alias:

FAX Asociado: Ninguno ▼

Temporizador (OUT): 0 (0 = unlimited)

Llamadas (IN-OUT): 2

Grabar: No grabar ▼

Capacidad de grabación: 10 (MB)

Capacidad del buzón de voz: 50 (cant)

Audio: ☑

NAT: ☑

SRTP: □

Musica en espera: Ninguno ▼

Figure 6.1: Enabling SRTP

This page has been intentionally left blank.

CHAPTER 7

SECURITY ABOUT THE NETWORK STRUCTURE

Here are our recommendations for the security of the network structure:

1. Modification of all the default passwords in the equipment to be installed (Switch, router, etc.). This is an important step for data network security.
2. Using VLANs to separate traffic
3. Use of MAC filtering in the different access points to the network, thus allowing only authorized equipment to have access to the specific port of the Switch, or to the Wi-Fi network.
4. In special cases, you can request the removal of the call recording and monitoring modules in the Denwa UC&C equipment.

This page has been intentionally left blank.

CHAPTER 8

FOLLOW ME

Follow-me is an application that diverts calls to contact the recipient of the call if they are not physically present at their extension. There are different operating options, which are detailed below. It should be noted that the forwarding time is the time that the extension to which the call was forwarded will ring, taking into account that the announcement consumes ringing time.

- **Alternate + Announcement**: The designated numbers will ring alternately, the user who originated the call must announce his name following the instructions, then the system will inform the transfer of the call to the next extension and play the previously recorded announcement .
- **Simultaneous + Announcement**: The designated numbers will ring simultaneously, the user who originated the call must announce his name following the instructions, then the system will inform the transfer of the call to the next extension and play the previously recorded announcement .
- **Alternate**: The designated numbers will ring alternately, while the system informs that it must wait while the communication is attempted.
- **Simultaneous**: The designated numbers will ring simultaneously, while the system informs you to wait while the communication is attempted.
- **Alternate + Silent**: The designated numbers will alternately ring, without making any report to the users.
- **Simultaneous + Silent**: The designated numbers will ring simultaneously, without making any information to the users.

8.1 Frequent problems

This document intends to list the most common problems that usually occur along with the main ones that each one of them can produce and the possible solutions to them.

8.1.1 Case 1: Calls can be made but cannot be received

8.1.1.1 Possible causes

- DND (Do Not Disturbed-Do Not Disturb) activated.
- Loss of equipment registration.
- IVR or DID configuration.

8.1.1.2 Solution

- Verify that the DND functionality is not active.
- Reboot the phone to register. Then enter the web to the Users section -> View users to verify the status in which you are. That is, if the Registered column shows the status in red, it indicates that the extension in question has not been registered; On the contrary , if the status is green, it indicates that the extension has been successfully registered.
- IVR configuration: verify that the access numbers are assigned and are the desired ones. The tree diagram can be observed and, if necessary, it is possible to assign the number directly to an extension to verify that the call enters correctly.
- DID configuration: verify if the access number is configured in the trunk and, later, if it is properly associated to a user.

8.1.2 Case 2: Unable to make outgoing calls

8.1.2.1 Possible causes

- Log loss.
- The extension does not have the necessary permissions.
- Wrong paths.

8.1.2.2 Solution

- Reboot the phone to register. Then enter the web to the Users section -> View users to verify the status in which you are. That is, if the Registered column shows the status in red, it indicates that the extension in question has not been registered; On the contrary , if the status is green, it indicates that the extension has been successfully registered. (Solution 2 previous case).
- Verify the user's call service permissions, from the web access the Users menu -> View users -> Services tab.
- 3. Verify that the path of the desired provider is correct.

8.1.3 Case 3: Access to Denwa Desktop is not allowed

8.1.3.1 Possible causes

- Wrong password.
- The user in question does not have the service enabled.

8.1.3.2 Solution

- Enter a new password.
- Enable the user the Desktop service.

8.1.4 Case 4: Firewall, IP of DROP phones in automatic rules

8.1.4.1 Possible causes

- Automatic firewall rules show in your IP list of computers belonging to the network.

8.1.4.2 Solution

- Remember that the firewall is 'sequential', therefore priority will be given to those rules that are found over the others. The sequence that this firewall uses (since update 092) is the following: Priority Rules, Automatic Rules, User Rules, Services (WAN) and Policy. Therefore, it is enough to add in priority rules the network in which said equipment is located.

8.1.5 Case 5: Detours

8.1.5.1 Use

- It is NOT allowed to make more than one diversion in the same call. This is to prevent it from entering a loop .

This page has been intentionally left blank.

CHAPTER 9

CONNECTING TO DENWA OPENVPN SERVER

According to the operating system used, the following instructions are carried out to connect via VPN to the central. Once the files have been downloaded and the . ovpn , the following files are available:

- ca.crt
- client.ovpn
- client.crt
- client.key

Name of files

The name « client » is added for illustrative purposes.

9.1 OpenVPN for Windows

OpenVPN client in Windows, we enter the following link `https://openvpn.net/index.php/open-source/downloads.html` and download the installer for 32-bit or 64-bit. This process was certified for Windows XP, Windows 7, Windows 8 and Windows 10

We run the installer with the recommended basic options:

At this point, it will ask us to install a virtual adapter to provide connection:

We accept by clicking on Install, and continue the installation

On the desktop we will see the following icon corresponding to the direct access to OpenVPN

But before accessing, we must configure the program loaded with the certificates obtained. To do this we go to the following directory C:\{}Program Files\{} OpenVPN \{} config and copy the certificates in this directory. For this example we will look at a Denwa VPN connection

provider.client.vpn file contains the following format:

```
##############################################
# DENWA-PBX VPN CLIENT #
##############################################

client
dev tun
proto-udp
remote support.denwaip.com 2288
```

```
    resolv-retry infinite
    nobind
    comp-lzo
    verb 3
    #   Certificates files ca "ca.crt"
    cert "denwasupport.crt" key "denwasupport.key"
```

Note that the ca, cert and key parameters refer to the name of the files and are referred to in double quotes (")

Now double click on the icon

opens on the taskbar, in the notification icons sector a new connection that is initially in red

Special permissions

On Windows 7, Windows 8 and Windows 10, this program must be run as «Administrator».

Clicking with the right button gives us a sub-menu , with different options in which we connect

Then we see the following window where the connection process marks us:

If the connection is successful we will see the following notification message with the IP assigned by the server

With this, in the address bar of the browser we place the IP address of the exchange that the Administrator gives us, and we will have access to the PBX administrator website.

9.2 OpenVPN for Linux

OpenVPN client in Linux, through the console with administrator permissions we must execute the command:

```
        apt-get install openvpn
```

Then we save the provided certificates in a directory in which we will later refer, in this example we will save it in the /home/ user directory then we must edit the file provider.client.vpn with the following format:

```
            ###############################################
            # DENWA-PBX VPN CLIENT #
            ###############################################

            client
            dev tun
            proto-udp
            remote support.denwaip.com 2288resolv-retry infinite
            nobind
            comp-lzo
            verb 3
            #   Certificates files ca /home/user/ca.crt
            cert /home/user/denwasupport.crt key /home/user/denwasupport.key
```

Note that the ca, cert and key parameters refer to the name of the files and are addressed according to where we save the files.

Then through the console, with administrator permissions, we execute:

```
                openvpn /home/user/provider.client.vpn
```

and we will see the connection process. then on another console

We verify the connection through the ifconfig command and it will be possible to observe

Where the virtual interface tun0 gives us the IP obtained from the connection to the support server.

With this, in the address bar of the browser we place the IP address of the central that gives us the

Administrator, and we will have access to the PBX administrator web.

This page has been intentionally left blank.

CHAPTER 10

VOIP GUIDE

10.1 VoIP protocols

Until today there is a clear division between two types of networks:

- Voice networks: based on circuit switching, which is why a circuit is occupied and routing during a communication is always carried out along the same path. For example: Conventional Telephone Network
- Data networks: based on packet switching, information is sent in packets and each of them can travel through different paths. For example: internet

In order to be able to send the information through Internet-type data networks based on packet switching, it is necessary to adopt protocols that allow the transmission and recovery of the information. The problem with circuit switching technology is that it requires a significant amount of bandwidth for each call and the circuit is not used efficiently as it uses one channel for the entire duration of the call but most of the telephone conversations. they are made of silence

Data networks, on the other hand, only transmit information when it is necessary, taking full advantage of the bandwidth and in which the delay, the alteration of the arrival order or the loss of packets are not an inconvenience, since in the The final system has a series of procedures for recovering the original information; but for voice and video these factors are highly influential, therefore networks and protocols that offer a high degree of QoS (quality of service) are required. Voice over IP (VoIP) defines the routing systems and protocols necessary for the transmission of voice conversations over the Internet, which is a packet-switched network based on the TCP/IP protocol for sending information.

There are currently two main VoIP architectures for voice transmission over the Internet that are widely used: SIP (*Session initiation Protocol*, a standard developed by the IETF, identified as RFC 3261, 2002).

SIP is a signaling protocol for establishing calls and conferences on IP networks. The start of the session, change or termination thereof, are independent of the type of media or application that will be used in the call; a session can include various types of data, including audio, video, and many other H.323 formats

H.323 was the first international multimedia communications standard, facilitating the convergence of voice, video, and data. It was initially built for networks based on packet switching, in which it found its strength by integrating with IP networks, being a protocol widely used in VoIP.

10.1.1 SIP Architecture

The SIP protocol (Session initiation Protocol) was developed by the IETF MMUSIC (Multimedia Session Control) group, defining a signaling and control architecture for VoIP. Initially it was published in February 1996 in RFC 2543, now obsolete with the publication of the new version RFC 3261 that was published in June 2002.

The purpose of SIP is communication between multimedia devices. SIP makes this communication possible thanks to two protocols that are RTP/RTCP and SDP. The RTP protocol is used to transport the voice data in real time (same as for the H.323 protocol, while the SDP protocol is used for the negotiation of the capabilities of the participants, type of encoding, etc.) SIP was designed according to the Internet model.

It is an end-to-end signaling protocol that implies that all the logic is stored in the end devices (except for the routing of SIP messages). The connection status is also stored in the end devices . The price to pay for this distribution capacity and its great scalability is an overload in the header of the messages as a result of having to send all the information between the end devices.

SIP is an application-level signaling protocol for establishing and managing sessions with multiple participants. It is based on request and response messages and reuses many concepts from earlier standards such as HTTP and SMTP.

10.2 H323

H.323 was designed with one primary goal: To provide users with teleconferencing that has voice, video, and data capabilities over packet-switched networks. The continuous research and development of H.323 continues for the same purpose, and as a result, H.323 becomes the optimal standard to cover this kind of aspects. In addition, H.323 and the convergence of voice, video and data allow service providers to provide these kinds of facilities for users in a way that reduces costs while improving performance for the user . The standard was specifically designed with the following objectives: - To be based on existing standards, including H.320, RTP and Q.931 - To incorporate some of the advantages that packet-switched networks offer to transport data in real time . - To solve the problem posed by sending data in real time over packet switching networks. H.323 designers know that communication requirements differ from place to place, between users and between companies and obviously over time the communication requirements also change. Given these factors, the designers of H.323 defined it in such a way that companies that manufacture the equipment can add their own specifications to the protocol and can define other standards structures that allow devices to acquire new classes of features or capabilities.

10.2.1 IAX (*Inter-Asterisk eXchange*)

The IAX protocol corresponds to *Inter-Asterisk eXchange protocol*. As its name indicates, it was designed as a protocol for VoIP connections between Asterisk servers, although today it is also used for connections between clients and servers that support the protocol. The current version is IAX2 since the first version of IAX has become obsolete. It is a protocol designed and intended for use in VoIP connections, although it can support other types of connections (for example, video). The objectives of IAX are: Minimize the width of band used in VoIP control and multimedia transmissionsAvoid NAT (Network Address) problems Translation)-Support for transmitting dial plans Among the measures to reduce bandwidth, it is worth noting that IAX or IAX2 is a binary protocol instead of being a text protocol like SIP and that makes messages use less bandwidth. To avoid NAT problems, the IAX or IAX2 protocol uses UDP as the transport protocol, normally over port 4569, (IAX1 used port 5036), and both the signaling information and the data travel together (unlike SIP). and therefore makes you less prone to NAT problems and allows you to get past routers and firewalls more easily.

10.3 QoS Quality Of service VoIP

The rise of IP telephony is evident and the main reason is the reuse of resources and the decrease in the cost of calls over the Internet. However, if VoIP still lacks something, it is the quality of traditional telephone systems. Problems of this quality are often inherent to the use of the network (Internet and its speed and bandwidth) and may be solved in the future. Meanwhile, the better we know the problems that occur and their possible solutions, the better quality we will enjoy.

The main problems regarding the quality of service (QoS) of a VoIP network are Latency, Jitter, packet loss and Echo. In VoIP these problems can be solved by various techniques that are explained in the following following sections.

VoIP service quality problems are mainly derived from two factors:

1. The Internet is a system based on packet switching and therefore information does not always travel the same way. This produces effects such as packet loss or jitter
2. VoIP communications are in real time which causes effects such as echo, packet loss and delay or latency to be very annoying and harmful and must be avoided.

10.3.1 Jitter

Jitter is technically defined as the time variation in packet arrival, caused by network congestion, loss of synchronization, or by the different paths followed by the packets to reach the destination. Real-time communications (such as VoIP) are especially sensitive to this effect.

10.3.1.1 Causes

Jitter is an effect of connectionless data networks based on packet switching. As the information is discretized in packets, each one of the packets can follow a different route to reach the destination.

In general, it is a frequent problem in slow or congested links. It is expected that the increase of QoS (quality of service) mechanisms such as queue priority, bandwidth reservation or higher speed links (100Mb Ethernet, E3/T3, SDH) can reduce jitter problems in the future although It will continue to be a problem for quite some time.

10.3.1.2 Recommended Values

The jitter between the start and end point of the communication should be less than 100 ms. If the value is less than 100 ms, the jitter can be compensated appropriately. Otherwise it should be minimized.

10.3.1.3 Possible Solutions

The most widely adopted solution is the use of the jitter buffer. The jitter buffer basically consists of allocating a small queue or storage to go receiving the packages and serving them with a small delay. If any packet is not in the buffer (it was lost or has not arrived yet) it is discarded when necessary. Normally in IP phones (hardware and software) you can modify the buffers. An increase in the buffer implies less packet loss but more delay. A decrease implies less delay but more packet loss.

10.3.2 Latency

Latency is also called delay; it is technically defined in VoIP as the time it takes for a packet to get from the source to the destination.

10.3.2.1 Causes

It is not a specific problem of connectionless networks and therefore of VoIP. It is a general problem of telecommunication networks. For example, latency on links via satellite is very high due to the distances that the information must travel. Real-time (such as VoIP) and full- duplex communications are sensitive to this effect. It is the problem of ”stepping on us”. Like jitter , it is a common problem on slow or congested links.

10.3.2.2 Recommended Values

The latency or delay between the initial and final point of the communication should be less than 150 ms. The human ear is capable of detecting latencies of about 250 ms, 200 ms in the case of quite sensitive people. If that threshold is exceeded, communication becomes annoying.

10.3.2.3 Possible Solutions

There is no solution that can be easily implemented. Many times it depends on the equipment through which the packets pass, that is, on the network itself. You can try to reserve a bandwidth from source to destination or signal the packets with TOS values to try to let the equipment know that it is real-time traffic and treat it with higher priority , but currently these are not very effective measures since We do not have control of the network. If the latency problem is in our own internal network, we can increase the bandwidth or link speed or prioritize those packets within our network.

10.3.3 echo

Echo is also often known as reverberation. Echo is defined as a delayed reflection of the original acoustic signal . The echo is especially annoying the greater the delay and the greater its intensity, which becomes a problem in VoIP since the delays are usually greater than in the traditional telephone network.

10.3.3.1 Causes

The echo is produced by a technical phenomenon that is the conversion of 2 to 4 wires in telephone systems or by a return of the signal that is heard through the speakers and sneaks back through the microphone .

10.3.3.2 Recommended Values

The human ear is capable of detecting the echo when its delay with the original signal is equal to or greater than 10 ms. But another important factor is the intensity of the echo since normally the return signal has less power than the original. It is tolerable that it reaches 65 ms and an attenuation of 25 to 30 dB.

10.3.3.3 Possible Solutions

In this case there are two possible solutions to avoid this annoying effect.

- **Echo suppressors**: It consists of preventing the emitted signal from being returned by converting at times the full- duplex line into a line half-duplex in such a way that if communication is detected in one direction, communication in the opposite direction is prevented. The switching time of the echo suppressors is very short. Prevents full- duplex communication .
- **Echo Cancellers**: It is the system by which the sending device saves the information it sends in memory and is capable of detecting the same information in the return signal (perhaps attenuated and with noise). The device filters that information and cancels those components of the voice. It requires more processing time.

10.3.4 Packet loss (*Packet loss*)

10.3.4.1 Causes

Real-time communications are based on the UDP protocol. This protocol is not connection oriented and if there is a loss of packets they are not forwarded . In addition , the loss of packets is also produced by discarding packets that do not reach the receiver on time. However , the voice is quite predictive and if isolated packets are lost, the voice can be recomposed in a quite optimal way. The problem is greater when bursty packet losses occur.

10.3.4.2 Recommended Values

The maximum packet loss allowed so that communication is not degraded must be less than 1%. But it is quite dependent on the codec that is used. The higher the compression of the codec , the more pernicious is the effect of packet loss. A loss of 1% further degrades communication if the G.729 codec is used instead of G.711.

10.3.4.3 Possible Solutions

To avoid packet loss, a very effective technique in congested or low-speed networks is not to transmit silence. Much of the conversations are filled with moments of silence. If we only transmit when there is audible information, we free up the links enough and avoid congestion phenomena . In any case , this phenomenon may also be closely related to jitter and the jitter buffer.

This page has been intentionally left blank.

CHAPTER 11

RAID INSTALLATION GUIDE

This guide starts from the consideration that the «*Install Denwa UC Manual Partition*» option has been selected, which allows manual partitioning of storage devices.

11.1 Define the size of the partitions

When defining the dimensioning, the following considerations must be taken into account:

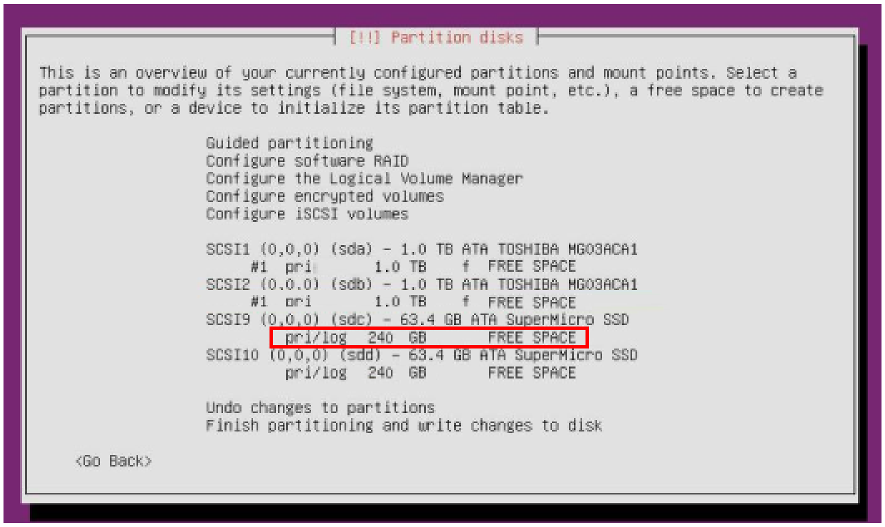
- You must create at least the following partitions:
  - «\boot» on the solid-state drive, for system boot files
  - «\\» on the solid-state drive, for the base OS (20GB minimum, 30GB recommended), for:
    - Operating System
    - System logs
    - Operating System user folders (« pbxadmin », «Denwa Support»)
    - Module files
  - «**swap**» on the solid state drive, 2GB to 8GB is recommended depending on your computer.
  - «\denwa» on the solid state disk, for all processes associated with the telephony engine
    - Telephony Engine
    - Databases
    - Web Interface
    - Recordings to be transferred to the FTP Server (if any)
  - «\persistent» on the mechanical disk (if any) for local storage of call recording

Queries If in doubt, consult the Denwa Technology Corp. support area .

11.2 Creating the partitions

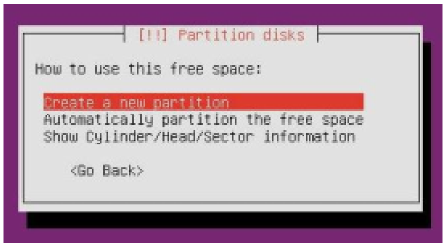
As a first step it is necessary to create all the partitions in «ext4» format without declaring their mount point (this will be done later). Storage devices participating in RAID arrays are required to be partitioned identically, giving each partition the same size.

1. Select disk



```
                         [!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

                   Guided partitioning
                   Configure software RAID
                   Configure the Logical Volume Manager
                   Configure encrypted volumes
                   Configure iSCSI volumes

                   SCSI1 (0,0,0) (sda) - 1.0 TB ATA TOSHIBA MG03ACA1
                        #1  pri       1.0 TB     f  FREE SPACE
                   SCSI2 (0.0.0) (sdb) - 1.0 TB ATA TOSHIBA MG03ACA1
                        #1  pri       1.0 TB     f  FREE SPACE
                   SCSI9 (0,0,0) (sdc) - 63.4 GB ATA SuperMicro SSD
                            pri/log   240  GB       FREE SPACE
                   SCSI10 (0,0,0) (sdd) - 63.4 GB ATA SuperMicro SSD
                            pri/log   240  GB       FREE SPACE

                   Undo changes to partitions
                   Finish partitioning and write changes to disk

    <Go Back>
```

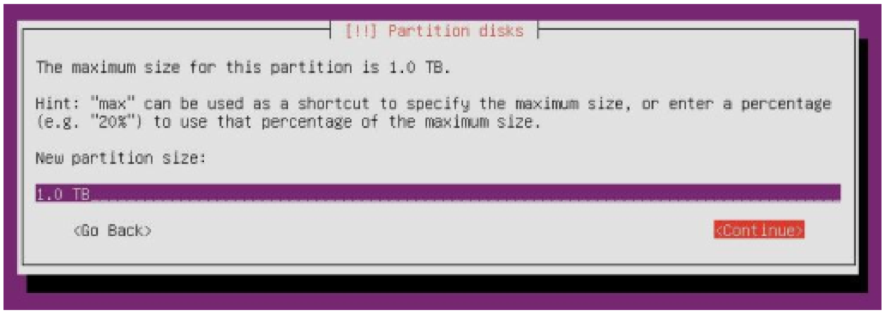
Figure 11.1: Creating the partitions: disk selection



```
          [!!] Partition disks

How to use this free space:

 Create a new partition
 Automatically partition the free space
 Show Cylinder/Head/Sector information

    <Go Back>
```

Figure 11.2: Creating the partitions: create a new partition

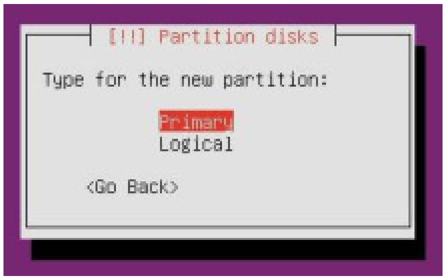
2. Assign size to each partition



```
                        [!!] Partition disks

The maximum size for this partition is 1.0 TB.

Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage
(e.g. "20%") to use that percentage of the maximum size.

New partition size:

1.0 TB_

    <Go Back>                                                          <Continue>
```

Figure 11.3: Creating the partitions: sizing

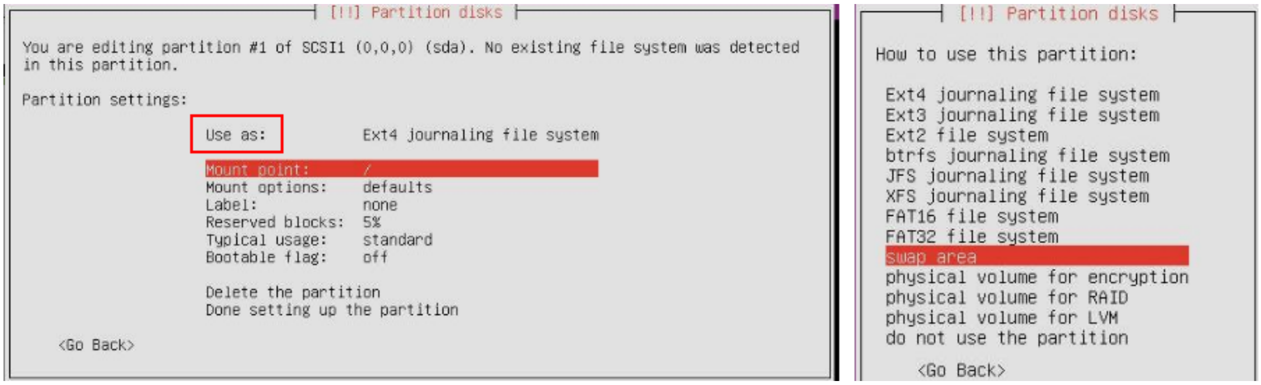
3. Define if the partition is primary or logical



```
[!!] Partition disks

Type for the new partition:

          Primary
          Logical

    <Go Back>
```

Figure 11.4: Creating the partitions: type of partition

4. Remove the mount point of all partitions and define them «ext4», except swap, which should be defined as «Swap Area »

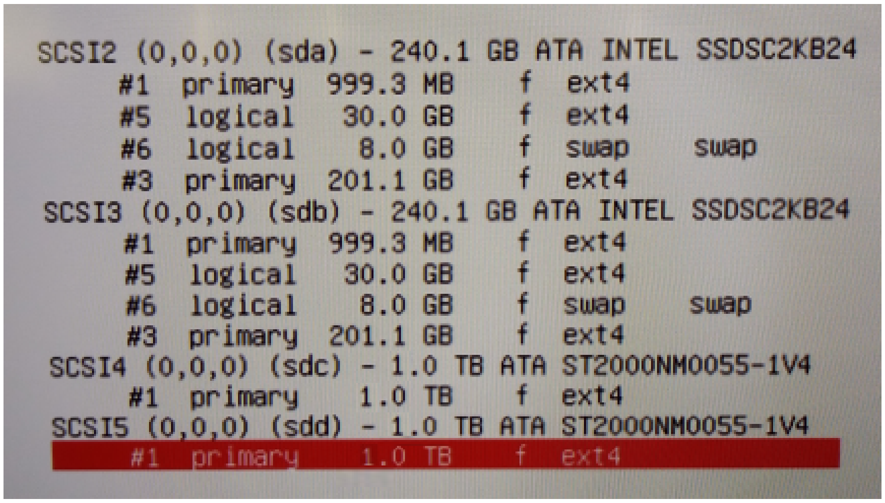


```
[!!] Partition disks

You are editing partition #1 of SCSI1 (0,0,0) (sda). No existing file system was detected
in this partition.

Partition settings:

          Use as:            Ext4 journaling file system

          Mount point:       /
          Mount options:     defaults
          Label:             none
          Reserved blocks:   5%
          Typical usage:     standard
          Bootable flag:     off

          Delete the partition
          Done setting up the partition

    <Go Back>
```

```
[!!] Partition disks

How to use this partition:

 Ext4 journaling file system
 Ext3 journaling file system
 Ext2 file system
 btrfs journaling file system
 JFS journaling file system
 XFS journaling file system
 FAT16 file system
 FAT32 file system
 swap area
 physical volume for encryption
 physical volume for RAID
 physical volume for LVM
 do not use the partition

    <Go Back>
```

Figure 11.5: Creating the partitions: file system format

5. Control equality of partitions between disks



```
SCSI2 (0,0,0) (sda) - 240.1 GB ATA INTEL SSDSC2KB24
      #1  primary  999.3 MB    f  ext4
      #5  logical   30.0 GB    f  ext4
      #6  logical    8.0 GB    f  swap    swap
      #3  primary  201.1 GB    f  ext4
SCSI3 (0,0,0) (sdb) - 240.1 GB ATA INTEL SSDSC2KB24
      #1  primary  999.3 MB    f  ext4
      #5  logical   30.0 GB    f  ext4
      #6  logical    8.0 GB    f  swap    swap
      #3  primary  201.1 GB    f  ext4
SCSI4 (0,0,0) (sdc) - 1.0 TB ATA ST2000NM0055-1V4
      #1  primary    1.0 TB    f  ext4
SCSI5 (0,0,0) (sdd) - 1.0 TB ATA ST2000NM0055-1V4
      #1  primary    1.0 TB    f  ext4
```

Figure 11.6: Creating the partitions: disk comparison

11.3 Configuring Software RAID

Create the RAIDs Assign type: RAID1 (mirror) (Join the identical partitions) Confirm use of 2 partitions for each RAID Spare devices : 0

11.4 Configuring mount points

11.5 Validation and saving of configurations

Part IV

Annex

CHAPTER 12

SIP PROTOCOL AND DEBUG

12.1 Components and Operation of a VoIP Network Definition of VoIP

VoIP comes from the English words *Voice Over Internet Protocol*. As the term says, VoIP attempts to allow voice to travel in IP packets and obviously over the Internet.

IP telephony combines two historically separate worlds: voice transmission and data transmission. It is about transporting the voice previously converted to data, between two distant points. This would make it possible to use data networks to make telephone calls, and therefore develop a single convergent network that is responsible for carrying out all types of communication, be it voice, data, video or any type of information.

Therefore, VoIP is not in itself a service but rather a technology that allows voice to be encapsulated in packets in order to be transported over data networks without the need for conventional switched circuits known as the PSTN, which are networks developed through over the years to transmit vocal signals.

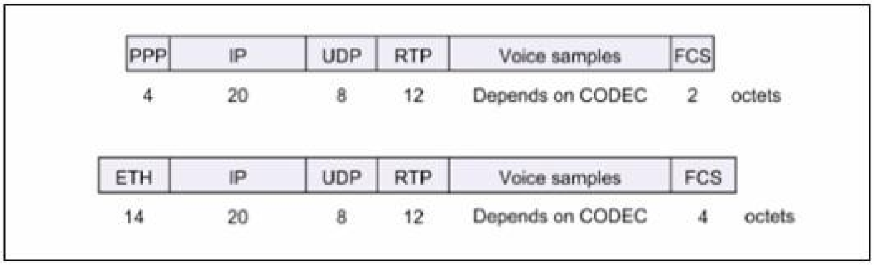
The PSTN was based on the concept of circuit switching, that is, the realization of a communication required the establishment of a physical circuit during the time it lasts, which means that the resources involved in the realization of a call cannot be used in another until the first one is finished, even during the silences that follow one another within a typical conversation.

On the other hand, IP telephony does not use physical circuits for the conversation, but sends multiple conversations through the same channel (virtual circuit) encoded in packets and in independent flows. When there is silence in a conversation, the data packets of other conversations can be transmitted over the network, which implies a more efficient use of it.

According to this, the advantages provided by VoIP networks are evident, since with the same infrastructure they could provide more services and also the quality of service and speed would be higher; but on the other hand there is also the great disadvantage of security, since it is not possible to determine the duration of the packet within the network until it reaches its destination and there is also the possibility of packet loss, since the IP protocol does not have this tool.

12.2 Encapsulation of a VoIP frame

Once the call has been established, the voice will be digitized and then transmitted across the network in IP frames. Voice samples are first encapsulated in RTP (Real Time Transport Protocol) and then in UDP or TCP before being transmitted in an IP frame. The following figure shows an example of a VoIP frame over a LAN and WAN.



PPP	IP	UDP	RTP	Voice samples	FCS	
4	20	8	12	Depends on CODEC	2	octets

ETH	IP	UDP	RTP	Voice samples	FCS	
14	20	8	12	Depends on CODEC	4	octets

Figure 12.1: SIP Protocol and Debug: Encapsulation

12.3 Session Initiation Protocol

Session Initiation Protocol (SIP or Session Initialization Protocol) is a simple signaling protocol used for Internet telephony and videoconferencing. Based on the Simple Mail Transport Protocol (SMTP) and on the Hypertext Transfer Protocol (HTTP) it was developed by the IETF MMUSIC Working Group with the intention of being the standard for the initiation, modification and termination of interactive user sessions where multimedia elements such as video, voice, instant messaging, online games and virtual reality are involved. SIP is one of the signaling protocols for voice over IP. SIP is fully defined in RFC 2543 and in RFC 3261.

SIP is an application layer protocol independent of the underlying packet protocols (TCP, UDP, ATM, X.25). SIP is based on a client-server architecture in which clients initiate calls and servers answer calls. It is an open protocol based on standards, widely supported and is not dependent on a single equipment manufacturer.

SIP is a newer protocol than H.323 and does not have industry maturity and support at the same time. However, due to its simplicity, scalability, modularity, and ease with which it integrates with other applications, this protocol is attractive for use in packetized voice architectures. SIP can establish two-party (ordinary calls), multi-party (everyone can hear and talk), and multicast (one sender, many receivers) sessions. Sessions can contain audio, video, or data. SIP only handles session establishment, management, and termination.

Some of the key features that SIP offers are:

- Address resolution, name mapping and call redirection.
- Dynamic discovery of the average capabilities of the endpoint, by using the Session Description Protocol (SDP).
- Dynamic discovery of endpoint availability.
- Origination and management of the session between the host and the endpoints.

12.3.1 Benefits of SIP

Some of the key benefits of SIP are:

- **Simplicity**: SIP is a very simple protocol. The software development time is very short compared to traditional telephony products. Due to the similarity of SIP to HTTP and SMTP, code refusal is possible.
- **Extensibility**: SIP has learned from HTTP and SMTP and has built an exquisite set of extensibility and compatibility features.
- **Modularity**: SIP was designed to be highly modular. A key feature is its independent use of protocols. For example, it sends invitations to the parties to the call, independent of the session itself.
- **Scalability**: SIP offers two scalability services:
- **Server Processing**: SIP has the ability to be *Stateful* or *Stateless*.
- **Conference Arrangement**: Since there is no requirement for a multipoint central controller, conference coordination can be completely distributed or centralized.
- **Integration**: SIP has the ability to integrate with the Web, E-mail, streaming media applications, and other protocols.
- **Interoperability**: Because it is an open standard, SIP can offer interoperability between platforms from different vendors.

12.3.2 Protocol design

SIP is an application layer protocol and can run on top of either UDP or TCP.
SIP clients use port 5060 in TCP (*Transmission Control Protocol*) and UDP (*User Datagram Protocol*) to connect with SIP servers. In case of using a secure protocol such as SIPS, the port to use is 5061, this point will be discussed later when we talk about TLS (*Transport Security Protocol*).
SIP is used simply to start and end voice and video calls. All voice/video communications go over RTP (*Real-time Transport Protocol*).

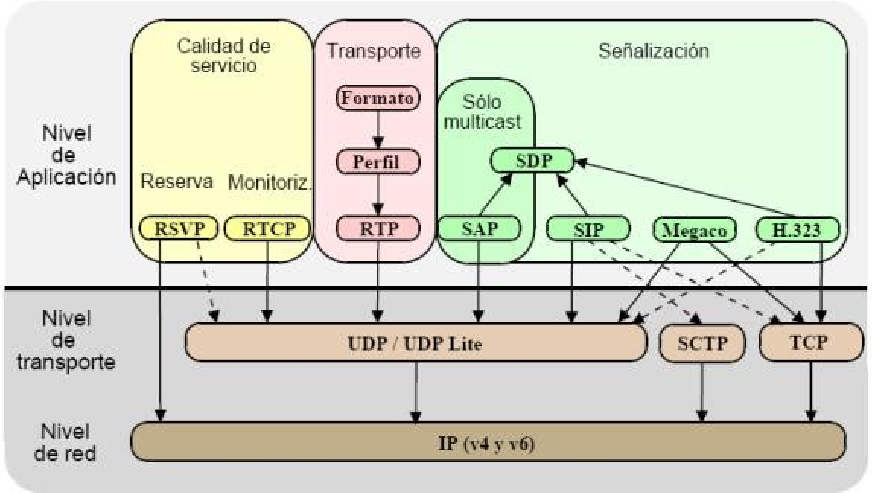


Figure 12.2: SIP Protocol and Debug: Design

The first proposed version of the standard (SIP 2.0) was defined in RFC 2543. The protocol was clarified in RFC 3261, although many implementations are still using draft versions. Note that the version number is still 2.0.

12.3.3 Transport layer in SIP

SIP can use in its transport layer (Layer 4 in the OSI model) both UDP, TCP and TLS *Transport Layer Security* (referring to TLS over TCP). TLS is used to provide a certain level of security, encrypting information that is usually vulnerable to attack since it is sent in plain text.

The use of SIP over TCP without encryption is tending to disappear in non-paid or VoIP uses on the Internet due to the simplicity of UDP, the increasing reliability of networks and the useless need for relaying on a voice or media connection where it is present. present the transmission in real time.

In any case, it is important that a high-performance User Agent (UA) such as a sipphone, for example, supports both TCP and UDP as transport protocols, since if a UA tries to establish a TCP session with its peer, and it does not support TCP in its transport layer, the session cannot be established, leading to an ICMP ”Not Supported” message or a reset of the TCP connection, where the calling end must change the transport protocol of its request message over UDP to create compatibility in the network and establish the connection. The most optimal case is compatibility at the first attempt to take advantage of the capacity and resources of the network.

Another crucial point when deciding the protocol to be used in the transport layer is the maximum segment size, which is directly involved with the codec to be used, taking into account the notable compression difference between, for example, G .729, G.711, etc. RFC 3261 defines the mandatory use of UDP and TCP, the latter in case some type of packet fragmentation that exceeds the MTU is necessary.

The negotiation of codecs, ports and multimedia services is carried out in the SDP (Session Description Protocol) embedded in SIP, where the commonly used SIP ports are 5060 in plain text (UDP and TCP) and port 5061 in case of TLS. However, in practice the use of ports between 5060 and 5070 may occur.

12.3.4 SIP network elements

The physical terminals known as user agents (UA) can be devices themselves or software installed on a PC, with the appearance and/or functionality of traditional telephones, but using SIP and RTP for communication. They are commercially available from many manufacturers. Some of them use electronic numbering (ENUM) or DUNDi to translate existing phone numbers to SIP addresses using DNS (*Domain Name Server*), thus calling other SIP users bypassing the telephone network, thus the service provider The service normally acts as a gateway to the public switched telephone network for traditional telephone numbers (charging for it).

SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users to serve them, enable the implementation of call routing policies, and provide added capabilities to the user. It also provides logging functions that allow the user to report their current location to proxy servers.

Although two SIP terminals can communicate without the intervention of SIP infrastructures (which is why the protocol is defined as point-to-point), this approach is impractical for a public service. There are various softswitch implementations (from Nortell, Sonus, Huawei, and many more) that can act as proxy and registry items. Other companies, such as Ubiquity Software and Dynamicsoft have products whose implementation is standards-based, built on top of the Java JAIN specification.

12.3.5 SIP protocol messages

12.3.5.1 SIP addresses

SIP works on a simple premise of client-server operation. Clients or endpoints are identified by unique addresses defined as URL's, that is, the addresses come in a format very similar to an email address, so that Web pages can contain them, which allows clicking on a link to start a phone call.

- SIP addresses are always in the format of user@host.
- The user can be: name, telephone number.
- The host can be: domain (DNS), network address (IP). b) SIP MESSAGES:

SIP uses messages for call connection and control. There are two types of SIP messages: request and response messages. SIP messages are defined as follows:

- **INVITE**: Requests the initiation of a call. The header fields contain:
  - Source address and destination address.
  - The subject of the call.
  - Priority of the call.
  - Call routing requests.
  - Preferences for user location.
- **TRYING**: Indicates that the Proxy server is trying to establish communication.
- **RINGING**: Call notice indication.
- **BYE**: Requests the termination of a call between two users.
- **REGISTER**: Informs a registration server about the current location of the user.
- **ACK**: Used to facilitate a reliable exchange of messages between peers. Confirmation of different fields of the INVITE message.
- **CANCEL**: Cancels a pending request.
- **OPTIONS**: Request information from a Host about its own capabilities. It is used before initiating the call to find out if that host is capable of transmitting VoIP etc.
- **200 OK**: It is used to send satisfactory confirmations of different events.
- **INFO**: Used for signaling media sessions.

12.3.5.2 PC to PC call over TCP

To establish a call, the caller creates a TCP connection with the called party. The connection is made using a three-way agreement.

- Sends an INVITE message in a TCP packet, indicating the caller's destination address, capacity, media types, and formats.
- If the called party accepts the call, it responds with an HTTP type response code (200 for acceptance). You can also optionally provide information about your capabilities, media types, and formats.
- The caller responds with an ACK message to terminate the protocol and acknowledge receipt of the 200 message.
- At this point, they can start streaming data using the RTP protocol.
- The data flow is controlled by the RTCP protocol.
- Anyone can request the termination of the call by sending a BYE message.
- When the other side confirms its reception, the call is terminated.

12.3.6 SIP calls and transactions

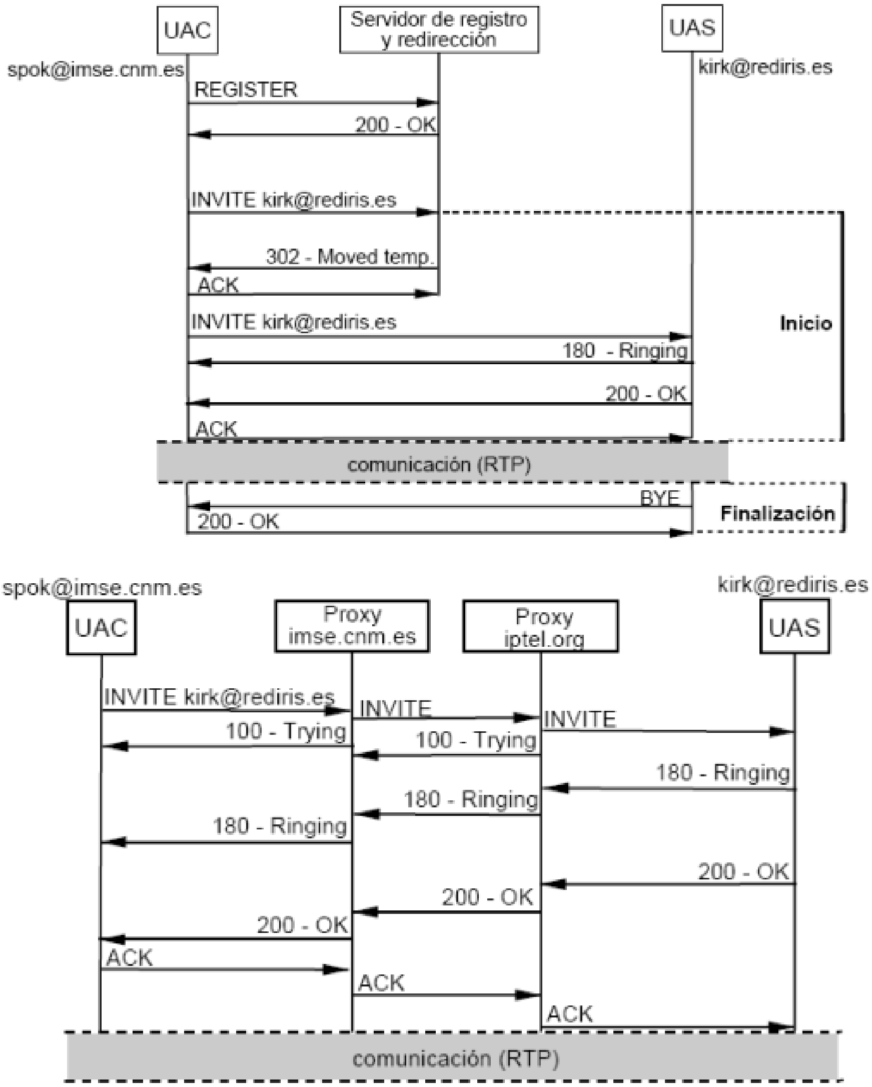


Figure 12.3: SIP Protocol and Debug: Transactions

12.3.6.1 Real-time Transport Protocol

RTP stands for ***R****eal-time* ***T****ransport* ***P****rotocol* (Real Time Transport Protocol), UDP on ports 10000 to 20000. It is a protocol application level (not transport level, as its name might suggest) used for the transmission of information in real time, such as audio and video.

It is developed by the IETF Audio and Video Transport Working Group, first published as a standard in 1996 as RFC 1889, and later updated in 2003 as RFC 3550, which is Internet Standard STD 64. published as a multicast protocol, although it has been used in various unicast applications. It is frequently used in streaming systems, along with RTSP, video conferencing and push to talk systems (in conjunction with H.323 or SIP). It also represents the basis of the VoIP industry.

RFC 1890, made obsolete by RFC 3551 (STD 65), defines a profile for audio and video conferencing with minimal control. RFC 3711, on the other hand, defines

SRTP (Secure Real-time Transport Protocol), an extension of the RTP profile for audio and video conferencing that can optionally be used to provide confidentiality, message authentication, and forwarding protection for audio and video streams. video. It goes hand in hand with RTCP (RTP Control Protocol) and sits on top of UDP in the OSI model.

- **V** (Version Number): 2 bits. The version defined by the current specification is 2.
- **P** (Padding): 1 bit. If the padding bit is set, there are one or more bytes at the end of the packet that are not part of the payload. The last byte in the packet indicates the number of padding bytes. Padding is used by some encryption algorithms.
- **X** (Extension): 1 bit. If the extension bit is set, then the sticky header is followed by a header extension. This extension mechanism enables implementations to add information to the RTP header.
- **CC** (CSRC Count): 4 bits. The number of CSRC identifiers that follow the sticky header. If the CSRC count is zero, then the synchronization source is the source of the payload.
- **M** (Marker): 1 bit. A marker bit defined by the particular media profile.
- **PT** (Payload): 7 bits. An index into a media profile table that describes the payload format. Payload mappings for audio and video are specified in RFC 1890.
- **Sequence Number**: 16 bits. A unique packet number that identifies the packet's position in the packet sequence. The packet number is incremented by one for each packet sent.
- **Timestamp**: 32 bits. It reflects the sampling time of the first byte in the payload. Several consecutive packets can have the same timestamp if they are logically generated at the same time - for example, if they are all part of the same video frame.
- **Synchronization Source (SSRC)**: 32 bits. Identifies the synchronization source. If the CSRC count is zero, then the payload source is the sync source. If the CSRC count is non-zero, then the SSRC identifies the mixer.
- **Content Source (CSRC)**: 32 bits each. Identifies the contributing sources for the payload. The number of contributing sources is indicated by the CSRC account field; There can be more than 16 contributing sources. If there are multiple contributing sources, then the payload is the mixed data from those sources.

12.4 Troubleshooting

12.4.1 Objectives

- Scope of the SIP protocol and its operation.
- Analysis of the IP packet, network layer, transport layer and application layer (SIP). Analysis of the establishment of a call. (SDP etc.)
- SIP protocol messages:
  - INVITE
  - Trying
  - Ringing
  - 200 okay
  - BYE

  - ▢ REGISTER
  - ▢ ACK
  - ▢ CANCEL
  - ▢ OPTIONS
- Verify the functioning of the protocol in the tests carried out.

12.4.2 Mockup

In the following graph we can see the diagram of the model used to make the captures.

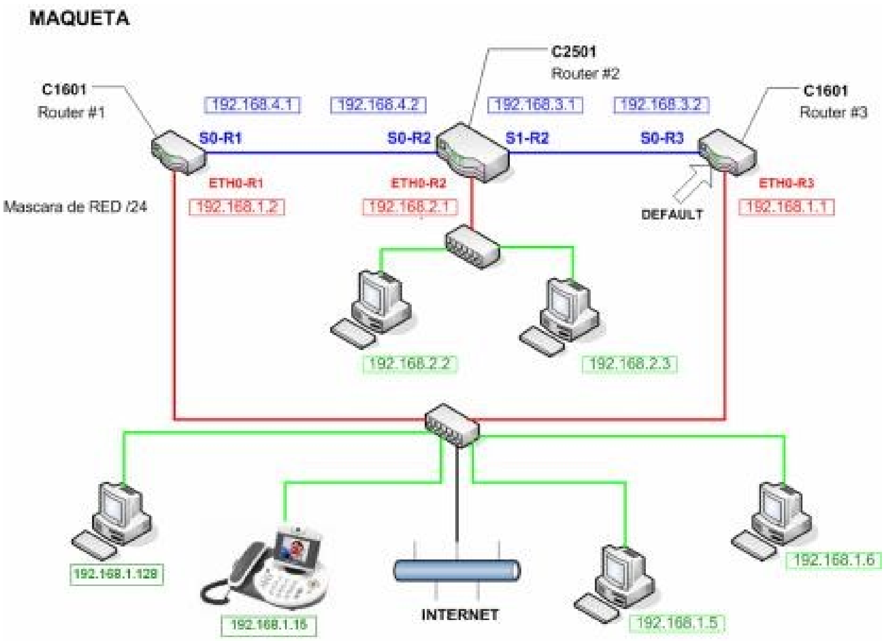


Figure 12.4: SIP Protocol and Debug: Mockup

12.4.3 Scenarios

12.4.3.1 Successful call from softphone to videophone

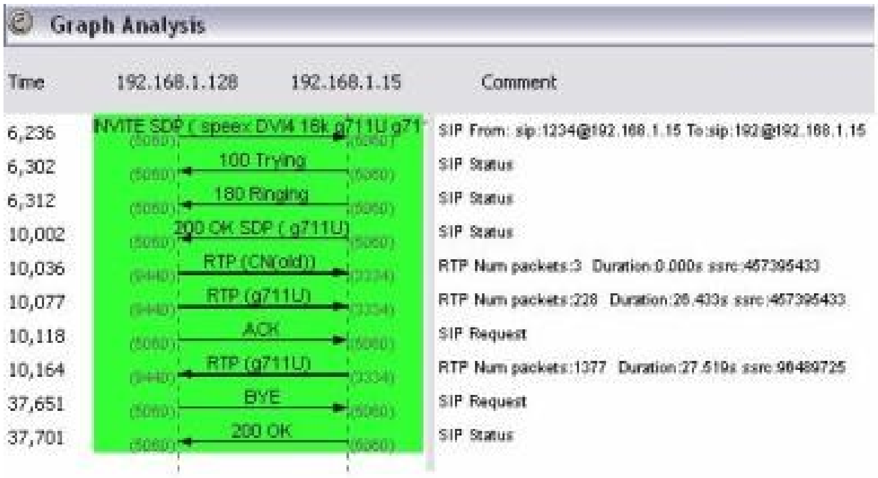
12.4.3.1.1 Objective Observe and analyze the establishment, course and disconnection of a communication with both available devices.

12.4.3.1.2 Development To achieve the proposed objective, the softphone was configured in peer to peer mode, this is because the tests carried out were within the same network without the intervention of a SIP proxy. This configuration is because the device should be registered to a Proxy (in this case the SIP phone) to make or receive calls. The IP address configured on the PC where the Eyebeam was installed was 192.168.1.128, as will be seen later in the screenshot, it is who initiates the communication. The ports configured in the software were from 5060 to 5062 and the enabled codecs were G.711, G.729, etc.

Figure 12.5: SIP Protocol and Debug: Softphone

The configuration in the videophone was basically the assignment of the IP address 192.168.1.15, in a static way. The codecs are not configurable on the phone used, the only codec it supports is G.711 A-law. In addition, to carry out internal network communications, the device must not be registered in any Proxy.

12.4.3.1.3 Execution To perform the test, a call was generated to the IP address of the SIP phone from the eyebeam. When the incoming call was detected it was accepted. After a few seconds from the softphone the call ended. The following graph shows the exchange of messages in the capture made from the PC where the softphone was located.



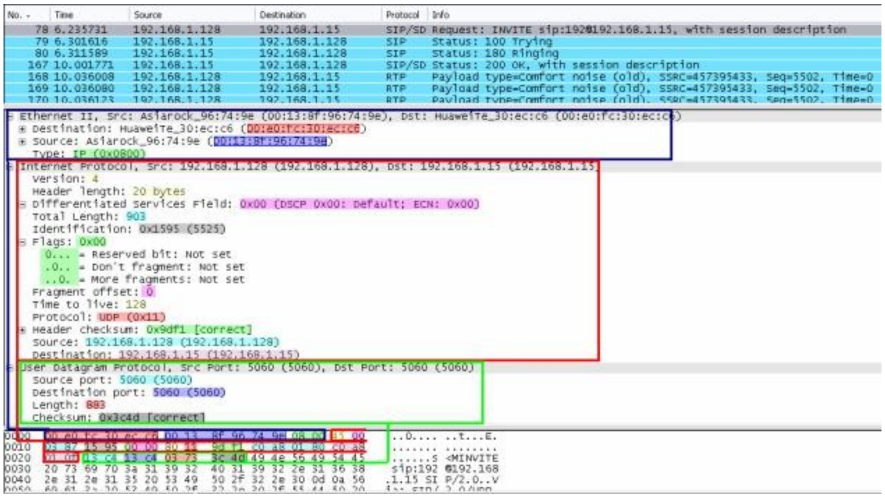
Time	192.168.1.128		192.168.1.15	Comment
6,236	(5060)	INVITE SDP (speex DVI4 16k g711U g71	(5060)	SIP From: sip:1234@192.168.1.15 To:sip:192@192.168.1.15
6,302	(5060)	100 Trying	(5060)	SIP Status
6,312	(5060)	180 Ringing	(5060)	SIP Status
10,002	(5060)	200 OK SDP (g711U)	(5060)	SIP Status
10,036	(9440)	RTP (CN(old))	(3334)	RTP Num packets:3 Duration:0.000s ssrc:467395433
10,077	(9440)	RTP (g711U)	(3334)	RTP Num packets:228 Duration:26.433s ssrc:467395433
10,118	(5060)	ACK	(5060)	SIP Request
10,164	(9440)	RTP (g711U)	(3334)	RTP Num packets:1377 Duration:27.519s ssrc:98489725
37,651	(5060)	BYE	(5060)	SIP Request
37,701	(5060)	200 OK	(5060)	SIP Status

Figure 12.6: SIP Protocol and Debug: Flow

As can be seen, the communication follows the aforementioned theoretical exchange of messages. The establishment of the call begins with an Invite message from the softphone, where an SDP (session description protocol) message is sent encapsulated over SIP, in order to negotiate codecs, ports, etc. This protocol will be analyzed in more detail in the following screenshot. Then the next message is a Trying sent by the sip phone in response to the Invite received, then in the same direction a Ringing message is sent to confirm that the incoming call is being notified. When accepting the communication (simply by lifting the tube on the videophone) it sends a 200 OK message with an SDP message, encapsulated over sip, proposing the codec to be used (G.711 U-Law). Next, RTP (real-time transport protocol) packets are sent, with Comfort noise payload, this packet is used to save bandwidth during voice silences, emulating noise at the other end, so that the user does not have the sensation of interruption of communication due to silences.

The sip phone confirms the negotiation with an ACK message and then begins the audio exchange through RTP, the protocol used for media exchange. In this sense, it is important to clarify that sip is the protocol used for signaling and in this communication stage does not appear. Finally, the communication is terminated from the softphone side and it sends a BYE sip message, to which the other end responds with 200 ok to confirm the end of the call.

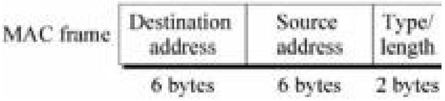
The analysis begins with the first message sent, which is called INVITE. The capture of the corresponding packet is shown below:



```
No. -  Time         Source          Destination     Protocol Info
    78 6.235731     192.168.1.128   192.168.1.15    SIP/SD  Request: INVITE sip:192@192.168.1.15, with session description
    79 6.301616     192.168.1.15    192.168.1.128   SIP     Status: 100 Trying
    80 6.311589     192.168.1.15    192.168.1.128   SIP     Status: 180 Ringing
   167 10.001771    192.168.1.15    192.168.1.128   SIP/SD  Status: 200 OK, with session description
   168 10.036008    192.168.1.128   192.168.1.15    RTP     Payload type=Comfort noise (old), SSRC=457395433, Seq=5502, Time=0
   169 10.036080    192.168.1.128   192.168.1.15    RTP     Payload type=Comfort noise (old), SSRC=457395433, Seq=5502, Time=0
   170 10.036123    192.168.1.128   192.168.1.15    RTP     Payload type=Comfort noise (old), SSRC=457395433, Seq=5502, Time=0

⊟ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
  ⊞ Destination: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
  ⊞ Source: Asiarock_96:74:9e (00:13:8f:96:74:9e)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
    Version: 4
    Header length: 20 bytes
  ⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 903
    Identification: 0x1595 (5525)
  ⊟ Flags: 0x00
      0... = Reserved bit: Not set
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0x9df1 [correct]
    Source: 192.168.1.128 (192.168.1.128)
    Destination: 192.168.1.15 (192.168.1.15)
⊟ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
    Source port: 5060 (5060)
    Destination port: 5060 (5060)
    Length: 883
    Checksum: 0x3c4d [correct]

0000  00 e0 fc 30 ec c6 00 13  8f 96 74 9e 08 00 45 00   ..0.... ..t...E.
0010  03 87 15 95 00 00 80 11  9d f1 c0 a8 01 80 c0 a8   ........ ........
0020  01 0f 13 c4 13 c4 03 73  3c 4d 49 4e 56 49 54 45   .......s <MINVITE
0030  20 73 69 70 3a 31 39 32  40 31 39 32 2e 31 36 38    sip:192 @192.168
0040  2e 31 2e 31 35 20 53 49  50 2f 32 2e 30 0d 0a 56   .1.15 SI P/2.0..V
```

Figure 12.7: SIP Protocol and Debug: Packet Capture

Here you can see the header at the link layer level in the upper blue box, let's remember its structure:



MAC frame	Destination address	Source address	Type/ length
	6 bytes	6 bytes	2 bytes

Figure 12.8: SIP Protocol and Debug: Link Layer Header

As you can see in the screenshot, the protocol used is Ethernet, therefore the third field indicates which protocol the next header corresponds to. In the case of being 802.3, this field reflects the length of the real Data field. We say real because 802.3 is in charge of controlling the minimum frame length, filling in the Data field if necessary. That is why it is necessary to indicate the real length of the Data field, to be able to discard the padding if there was one. If this field has a value greater than 1536, it is Ethernet, otherwise we would be talking about 802.3.

It is possible to see the destination MAC address highlighted in red: 00:e0:fc:30:ec:c6, where the first 24 bits indicate the manufacturer of the device, in this case it would be HuaweiTe_30:ec:c6, because it is Huawei Technologies the manufacturer.

The source MAC address highlighted in blue is: 00:13:8f:96:74:9e (Asiarock_96:74:9e), where Asiarock is the manufacturer of the network card of the pc on which the software is installed. software. Then in the next field, highlighted in green, we can see that the encapsulating network protocol is ip.

Next, the IP header boxed in red in the previous capture is analyzed.

The structure of the ip header is as follows:

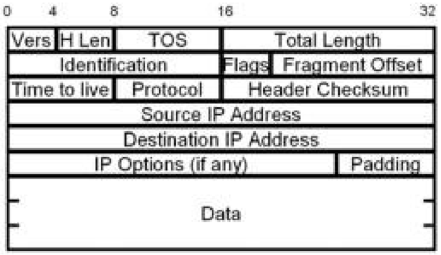


Figure 12.9: SIP Protocol and Debug: IP Header

- In this case we can see that it is an IP version 4 datagram and is 20 bytes long (fields highlighted in yellow), it is important to clarify that the value of this last field corresponds to 32-bit words, so Therefore, the value that appears is 5. That is, 5 x 32 bits=160 bits=20 Bytes, from this value we can infer that it is a datagram without options, otherwise the header would have a size greater than 20 Bytes.
- Below we see that the Type of Service field (highlighted in purple) has a null value, no distinction is made for this datagram in terms of reliability, priority, delay or throughput.
- The next field (highlighted in light blue) is the total size of the datagram that has a value of 903 Bytes.
- Then the identification field (in gray) of the packet shows a value of 5525 that serves to distinguish it from other packets, this is necessary to identify the fragments corresponding to a datagram that has been fragmented.
- We see that the flags field (in green) has a null value, that is to say that the datagram can be fragmented (Don't fragment=0) and that either it has not been fragmented or it is the last fragment.
- Then the next fragment offset field (in purple) is zero, this means that it is the first fragment or it has not been fragmented. From these last two values we infer that the datagram was not fragmented.
- The Time to Live field (in yellow) has a value of 128, meaning that this packet could go through a maximum of 128 networks until it reaches its destination, this value decreases for each hop, if it reaches 1, it will be discarded the package.
- The next field indicates the protocol that contains the payload, here it can be seen that the protocol used in the transport layer is UDP, the value is 9 for this protocol.
- Next we have the checksum (in green), which is used to control header errors, in this case we see that the header does not contain errors.
- The next fields are the source and destination IP addresses respectively. In this case, 192.168.1.128 is the one who generated the datagram and 192.168.1.15 is the destination of said datagram. (in light blue and gray respectively)

The analysis continues with the next header, the transport header, which in this case, as previously mentioned, will use UDP. Let's remember its structure.

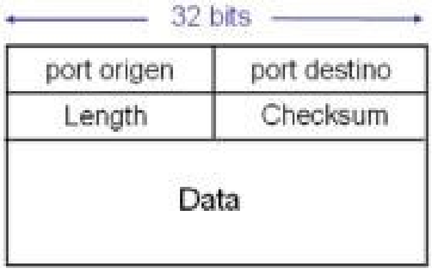
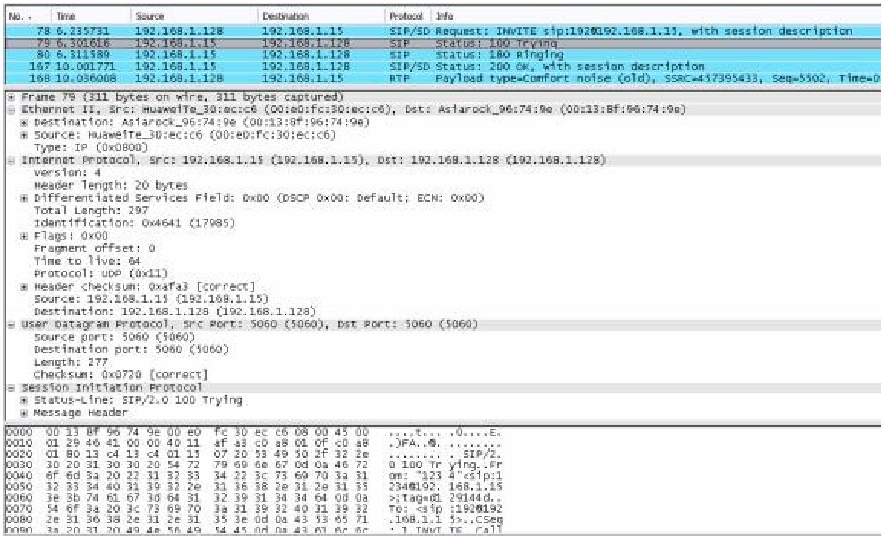


Figure 12.10: SIP Protocol and Debug: Transport Header

- The first field indicates the source port, in this case, since it is a sip port, it was expected to be 5060 as well as the destination port (highlighted in light blue and blue respectively).
- Then we see that the next field (in red) is the one that indicates the size of the UDP segment including the header, as expected it has a value of 883 Bytes, 20 Bytes less than the datagram, the size of its header.
- And finally (in gray) we have the checksum of the segment, this is optional and when it is not calculated, this field is set to zero. Here we see that it has been used and there were no errors.

In the application layer we have the message encapsulated in sip and its dependent protocols, in the next scenarios these protocols will be analyzed in more detail.

The next message that is sent in response to the previous INVITE is a TRYING, below we can see the capture:



```
No. -  Time        Source          Destination     Protocol Info
    78 6.235731    192.168.1.128   192.168.1.15    SIP/SD Request: INVITE sip:192@192.168.1.15, with session description
    79 6.301616    192.168.1.15    192.168.1.128   SIP    Status: 100 Trying
    80 6.311589    192.168.1.15    192.168.1.128   SIP    Status: 180 Ringing
   167 10.001771   192.168.1.15    192.168.1.128   SIP/SD Status: 200 OK, with session description
   168 10.036008   192.168.1.128   192.168.1.15    RTP    Payload type=Comfort noise (old), SSRC=437395433, Seq=5502, Time=0

⊞ Frame 79 (311 bytes on wire, 311 bytes captured)
⊟ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
  ⊞ Destination: Asiarock_96:74:9e (00:13:8f:96:74:9e)
  ⊞ Source: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 297
    Identification: 0x4641 (17985)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0xafa3 [correct]
    Source: 192.168.1.15 (192.168.1.15)
    Destination: 192.168.1.128 (192.168.1.128)
⊟ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
    Source port: 5060 (5060)
    Destination port: 5060 (5060)
    Length: 277
    Checksum: 0x0720 [correct]
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 100 Trying
  ⊞ Message Header

0000  00 13 8f 96 74 9e 00 e0  fc 30 ec c6 08 00 45 00   ....t... .0....E.
0010  01 29 46 41 00 00 40 11  af a3 c0 a8 01 0f c0 a8   .)FA..@. ........
0020  01 80 13 c4 13 c4 01 15  07 20 53 49 50 2f 32 2e   ........ . SIP/2.
0030  30 20 31 30 30 20 54 72  79 69 6e 67 0d 0a 46 72   0 100 Tr ying..Fr
0040  6f 6d 3a 20 22 31 32 33  34 22 3c 73 69 70 3a 31   om: "123 4"<sip:1
0050  32 33 34 40 31 39 32 2e  31 36 38 2e 31 2e 31 35   234@192. 168.1.15
0060  3e 3b 74 61 67 3d 64 31  32 39 31 34 34 64 0d 0a   >;tag=d1 29144d..
0070  54 6f 3a 20 3c 73 69 70  3a 31 39 32 40 31 39 32   To: <sip :192@192
0080  2e 31 36 38 2e 31 2e 31  35 3e 0d 0a 43 53 65 71   .168.1.1 5>..CSeq
0090  3a 20 31 20 49 4e 56 49  54 45 0d 0a 43 61 6c 6c   : 1 INVI TE..Call
```

Figure 12.11: SIP Protocol and Debug: TRYING

The analysis of this message is very similar to the previous one, only the most important differences at each level will be indicated.

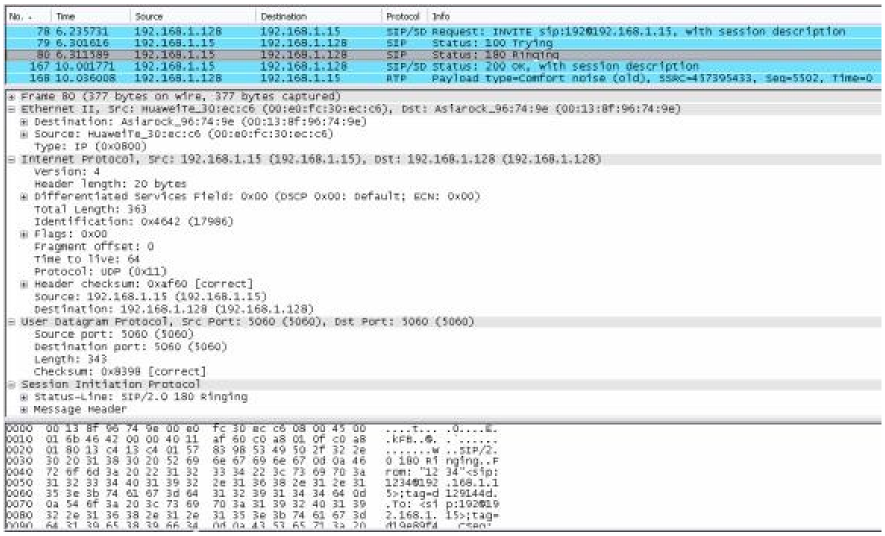
At the link level we can see that the mac address fields are inverted since the frame is sent in the reverse direction, from the videophone to the softphone. Again in the type field we see that there is IP as the next header.

At the network level, it can also be seen that the IP addresses have been inverted just like the Mac ones. As the most important difference, we can see that the size of the datagram decreased since this message does not encapsulate any auxiliary protocol.

Regarding the UDP header, it can be verified again that it differs by 20 bytes from the IP header.

The application-level message is then checked to be the TRYING mentioned above.

The next message is the RINGING, we can see its capture, here it is important to take into account that the direction of this datagram is the same as the previous one (trying), coinciding with what was theoretically anticipated.

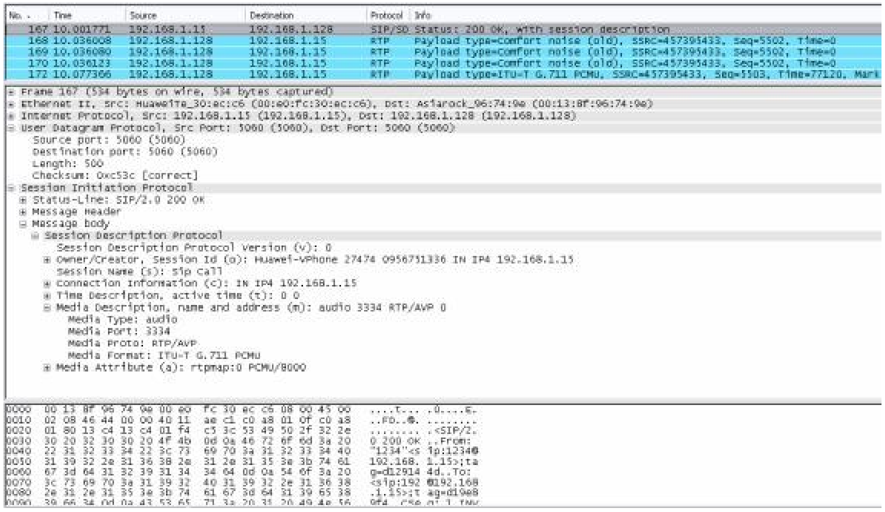


```
No. .  Time          Source          Destination     Protocol Info
   78 6.235731      192.168.1.128   192.168.1.15    SIP/SD Request: INVITE sip:192@192.168.1.15, with session description
   79 6.301616      192.168.1.15    192.168.1.128   SIP    Status: 100 Trying
   80 6.311589      192.168.1.15    192.168.1.128   SIP    Status: 180 Ringing
  167 10.001771     192.168.1.15    192.168.1.128   SIP/SD Status: 200 OK, with session description
  168 10.036008     192.168.1.128   192.168.1.15    RTP    Payload type=Comfort noise (old), SSRC=457395433, Seq=5502, Time=0

⊞ Frame 80 (377 bytes on wire, 377 bytes captured)
⊟ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
  ⊞ Destination: Asiarock_96:74:9e (00:13:8f:96:74:9e)
  ⊞ Source: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 363
    Identification: 0x4642 (17986)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0xaf60 [correct]
    Source: 192.168.1.15 (192.168.1.15)
    Destination: 192.168.1.128 (192.168.1.128)
⊟ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
    Source port: 5060 (5060)
    Destination port: 5060 (5060)
    Length: 343
    Checksum: 0x8398 [correct]
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 180 Ringing
  ⊞ Message Header

0000  00 13 8f 96 74 9e 00 e0  fc 30 ec c6 08 00 45 00   ....t... .0....E.
0010  01 6b 46 42 00 00 40 11  af 60 c0 a8 01 0f c0 a8   .kFB..@. .`......
0020  01 80 13 c4 13 c4 01 57  83 98 53 49 50 2f 32 2e   .......W ..SIP/2.
0030  30 20 31 38 30 20 52 69  6e 67 69 6e 67 0d 0a 46   0 180 Ri nging..F
0040  72 6f 6d 3a 20 22 31 32  33 34 22 3c 73 69 70 3a   rom: "12 34"<sip:
0050  31 32 33 34 40 31 39 32  2e 31 36 38 2e 31 2e 31   1234@192 .168.1.1
0060  35 3e 3b 74 61 67 3d 64  31 32 39 31 34 34 64 0d   5>;tag=d 129144d.
0070  0a 54 6f 3a 20 3c 73 69  70 3a 31 39 32 40 31 39   .To: <si p:192@19
0080  32 2e 31 36 38 2e 31 2e  31 35 3e 3b 74 61 67 3d   2.168.1. 15>;tag=
0090  64 31 39 65 38 39 66 34  0d 0a 43 53 65 71 3a 20   d19e89f4 ..CSeq: 
```

Figure 12.12: SIP Protocol and Debug: RINGING

Here it is verified in the mac and ip address fields that the direction of the message is again from the sip phone to the eyebeam. At the application level we can verify that it is a ringing message.

The next message is a 200 OK, sent from the softphone. The screenshot is shown below:



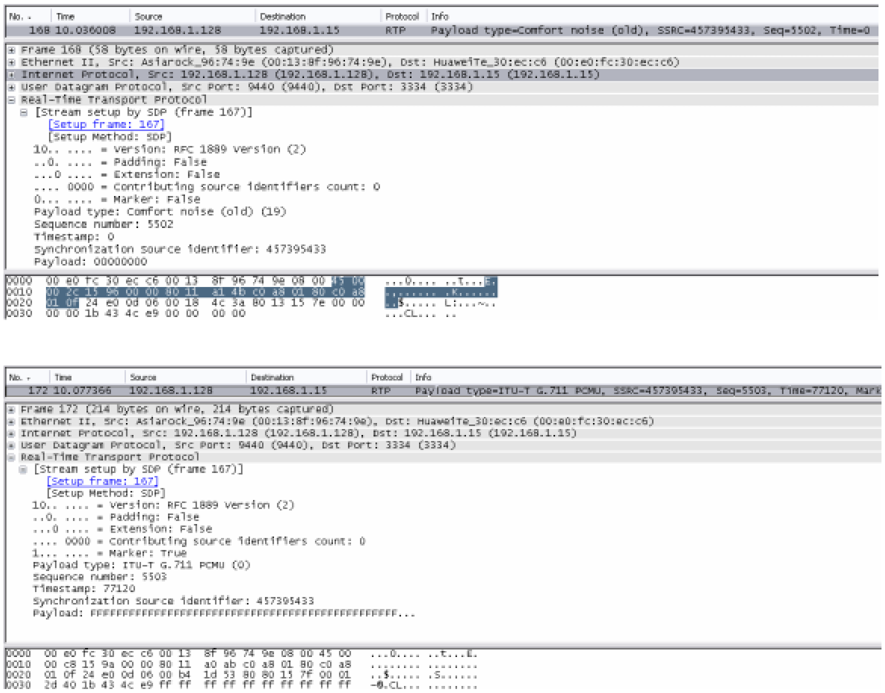
```
No. .  Time          Source          Destination     Protocol Info
  167 10.001771     192.168.1.15    192.168.1.128   SIP/SD Status: 200 OK, with session description
  168 10.036008     192.168.1.128   192.168.1.15    RTP    Payload type=Comfort noise (old), SSRC=457395433, Seq=5502, Time=0
  169 10.036080     192.168.1.128   192.168.1.15    RTP    Payload type=Comfort noise (old), SSRC=457395433, Seq=5502, Time=0
  170 10.036123     192.168.1.128   192.168.1.15    RTP    Payload type=Comfort noise (old), SSRC=457395433, Seq=5502, Time=0
  172 10.077366     192.168.1.128   192.168.1.15    RTP    Payload type=ITU-T G.711 PCMU, SSRC=457395433, Seq=5503, Time=77120, Mark

⊞ Frame 167 (534 bytes on wire, 534 bytes captured)
⊞ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
⊞ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
⊟ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
    Source port: 5060 (5060)
    Destination port: 5060 (5060)
    Length: 500
    Checksum: 0xc53c [correct]
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊞ Message Header
  ⊟ Message body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): Huawei-VPhone 27474 0956731336 IN IP4 192.168.1.15
        Session Name (s): sip call
      ⊞ Connection Information (c): IN IP4 192.168.1.15
      ⊞ Time Description, active time (t): 0 0
      ⊟ Media Description, name and address (m): audio 3334 RTP/AVP 0
          Media Type: audio
          Media Port: 3334
          Media Proto: RTP/AVP
          Media Format: ITU-T G.711 PCMU
      ⊞ Media Attribute (a): rtpmap:0 PCMU/8000

0000  00 13 8f 96 74 9e 00 e0  fc 30 ec c6 08 00 45 00   ....t... .0....E.
0010  02 08 46 44 00 00 40 11  ae c1 c0 a8 01 0f c0 a8   ..FD..@. ........
0020  01 80 13 c4 13 c4 01 f4  c5 3c 53 49 50 2f 32 2e   ........ .<SIP/2.
0030  30 20 32 30 30 20 4f 4b  0d 0a 46 72 6f 6d 3a 20   0 200 OK ..From: 
0040  22 31 32 33 34 22 3c 73  69 70 3a 31 32 33 34 40   "1234"<s ip:1234@
0050  31 39 32 2e 31 36 38 2e  31 2e 31 35 3e 3b 74 61   192.168. 1.15>;ta
0060  67 3d 64 31 32 39 31 34  34 64 0d 0a 54 6f 3a 20   g=d12914 4d..To: 
0070  3c 73 69 70 3a 31 39 32  40 31 39 32 2e 31 36 38   <sip:192 @192.168
0080  2e 31 2e 31 35 3e 3b 74  61 67 3d 64 31 39 65 38   .1.15>;t ag=d19e8
0090  39 66 34 0d 0a 43 53 65  71 3a 20 31 20 49 4e 56   9f4..CSe q: 1 INV
```

Figure 12.13: SIP Protocol and Debug: 200 OK

This message has the function of confirming the acceptance of the call.

Here it can be seen that there is an SDP message encapsulated in SIP in order to confirm the codec that will be used in the communication. In this case, G.711 U-Law is confirmed as previously anticipated. This will be discussed in detail later.

The following messages are from RTP, the first one contains a Comfort Noise message, this serves to accommodate the parameters of the FIR filters that will emulate a slight noise when detecting silences for user comfort. Here you see this type of message given the codec being used, G.711 does not come by default with this option, therefore this facility is made.

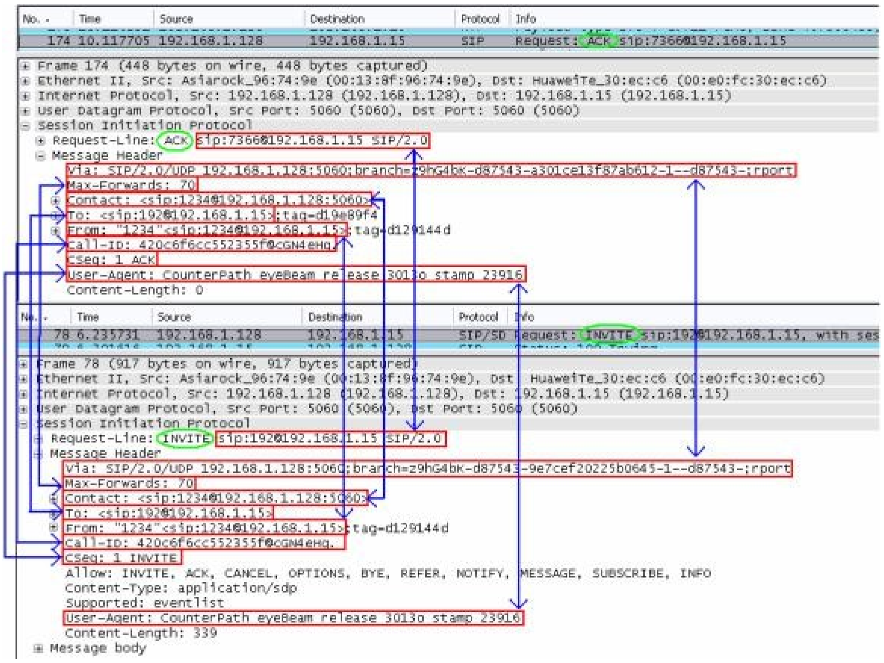


```
No. -  Time          Source          Destination     Protocol  Info
  168 10.036008     192.168.1.128   192.168.1.15    RTP       Payload type=Comfort noise (old), SSRC=457395433, Seq=5502, Time=0

⊞ Frame 168 (58 bytes on wire, 58 bytes captured)
⊞ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
⊞ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
⊞ User Datagram Protocol, Src Port: 9440 (9440), Dst Port: 3334 (3334)
⊟ Real-Time Transport Protocol
  ⊟ [Stream setup by SDP (frame 167)]
      [Setup frame: 167]
      [Setup Method: SDP]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: Comfort noise (old) (19)
    Sequence number: 5502
    Timestamp: 0
    Synchronization Source identifier: 457395433
    Payload: 00000000

0000  00 e0 fc 30 ec c6 00 13  8f 96 74 9e 08 00 45 00   ...0.... ..t...E.
0010  00 2c 15 96 00 00 80 11  a1 4b c0 a8 01 80 c0 a8   .,...... .K......
0020  01 0f 24 e0 0d 06 00 18  4c 3a 80 13 15 7e 00 00   ..$..... L:...~..
0030  00 00 1b 43 4c e9 00 00  00 00                     ...CL... ..
```

```
No. -  Time          Source          Destination     Protocol  Info
  172 10.077366     192.168.1.128   192.168.1.15    RTP       Payload type=ITU-T G.711 PCMU, SSRC=457395433, Seq=5503, Time=77120, Mark

⊞ Frame 172 (214 bytes on wire, 214 bytes captured)
⊞ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
⊞ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
⊞ User Datagram Protocol, Src Port: 9440 (9440), Dst Port: 3334 (3334)
⊟ Real-Time Transport Protocol
  ⊟ [Stream setup by SDP (frame 167)]
      [Setup frame: 167]
      [Setup Method: SDP]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    1... .... = Marker: True
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 5503
    Timestamp: 77120
    Synchronization Source identifier: 457395433
    Payload: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF...

0000  00 e0 fc 30 ec c6 00 13  8f 96 74 9e 08 00 45 00   ...0.... ..t...E.
0010  00 c8 15 9a 00 00 80 11  a0 ab c0 a8 01 80 c0 a8   ........ ........
0020  01 0f 24 e0 0d 06 00 b4  1d 53 80 80 15 7f 00 01   ..$..... .S......
0030  2d 40 1b 43 4c e9 ff ff  ff ff ff ff ff ff ff ff   -@.CL... ........
```

Figure 12.14: SIP Protocol and Debug: RTP

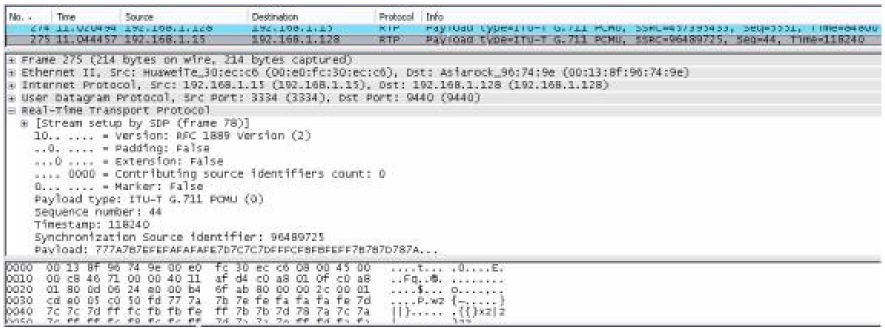
The following message is sent from the software to the videophone and it is an ACK, whose function is to confirm different values of the fields sent in the INVITE message. Let’s see below how these fields match in both messages.



```
No. .  Time       Source          Destination    Protocol  Info
   174 10.117705  192.168.1.128   192.168.1.15   SIP       Request: ACK sip:7366@192.168.1.15

+ Frame 174 (448 bytes on wire, 448 bytes captured)
+ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
+ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
+ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
  + Request-Line: ACK sip:7366@192.168.1.15 SIP/2.0
  - Message Header
      Via: SIP/2.0/UDP 192.168.1.128:5060;branch=z9hG4bK-d87543-a301ce13f87ab612-1--d87543-;rport
      Max-Forwards: 70
    + Contact: <sip:1234@192.168.1.128:5060>
    + To: <sip:192@192.168.1.15>;tag=d19e89f4
    + From: "1234"<sip:1234@192.168.1.15>;tag=d129144d
      Call-ID: 420c6f6cc552355f@cGN4eHq.
      CSeq: 1 ACK
      User-Agent: CounterPath eyeBeam release 3013o stamp 23916
      Content-Length: 0

No. .  Time       Source          Destination    Protocol  Info
    78 6.235731   192.168.1.128   192.168.1.15   SIP/SD    Request: INVITE sip:192@192.168.1.15, with ses

+ Frame 78 (917 bytes on wire, 917 bytes captured)
+ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst  HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
+ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
+ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
  + Request-Line: INVITE sip:192@192.168.1.15 SIP/2.0
  - Message Header
      Via: SIP/2.0/UDP 192.168.1.128:5060;branch=z9hG4bK-d87543-9e7cef20225b0645-1--d87543-;rport
      Max-Forwards: 70
    + Contact: <sip:1234@192.168.1.128:5060>
    + To: <sip:192@192.168.1.15>
    + From: "1234"<sip:1234@192.168.1.15>;tag=d129144d
      Call-ID: 420c6f6cc552355f@cGN4eHq.
      CSeq: 1 INVITE
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
      Content-Type: application/sdp
      Supported: eventlist
      User-Agent: CounterPath eyeBeam release 3013o stamp 23916
      Content-Length: 339
  + Message body
```

Figure 12.15: SIP Protocol and Debug: ACK

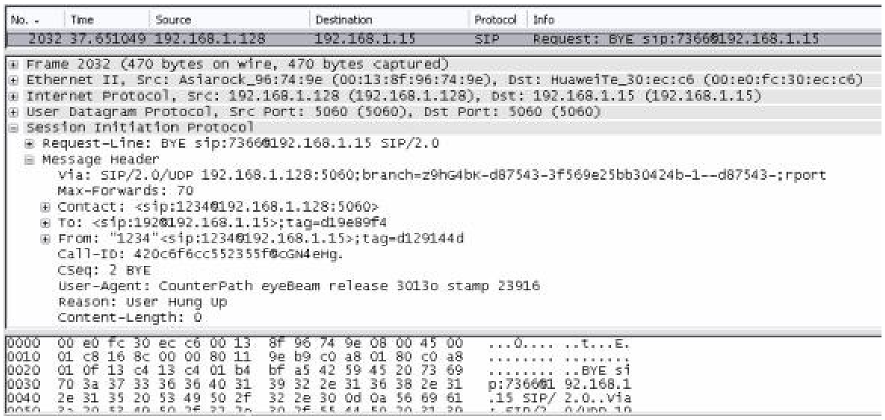
From now on the exchange of audio over RTP begins. As can be seen in the first graph of the exchange of messages, there are only packets from the videophone to the softphone, this is because at the time of the captures we did not have a microphone on the PC, therefore no packets were sent in this sense. Below is just an example RTP packet.



```
No. .  Time       Source          Destination     Protocol  Info
   275 11.044457  192.168.1.15    192.168.1.128   RTP       Payload type=ITU-T G.711 PCMU, SSRC=96489725, Seq=44, Time=118240

+ Frame 275 (214 bytes on wire, 214 bytes captured)
+ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
+ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
+ User Datagram Protocol, Src Port: 3334 (3334), Dst Port: 9440 (9440)
- Real-Time Transport Protocol
  + [Stream setup by SDP (frame 78)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 44
    Timestamp: 118240
    Synchronization Source identifier: 96489725
    Payload: 777A7B7EFEFAFAFAFE7D7C7C7DFFFCFBFBFEFF7B7B7D7B7A...

0000  00 13 8f 96 74 9e 00 e0  fc 30 ec c6 08 00 45 00   ....t... .0....E.
0010  00 c8 46 71 00 00 40 11  af d4 c0 a8 01 0f c0 a8   ..Fq..@. ........
0020  01 80 0d 06 24 e0 00 b4  6f ab 80 00 00 2c 00 01   ....$... o....,..
0030  cd e0 05 c0 50 fd 77 7a  7b 7e fe fa fa fa fe 7d   ....P.wz {~.....}
0040  7c 7c 7d ff fc fb fb fe  ff 7b 7b 7d 7b 7a 7c 7a   ||}..... .{{}{z|z
```

Figure 12.16: SIP Protocol and Debug: Audio over RTP

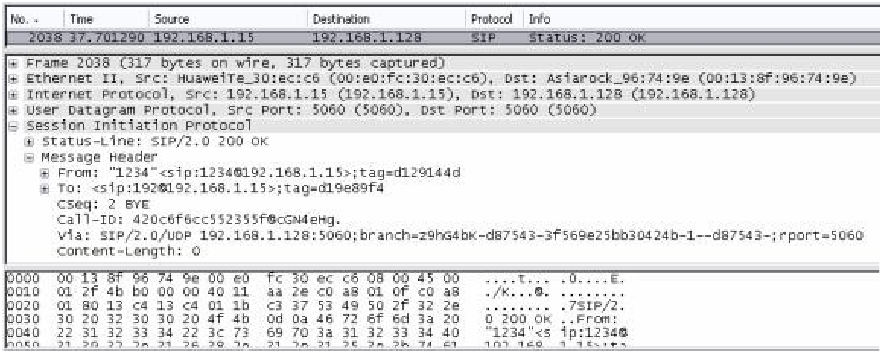
In this example, the communication from the softphone was terminated. Here it is seen, since it is that end that sends the BYE message. Below we can see the capture of this packet.



```
No. -   Time        Source          Destination     Protocol  Info
 2032 37.651049 192.168.1.128      192.168.1.15    SIP       Request: BYE sip:7366@192.168.1.15

+ Frame 2032 (470 bytes on wire, 470 bytes captured)
+ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
+ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
+ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
  + Request-Line: BYE sip:7366@192.168.1.15 SIP/2.0
  - Message Header
      Via: SIP/2.0/UDP 192.168.1.128:5060;branch=z9hG4bK-d87543-3f569e25bb30424b-1--d87543-;rport
      Max-Forwards: 70
    + Contact: <sip:1234@192.168.1.128:5060>
    + To: <sip:192@192.168.1.15>;tag=d19e89f4
    + From: "1234"<sip:1234@192.168.1.15>;tag=d129144d
      Call-ID: 420c6f6cc552355f@cGN4eHg.
      CSeq: 2 BYE
      User-Agent: CounterPath eyeBeam release 3013o stamp 23916
      Reason: User Hung Up
      Content-Length: 0

0000  00 e0 fc 30 ec c6 00 13  8f 96 74 9e 08 00 45 00   ...0.... ..t...E.
0010  01 c8 16 8c 00 00 80 11  9e b9 c0 a8 01 80 c0 a8   ........ ........
0020  01 0f 13 c4 13 c4 01 b4  bf a5 42 59 45 20 73 69   ........ ..BYE si
0030  70 3a 37 33 36 36 40 31  39 32 2e 31 36 38 2e 31   p:7366@1 92.168.1
0040  2e 31 35 20 53 49 50 2f  32 2e 30 0d 0a 56 69 61   .15 SIP/ 2.0..Via
```

Figure 12.17: SIP Protocol and Debug: Cut Request

As seen previously, this message notifies the termination of a call. At the other end, this message is answered with a 200 OK confirming the end of the call.



```
No. -   Time        Source          Destination     Protocol  Info
 2038 37.701290 192.168.1.15       192.168.1.128   SIP       Status: 200 OK

+ Frame 2038 (317 bytes on wire, 317 bytes captured)
+ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
+ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
+ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
  + Status-Line: SIP/2.0 200 OK
  - Message Header
    + From: "1234"<sip:1234@192.168.1.15>;tag=d129144d
    + To: <sip:192@192.168.1.15>;tag=d19e89f4
      CSeq: 2 BYE
      Call-ID: 420c6f6cc552355f@cGN4eHg.
      Via: SIP/2.0/UDP 192.168.1.128:5060;branch=z9hG4bK-d87543-3f569e25bb30424b-1--d87543-;rport=5060
      Content-Length: 0

0000  00 13 8f 96 74 9e 00 e0  fc 30 ec c6 08 00 45 00   ....t... .0....E.
0010  01 2f 4b b0 00 00 40 11  aa 2e c0 a8 01 0f c0 a8   ./K...@. ........
0020  01 80 13 c4 13 c4 01 1b  c3 37 53 49 50 2f 32 2e   ........ .7SIP/2.
0030  30 20 32 30 30 20 4f 4b  0d 0a 46 72 6f 6d 3a 20   0 200 OK ..From:
0040  22 31 32 33 34 22 3c 73  69 70 3a 31 32 33 34 40   "1234"<s ip:1234@
```

Figure 12.18: SIP Protocol and Debug: Cut Confirmation

To finish with this scenario we can conclude that the theoretical framework presented above was met. Communication was established within normal parameters, successfully. No unexpected messages found. The link layer, network and transport fields that were analyzed in each case coincided with the expected results.

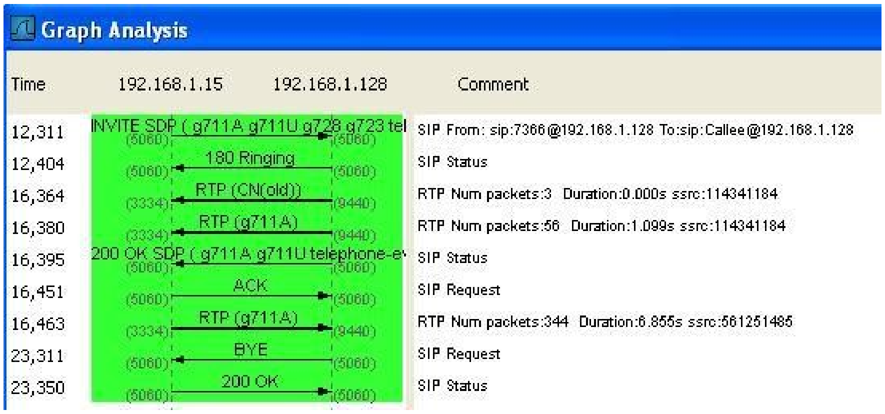
12.4.3.2 Successful call from videophone to softphone

12.4.3.2.1 Objective Observe and analyze the establishment, progress and disconnection of a communication with both available devices, as well as note differences with the previous case.

12.4.3.2.2 Execution The scenario in this case is as follows:

1. User A (Huawei phone) calls user B (softphone).
2. After letting the softphone ring, the call is answered.
3. Wait a few seconds. User B ends the call.

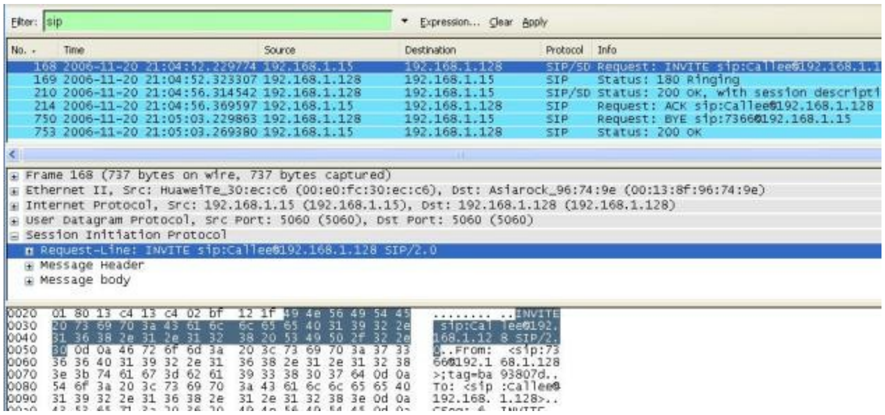
The following figure shows the flow of said call:



```
Time     192.168.1.15        192.168.1.128         Comment
12,311   INVITE SDP ( g711A g711U g728 g723 tel    SIP From: sip:7366@192.168.1.128 To:sip:Callee@192.168.1.128
         (5060)                         (5060)
12,404            180 Ringing                      SIP Status
         (5060)                         (5060)
16,364            RTP (CN(old))                    RTP Num packets:3  Duration:0.000s ssrc:114341184
         (3334)                         (9440)
16,380            RTP (g711A)                      RTP Num packets:56  Duration:1.099s ssrc:114341184
         (3334)                         (9440)
16,395   200 OK SDP ( g711A g711U telephone-e\    SIP Status
         (5060)                         (5060)
16,451            ACK                              SIP Request
         (5060)                         (5060)
16,463            RTP (g711A)                      RTP Num packets:344  Duration:6.855s ssrc:561251485
         (3334)                         (9440)
23,311            BYE                              SIP Request
         (5060)                         (5060)
23,350            200 OK                           SIP Status
         (5060)                         (5060)
```

Figure 12.19: SIP Protocol and Debug: Call Flow

12.4.3.2.2.1 Invite The call is initiated by User A, using the INVITE method. It is interesting to see the bytes of the message as they are presented by the ethereal:



```
No. .  Time                        Source          Destination     Protocol Info
  168 2006-11-20 21:04:52.229774 192.168.1.15    192.168.1.128   SIP/SD   Request: INVITE sip:Callee@192.168.1.1
  169 2006-11-20 21:04:52.323307 192.168.1.128   192.168.1.15    SIP      Status: 180 Ringing
  210 2006-11-20 21:04:56.314542 192.168.1.128   192.168.1.15    SIP/SD   Status: 200 OK, with session descripti
  214 2006-11-20 21:04:56.369597 192.168.1.15    192.168.1.128   SIP      Request: ACK sip:Callee@192.168.1.128
  750 2006-11-20 21:05:03.229863 192.168.1.128   192.168.1.15    SIP      Request: BYE sip:7366@192.168.1.15
  753 2006-11-20 21:05:03.269380 192.168.1.15    192.168.1.128   SIP      Status: 200 OK
```

```
+ Frame 168 (737 bytes on wire, 737 bytes captured)
+ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
+ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
+ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol
  + Request-Line: INVITE sip:Callee@192.168.1.128 SIP/2.0
  + Message Header
  + Message body
```

```
0020  01 80 13 c4 13 c4 02 bf  12 1f 49 4e 56 49 54 45   ........ ..INVITE
0030  20 73 69 70 3a 43 61 6c  6c 65 65 40 31 39 32 2e    sip:Cal lee@192.
0040  31 36 38 2e 31 2e 31 32  38 20 53 49 50 2f 32 2e   168.1.12 8 SIP/2.
0050  30 0d 0a 46 72 6f 6d 3a  20 3c 73 69 70 3a 37 33   0..From:  <sip:73
0060  36 36 40 31 39 32 2e 31  36 38 2e 31 2e 31 32 38   66@192.1 68.1.128
0070  3e 3b 74 61 67 3d 62 61  39 33 38 30 37 64 0d 0a   >;tag=ba 93807d..
0080  54 6f 3a 20 3c 73 69 70  3a 43 61 6c 6c 65 65 40   To: <sip :Callee@
0090  31 39 32 2e 31 36 38 2e  31 2e 31 32 38 3e 0d 0a   192.168. 1.128>..
```

Figure 12.20: SIP Protocol and Debug: INVITE

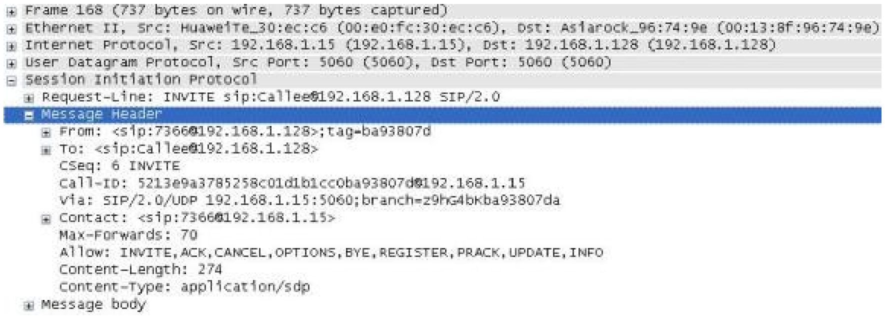
It can be seen that the message is encoded in ASCII, which makes it easy for users and administrators to decode. The cost of sending messages in plain text is a higher use of bandwidth, but as we will see below, signaling under normal conditions requires few messages to establish the call.

As can be seen in the figure, 3 segments are identified within the INVITE message:

- **Request Line**: In this section of the message you can mainly see the SIP Method used (INVITE, TRYING, etc.) and the SIP version. Unlike H.323, SIP does not ensure backward compatibility between versions, so a method supported in 1.0 might no longer be used in a later version.
  In the case of the INVITE message, you can see the recipient (TO) of the message:[|mailto:Callee@192.168.1.128]Callee@192.168.1.128

```
Request Line: INVITE sip:Callee@192.168.1.128 SIP/2.0
```

- **Message Header**: The SIP header can be seen in the following figure:

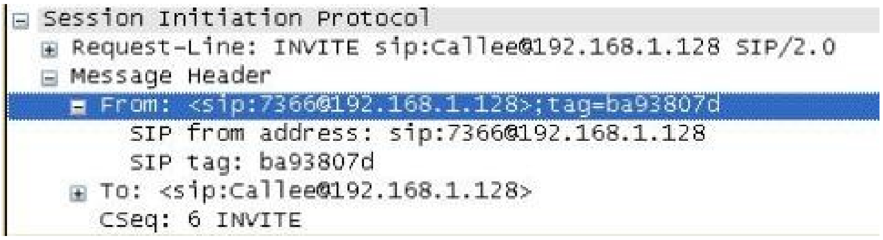


```
⊞ Frame 168 (737 bytes on wire, 737 bytes captured)
⊞ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
⊞ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:Callee@192.168.1.128 SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:7366@192.168.1.128>;tag=ba93807d
    ⊞ To: <sip:Callee@192.168.1.128>
      CSeq: 6 INVITE
      Call-ID: 5213e9a3785258c01d1b1cc0ba93807d@192.168.1.15
      Via: SIP/2.0/UDP 192.168.1.15:5060;branch=z9hG4bKba93807da
    ⊞ Contact: <sip:7366@192.168.1.15>
      Max-Forwards: 70
      Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REGISTER,PRACK,UPDATE,INFO
      Content-Length: 274
      Content-Type: application/sdp
  ⊞ Message body
```

Figure 12.21: SIP Protocol and Debug: SIP Header

The SIP header is made up of the following fields delimited by ASCII 13-10 (CR-CF):

- **From**: The FROM field is the logical identifier of the User Agent that generates the request (UA Client). It is made up of the URI (Uniform Resource Identifier) and optionally the DISPLAY Name parameter, which is the name that will be displayed if the user has the active caller ID service. Additionally, within the FROM is the TAG parameter, which is an identifier generated by the user agent client at the time of making the request. This identifier, together with the parameter with the call identifier (Call-ID), serve to identify the dialogue between the User Agent Client and the User Agent Server (UAS).
  In the following figure you can see the FROM field captured, within the INVITE:

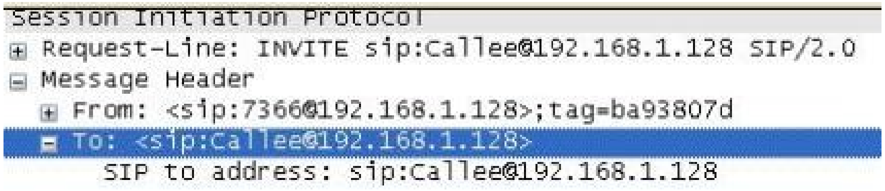


```
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:Callee@192.168.1.128 SIP/2.0
  ⊟ Message Header
    ⊟ From: <sip:7366@192.168.1.128>;tag=ba93807d
        SIP from address: sip:7366@192.168.1.128
        SIP tag: ba93807d
    ⊞ To: <sip:Callee@192.168.1.128>
      CSeq: 6 INVITE
```

Figure 12.22: SIP Protocol and Debug: FROM Field

  It is interesting to note that in this case the URI: 7366@192.168.1.128 is using the Videophone identifier (7366), but the IP that was used to form said message is that of the softphone. This is because the UACs make up the URI using the IP of the SIP-Proxy, and in this scenario, since the terminal was configured to work in peer to peer mode, the recipient's IP is used.
  The tag that was generated to establish this dialog is: **ba93807d**.

- **To**: The TO field indicates the logical recipient of the order. The UAC generates the TO field from what is entered by the videophone user. In this case, the call was generated by dialing the IP of the destination, so the UAC client generated the URI automatically:



```
Session Initiation Protocol
⊞ Request-Line: INVITE sip:Callee@192.168.1.128 SIP/2.0
⊟ Message Header
  ⊞ From: <sip:7366@192.168.1.128>;tag=ba93807d
  ⊟ To: <sip:Callee@192.168.1.128>
      SIP to address: sip:Callee@192.168.1.128
```

Figure 12.23: SIP Protocol and Debug: TO Field

The automatically generated URI uses the string ”Callee@<dialled IP>”. Note that the TAG is not being used within the TO.

- **CSeq**: This parameter defines the order of the transactions. It consists of a sequence number and a method. This sequence number is incremented by 1 at a time. In the case of this capture, this parameter has the value: CSeq: 6 INVITE. The method used to build the CSeq must be the same method used to generate the dialog.
- **Call-ID**: This parameter is a unique identifier that will group together a series of messages. It is mandatory that it be the same during all the messages that are exchanged between UAC and UAS. To ensure that the identifier is unique, it is recommended to use RFC 1750. (Use of cryptographically random identifiers)
  The captured call-ID is:

```
  Call ID: 5213e9a3785258c01d1b1cc0ba93807d@192.168.1.15
```

  It is interesting to note that the UAC of the Videophone uses its own IP as part of the new call ID.
- **Via**: The VIA parameter identifies the transport protocol and the location where the response should be sent. The UAC must insert this parameter compulsorily whenever the request is generated. It is important to note that this parameter is present in messages sent by UAC only.
  The VIA field includes the Branch parameter, which is used to identify the transaction within the UAC. This parameter must be unique.
  RFC 3261 specifies that the default value of the Branco ID begins with z9hG4bK. In the screenshot you can see that the transport protocol is UDP, and its IP and port is that of the Videophone.

```
  Via: SIP/2.0/UDP 192.168.1.15:5060;branch=z9hG4bKba93807da
```

- **Contact**: This parameter is used to identify the specific instance of the UA where requests can be sent, outside of the current dialog.
  In this capture, this parameter has the value:

```
  Contact: <sip:7366@192.168.1.15>
```

- **Max Forwards**: This parameter is used to limit the number of hops that a request can transit. By default this value is set to 70 hops. If this parameter reaches 0, the call is terminated with code 483 (too many hops).
- **Allow**: Indicates all the methods supported by the UA. If this parameter is not present, it does not mean that the UA does not support any methods, but rather that it did not provide them itself. This message seeks to optimize the number of messages needed to complete.
  In the case of the invite message, this parameter included:

```
  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, PRACK, UPDATE, INFO
```

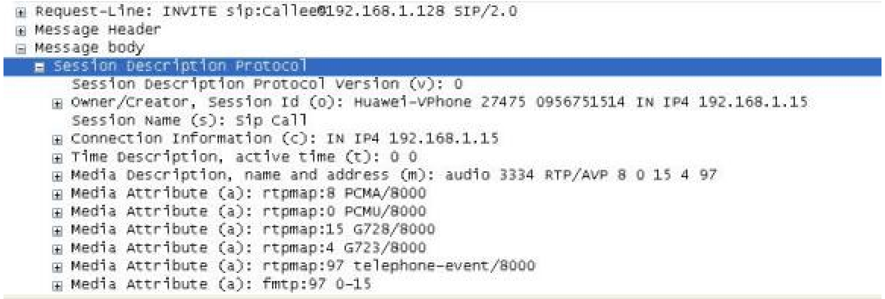
- **Content-Length**: Indicates the number of bytes in the message body. If there is no information in the message body, this parameter must be set to 0. This parameter can be abbreviated using ”l:”.
  In this case the length of the message is:

```
    Content-Length: 274
```

- **Content-Type**: This parameter indicates the type of information contained in the body. Some examples are: Content-Type: application/sdp c: text/html; charset=ISO-8859-4 In this case, the protocol that was used:

```
    Content-Type: application/sdp
```

- **Message Body**: The body of the SIP message, as seen in the header, is using SDP:

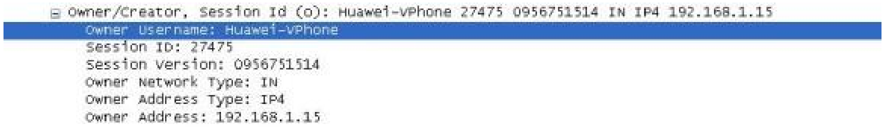


```
⊞ Request-Line: INVITE sip:Callee@192.168.1.128 SIP/2.0
⊞ Message Header
⊟ Message body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): Huawei-vPhone 27475 0956751514 IN IP4 192.168.1.15
      Session Name (s): Sip Call
    ⊞ Connection Information (c): IN IP4 192.168.1.15
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 3334 RTP/AVP 8 0 15 4 97
    ⊞ Media Attribute (a): rtpmap:8 PCMA/8000
    ⊞ Media Attribute (a): rtpmap:0 PCMU/8000
    ⊞ Media Attribute (a): rtpmap:15 G728/8000
    ⊞ Media Attribute (a): rtpmap:4 G723/8000
    ⊞ Media Attribute (a): rtpmap:97 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:97 0-15
```

Figure 12.24: SIP Protocol and Debug: Message Body

The Session Description Protocol is defined in RFC 2327. The advantage of using an additional protocol to set the parameters that will define the session establishment is that this allows SIP to be easily adapted for both voice communications and multimedia applications.
The SDP protocol consists of different tags, each of which describes a particular parameter of the session. You can see the following parameters:

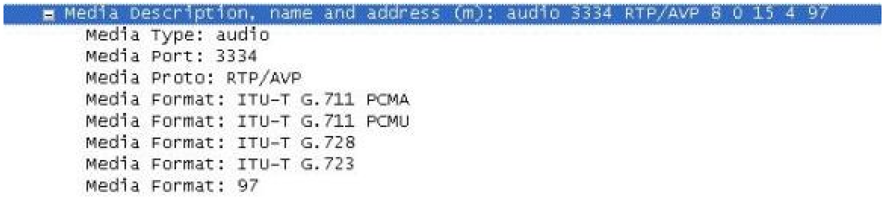
- v - SDP Protocol Version
- o – Owner-Creator, Session Id: Within these parameters you can see the session identifier, the IP and the owner:



```
⊟ Owner/Creator, Session Id (o): Huawei-vPhone 27475 0956751514 IN IP4 192.168.1.15
    Owner Username: Huawei-vPhone
    Session ID: 27475
    Session Version: 0956751514
    Owner Network Type: IN
    Owner Address Type: IP4
    Owner Address: 192.168.1.15
```

Figure 12.25: SIP Protocol and Debug: Owner Username

- c – Connection Information: This parameter presents the IP where the audio stream should be sent. In this case it is the same IP of the VideoPhone: 192.168.1.15.
- t- Time description: It is the time that the audio stream has been active.
- m- Media Description: This tag has the description of all the codecs supported by the UAC that started the conversation. The media type is specified, which informs that the content of the session is audio, the media port, which defines the UDP port that was assigned to receive the RTP stream. Audio codecs (video or dtmfs) are identified using standard presets: 8 G.711A , 0 G711U, 4 G.723, etc.

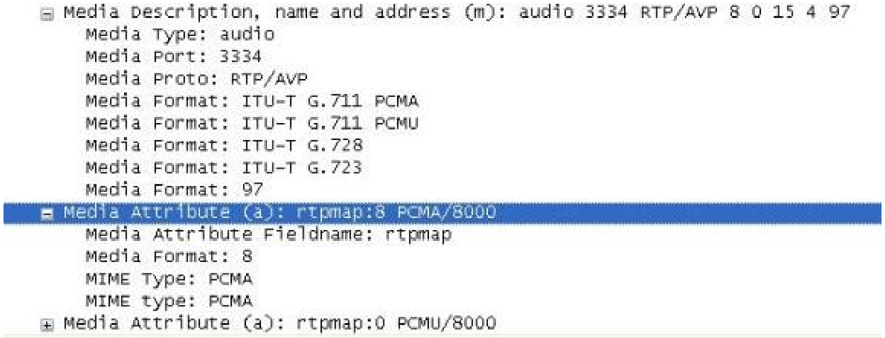


```
⊟ Media Description, name and address (m): audio 3334 RTP/AVP 8 0 15 4 97
     Media Type: audio
     Media Port: 3334
     Media Proto: RTP/AVP
     Media Format: ITU-T G.711 PCMA
     Media Format: ITU-T G.711 PCMU
     Media Format: ITU-T G.728
     Media Format: ITU-T G.723
     Media Format: 97
```

Figure 12.26: SIP Protocol and Debug: Media Description

As necessary, each codec adapts its parameters using media attributes:

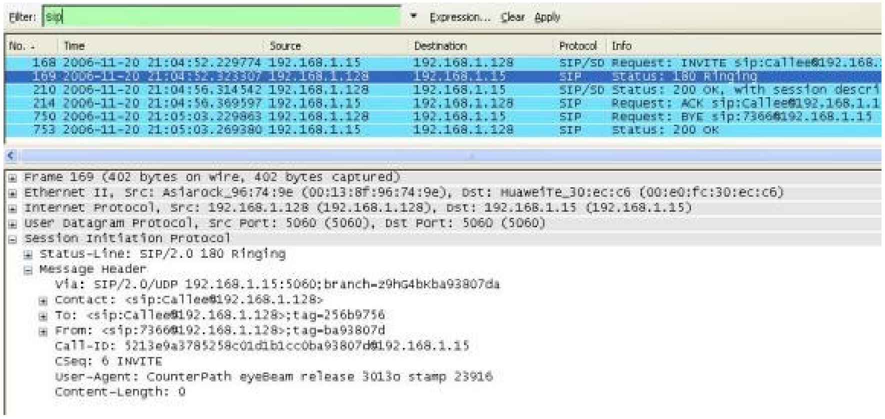
- a – Media attributes: In the figure you can see how the different parameters are specified for each particular codec. The attributes are related to the codec via the ”Media Format” parameter.



```
⊟ Media Description, name and address (m): audio 3334 RTP/AVP 8 0 15 4 97
     Media Type: audio
     Media Port: 3334
     Media Proto: RTP/AVP
     Media Format: ITU-T G.711 PCMA
     Media Format: ITU-T G.711 PCMU
     Media Format: ITU-T G.728
     Media Format: ITU-T G.723
     Media Format: 97
⊟ Media Attribute (a): rtpmap:8 PCMA/8000
     Media Attribute Fieldname: rtpmap
     Media Format: 8
     MIME Type: PCMA
     MIME type: PCMA
⊞ Media Attribute (a): rtpmap:0 PCMU/8000
```

Figure 12.27: SIP Protocol and Debug: Message Attibutes

12.4.3.2.2.2 Ringing This message is sent by the UAS (in this case, the softhpone) to indicate that the user is being alerted about the invitation. It is important to note that compared to scenario 1, the TRYING message is not being sent. This is typical of the softphone implementation, since there is no interface to excite, as for example in a telephone in which there is an interface with an analog line, which takes a while until it starts ringing.



```
No. -  Time                       Source          Destination     Protocol Info
  168 2006-11-20 21:04:52.229774 192.168.1.15    192.168.1.128   SIP/SD Request: INVITE sip:Callee@192.168.
  169 2006-11-20 21:04:52.323307 192.168.1.128   192.168.1.15    SIP    Status: 180 Ringing
  210 2006-11-20 21:04:56.314542 192.168.1.128   192.168.1.15    SIP/SD Status: 200 OK, with session descri
  214 2006-11-20 21:04:56.369597 192.168.1.15    192.168.1.128   SIP    Request: ACK sip:Callee@192.168.1.1
  750 2006-11-20 21:05:03.229863 192.168.1.128   192.168.1.15    SIP    Request: BYE sip:7366@192.168.1.15
  753 2006-11-20 21:05:03.269380 192.168.1.15    192.168.1.128   SIP    Status: 200 OK
```

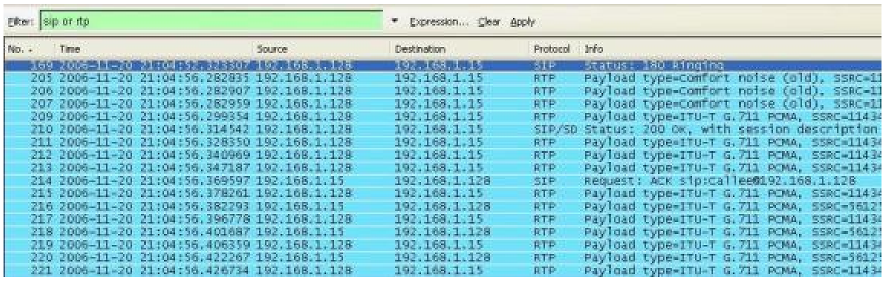
```
⊞ Frame 169 (402 bytes on wire, 402 bytes captured)
⊞ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
⊞ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 180 Ringing
  ⊟ Message Header
       Via: SIP/2.0/UDP 192.168.1.15:5060;branch=z9hG4bKba93807da
     ⊞ Contact: <sip:Callee@192.168.1.128>
     ⊞ To: <sip:Callee@192.168.1.128>;tag=256b9756
     ⊞ From: <sip:7366@192.168.1.128>;tag=ba93807d
       Call-ID: 5213e9a3785258c01d1b1cc0ba93807d@192.168.1.15
       CSeq: 6 INVITE
       User-Agent: CounterPath eyeBeam release 3013o stamp 23916
       Content-Length: 0
```

Figure 12.28: SIP Protocol and Debug: Ringing

Looking at this message in detail, and comparing it against the fields previously seen in the INVITE, it can be seen that:

1. THE FROM and TO sent in the INVITE header ARE MAINTAINED, that is, the UAS does not change the values provided by the UAC. The only difference is that the UAS adds the TAG in the TO, with which the call is identified by the Call-ID, tag provided by the UAC, tag provided by UAS.
2. The CSeq maintains the identifier provided in the INVITE.
3. The VIA parameter maintains the same values as in the INVITE, and the same is valid for the Branch.
4. The CONTACT parameter is updated with the values of the UAS.

It is interesting to see a detail of what happens once the Ringing message is received:



```
No. -  Time                        Source          Destination     Protocol Info
  169 2006-11-20 21:04:52.323307 192.168.1.128   192.168.1.15    SIP      Status: 180 Ringing
  205 2006-11-20 21:04:56.282835 192.168.1.128   192.168.1.15    RTP      Payload type=Comfort noise (old), SSRC=11
  206 2006-11-20 21:04:56.282907 192.168.1.128   192.168.1.15    RTP      Payload type=Comfort noise (old), SSRC=11
  207 2006-11-20 21:04:56.282959 192.168.1.128   192.168.1.15    RTP      Payload type=Comfort noise (old), SSRC=11
  209 2006-11-20 21:04:56.299354 192.168.1.128   192.168.1.15    RTP      Payload type=ITU-T G.711 PCMA, SSRC=11434
  210 2006-11-20 21:04:56.314542 192.168.1.128   192.168.1.15    SIP/SD   Status: 200 OK, with session description
  211 2006-11-20 21:04:56.328350 192.168.1.128   192.168.1.15    RTP      Payload type=ITU-T G.711 PCMA, SSRC=11434
  212 2006-11-20 21:04:56.340969 192.168.1.128   192.168.1.15    RTP      Payload type=ITU-T G.711 PCMA, SSRC=11434
  213 2006-11-20 21:04:56.347187 192.168.1.128   192.168.1.15    RTP      Payload type=ITU-T G.711 PCMA, SSRC=11434
  214 2006-11-20 21:04:56.369597 192.168.1.15    192.168.1.128   SIP      Request: ACK sip:Callee@192.168.1.128
  215 2006-11-20 21:04:56.378261 192.168.1.128   192.168.1.15    RTP      Payload type=ITU-T G.711 PCMA, SSRC=11434
  216 2006-11-20 21:04:56.382293 192.168.1.15    192.168.1.128   RTP      Payload type=ITU-T G.711 PCMA, SSRC=56125
  217 2006-11-20 21:04:56.396778 192.168.1.128   192.168.1.15    RTP      Payload type=ITU-T G.711 PCMA, SSRC=11434
  218 2006-11-20 21:04:56.401687 192.168.1.15    192.168.1.128   RTP      Payload type=ITU-T G.711 PCMA, SSRC=56125
  219 2006-11-20 21:04:56.406359 192.168.1.128   192.168.1.15    RTP      Payload type=ITU-T G.711 PCMA, SSRC=11434
  220 2006-11-20 21:04:56.422267 192.168.1.15    192.168.1.128   RTP      Payload type=ITU-T G.711 PCMA, SSRC=56125
  221 2006-11-20 21:04:56.426734 192.168.1.128   192.168.1.15    RTP      Payload type=ITU-T G.711 PCMA, SSRC=11434
```

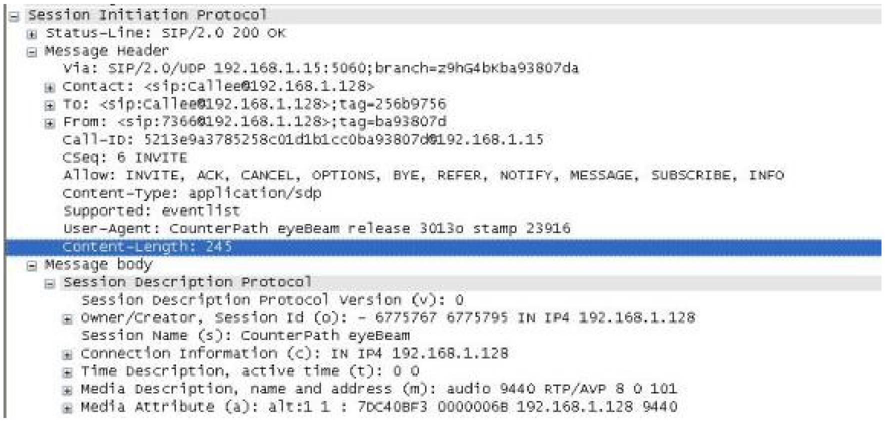
Figure 12.29: SIP Protocol and Debug: Comfort Noise

It can be seen that the softphone, once I send the Ringing message, since it has the SDP information from the Videophone, can already start sending audio (in one direction). Before sending the 200 OK with the necessary information for the videophone to open the channel in the opposite direction, it sends RTP packets with comfort noise, so that the user is not left listening to a silent channel, which would give the impression that the communication failed.

Then the softphone sends the 200OK message with the SDP so that the UAC can open the channel, in the reverse direction.

12.4.3.2.2.3 200 OK This message keeps the same values in the parameters as the RINGING.

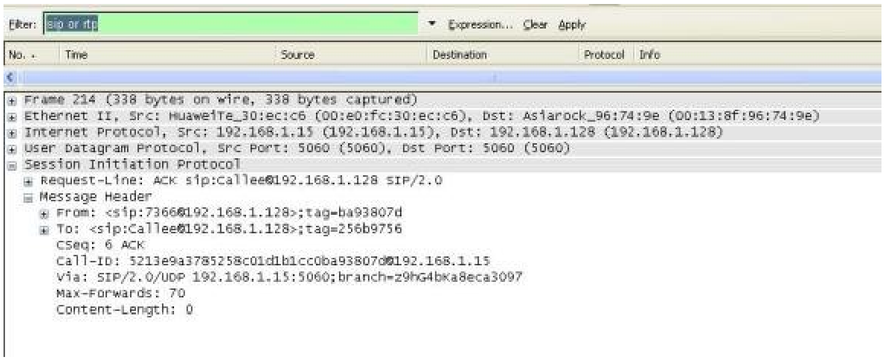
In the Message Body it can be seen that G.711 Mu (8) is being sent as the preferred protocol, and RTP/AVP (101) will also be used for telephone events (dtmfs). Audio will be directed to UDP port 9440.



```
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊟ Message Header
      Via: SIP/2.0/UDP 192.168.1.15:5060;branch=z9hG4bKba93807da
    ⊞ Contact: <sip:Callee@192.168.1.128>
    ⊞ To: <sip:Callee@192.168.1.128>;tag=256b9756
    ⊞ From: <sip:7366@192.168.1.128>;tag=ba93807d
      Call-ID: 5213e9a3785258c01d1b1cc0ba93807d@192.168.1.15
      CSeq: 6 INVITE
      Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
      Content-Type: application/sdp
      Supported: eventlist
      User-Agent: CounterPath eyeBeam release 3013o stamp 23916
      Content-Length: 245
  ⊟ Message body
    ⊟ Session Description Protocol
        Session Description Protocol Version (v): 0
      ⊞ Owner/Creator, Session Id (o): - 6775767 6775795 IN IP4 192.168.1.128
        Session Name (s): CounterPath eyeBeam
      ⊞ Connection Information (c): IN IP4 192.168.1.128
      ⊞ Time Description, active time (t): 0 0
      ⊞ Media Description, name and address (m): audio 9440 RTP/AVP 8 0 101
      ⊞ Media Attribute (a): alt:1 1 : 7DC40BF3 0000006B 192.168.1.128 9440
```

Figure 12.30: SIP Protocol and Debug: 200 OK

12.4.3.2.2.4 ACK VideoPhone | Softphone This message confirms that the Videophone received the 200 OK notification from the UAS, and that the port was opened with the information provided in said message. It can be seen that after this message, the Videophone starts sending RTP using G.711 to port 9440.


Filter: sip or rtp
Expression... Clear Apply
No. Time Source Destination Protocol Info

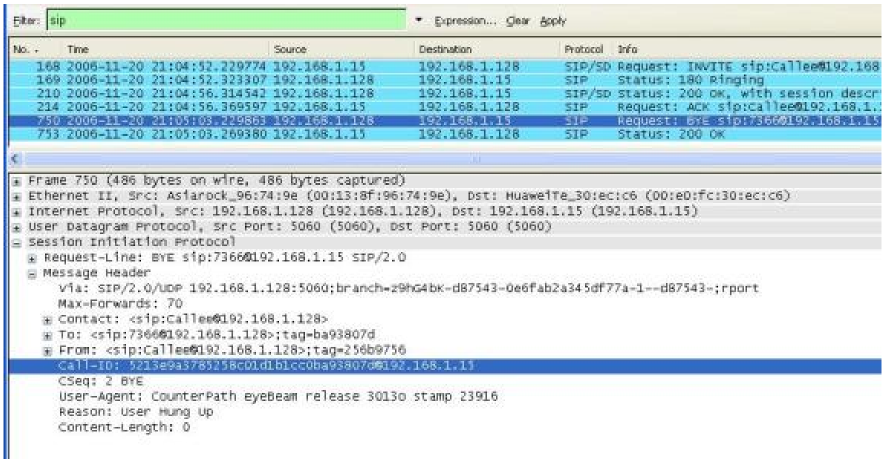
```
⊞ Frame 214 (338 bytes on wire, 338 bytes captured)
⊞ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
⊞ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
  ⊞ Request-Line: ACK sip:Callee@192.168.1.128 SIP/2.0
  ⊟ Message Header
    ⊞ From: <sip:7366@192.168.1.128>;tag=ba93807d
    ⊞ To: <sip:Callee@192.168.1.128>;tag=256b9756
      CSeq: 6 ACK
      Call-ID: 5213e9a3785258c01d1b1cc0ba93807d@192.168.1.15
      Via: SIP/2.0/UDP 192.168.1.15:5060;branch=z9hG4bKa8eca3097
      Max-Forwards: 70
      Content-Length: 0
```

Figure 12.31: SIP Protocol and Debug: ACK

12.4.3.2.2.5 BYE Softphone | videophone The first thing that is interesting is that the BYE message is generated by the softphone instead of the videophone, which was the one that had started the conversation.

Since in this case the UAC is the softphone, the FROM and TO are inverted, and the VIA is updated with the values corresponding to the Softphone.

However, both the tags and the call-ID remain as in the other messages.

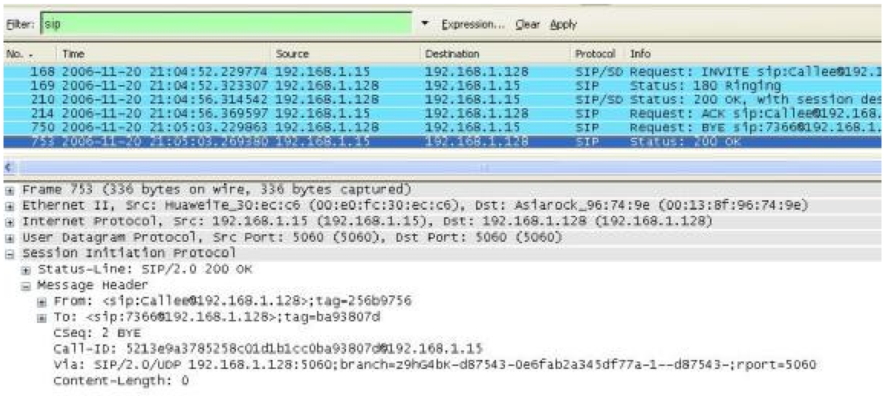


```
No. .  Time                        Source          Destination     Protocol Info
  168 2006-11-20 21:04:52.229774 192.168.1.15    192.168.1.128   SIP/SD Request: INVITE sip:Callee@192.168
  169 2006-11-20 21:04:52.323307 192.168.1.128   192.168.1.15    SIP    Status: 180 Ringing
  210 2006-11-20 21:04:56.314542 192.168.1.128   192.168.1.15    SIP/SD Status: 200 OK, with session descr
  214 2006-11-20 21:04:56.369597 192.168.1.15    192.168.1.128   SIP    Request: ACK sip:Callee@192.168.1.
  750 2006-11-20 21:05:03.229863 192.168.1.128   192.168.1.15    SIP    Request: BYE sip:7366@192.168.1.15
  753 2006-11-20 21:05:03.269380 192.168.1.15    192.168.1.128   SIP    Status: 200 OK
```

```
⊞ Frame 750 (486 bytes on wire, 486 bytes captured)
⊞ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
⊞ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
  ⊞ Request-Line: BYE sip:7366@192.168.1.15 SIP/2.0
  ⊟ Message Header
      Via: SIP/2.0/UDP 192.168.1.128:5060;branch=z9hG4bK-d87543-0e6fab2a345df77a-1--d87543-;rport
      Max-Forwards: 70
    ⊞ Contact: <sip:Callee@192.168.1.128>
    ⊞ To: <sip:7366@192.168.1.128>;tag=ba93807d
    ⊞ From: <sip:Callee@192.168.1.128>;tag=256b9756
      Call-ID: 5213e9a3785258c01d1b1cc0ba93807d@192.168.1.15
      CSeq: 2 BYE
      User-Agent: CounterPath eyeBeam release 3013o stamp 23916
      Reason: User Hung Up
      Content-Length: 0
```

Figure 12.32: SIP Protocol and Debug: Message Attibutes

12.4.3.2.2.6 200 OK Videophone | Softphone This message confirms that the call was disconnected on the Videophone side. It is important to note that in this case the Content-Length is set to 0 because no SDP information is included.



```
No. -  Time                       Source          Destination     Protocol Info
   168 2006-11-20 21:04:52.229774 192.168.1.15    192.168.1.128   SIP/SD   Request: INVITE sip:Callee@192.1
   169 2006-11-20 21:04:52.323307 192.168.1.128   192.168.1.15    SIP      Status: 180 Ringing
   210 2006-11-20 21:04:56.314542 192.168.1.128   192.168.1.15    SIP/SD   Status: 200 OK, with session des
   214 2006-11-20 21:04:56.369597 192.168.1.15    192.168.1.128   SIP      Request: ACK sip:Callee@192.168.
   750 2006-11-20 21:05:03.229863 192.168.1.128   192.168.1.15    SIP      Request: BYE sip:7366@192.168.1.
   753 2006-11-20 21:05:03.269360 192.168.1.15    192.168.1.128   SIP      Status: 200 OK

⊞ Frame 753 (336 bytes on wire, 336 bytes captured)
⊞ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
⊞ Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 200 OK
  ⊟ Message Header
    ⊞ From: <sip:Callee@192.168.1.128>;tag=256b9756
    ⊞ To: <sip:7366@192.168.1.128>;tag=ba93807d
      CSeq: 2 BYE
      Call-ID: 5213e9a3785258c01d1b1cc0ba93807d@192.168.1.15
      Via: SIP/2.0/UDP 192.168.1.128:5060;branch=z9hG4bK-d87543-0e6fab2a345df77a-1--d87543-;rport=5060
      Content-Length: 0
```

Figure 12.33: SIP Protocol and Debug: 200 OK - Disconnect

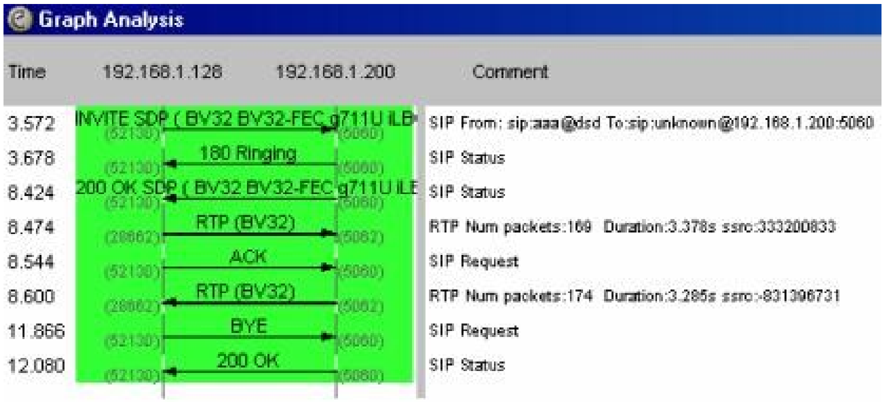
12.4.3.2.3 Conclusions From the previous analysis it is interesting to note that the FROM, TO, VIA and CONTACT parameters are adapted according to the role that each Terminal is fulfilling at each moment (UAC or UAS).

It is also interesting to note how the flow control of SIP messages is carried out, which justifies why most manufacturers use UDP as transport protocol instead of TCP.

12.4.3.3 Successful call from softphone 1 to softphone 2 and vice versa

12.4.3.3.1 Objective Observe and analyze the establishment, progress and disconnection of a communication with both available devices, as well as note differences with the previous case.

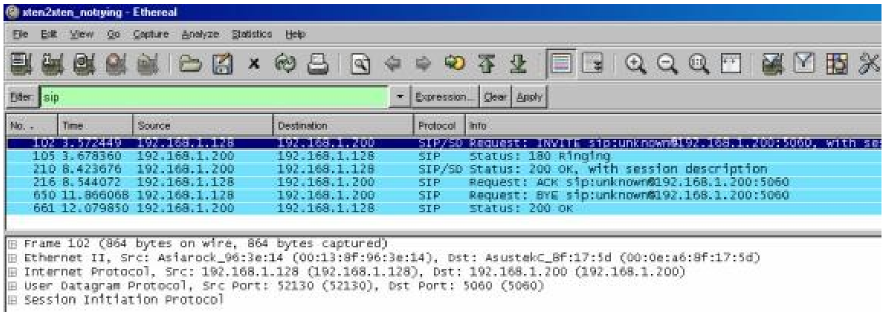
12.4.3.3.2 Development In the present scenario there is a successful communication between two softphones. The purpose of this screenshot is to verify that since there is no sip proxy between the devices, no trying message appears. To carry out the communication again, both sides had to be configured as peer-to-peer. We see below the exchange of messages.



```
Time    192.168.1.128   192.168.1.200   Comment
3.572   INVITE SDP ( BV32 BV32-FEC g711U iLB   SIP From: sip:aaa@dsd To:sip:unknown@192.168.1.200:5060
          (52130)  ------------------>  (5060)
3.678             180 Ringing                   SIP Status
          (52130)  <------------------  (5060)
8.424   200 OK SDP ( BV32 BV32-FEC g711U iLE    SIP Status
          (52130)  <------------------  (5060)
8.474             RTP (BV32)                    RTP Num packets:169  Duration:3.378s ssrc:333200833
          (28862)  ------------------>  (5062)
8.544             ACK                           SIP Request
          (52130)  ------------------>  (5060)
8.600             RTP (BV32)                    RTP Num packets:174  Duration:3.285s ssrc:-831396731
          (28862)  <------------------  (5062)
11.866            BYE                           SIP Request
          (52130)  ------------------>  (5060)
12.080            200 OK                        SIP Status
          (52130)  <------------------  (5060)
```

Figure 12.34: SIP Protocol and Debug: Call Flow

Here we verify that after the first INVITE message, the other end responds directly with a RINGING type message, ignoring the TRYING. This is again due to the fact that since there is no Proxy, it does not make sense in a point-to-point connection to send this message. Next we see the capture.


xten2xten_notrying - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: sip
Expression... Clear Apply

```
No. .  Time       Source          Destination     Protocol Info
  102 3.572449   192.168.1.128   192.168.1.200   SIP/SD Request: INVITE sip:unknown@192.168.1.200:5060, with se
  105 3.678360   192.168.1.200   192.168.1.128   SIP    Status: 180 Ringing
  210 8.423676   192.168.1.200   192.168.1.128   SIP/SD Status: 200 OK, with session description
  216 8.544072   192.168.1.128   192.168.1.200   SIP    Request: ACK sip:unknown@192.168.1.200:5060
  650 11.866068  192.168.1.128   192.168.1.200   SIP    Request: BYE sip:unknown@192.168.1.200:5060
  661 12.079850  192.168.1.200   192.168.1.128   SIP    Status: 200 OK

⊞ Frame 102 (864 bytes on wire, 864 bytes captured)
⊞ Ethernet II, Src: Asiarock_96:3e:14 (00:13:8f:96:3e:14), Dst: AsustekC_8f:17:5d (00:0e:a6:8f:17:5d)
⊞ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.200 (192.168.1.200)
⊞ User Datagram Protocol, Src Port: 52130 (52130), Dst Port: 5060 (5060)
⊞ Session Initiation Protocol
```

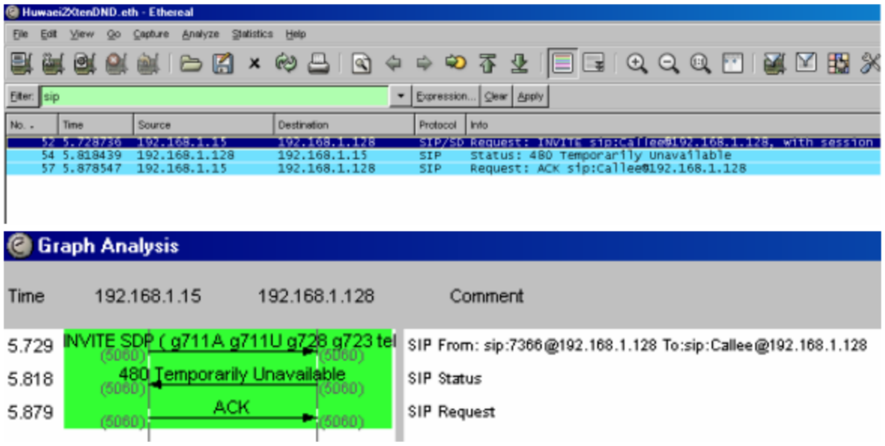
Figure 12.35: SIP Protocol and Debug: Ringing

This communication takes place in normal terms just like the previous two scenarios. In this case we can mention that although there were no microphones at either end, there is audio exchange via RTP. This is because as the G.711 U-Law codec has been negotiated, silence suppression is not implemented, that is, there is an exchange of audio but without any content. In conclusion, the previously stated hypothesis regarding Trying is verified.

12.4.3.4 Call from videophone to softphone in DND (Do Not Disturb) mode

12.4.3.4.1 Objective Observe and analyze the failed establishment in a communication with the unavailable softphone.

12.4.3.4.2 Development The messages exchanged are shown below.


HuwaeiZXtenDND.eth - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: sip
Expression... Clear Apply
Graph Analysis
(5060)
(5060)
(5060)
(5060)
(5060)
(5060)

```
No. .  Time       Source          Destination     Protocol Info
   52 5.728736   192.168.1.15    192.168.1.128   SIP/SD Request: INVITE sip:Callee@192.168.1.128, with session
   54 5.818439   192.168.1.128   192.168.1.15    SIP    Status: 480 Temporarily Unavailable
   57 5.878547   192.168.1.15    192.168.1.128   SIP    Request: ACK sip:Callee@192.168.1.128
```

Time	192.168.1.15	192.168.1.128	Comment
5.729	INVITE SDP (g711A g711U g728 g723 tel		SIP From: sip:7366@192.168.1.128 To:sip:Callee@192.168.1.128
5.818	480 Temporarily Unavailable		SIP Status
5.879	ACK		SIP Request

Figure 12.36: SIP Protocol and Debug: Call Flow

This is the image of the Soft Phone configured in Do not Disturb mode.

Figure 12.37: SIP Protocol and Debug: Soft Phone with DND

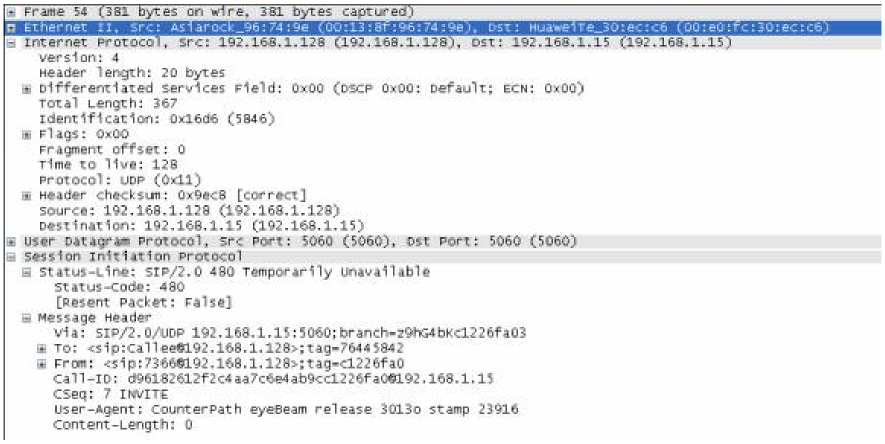
Like all communication, it starts with an INVITE from the VideoPhone, who initiates the call, to the Softphone. This package has identical characteristics to the previous ones.

The fundamental difference with scenarios 1, 2 and 3 where the calls were established is that when the softphone is in DnD mode, it responds with the message 480 Temporarily

Unavailable requesting the end of the call to which it responds with the ACK message, thus ending the call.

12.4.3.4.2.1 Message 480 Temporarily unavailable This message is given when the other device is connected correctly but is not able to answer the call. For example: when it is not logged in, when it is logged in but in a state that does not allow the entry of another communication or is in Do not Disturb (DnD) mode. The phone that made the call usually displays a message saying that the destination phone is not available, please try again later.

Below is the screenshot of the 480 message:



```
⊞ Frame 54 (381 bytes on wire, 381 bytes captured)
⊞ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6)
⊟ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 367
    Identification: 0x16d6 (5846)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0x9ec8 [correct]
    Source: 192.168.1.128 (192.168.1.128)
    Destination: 192.168.1.15 (192.168.1.15)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 480 Temporarily Unavailable
      Status-Code: 480
      [Resent Packet: False]
  ⊟ Message Header
      Via: SIP/2.0/UDP 192.168.1.15:5060;branch=z9hG4bKc1226fa03
    ⊞ To: <sip:Callee@192.168.1.128>;tag=76445842
    ⊞ From: <sip:7366@192.168.1.128>;tag=c1226fa0
      Call-ID: d96182612f2c4aa7c6e4ab9cc1226fa0@192.168.1.15
      CSeq: 7 INVITE
      User-Agent: CounterPath eyeBeam release 3013o stamp 23916
      Content-Length: 0
```

Figure 12.38: SIP Protocol and Debug: Message 480

In the Status Line it is displayed that the message sent is 480, the fields it contains are the same as those of the rest of the SIP messages.

Every time a call is terminated or does not go through for some special reason, an error message is sent in response to the different failures detected.

As previously indicated, it corresponds to the answers of the class:

- **4xx**: Method failure responses.
- **5xx**: Server fault responses.
- **6xx**: Global fault responses.

SIP error list

In the «**??**» section found on the **??** page, there is a complete list of SIP protocol error messages.

12.4.3.4.3 Conclusions

The appearance of several unusual messages such as DECLINE, Request Terminated, etc., broadens the basic scenarios that could appear in a SIP connection (analyze SIP event table) Æ (RFC 3261).

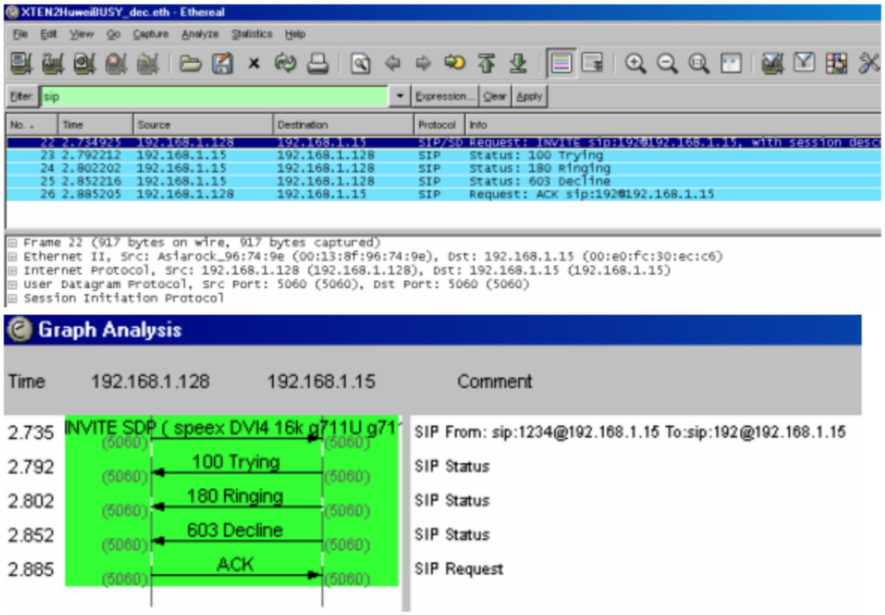
12.4.3.5 Call from the softphone to the busy videophone

12.4.3.5.1 Objective

Observe and analyze the failed establishment in a communication with the videophone in use.

12.4.3.5.2 Development

The following shows the packets exchanged between the Soft Phone and the VideoPhone.


XTEN2HuweiBUSY_dec.eth - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: sip
Expression... Clear Apply
Graph Analysis

```
No. .  Time      Source         Destination    Protocol Info
  22 2.734925  192.168.1.128  192.168.1.15   SIP/SD   Request: INVITE sip:192@192.168.1.15, with session desc
  23 2.792212  192.168.1.15   192.168.1.128  SIP      Status: 100 Trying
  24 2.802202  192.168.1.15   192.168.1.128  SIP      Status: 180 Ringing
  25 2.852216  192.168.1.15   192.168.1.128  SIP      Status: 603 Decline
  26 2.885205  192.168.1.128  192.168.1.15   SIP      Request: ACK sip:192@192.168.1.15
```

```
⊞ Frame 22 (917 bytes on wire, 917 bytes captured)
⊞ Ethernet II, Src: Asiarock_96:74:9e (00:13:8f:96:74:9e), Dst: 192.168.1.15 (00:e0:fc:30:ec:c6)
⊞ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.15 (192.168.1.15)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊞ Session Initiation Protocol
```

```
Time    192.168.1.128          192.168.1.15          Comment
2.735   INVITE SDP ( speex DVI4 16k g711U g71        SIP From: sip:1234@192.168.1.15 To:sip:192@192.168.1.15
        (5060)  ------------------->  (5060)
2.792           100 Trying                           SIP Status
        (5060)  <-------------------  (5060)
2.802           180 Ringing                          SIP Status
        (5060)  <-------------------  (5060)
2.852           603 Decline                          SIP Status
        (5060)  <-------------------  (5060)
2.885           ACK                                  SIP Request
        (5060)  ------------------->  (5060)
```

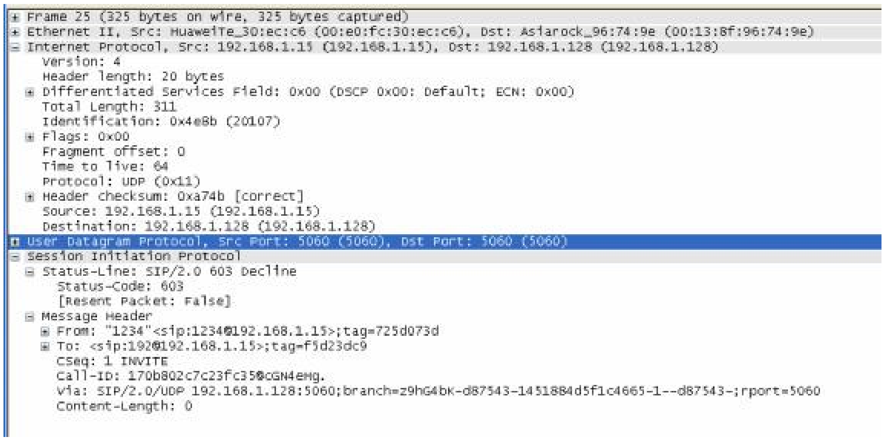
Figure 12.39: SIP Protocol and Debug: Call Flow

In this case, a call was made from the Softphone to the Videophone, which was busy. The videophone responds to the INVITE message with a TRYING and RINGING, but upon detecting that it is not able to receive the call, it sends the error message 603 DECLINE or call rejected, to which the softphone responds with the ACK, ending the connection.

12.4.3.5.2.1 Message 603 DECLINE The 603 DECLINE message indicates that the phone being called is correctly connected but the recipient explicitly does not want to answer the call.

In this case, the Cancel key was pressed on the Video Phone while ringing, thus ending the call. The message ”Try again later” appears on the caller’s display.

Below is the capture.



```
+ Frame 25 (325 bytes on wire, 325 bytes captured)
+ Ethernet II, Src: HuaweiTe_30:ec:c6 (00:e0:fc:30:ec:c6), Dst: Asiarock_96:74:9e (00:13:8f:96:74:9e)
= Internet Protocol, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.128 (192.168.1.128)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 311
    Identification: 0x4e8b (20107)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0xa74b [correct]
    Source: 192.168.1.15 (192.168.1.15)
    Destination: 192.168.1.128 (192.168.1.128)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
= Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 603 Decline
      Status-Code: 603
      [Resent Packet: False]
  ⊟ Message Header
    ⊞ From: "1234"<sip:1234@192.168.1.15>;tag=725d073d
    ⊞ To: <sip:192@192.168.1.15>;tag=f5d23dc9
      CSeq: 1 INVITE
      Call-ID: 170b802c7c23fc35@cGN4eMg.
      Via: SIP/2.0/UDP 192.168.1.128:5060;branch=z9hG4bK-d87543-1451884d5f1c4665-1--d87543-;rport=5060
      Content-Length: 0
```

Figure 12.40: SIP Protocol and Debug: Call Flow

In the Status Line field it can be seen that this packet is code 603, which does not have additional content describing the reason, so it has similar characteristics to the rest of the SIP messages.

As previously indicated, it corresponds to the answers of the class:

- **4xx**: Method failure responses.
- **5xx**: Server fault responses.
- **6xx**: Global fault responses.

SIP error list

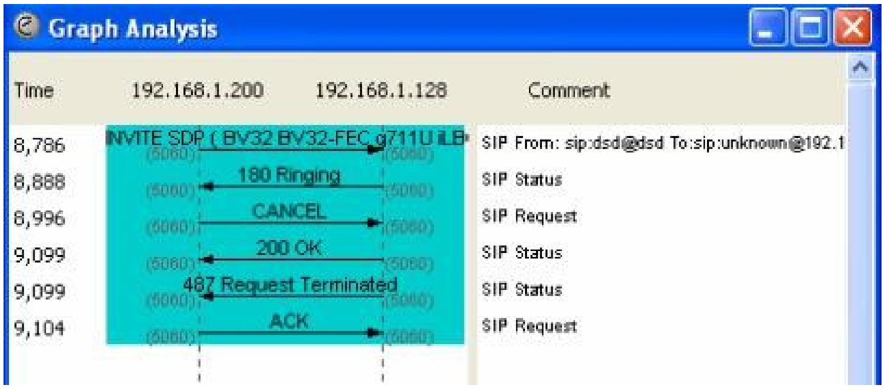
In the «**??**» section found on the **??** page, there is a complete list of SIP protocol error messages.

12.4.3.5.3 Conclusions The appearance of several unusual messages such as DECLINE, Request Terminated, etc., broadens the basic scenarios that could appear in a SIP connection (analyze SIP event table) Æ (RFC 3261).

12.4.3.6 Failed calls from softphone 1 to softphone 2

12.4.3.6.1 Objective Observe and analyze the causes for which it was not possible to establish communications.

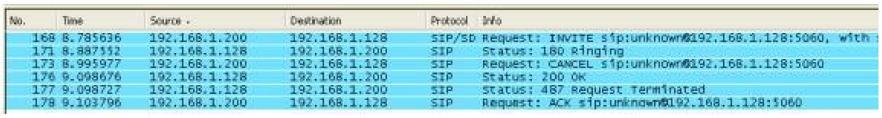
12.4.3.6.2 Development The diagram of packets exchanged between softphones is shown below.



Time	Comment
8,786	SIP From: sip:dsd@dsd To:sip:unknown@192.1
8,888	SIP Status
8,996	SIP Request
9,099	SIP Status
9,099	SIP Status
9,104	SIP Request

Figure 12.41: SIP Protocol and Debug: Call Flow

In this communication, IP Softphone: 192.168.1.200 generates a call to IP Softphone: 192.168.1.128, which responds with a Ringing indicating that it is connected and is ringing.



No.	Time	Source	Destination	Protocol	Info
168	8.785636	192.168.1.200	192.168.1.128	SIP/SD	Request: INVITE sip:unknown@192.168.1.128:5060, with
171	8.887552	192.168.1.128	192.168.1.200	SIP	Status: 180 Ringing
173	8.995977	192.168.1.200	192.168.1.128	SIP	Request: CANCEL sip:unknown@192.168.1.128:5060
176	9.098676	192.168.1.128	192.168.1.200	SIP	Status: 200 OK
177	9.098727	192.168.1.128	192.168.1.200	SIP	Status: 487 Request Terminated
178	9.103796	192.168.1.200	192.168.1.128	SIP	Request: ACK sip:unknown@192.168.1.128:5060

Figure 12.42: SIP Protocol and Debug: Ringing

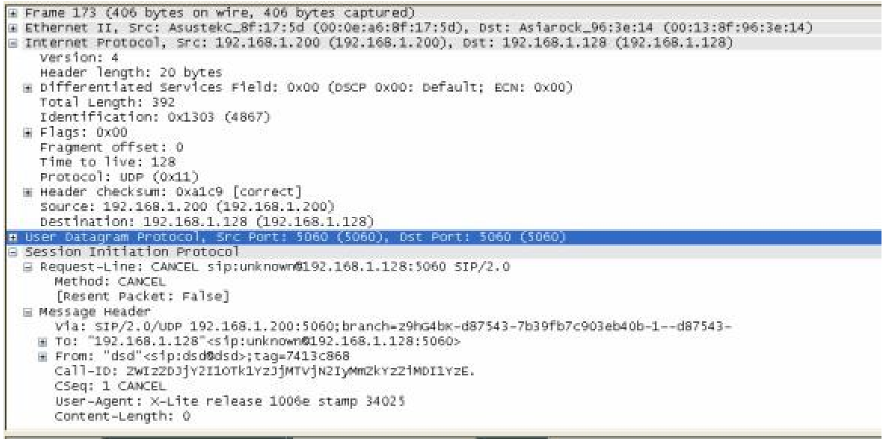
Before the receiver answers the call, the softphone that generated it terminates it, so it sends a CANCEL message to the softphone indicating that the INVITE session is canceled and asking the other softphone to stop ringing, to which it responds with an confirmation message 200 OK. Then the Softphone 128 sends the corresponding message to end the call, in this case it sends the 487 Request Terminated message, which indicates that it received a CANCEL. To which the other party responds with the ACK ending the call.

The INVITE and RINGING packages have already been explained so they are not shown.

12.4.3.6.2.1 CANCEL message The CANCEL message is sent when the person who initiated the call wants to end it before the recipient has answered or finished it, that is, cancel the INVITE request.

Sending this message is similar to asking the other party to stop calling, to which the other party responds by sending the 200 OK and the 487 message, thus allowing the call to end.

In the screenshot we see that the Req Line describes a CANCEL packet, which does not differ from the rest of the packets, because it does not contain a clarification or content field.

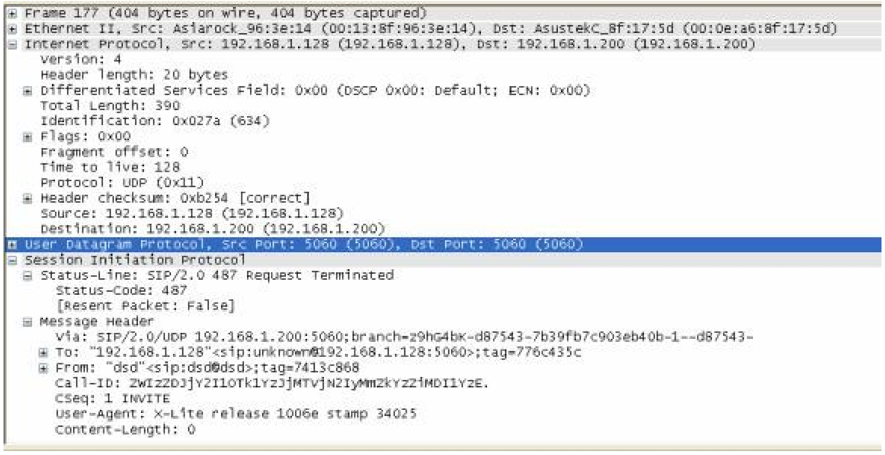


```
⊞ Frame 173 (406 bytes on wire, 406 bytes captured)
⊞ Ethernet II, Src: AsustekC_8f:17:5d (00:0e:a6:8f:17:5d), Dst: Asiarock_96:3e:14 (00:13:8f:96:3e:14)
⊟ Internet Protocol, Src: 192.168.1.200 (192.168.1.200), Dst: 192.168.1.128 (192.168.1.128)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 392
    Identification: 0x1303 (4867)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0xa1c9 [correct]
    Source: 192.168.1.200 (192.168.1.200)
    Destination: 192.168.1.128 (192.168.1.128)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: CANCEL sip:unknown@192.168.1.128:5060 SIP/2.0
      Method: CANCEL
      [Resent Packet: False]
  ⊟ Message Header
      Via: SIP/2.0/UDP 192.168.1.200:5060;branch=z9hG4bK-d87543-7b39fb7c903eb40b-1--d87543-
    ⊞ To: "192.168.1.128"<sip:unknown@192.168.1.128:5060>
    ⊞ From: "dsd"<sip:dsd@dsd>;tag=7413c868
      Call-ID: ZWIzZDJjY2I1OTk1YzJjMTVjN2IyMmZkYzZiMDI1YzE.
      CSeq: 1 CANCEL
      User-Agent: X-Lite release 1006e stamp 34025
      Content-Length: 0
```

Figure 12.43: SIP Protocol and Debug: CANCEL

12.4.3.6.2.2 487 Request Terminated This message is sent in response to a CANCEL or BYE allowing the termination of the call.

Below is the capture.



```
⊞ Frame 177 (404 bytes on wire, 404 bytes captured)
⊞ Ethernet II, Src: Asiarock_96:3e:14 (00:13:8f:96:3e:14), Dst: AsustekC_8f:17:5d (00:0e:a6:8f:17:5d)
⊟ Internet Protocol, Src: 192.168.1.128 (192.168.1.128), Dst: 192.168.1.200 (192.168.1.200)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 390
    Identification: 0x027a (634)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0xb254 [correct]
    Source: 192.168.1.128 (192.168.1.128)
    Destination: 192.168.1.200 (192.168.1.200)
⊞ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
⊟ Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 487 Request Terminated
      Status-Code: 487
      [Resent Packet: False]
  ⊟ Message Header
      Via: SIP/2.0/UDP 192.168.1.200:5060;branch=z9hG4bK-d87543-7b39fb7c903eb40b-1--d87543-
    ⊞ To: "192.168.1.128"<sip:unknown@192.168.1.128:5060>;tag=776c435c
    ⊞ From: "dsd"<sip:dsd@dsd>;tag=7413c868
      Call-ID: ZWIzZDJjY2I1OTk1YzJjMTVjN2IyMmZkYzZiMDI1YzE.
      CSeq: 1 INVITE
      User-Agent: X-Lite release 1006e stamp 34025
      Content-Length: 0
```

Figure 12.44: SIP Protocol and Debug: 487 Request Terminated

In the Status Line we see that the message sent is 487 Request Terminated. The fields of this message are similar to the previous ones because they do not have a field for clarifications or content either.

12.4.3.6.3 Conclusions We can observe in this analysis that there is an agreement with the previously detailed theoretical description regarding the CANCEL message, where the UA with the IP address: 192.168.1.128 sends a cancellation request after its INVITE request, thus concluding with the communication .

CHAPTER 13

STRESS TEST

During the *stress* tests of the Denwa UC&C 4.0.1 platforms , it will be necessary to use different tools in order to monitor the behavior of both the platform and the active computers on the local network where it will be carried out. To do this, Denwa Technology Corp. will provide a virtual machine in OVA format that will contain all the necessary elements for the process.

13.1 Virtual Machine

The virtual machine consists of an Ubuntu 16.04 LTS Desktop where ssh connection multiplexing tools , a call generator and ” The Dude” by MikroTik have been made available .

13.1.1 Initial Configuration

The virtual machine has a graphical environment from where it will be necessary to perform the network configuration manually. What is described below corresponds to the content of a PDF file, found on the user’s Desktop, in which the step by step for network configuration is described.

> **Instructions**
>
> **Preparations** Before carrying out any configuration, some network information must be validated, for this it will be necessary to open a new terminal (Crtl + Alt + T) and write the following command
>
> ```
> ifconfig -a
> ```
>
> With this information it will be possible to obtain the name of the network card within the system, which could be: eth0, enp3s0, etc.
>
> **Network Configuration** The first time you enter this virtual machine, you must configure the network parameters for it to work correctly. You can do this by clicking on the icon that you will find in the upper right

> corner of your screen. Subsequently, the option “ Edit Connections ...” After doing so, you must press the “ Add ” button, which will display a new window where you will select “Ethernet” as the connection type and you must click on “ Create ”. In the next window the following settings will be made: ethernet
>
> - Device : the network card obtained by the ifconfig –a command will be selected
> - IPv4 Settings
>   - Method: Manual
> - Addresses:
>   - Address: IP that will be assigned to the VM
>   - Netmask : Netmask (in four octets or in cidr format)
>   - Gateway: Gateway
>
> DNS Servers: IP of the DNS servers to use (must be able to resolve the domain `supportvpn.denwaip.com`). After making the above settings, you must press the ” Save ” button
>
> **Connectivity validation** Using a terminal (Crtl + Alt + T) it is possible to perform connectivity tests using the system’s own tools, such as:
>
> - ping
> - traceroute
> - telnet
> - mtr
>
> It is necessary to verify that the domain supportvpn.denwaip.com can be resolved and that the port 1199 of said domain is reachable by udp .
>
> **Support VPN Connection** From the terminal (Crtl + Alt + T) it is possible to connect the device to the Support VPN, this will be done by using the command:
>
> ```
> sudo openvpn / etc /155.ovpn &
> ```
>
> When prompted for the [sudo] password , you will need to enter: config and press the Enter key . Subsequently, through the ifconfig command , you will be able to know the IP assigned by the Support VPN, in order to provide it to the Denwa Technology Corp.
> staff
>
> ***PDF on Virtual Machine user’s Desktop***

From the above, it is important to emphasize the need for the IP assigned to this virtual machine to have the possibility of connecting to our Support VPN, in order to be able to manage it remotely.

13.1.2 Terminator

This tool is an ssh connection multiplexer , which will allow organizing the display of different queries to the Denwa teams involved in the tests, such as :

- CPU Usage
- RAM usage
- Registered Users or Agents
- Concurrent Calls

- Disk Utilization
- etc.

Each of these queries being in a different ssh session .

13.1.3 The Dude

MikroTik monitoring tool will provide us visually with the status of the network at the time of carrying out the different tests; For this, it will be necessary to have the following information:

- COMPLETE Topology the network where the monitoring will be carried out, indicating:
  - IP addresses of each unit indicating which panel it belongs to.
  - Connection ports of the equipment involved in the test.
  - Connection ports of ALL intermediate equipment, namely:
  - Routers
  - Switches
  - etc.
- Description of the type of connection between the devices:
  - ethernet
  - Giga
  - SPF
  - SPF+
  - etc.
- Credentials for queries via SNMP in any of its versions (1, 2 or 3) in:
  - Agent devices
  - ALL intermediate devices, namely:
    - Routers
    - Managed Switches
    - etc.

For example:

Figure 13.1: *stress* tests: Client-sent topology

Figure 13.2: Testing *stress*: Monitoring by «*The Dude*»

13.2 Test Bench

Once it has been possible to replicate the topology in the MikroTik «*The Dude*» tool and we have information related to the bandwidth used in each of the connections of the different equipment by which (consulted by SNMP) we will proceed to carry out the *stress* tests by using the call generator contained in the virtual machine.

In order to validate the results, each test must be repeated at least two (2) times, maintaining the maximum flow of calls for at least five (5) consecutive minutes. The tests will be carried out in stages, as follows:

- **Test 1**: 10% of the total concurrent calls contracted
- **Test 2**: 25% of the total concurrent calls contracted
- **Test 3**: 50% of the total concurrent calls contracted
- **Test 4**: 100% of the total concurrent calls contracted
- **Test 5**: 110% of the total concurrent calls contracted

The growth rate of concurrent calls, until reaching the aforementioned threshold, will be constant, and will be defined by the maximum number of simultaneous calls, since for these tests we use an audio file that has a defined duration of one hundred and twenty (120) seconds. Rate = Maximum $\frac{}{Duration}$ It should be noted that, under this test scenario, it is possible that most of the calls will not be answered by the Contact Center staff assigned for this purpose, so they will appear as ”Unanswered” in the platform Reporting .

Additionally, it is necessary to consider that the file used in our test scenarios uses the G.711-A codec, therefore, in the event that the agents’ internals or the trunk use another codec, it could generate a greater use of resources of the platform because of transcoding.

Part V

Índices

CONTENTS

This page has been intentionally left blank.

LIST OF FIGURES