

INSTALACION DE VOIP

PROYECTO CFGS-ASIR



salesianos

ATOCHA

ALEJANDRO MIGUEL SÁNCHEZ

SERGIO FERNÁNDEZ

Contenido

1.	Introducción y objetivos.....	1
1.1.	Fundamentos de la telefonía IP	1
1.2.	Objetivos	2
2.	Introducción a la voz sobre IP (VoIP)	3
2.1.	Ventajas y desventajas de VoIP.....	4
3.	Descripción de los aspectos tecnológicos	6
3.1.	Protocolos de señalización.....	6
3.1.1.	H323	6
3.1.2.	SIP	7
3.1.3.	MGCP.....	9
4.	Demostración del Funcionamiento.....	10
4.1.	Introducción	10
4.2.	Equipamiento	10
4.3.	Funcionamiento	11
4.3.1.	3CX.....	11
4.3.2.	FreePBX	26
5.	Caso Real	38
5.1.	Requisitos cliente	38
5.2.	Equipamiento	38
5.3.	Diseño de la solución.....	39
5.4.	Descripción de la solución.....	41
5.5.	Protocolos de Seguridad	42
6.	Conclusiones.....	45
7.	Bibliografía	46

Índice de ilustraciones

Ilustración 1-Conexión SIP telefonía IP	3
Ilustración 2 Protocolo H323.....	6
Ilustración 3 - Protocolo SIP	7
Ilustración 4-3CX Instalación	11
Ilustración 5-3CX	11
Ilustración 6-IP del servidor	12
Ilustración 7-3CX configuración	12
Ilustración 8-3CX subscriptions	12
Ilustración 9-3CX confirmación IP	13
Ilustración 10 - 3CX static IP	13
Ilustración 11 - 3CX dominio	14
Ilustración 12 - 3CX puertos	14
Ilustración 13 - 3CX Local IP	15
Ilustración 14 - 3CX extension length.....	15
Ilustración 15 - 3CX Email.....	16
Ilustración 16 - 3CX Time Zone.....	16
Ilustración 17 - 3CX Operator extension	17
Ilustración 18 - 3CX Countries	17
Ilustración 19 - 3CX lenguaje	18
Ilustración 20 - 3CX resumen	18
Ilustración 21 - 3CX Login	19
Ilustración 22 - 3CX Pantalla de configuración.....	19
Ilustración 23 - Tlf1 Configuración	20
Ilustración 24 - Tlf1 Estado.....	21
Ilustración 25 - Tlf1 Extensiones	21
Ilustración 26 - Tlf1 Nueva extensión.....	22
Ilustración 27 - Tlf1 Configuración extensión.....	22
Ilustración 28 - Tlf1 Asignación del teléfono a la extensión.....	23
Ilustración 29 - Tlf1 Registro completado	23
Ilustración 30 - Softphone1	24
Ilustración 31 - Softphone2.....	24
Ilustración 32 - 3CX QR conexión con softphone	25
Ilustración 33 - RasPBX ISO	26
Ilustración 34 - RasPBX Instalación	26
Ilustración 35 - FreePBX User	27
Ilustración 36 - FreePBX Información.....	27
Ilustración 37 - FreePBX Welcome	28
Ilustración 38 - FreePBX Configuración SIP	28
Ilustración 39 - FreePBX Configuración 2 SIP	29
Ilustración 40 - FreePBX Configuración puerto	29
Ilustración 41 - FreePBX Configuración 3 SIP	30
Ilustración 42 - FreePBX Configuración 4 SIP	30
Ilustración 43 - FreePBX Extensión.....	31
Ilustración 44 - FreePBX Extensión2.....	31
Ilustración 45 - FreePBX Añadir Extensión	31

Ilustración 46 - FreePBX Configurar Extensión.....	32
Ilustración 47 - Tlf2.....	32
Ilustración 48 - Tlf2 Status.....	33
Ilustración 49 - Tlf2 configuración.....	33
Ilustración 50 - Tlf2 Account 1.....	34
Ilustración 51 - Tlf2 SIP Server 1.....	34
Ilustración 52 - Zoiper	35
Ilustración 53 - Zoiper SIP UDP.....	36
Ilustración 54 - Login base de datos.....	37
Ilustración 55 - Registro de llamadas	37
Ilustración 56 - Diseño de la red.....	39
Ilustración 57- Distribución Recepción y planta 2.....	40
Ilustración 58 - Distribución planta 3 y 4	40
Ilustración 59 - Protocolo ARP petición	42
Ilustración 60 - Protocolo ARP respuesta.....	43

1. Introducción y objetivos

1.1. Fundamentos de la telefonía IP

La tecnología de voz sobre IP o VoIP es un protocolo de Internet, o lo que también puede entenderse como telefonía IP. Esta tecnología permite enviar información de voz a través de la red de datos, de manera que físicamente parece una llamada convencional, pero la forma que tiene de transmitirse es a través de internet y por la red telefónica local. Esto significa que se envía señal de voz en forma digital, en paquetes de datos, en lugar de enviarla de forma analógica. Para transformar la voz en paquetes IP es necesario que pase por un proceso de digitalización, este proceso consiste en transformar la voz en señales PCM (Pulse Code Modulation). El tráfico de voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las LAN (local area network: redes de área local). Es importante saber diferenciar entre voz sobre IP (VoIP) y telefonía sobre IP. VoIP es el conjunto de normas, dispositivos, protocolos que permite transmitir voz sobre el protocolo IP, en cambio, la telefonía sobre IP es el servicio telefónico disponible al público, por tanto, con numeración realizado con la tecnología de VoIP. Para que exista una comunicación deben existir varios factores o elementos: cliente, servidores, Gateway.

El **cliente** comienza la comunicación mediante voz, esta información se recibe a través del micrófono del usuario, esta información se codifica y empaqueta, y de la misma forma se decodifica y reproduce a través de los altavoces o auriculares (salida de la información).

El **servidor** se encarga de manejar operaciones de bases de datos, realizado en un tiempo real como en uno fuera de él. El servidor hace posible que la información se transmita entre los dos usuarios.

Los **Gateway** o puertas de enlace brindan un puente de comunicación entre todos los usuarios, su función principal es la de proveer interfaces con la telefonía tradicional adecuada, la cual funcionara como una plataforma para los usuarios. Los Gateway se utilizan para dar por finalizada la llamada.

1.2. Objetivos

El crecimiento de los servicios de telefonía sobre IP en el ámbito empresarial abre una oportunidad de negocio para las empresas integradoras de este servicio. Para este proyecto se pretende profundizar en la tecnología de VoIP, así como tratar de explicar detalladamente el diseño e implementación en un caso real la infraestructura de una red compuesta por dicha tecnología. Otros objetivos que se adquirirán:

- ❖ Ampliación de los conocimientos sobre protocolos, complementado los con los adquiridos durante el curso.
- ❖ Conocimientos sobre la tecnología de VoIP, así como su instalación y configuración.
- ❖ Desarrollo de una red de telefonía IP.
- ❖ Conocimientos de configuración e instalación de los servicios requeridos para la realización del proyecto.

2. Introducción a la voz sobre IP (VoIP)

La historia de la VoIP es relativamente reciente, comenzó con un proveedor israelí de equipamiento de telecomunicaciones, lanzó el primer softphone llamado "Internet Phone Software". En 1998 aparecieron los primeros adaptadores telefónicos analógicos (ATA) y Gateway que permitían la comunicación desde un ordenador a teléfono convencional (PSTN) y también de un teléfono convencional a otro mediante convertidores externos. Es en 1999 cuando la empresa Cisco comercializa por primera vez sus primeras plataformas corporativas para VoIP. Pero fue en el 2000, gracias a Mark Spencer de la Universidad de Auburn, cuando crea la primera central telefónica basada en Linux y de código abierto, Asterisk. 2 años más tarde, en 2002, surge el protocolo de señalización SIP y este comienza a desplazar al protocolo anterior, H323 comercializado por Cisco en 1999. Hoy en día se ha vuelto fundamental la voz sobre IP para el desarrollo de las Telecomunicaciones siendo más fácil y práctico el uso de la tecnología.

Hoy en día existen dos tipos de implementación de VoIP, la primera forma es la más sencilla, VoIP alojado, es decir comprar el servicio a un proveedor externo. El desplazamiento a la nube está haciendo que muchos productos recurran a este tipo de servicios porque ofrecen mejores funciones en cuanto a acceso, flexibilidad y movilidad. Es sencillo puesto que solo es necesaria una conexión a internet, con suficiente ancho de banda y teléfonos habilitados para la VoIP. Este servicio conlleva que no se tenga que mantener tu propio sistema telefónico. En cambio, existe otra manera de implementación del sistema, este método es SIP Trunk, es similar a los sistemas PBX tradicionales. Para poder realizar esta implementación es necesario tener un servidor con PBX y otros equipos telefónicos en la instalación. Es necesario tener conectado el SIP Trunk con la compañía de internet o cualquier red de datos pues que es la que va a dar el soporte de internet requerido.

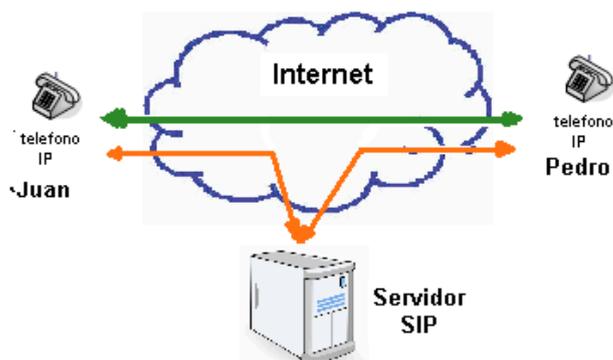


Ilustración 1-Conexión SIP telefonía IP

2.1. Ventajas y desventajas de VoIP

La principal ventaja que se puede apreciar en este tipo de servicios es su bajo coste, debido al ahorro en gastos de telefonía debido a que la información se transmite en forma de paquetes. La codificación de la información es otra de las ventajas que se puede apreciar en este tipo de servicios, para ello se han desarrollado los llamados códecs, han permitido que la voz se codifique en paquetes de datos cada vez más pequeños. Esto deriva en que las comunicaciones de voz sobre IP requieran anchos de banda muy reducidos.

Otro factor a favor de la tecnología de VoIP es la integración de sus elementos con otros servicios existentes como video, mensajería, intercambio de datos, etc. de forma simultánea y con otros usuarios que también estén en línea. El número de canales de comunicación es más amplio, debido a que en la comunicación telefónica analógica había que elegir el número de líneas que necesitabas contratar, en este caso es ilimitado puesto que se pueden contar con los canales simultáneos que se necesiten.

Diversidad de funciones incluidas en el propio servidor, puesto que la VoIP no solo se limita a llamadas telefónicas, sino que hay diferentes servicios dentro del mismo como la identificación de llamadas, respuestas de voz interactivas, videollamadas, grabación de llamadas, envío de la grabación que alguien deja en el buzón a una cuenta de correo. La alta calidad del sonido, los datos al transmitirse por paquetes no existen interferencias o ruidos como si puede ocurrir en la tecnología telefónica analógica.

Las posibles desventajas de este servicio son las relacionadas con la conexión y el ancho de banda proporcionado por la compañía de internet. Pues que los principales problemas son los retrasos, cortes por la conexión, etc. La calidad de la llamada puede verse afectada, ya que los datos viajan en forma de paquetes y algunos de esos paquetes se pueden perder. Al igual que se solventan algunos problemas respecto a la telefonía analógica, como se ha visto anteriormente, como el ruido o interferencias, surgen nuevos problemas, al distribirse la información en paquetes.

Otra desventaja relacionada con esto es la latencia, debido a que en una comunicación no es adecuado tener un retardo en la transmisión de información, por eso hay que controlar el uso de la red correctamente para garantizar una transmisión adecuada. Para ello también existen protocolos de actuación como es el protocolo RTP (Real-Time Protocol), que asegura que los paquetes han llegado a su destino en el tiempo en que se envían.

Debido a que está basado en la conexión a internet, otra desventaja es la seguridad en el sistema, puesto que puede haber robo de datos si la seguridad no es la correcta. Un cracker puede tener acceso al servido VoIP y a los datos almacenados y al propio servicio telefónico para escuchar conversaciones, si la empresa utiliza este tipo de servicio para comunicarse con información delicada. Relacionado con la seguridad, un virus puede afectar al sistema y corromperlo entero, puede infectar algún equipo del servidor y el servicio telefónico puede quedar interrumpido. También pueden verse afectados otros equipos que estén conectados al sistema. Debido a este problema pueden surgir otros nuevos, como la suplantación de ID y engaños especializados. Al ser una comunicación entre dos usuarios, si existe una brecha de seguridad como la que se comenta, es posible que se cuele un *man in the middle* este tipo de hackeo consiste en que entre medias de la comunicación se establece el hacker interceptando la información transmitida entre los dos usuarios. La mejor forma de solventar estas opciones es realizando una buena seguridad en la instalación, y aunque es imposible tener todo al 100% seguro, es posible evitar cierto tipo de ataques con una buena seguridad en el sistema.

3. Descripción de los aspectos tecnológicos

3.1. Protocolos de señalización

El protocolo de señalización es un lenguaje común en teléfonos, servidores de gestión de llamadas, sistemas PBX, etc., estos sistemas necesitan un medio para establecer, controlar y finalizar las llamadas. La tecnología de VoIP ofrece varios protocolos de señalización. Los protocolos más utilizados en Asterisk son SIP, IAX2, H323, MGCP. En los próximos puntos se estudiarán algunos de los protocolos citados anteriormente.

3.1.1. H323

El protocolo H323 aparece por primera vez en 1999, gracias a la empresa Cisco cuando comienzan a comercializar plataformas corporativas para VoIP con este tipo de protocolo de señalización. Se creó originalmente para proveer de un mecanismo para el transporte de aplicaciones multimedia en LANs (Redes de área local) pero ha evolucionado rápidamente para dirigir las necesidades de las redes de VoIP. El protocolo H323 es un protocolo diseñado para la configuración, administración y terminación de una sesión de comunicación (media). Es un conjunto de estándares ITU-T, los cuales definen un conjunto de protocolos para proveer comunicación visual y de audio sobre una red de computadores.

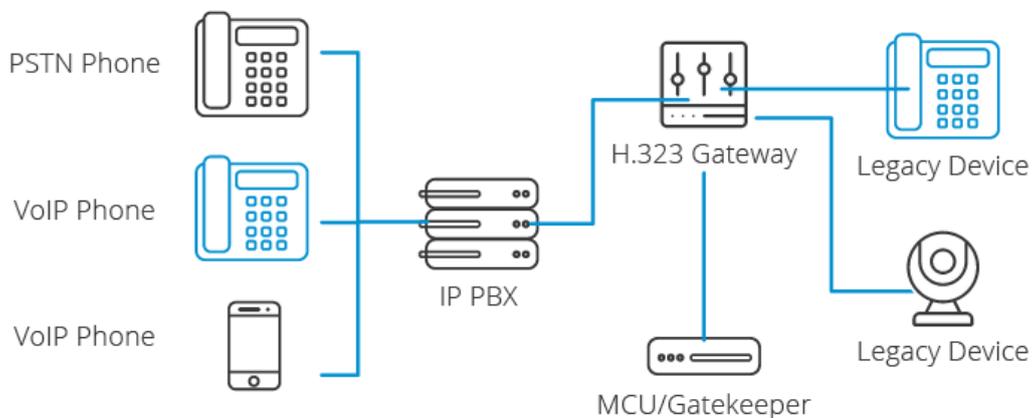


Ilustración 2 Protocolo H323

H323 es un protocolo relativamente antiguo, reemplazado en gran medida por SIP (Session Initiation Protocol), siendo este último mucho menos complejo. El H323 no fue diseñado para una fácil expansibilidad, está diseñado desde cero para ser extensible. Es independiente de la topología de la red y admite pasarelas, permitiendo usar más de un canal de cada tipo (voz, video, datos) al mismo tiempo. La topología de una red basada en H323:

- Portero: realiza el control de llamada en una zona. Es opcional pero su uso está recomendado. Traduce direcciones, ofrece servicio de directorio, control de admisión de terminales, control de consumo de recursos y procesa la autorización de llamadas, así como también puede encaminar la señalización.
- Pasarela: es el acceso a otras redes, de modo que realiza funciones de transcodificación y de traducción de señalización.
- MCU: soporte multiconferencia. Se encarga de la negociación de capacidades.

3.1.2. SIP

El protocolo de inicio de sesión o SIP es un protocolo desarrollado por el grupo de trabajo MMUSIC de IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia. Este protocolo se vale de las funciones aportadas por otros protocolos, que da por hechas y no vuelve a desarrollar. Debido a esto, SIP funciona en colaboración con otros muchos protocolos. Otro concepto importante en su diseño es de extensibilidad. Esto significa que las funciones básicas del protocolo, definidas en la [RFC 3261](#), pueden ser extendidas mediante otra RFC (*Request for Comments*) dotando al protocolo de funciones más potentes. Las funciones básicas del protocolo incluyen:

- Determinar la ubicación de los usuarios, aportando movilidad.
- Establecer, modificar y terminar sesiones multipartitas entre usuarios.

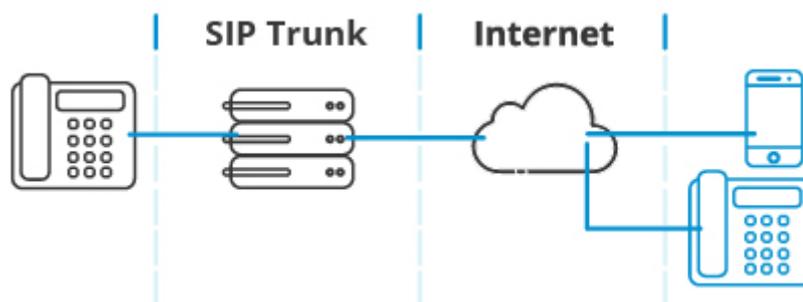


Ilustración 3 - Protocolo SIP

El protocolo SIP permite el establecimiento de sesiones multimedia entre dos o más usuarios. Para hacerlo se vale del intercambio de mensajes entre las partes que quieren comunicarse. Para que se lleve a cabo el funcionamiento de este protocolo intervienen una serie de elementos que se explican a continuación.

Los usuarios que pueden ser seres humanos o aplicaciones de software utilizan para establecer sesiones lo que el protocolo SIP denomina "**Agentes de usuario**". Estos no son más que los puntos extremos del protocolo, es decir son los que emiten y consumen los mensajes del protocolo SIP. Un videoteléfono, un teléfono, un cliente de software (softphone) y cualquier otro dispositivo similar es para el protocolo SIP un agente de usuario. El protocolo SIP no se ocupa de la interfaz de estos dispositivos con el usuario final, sólo se interesa por los mensajes que estos generan y cómo se comportan al recibir determinados mensajes.

Los agentes de usuario se comportan como clientes (UAC: User Agent Clients) y como servidores (UAS: User Agent Servers). Son UAC cuando realizan una petición y son UAS cuando la reciben. Por esto los agentes de usuario deben implementar un UAC y un UAS.

El protocolo SIP permite establecer la ubicación física de un usuario determinado, eso es, en qué punto de la red está conectado. Para ello se vale del **mecanismo de registro**. Este mecanismo funciona de tal forma que cada usuario tiene una dirección lógica que es invariable respecto de la ubicación física del usuario. Una dirección lógica del protocolo SIP es de la forma *usuario@dominio*, es decir, tiene la misma forma que una dirección de correo electrónico. La dirección física es dependiente del lugar en donde el usuario está conectado. Cuando un usuario inicializa su terminal (por ejemplo, conectando su teléfono o abriendo su software de telefonía SIP) el agente de usuario SIP que reside en dicho terminal envía una petición con el método REGISTER a un Servidor de Registro, informado a qué dirección física debe asociarse la dirección lógica del usuario. El servidor de registro realiza entonces dicha asociación. Esta asociación tiene un período de vigencia y si no es renovada, caduca. También puede terminarse mediante un des-registro. La forma en que dicha asociación es almacenada en la red no es determinada por el protocolo SIP, pero es vital que los elementos de la red SIP accedan a dicha información.

Los **servidores proxy** o de redirección se utilizan para encaminar un mensaje entre un agente de usuario cliente y un agente de usuario servidor. Estos servidores pueden actuar de dos maneras:

- Como proxy, encaminando el mensaje hacia destino
- Como redirector generando una respuesta que indica al origen la dirección del destino o de otro servidor que lo acerque al destino

3.1.3. MGCP

El protocolo Media Gateway Control Protocol (MGCP) es un protocolo de control de dispositivos, donde un gateway esclavo es controlado por uno maestro. Ese es un protocolo interno de voz sobre IP cuya arquitectura se diferencia del resto de los protocolos VoIP por ser del tipo cliente – servidor. MGCP está definido informalmente RFC 3435, y aunque no ostenta el rango de estándar, su sucesor Megaco está aceptado y definido como una recomendación RFC 3015. El punto fuerte de este protocolo es la centralización de la administración en un solo Gateway como consecuencia de una gran escalabilidad. Estos dos tipos de gateway están definidos en el protocolo de la siguiente manera:

- ❖ Media Gateway: este es equipo esclavo, es en este tipo de equipos donde se conectan los puntos finales, y cada vez que ocurre cualquier evento es necesario informar al otro tipo de equipos que componen este protocolo.
- ❖ Media Gateway Controller: En este tipo de Gateway es donde reside la inteligencia del protocolo, este equipo tiene la funcionalidad de controlar al resto de gateway.

4. Demostración del Funcionamiento

4.1. Introducción

El sistema de VoIP utilizado en este proyecto se exponen dos casos de instalación. En el primer caso se instala en el servidor una centralita con el software 3cx. Este es un software cerrado que permite la gestión del servicio. Gracias a este software se pueden gestionar diferentes procesos, y diferentes funcionamientos de la aplicación, como la gestión de videollamadas, correo, etc.

Por otro lado, se procederá a la instalación de un servidor LAMP con FreePBX. El servidor LAMP se encargará de dar servicios como un Sistema Operativo, Linux, un servidor web como es Apache. Un gestor de base de datos, MySQL y PHP, un desarrollador web, utilizado para visualizar un tipo concreto de lenguaje de programación como es php. A este servidor hay que complementarle una interfaz gráfica de código abierto basado en web que dirige y contra Asterisk, un servidor de VoIP, esta interfaz es FreePBX.

4.2. Equipamiento

Para la realización de este proyecto hay elementos con los que se deben contar para ello se muestran a continuación.

El primer componente que se debe tener en cuenta es el **router**, es el que va a distribuir toda la red y proporcionará las IP correspondientes. A este dispositivo se conectará un Switch de capa 2, cuya función tendrá poder conectar los dispositivos que necesiten tener una conectividad a la red con cable, como los **teléfonos IP**, el **ordenador** para realizar la configuración, y la **raspberry**, que funcionará como servidor.

Los **teléfonos IP** es un teléfono convencional diseñado para trabajar con la tecnología de VoIP, SIP la más popular. Para realizar la configuración de estos teléfonos se necesitará un **ordenador** conectado a la misma red, puesto que si este requisito no se cumple no se podrá acceder a la configuración de estos. Se utilizará este dispositivo también para realizar la instalación del software necesario en la **raspberry** mediante los protocolos SSH o VNC, protocolos diseñados para conectar un dispositivo con otro de forma remota, esta última será utilizada para la instalación de los servicios necesarios, principalmente el servicio de VoIP se trabajará con ella simulando un servidor mucho mas grande como se podrá comprobar en el caso real expuesto en el siguiente apartado. En este dispositivo se realizará la instalación de un Sistema Operativo, dependerá del caso escogido se instalará uno con interfaz gráfica, en el otro caso el Sistema Operativo se deberá manejar mediante línea de consola.

4.3.Funcionamiento

4.3.1. 3CX

Para utilizar 3CX lo único que se necesita es un sistema operativo, basado en Linux o en Windows que se instalemos esta plataforma de comunicaciones. En nuestro caso hemos utilizado Debian, una variante de Linux, y la hemos instalado en una Raspberry Pi, a la que hemos asignado una IP fija: 172.16.112.61.

Lo siguiente sería instalar 3CX en nuestra Raspberry, por lo que tendremos que abrir la consola de comandos y ejecutar el siguiente script de instalación:

```
“wget https://downloads-global.3cx.com/downloads/misc/d10pi.zip; sudo bash d10pi.zip “
```

Esto hará que se inicie el proceso de instalación de 3CX. Pasados unos segundos se nos abrirá una ventana en la que seleccionaremos la variante de 3CX que queremos instalar, en nuestro caso hemos seleccionado la variante estándar, es decir, la primera opción:

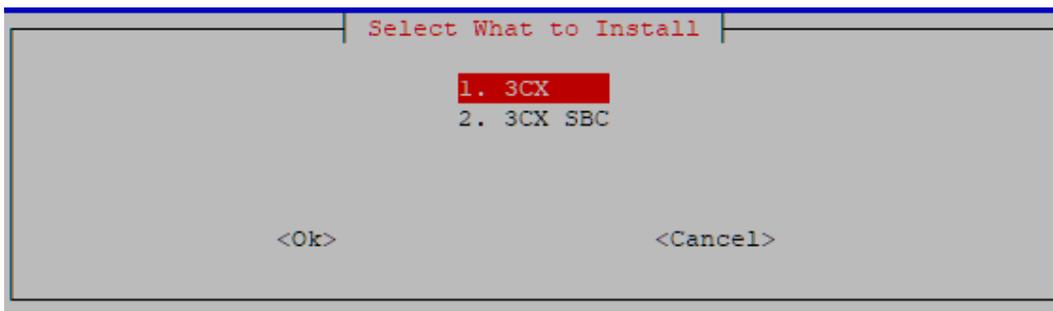


Ilustración 4-3CX Instalación

Al cabo de un rato, nos dará a elegir cómo queremos configurar 3CX e introducir nuestra información personal, a través del navegador o de la línea de comandos. Nosotros hemos utilizado la primera opción, mediante el navegador.

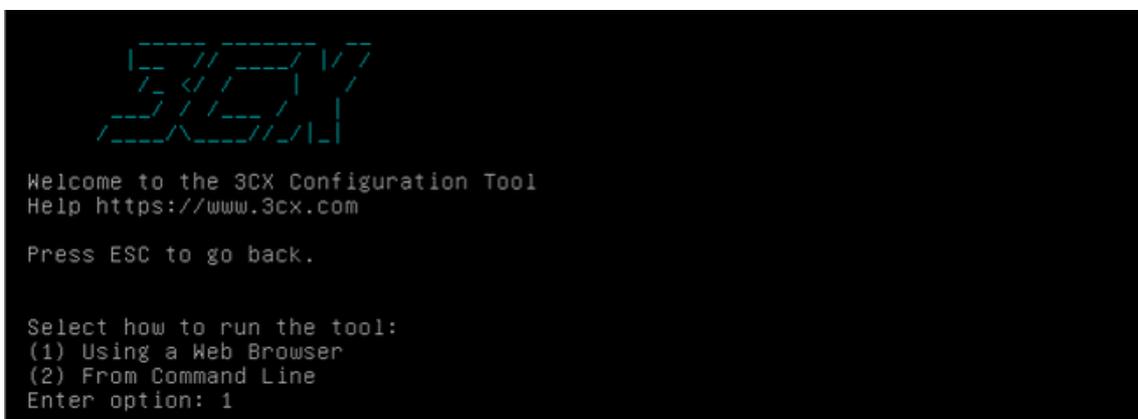


Ilustración 5-3CX

Cuando seleccionamos la opción 1, nos dará unas indicaciones junto con la dirección IP seguido del puerto 5015, que tendremos que introducir en el navegador.



Ilustración 6-IP del servidor

Al introducirlo, se nos abrirá un asistente de configuración que nos guiará por diversos pasos que tendremos que completar antes de poder acceder a 3CX. El primer paso es el siguiente:

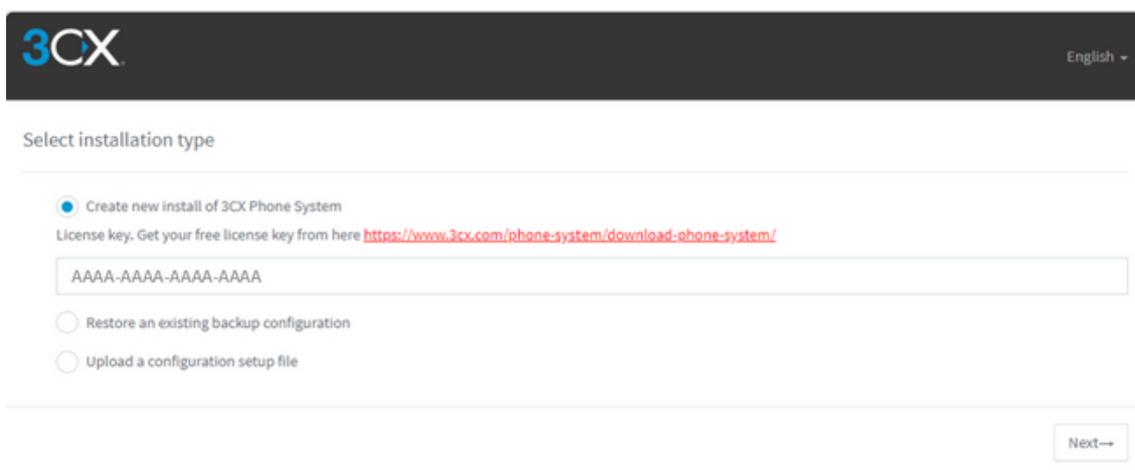


Ilustración 7-3CX configuración

Seleccionaremos la primera opción en la que tendremos que añadir la clave de la cuenta. Si aún no tenemos la clave, solo tendremos que ir al enlace que hay en pantalla, registrarnos con nuestros datos, y consultar nuestra clave en el apartado SUBSCRIPTIONS.

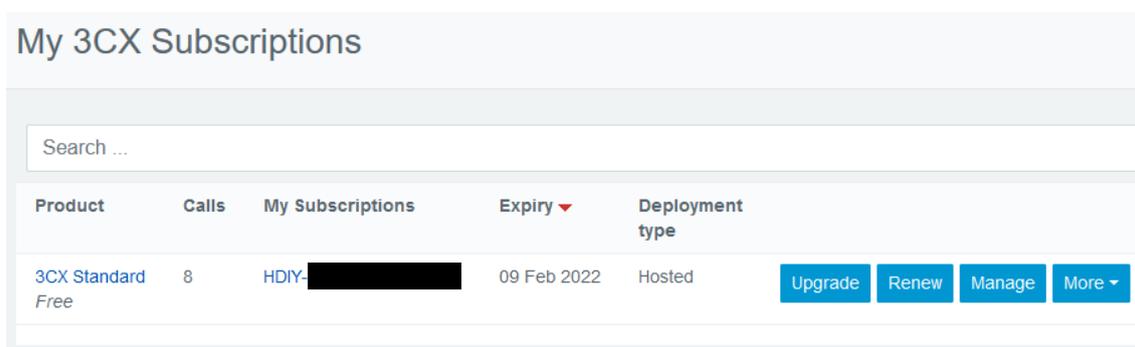


Ilustración 8-3CX subscriptions

Una vez introducida, le daremos a NEXT y el siguiente paso será asignarnos un nombre de usuario y una contraseña que permitirá acceder a la consola de administración de nuestra centralita.

El tercer paso sería confirmar que nuestra IP publica es detectada correctamente por el software.



Ilustración 9-3CX confirmación IP

En el siguiente paso el asistente de configuración nos pregunta si vamos a utilizar una IP estática o una IP dinámica, en nuestro caso seleccionamos estática.

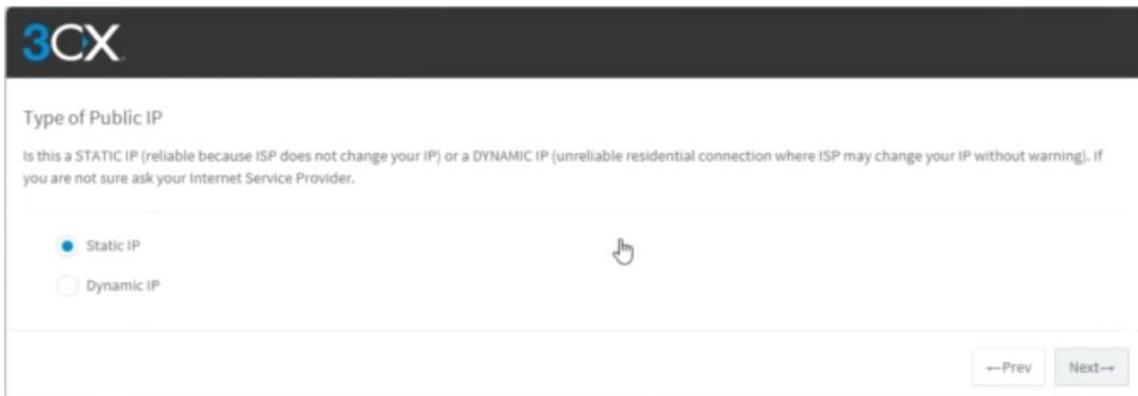


Ilustración 10 - 3CX static IP

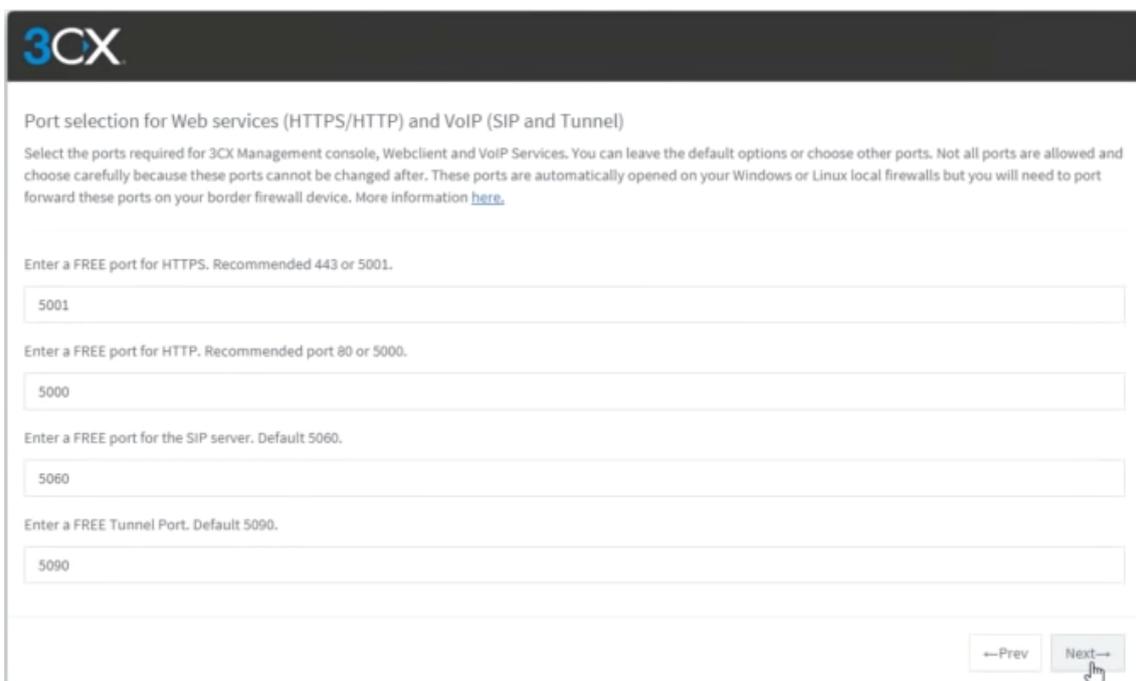
A continuación, seleccionamos el nombre del dominio y la región a la que pertenecemos



The screenshot shows the 3CX installation wizard interface. At the top left is the 3CX logo. The main heading is "Select your preferred Subdomain/FQDN". Below this, there is a text input field labeled "Enter a name:". Underneath is a dropdown menu labeled "Select Domain Group:" with "Africa" selected. Below that is another dropdown menu labeled "Select your preferred domain suffix:" with "3cx.co.za (South Africa)" selected. At the bottom right, there are two buttons: "←Prev" and "Next→".

Ilustración 11 - 3CX dominio

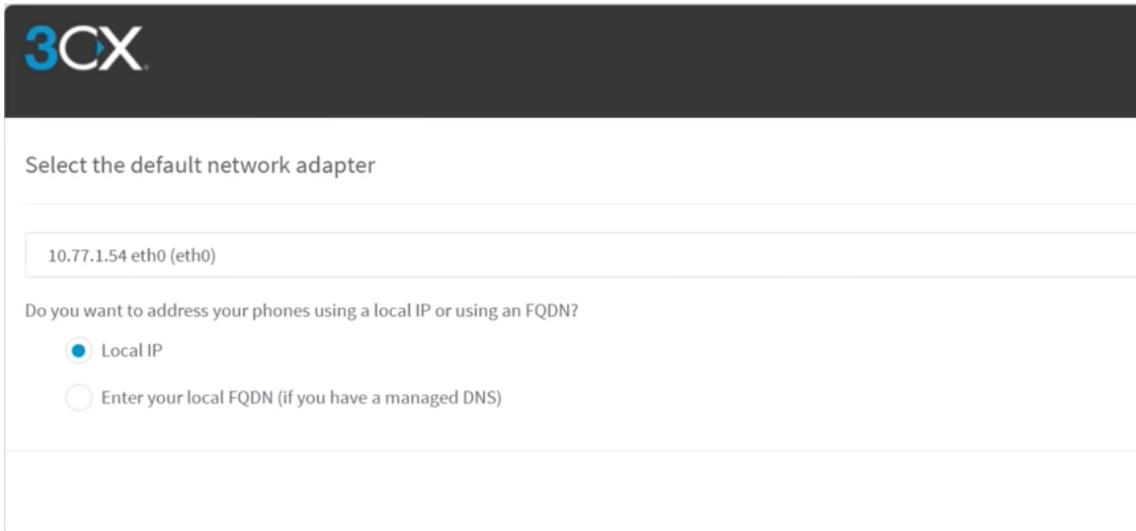
En la siguiente ventana, introduciremos los puertos de los diferentes protocolos que manejaremos, aunque nosotros los hemos dejado por defecto.



The screenshot shows the 3CX installation wizard interface for port selection. At the top left is the 3CX logo. The main heading is "Port selection for Web services (HTTPS/HTTP) and VoIP (SIP and Tunnel)". Below this is a paragraph of instructions: "Select the ports required for 3CX Management console, Webclient and VoIP Services. You can leave the default options or choose other ports. Not all ports are allowed and choose carefully because these ports cannot be changed after. These ports are automatically opened on your Windows or Linux local firewalls but you will need to port forward these ports on your border firewall device. More information [here](#)." Below the instructions are four input fields, each with a label and a default value: "Enter a FREE port for HTTPS. Recommended 443 or 5001." with "5001" entered; "Enter a FREE port for HTTP. Recommended port 80 or 5000." with "5000" entered; "Enter a FREE port for the SIP server. Default 5060." with "5060" entered; and "Enter a FREE Tunnel Port. Default 5090." with "5090" entered. At the bottom right, there are two buttons: "←Prev" and "Next→", with a mouse cursor clicking on the "Next→" button.

Ilustración 12 - 3CX puertos

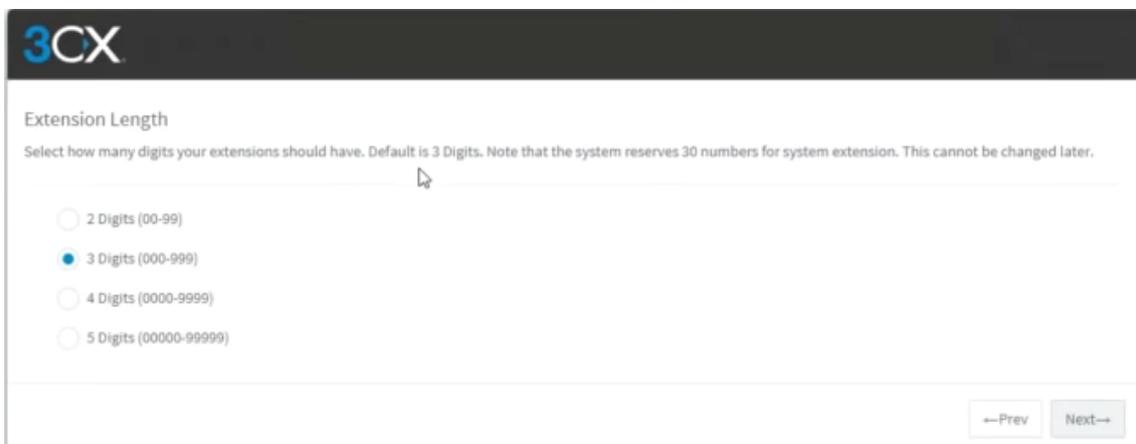
Seleccionamos el tipo de adaptador de red que queramos, en nuestro caso seleccionamos la IP Local como adaptador por defecto.



The screenshot shows the 3CX configuration interface. At the top, the 3CX logo is displayed. Below it, the heading "Select the default network adapter" is visible. A text input field contains the IP address "10.77.1.54" and the interface name "eth0 (eth0)". Below this, a question asks "Do you want to address your phones using a local IP or using an FQDN?". There are two radio button options: "Local IP" (which is selected) and "Enter your local FQDN (if you have a managed DNS)".

Ilustración 13 - 3CX Local IP

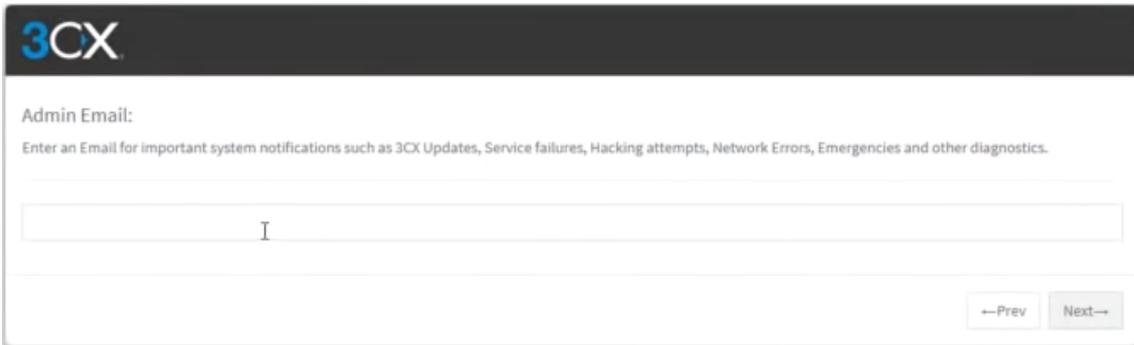
Cuando hayamos terminado este paso, se llevará a cabo un proceso de carga durante unos minutos. Al concluir este, tendremos que seleccionar el número de dígitos que queremos que nuestras extensiones tengan. Nosotros hemos seleccionado 4 dígitos, pero son preferencias independientes a cada usuario.



The screenshot shows the 3CX configuration interface for "Extension Length". The heading is "Extension Length". Below it, a note states: "Select how many digits your extensions should have. Default is 3 Digits. Note that the system reserves 30 numbers for system extension. This cannot be changed later." There are four radio button options: "2 Digits (00-99)", "3 Digits (000-999)", "4 Digits (0000-9999)", and "5 Digits (00000-99999)". The "3 Digits (000-999)" option is selected. At the bottom right, there are "Prev" and "Next" navigation buttons.

Ilustración 14 - 3CX extension length

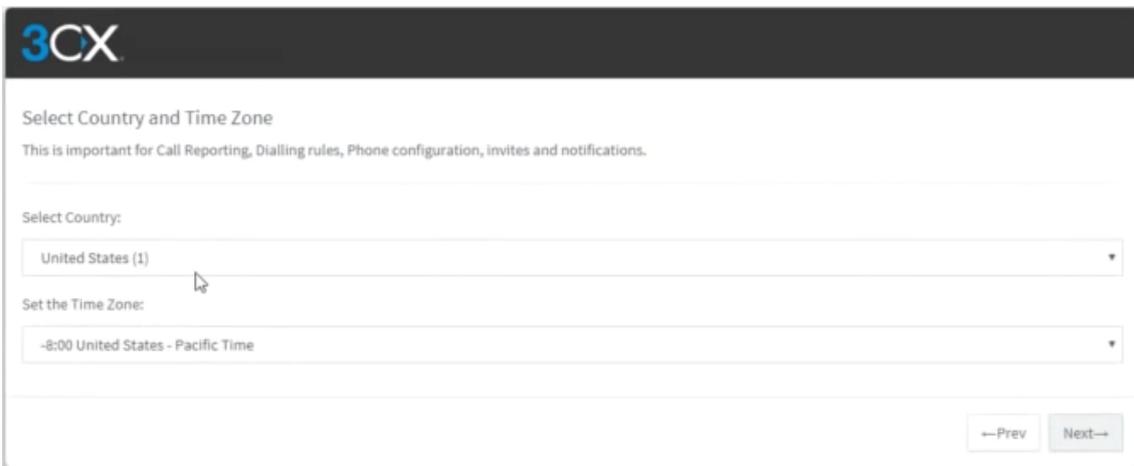
Añadimos una dirección de correo para la administración.



The screenshot shows the 3CX Admin Email configuration page. At the top left is the 3CX logo. Below it, the text 'Admin Email:' is followed by a descriptive sentence: 'Enter an Email for important system notifications such as 3CX Updates, Service failures, Hacking attempts, Network Errors, Emergencies and other diagnostics.' There is a large text input field with a cursor. At the bottom right, there are two buttons: '←Prev' and 'Next→'.

Ilustración 15 - 3CX Email

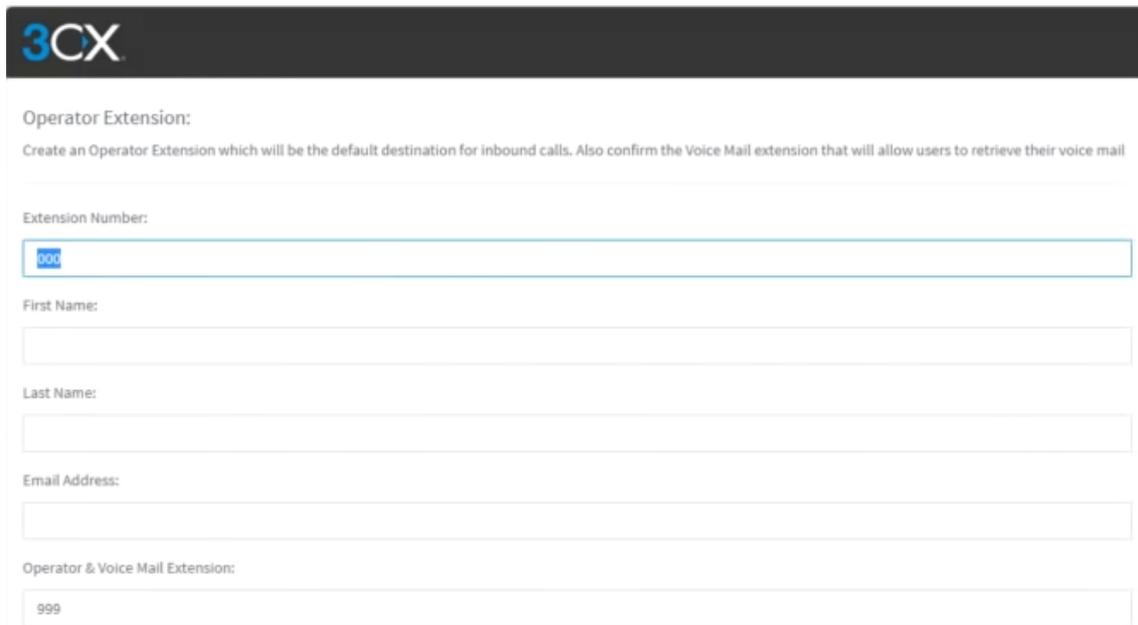
Seleccionamos nuestro país y zona horaria



The screenshot shows the 3CX 'Select Country and Time Zone' configuration page. At the top left is the 3CX logo. Below it, the text 'Select Country and Time Zone' is followed by a descriptive sentence: 'This is important for Call Reporting, Dialling rules, Phone configuration, invites and notifications.' There are two dropdown menus. The first is labeled 'Select Country:' and has 'United States (1)' selected. The second is labeled 'Set the Time Zone:' and has '-8:00 United States - Pacific Time' selected. At the bottom right, there are two buttons: '←Prev' and 'Next→'.

Ilustración 16 - 3CX Time Zone

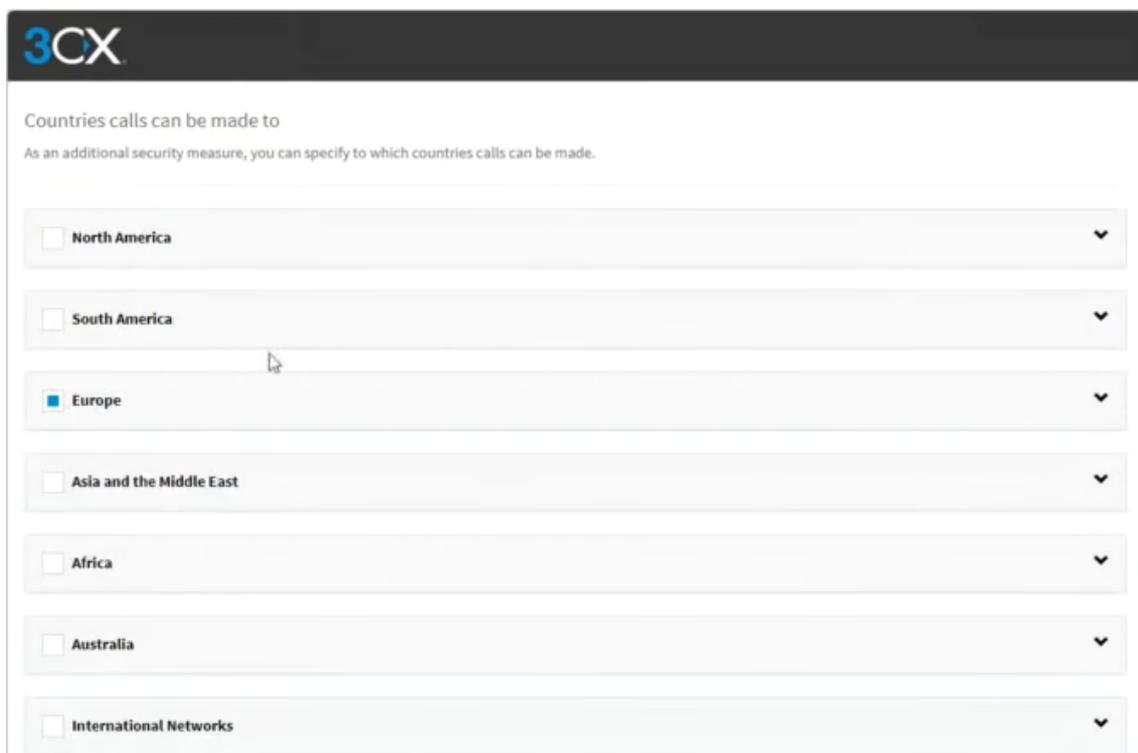
Ahora vamos a crear una extensión para el Operador, que es el destino por defecto de las llamadas perdidas. Añadimos una extensión, un nombre, email y una extensión para el buzón de voz.



The screenshot shows the 'Operator Extension' configuration page in the 3CX interface. The page title is 'Operator Extension:' and it includes a sub-header: 'Create an Operator Extension which will be the default destination for inbound calls. Also confirm the Voice Mail extension that will allow users to retrieve their voice mail'. The form contains several input fields: 'Extension Number' (with '300' entered), 'First Name', 'Last Name', 'Email Address', and 'Operator & Voice Mail Extension' (with '999' entered).

Ilustración 17 - 3CX Operator extension

Lo siguiente que tendremos que hacer es seleccionar la región desde la cual podemos recibir llamadas, en nuestro caso hemos seleccionado únicamente Europa y España.



The screenshot shows the 'Countries calls can be made to' configuration page in the 3CX interface. The page title is 'Countries calls can be made to' and it includes a sub-header: 'As an additional security measure, you can specify to which countries calls can be made.' The form contains a list of regions with checkboxes and dropdown arrows: 'North America', 'South America', 'Europe' (selected), 'Asia and the Middle East', 'Africa', 'Australia', and 'International Networks'.

Ilustración 18 - 3CX Countries

Seleccionamos el lenguaje deseado.

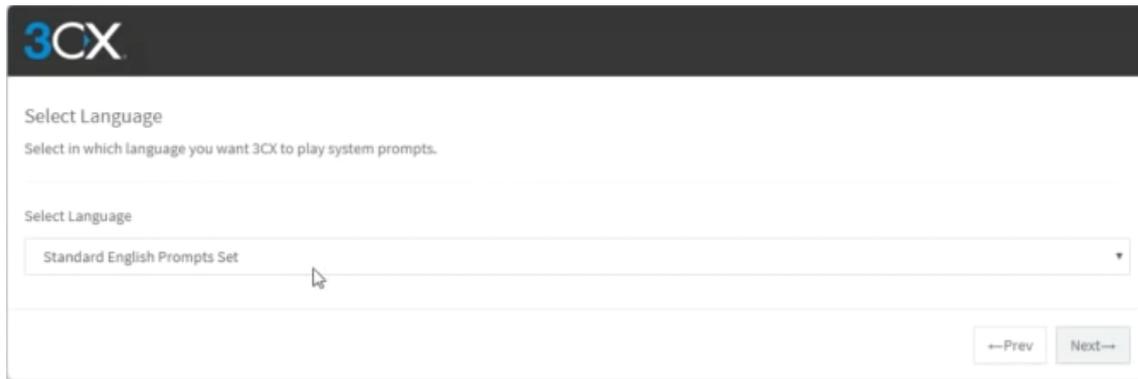


Ilustración 19 - 3CX lenguaje

Al darle a NEXT se iniciará otro proceso de carga. Por último, nos mostrará una especie de resumen de nuestras configuraciones, y del siguiente paso a realizar.

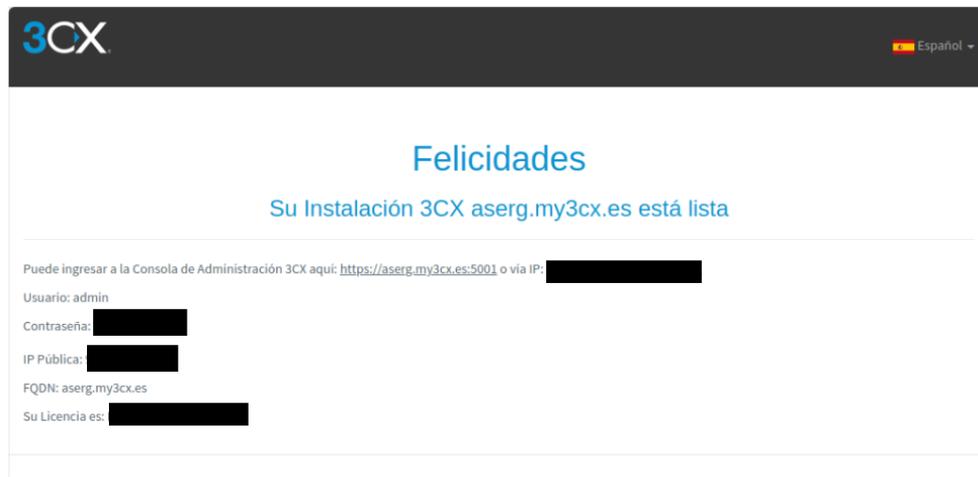


Ilustración 20 - 3CX resumen

Como vemos en la primera línea de la imagen anterior, para ingresar en la consola de administración tendremos que ir al navegador y entrar en la URL que nos indica. Al ser un nombre de dominio podemos utilizar si lo deseamos la IP por lo que en este caso buscaríamos esto: <http://172.16.112.61:5001>, que nos llevará al Login de nuestra consola de administración

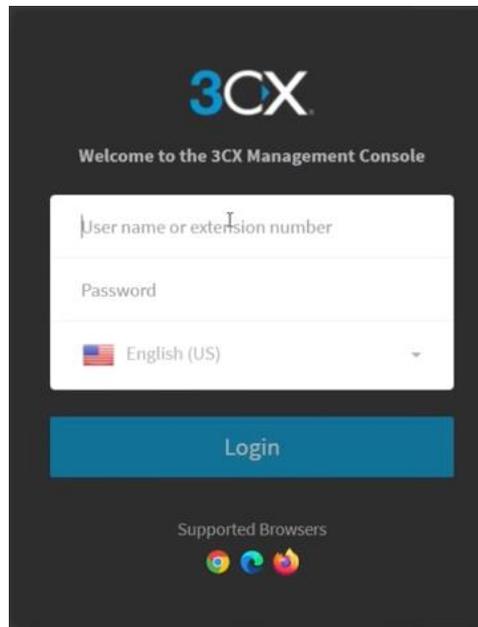


Ilustración 21 - 3CX Login

Añadimos el nombre de usuario y la contraseña que previamente hemos configurado y con esto ya entraríamos en la consola.

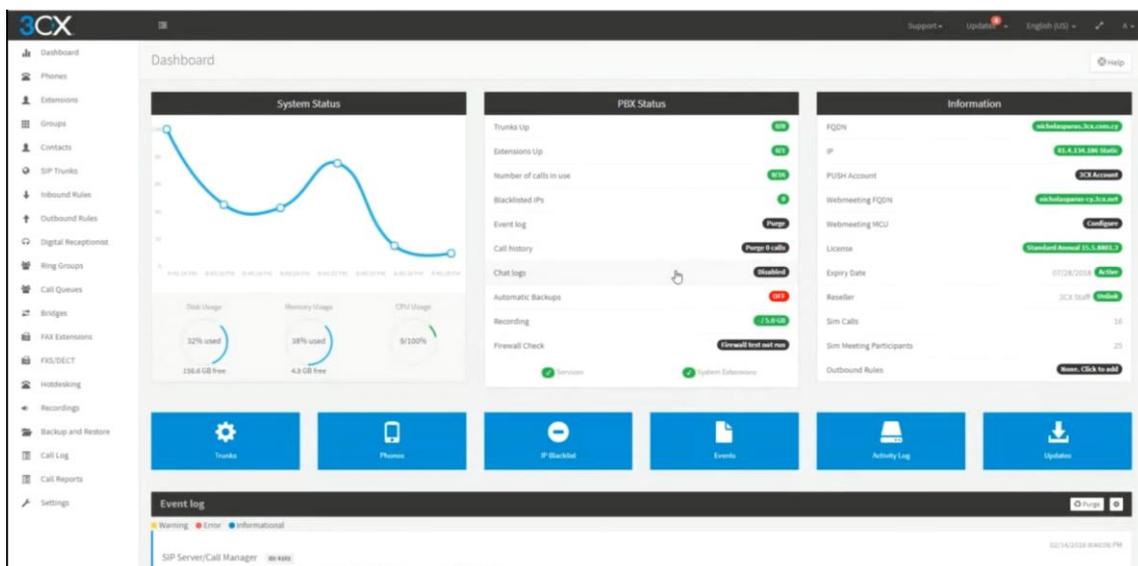


Ilustración 22 - 3CX Pantalla de configuración

Ahora vamos a pasar a la configuración de los teléfonos IP y de los móviles. Lo primero que tenemos que hacer es conectar nuestro teléfono fijo a nuestra red, y asignarle una IP fija. En nuestro caso podemos hacerlo de dos maneras, físicamente en el teléfono en cuestión, en el menú de configuración o a través del navegador, introduciendo la IP actual y cambiándola en los ajustes. Nosotros hemos optado por la segunda opción, por lo que el primer paso es buscar la IP que nos ha asignado el router en cuestión. Esto se consigue metiéndose en la configuración del teléfono fijo, si no consiguiéramos encontrarla, podríamos recurrir al manual del teléfono. La IP asignada al nuestro teléfono es la 172.16.113.115, por lo que cogemos esa dirección IP y la introducimos en nuestro navegador.

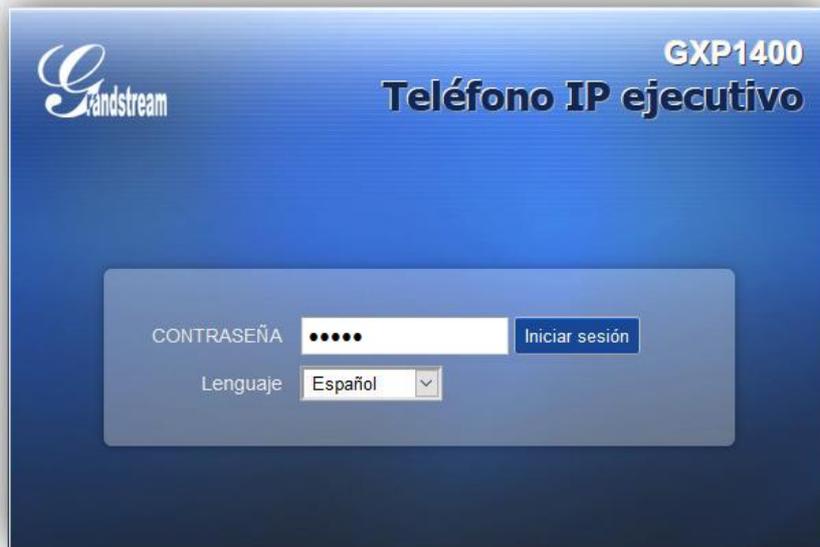
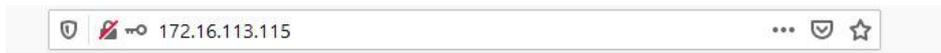


Ilustración 23 - Tlf1 Configuración

Al introducir la IP nos saldrá un formulario para introducir la contraseña de administración del teléfono IP. Si no conocemos la contraseña por defecto, podremos buscar el modelo del teléfono en internet y encontrarla fácilmente, por lo general en muchos modelos es “admin”.

Al entrar nos aparecerá un menú como el siguiente



Ilustración 24 - Tlf1 Estado

Para configurar una IP fija, tendremos que irnos a SETTINGS y a BASIC SETTINGS, y cambiar la opción DHCP por IPV4 estática y asignarle una IP válida que queramos, junto con la máscara de red, dirección de gateway predeterminado y servidor DNS. En nuestro caso hemos puesto la IP 172.16.112.66, máscara de red 255.255.254.0, gateway predeterminado 172.16.112.1, y servidor DNS 8.8.8.8. Para validar la configuración le daremos a GUARDAR Y APLICAR, lo que hará que se reinicié el teléfono.

Una vez hecho esto, tendremos que ir a nuestra consola de administración de 3CX y añadir una extensión, que posteriormente asignaremos a un teléfono. Para ello, en la consola de administración, en el menú de la izquierda seleccionamos extensiones.

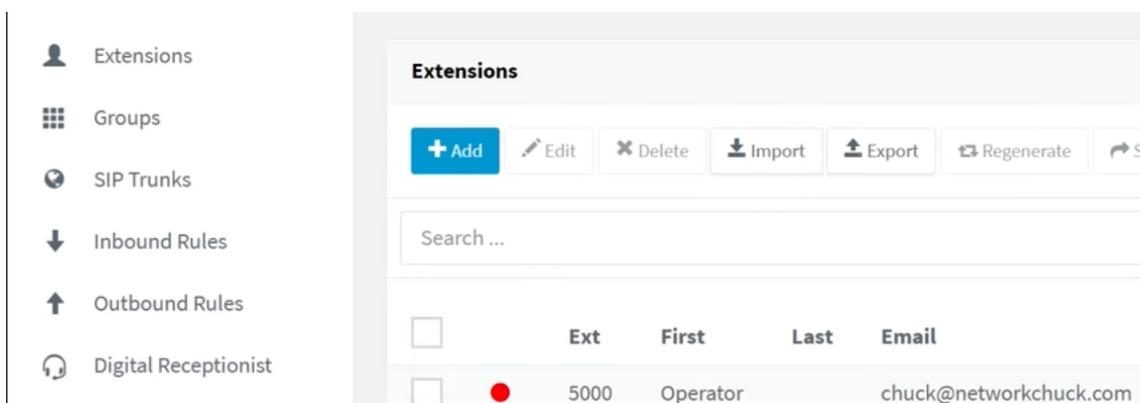


Ilustración 25 - Tlf1 Extensiones

En este apartado nos saldrá una extensión añadida por defecto, que es la que hemos asignado al principio de la configuración. Para añadir una nueva le daremos a ADD.

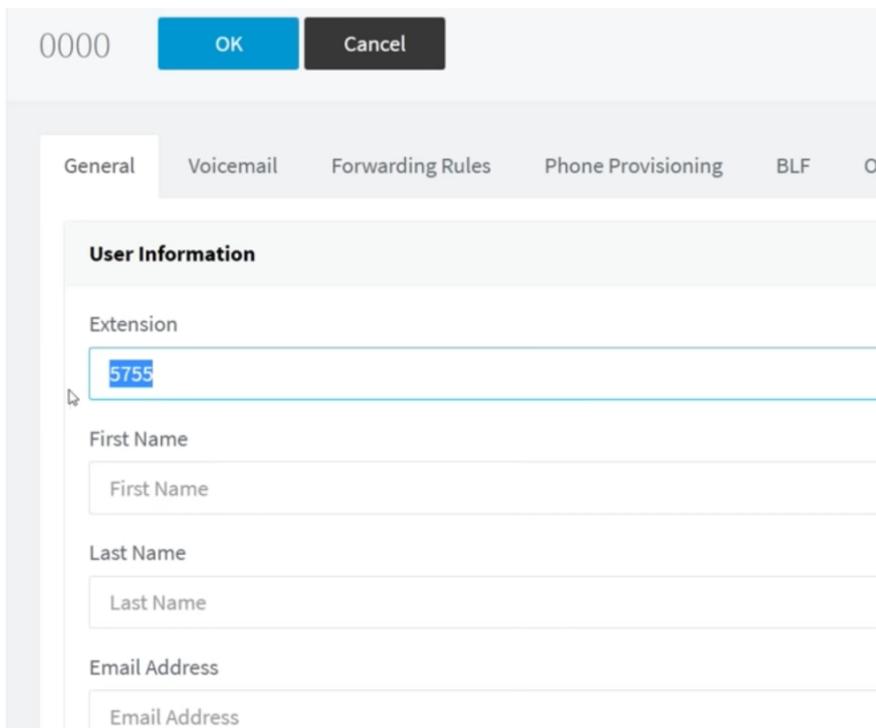


Ilustración 26 - Tlf1 Nueva extensión

En este menú asignaremos un numero de extensión, un nombre y un correo, y le daremos a OK. Ahora nos iremos al apartado PHONES en el menú de la izquierda.

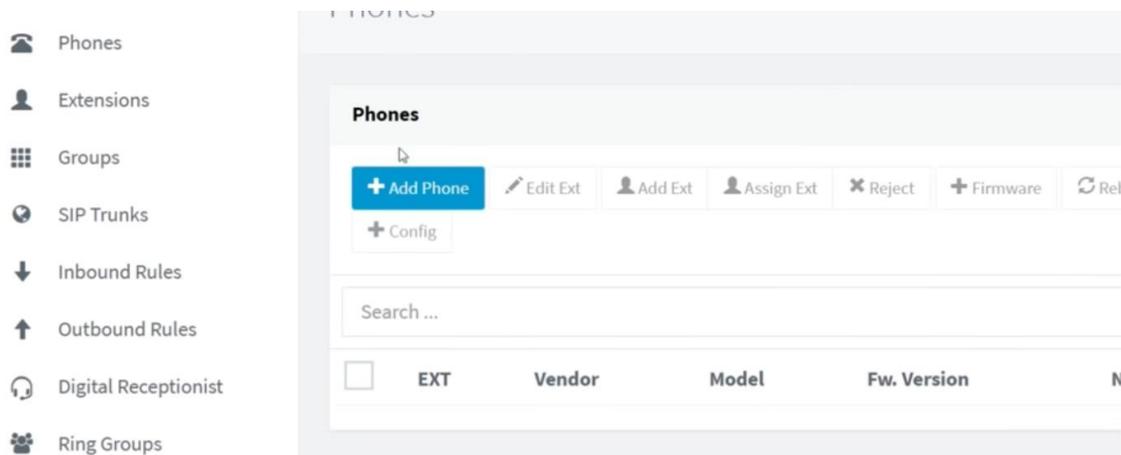


Ilustración 27 - Tlf1 Configuración extensión

En principio si tienes el teléfono IP en la misma red que el servidor 3cx, nos tendría que aparecer automáticamente en la lista de teléfonos disponibles. Si no nos aparece, podremos añadirlo manualmente haciendo click en ADD PHONE, asignándole una de las extensiones que hemos creado anteriormente y añadiendo la dirección MAC del teléfono.



Ilustración 28 - Tlf1 Asignación del teléfono a la extensión

Con esto habríamos completado la configuración del teléfono, y después de haberse reiniciado, nos tendría que salir registrado en el apartado teléfonos.

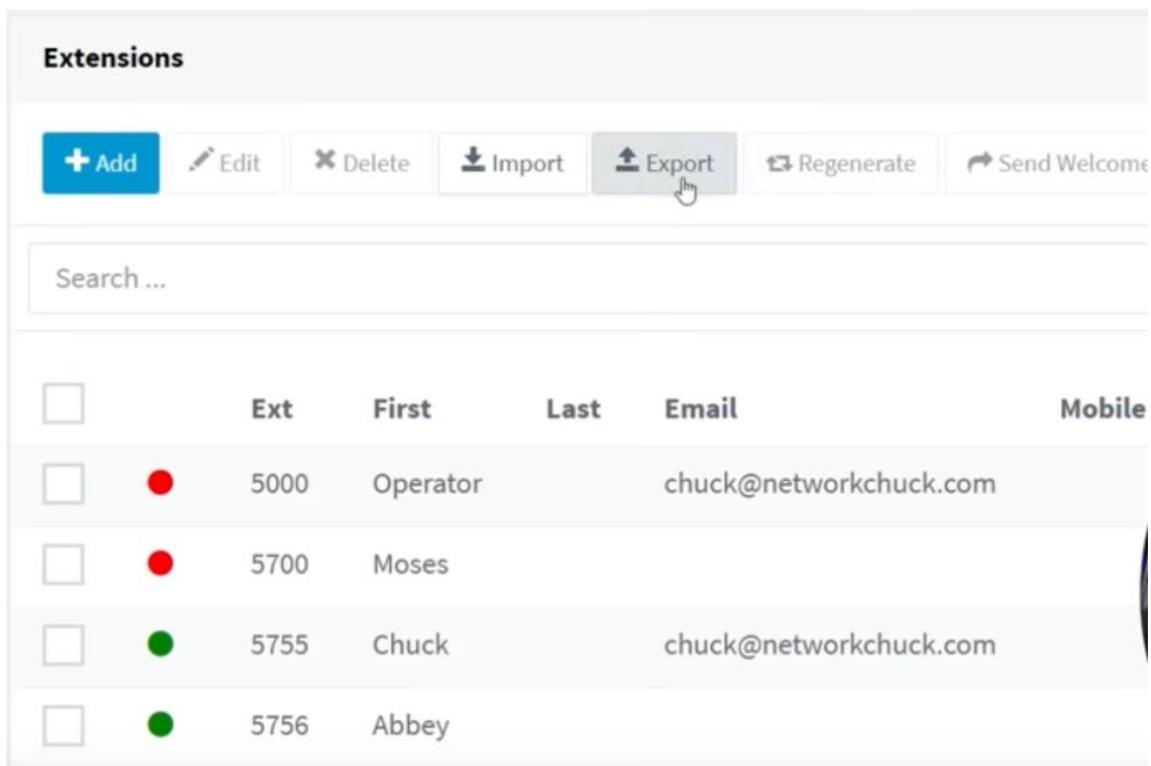


Ilustración 29 - Tlf1 Registro completado

Una de las ventajas de 3CX es que tiene su propia aplicación para móvil por lo que podemos utilizar este servicio y realizar llamadas IP desde el teléfono que hemos configurado a un móvil, o entre dos móviles o dos teléfonos fijos. Para añadir un móvil a nuestro servidor, es mucho más sencillo que añadir un teléfono fijo ya que prácticamente todo el proceso esta automatizado.

Para empezar, volvemos al apartado de EXTENSIONES y le daremos a ADD. Una vez aquí podremos ir a nuestro teléfono y descargar la aplicación 3CX. Cuando esta descargada e instalada, entraremos y nos saldrá un teclado en pantalla como el siguiente. Entraremos a los ajustes, entrando en el menú superior izquierdo indicado con 3 líneas, y dándole a ESCANEAR CODIGO QR.

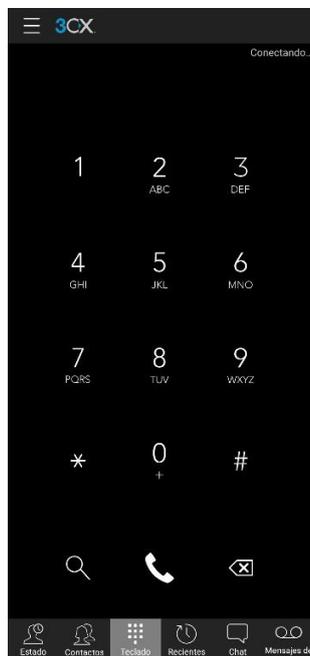


Ilustración 30 - Softphone1

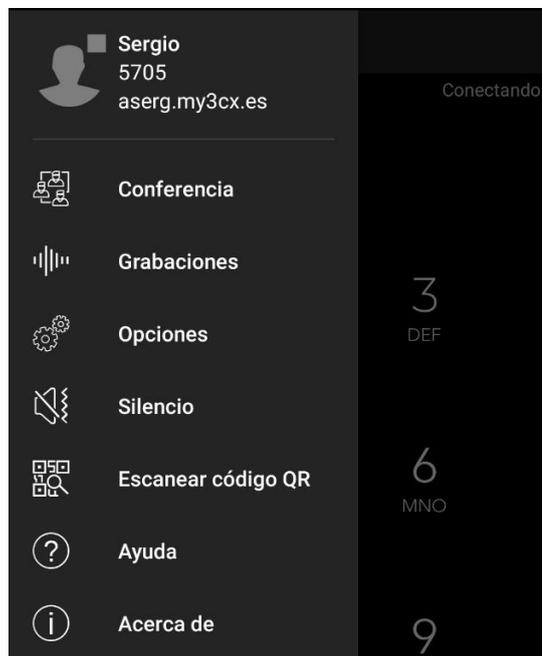


Ilustración 31 - Softphone2

Se nos abrirá la cámara y tendremos que escanear el código QR que nos aparece en la parte derecha de la ventana de añadir extensión en la consola de administración



Ilustración 32 - 3CX QR conexión con softphone

Esto hará que se añada el telefono directamente al servidor, por lo que ya lo tendremos listo para realizar llamadas entre el movil y telefono fijo.

4.3.2. FreePBX

En esta ocasión vamos a utilizar un sistema operativo basado en Linux, pero sin interfaz gráfica, junto con FreePBX y Asterisk. Los desarrolladores de este sistema operativo híbrido lo llaman raspbx.

Downloads

RasPBX images based on Raspbian 10 Buster:

The latest image supports Pi 4, Pi 3 and Pi 2 (Pi 1 and Pi zero no longer supported):

Torrent	raspbx-10-10-2020.zip.torrent
HTTP	raspbx-10-10-2020.zip
SHA-1	b36d0cc9c4986611376df6ce5141cdc3ee296540
Contents	Asterisk 16.13.0 & FreePBX 15.0.16.75

Ilustración 33 - RasPBX ISO

Una vez instalado en sistema operativo vamos a hacer una configuración inicial básica, con unos comandos que te indican al iniciar el sistema.

```
List of RasPBX specific commands:
-----
raspbx-upgrade      Keep your system up to date with the latest add-ons and
                    security fixes
configure-timezone  Set timezone for both system and PHP
install-fax         Install HylaFAX
add-fax-extension   Add additional fax extension for use with HylaFAX
install-fail2ban    Install Fail2Ban for additional security
install-dongle      Install GSM/3G calling capability with chan_dongle
raspbx-backup       Backup your complete system to an image file
```

Ilustración 34 - RasPBX Instalación

Ejecutamos “*raspbx-upgrade*”, “*configure timezone*”, “*install-fax*” y “*install-fail2ban*”.

Con esto ya tendremos una configuración básica de la raspberry. Nosotros además le hemos asignado una IP estática, correspondiente a la 172.16.112.61. Una vez realizado todo lo anterior, podremos ir a otro terminal que este en la misma red, e introducir la IP en el navegador. Esto hará que se nos habrá el terminal de administración de FreePBX.



Ilustración 35 - FreePBX User

Entraremos en la primera opción y nos pedirán distintos datos de nuestra información para crearnos una cuenta con la que administrar FreePBX.

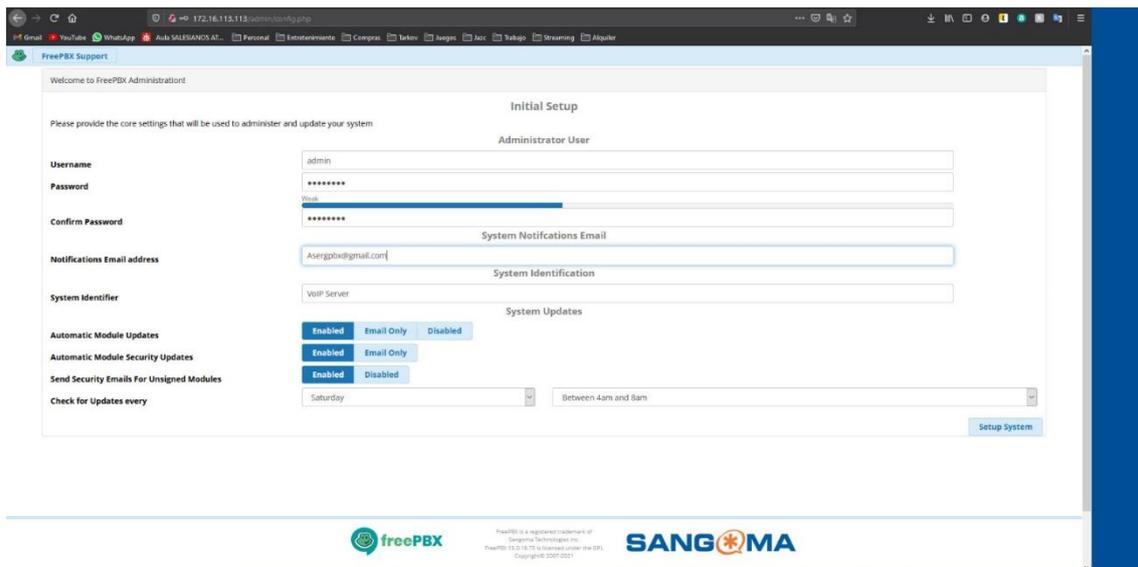


Ilustración 36 - FreePBX Información

Una vez hecho esto se reiniciará el sistema y repetiremos la operación anterior, pero esta vez nos pedirá únicamente los datos de identificación para poder entrar.

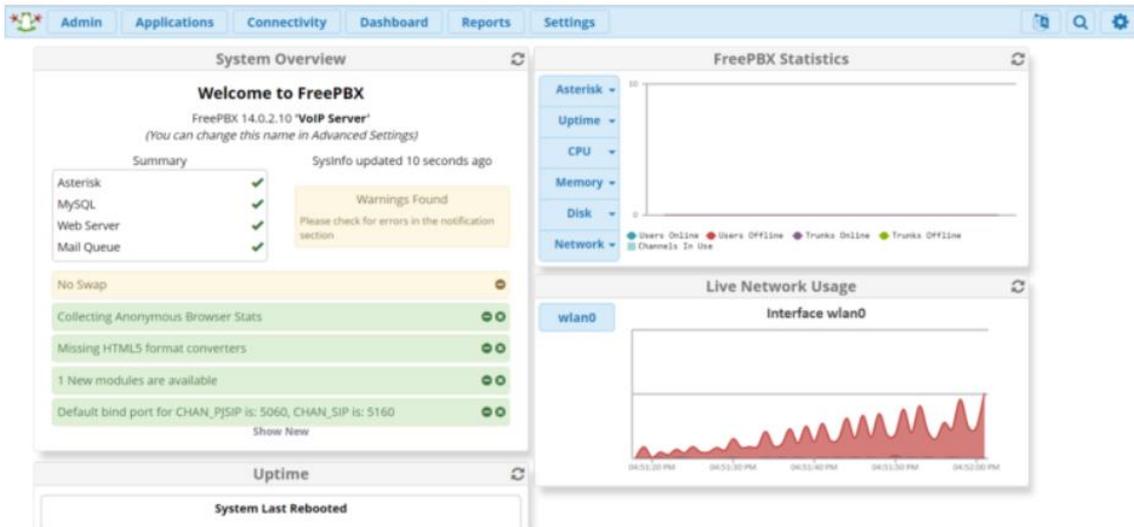


Ilustración 37 - FreePBX Welcome

Vamos a configurar los ajustes del servidor SIP que será el que enlace los teléfonos con la consola de administración. Para ello vamos a SETTING y ASTERISK SIP SETTINGS

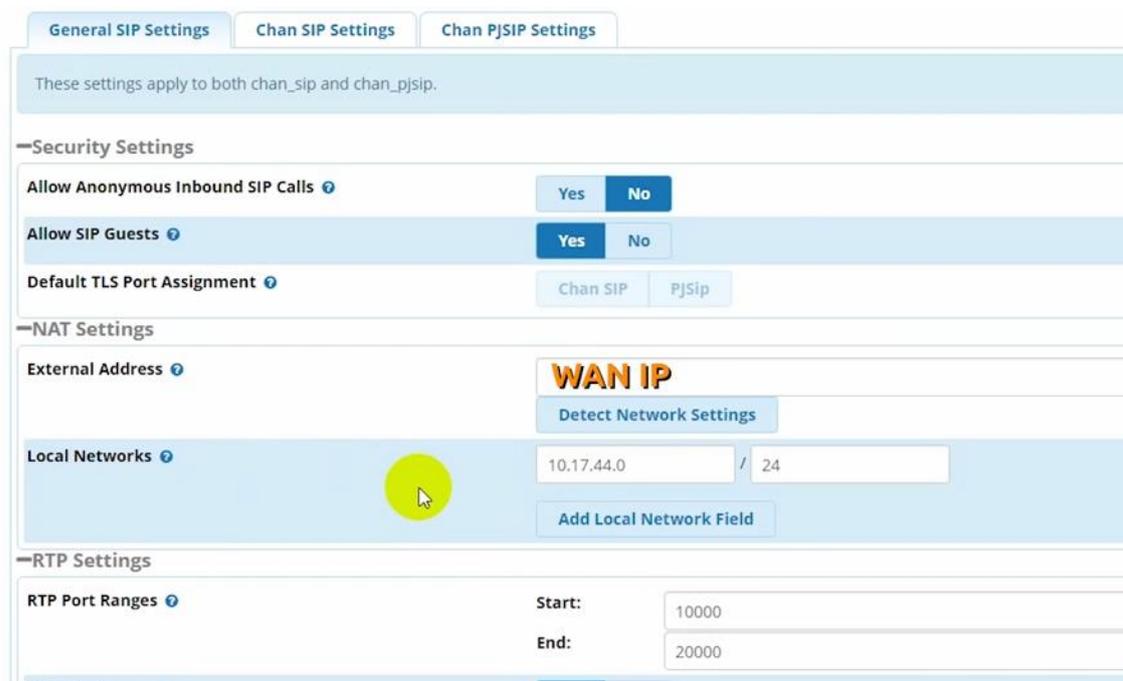
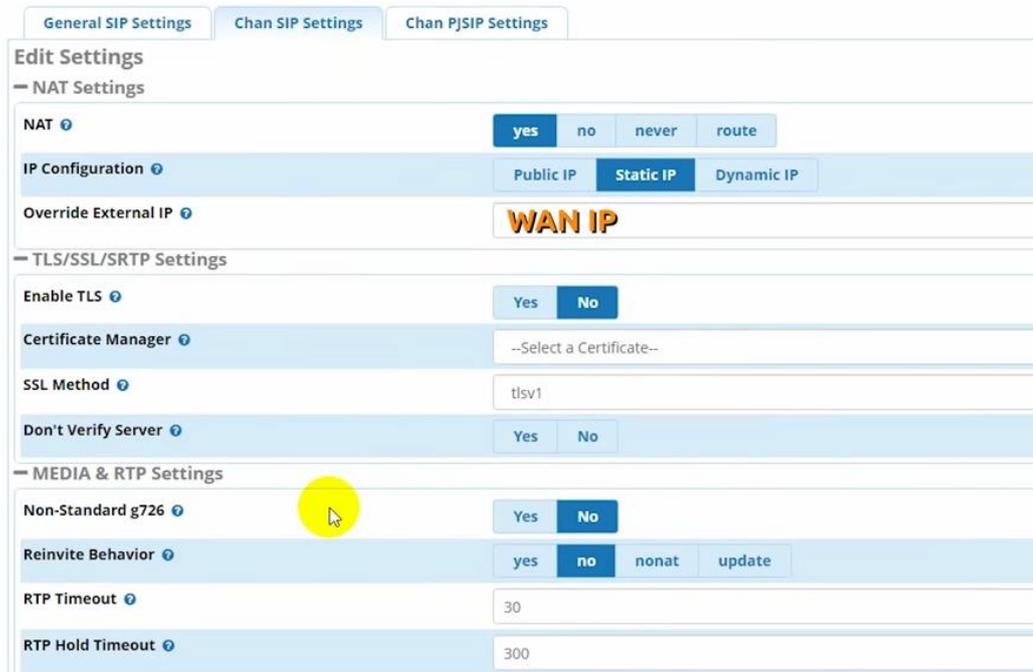


Ilustración 38 - FreePBX Configuración SIP

Lo único que tendremos que cambiar de esta pestaña es LOCAL NETWORKS que tendremos cambiar por nuestra dirección de red.

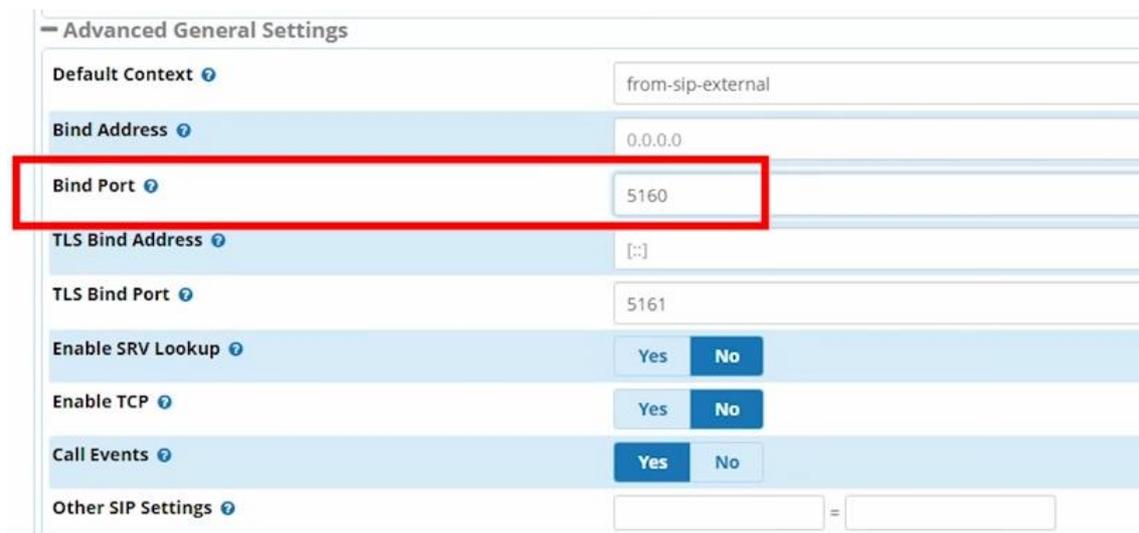
Cambiamos de ventana y configuramos los ajustes de CHAN SIP SETTINGS



The screenshot shows the 'Chan SIP Settings' configuration page in FreePBX. It is divided into several sections: NAT Settings, TLS/SSL/SRTP Settings, and MEDIA & RTP Settings. In the NAT Settings section, 'NAT' is set to 'yes', 'IP Configuration' is set to 'Static IP', and 'Override External IP' is set to 'WAN IP'. In the MEDIA & RTP Settings section, 'Non-Standard g726' is highlighted with a yellow circle and set to 'No', 'Reinvite Behavior' is set to 'no', 'RTP Timeout' is set to '30', and 'RTP Hold Timeout' is set to '300'.

Ilustración 39 - FreePBX Configuración 2 SIP

En esta pestaña tendremos que fijarnos en el apartado de BIND PORT, que será el puerto correspondiente al protocolo que utilizaremos para enlazar los teléfonos.



The screenshot shows the 'Advanced General Settings' configuration page in FreePBX. The 'Bind Port' field is highlighted with a red rectangle and is set to '5160'. Other settings include 'Default Context' set to 'from-sip-external', 'Bind Address' set to '0.0.0.0', 'TLS Bind Address' set to '[:,]', 'TLS Bind Port' set to '5161', 'Enable SRV Lookup' set to 'No', 'Enable TCP' set to 'No', and 'Call Events' set to 'Yes'.

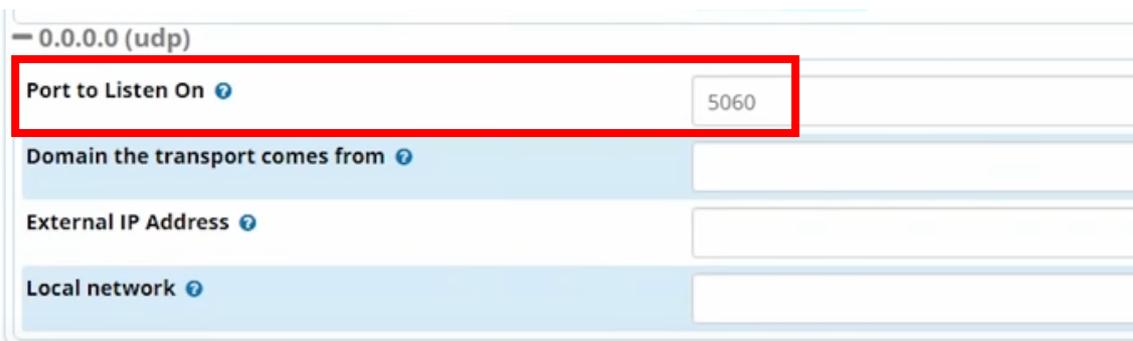
Ilustración 40 - FreePBX Configuración puerto

Tendremos que hacer lo mismo en la configuración de CHAN PJSIP SETTINGS, que no es más que otro protocolo distinto y más nuevo.



The screenshot shows the 'Chan PJSIP Settings' tab in the FreePBX interface. It is divided into three sections: 'Misc PJSip Settings', 'TLS/SSL/SRTP Settings', and 'Transports'. In the 'Misc PJSip Settings' section, there are two rows of settings: 'Allow Reload' and 'Show Advanced Settings', each with 'Yes' and 'No' radio buttons. The 'No' button for 'Show Advanced Settings' is selected. In the 'TLS/SSL/SRTP Settings' section, there are four rows: 'Certificate Manager' with a dropdown menu showing '--Select a Certificate--', 'SSL Method' with a dropdown menu showing 'Default', 'Verify Client' with 'Yes' and 'No' radio buttons, and 'Verify Server' with 'Yes' and 'No' radio buttons. A yellow circle with a hand cursor is positioned over the 'Verify Server' row. Below the settings is a note: 'Note that the interface is only displayed for your information, and is not referenced by asterisk. You have Asterisk 13.19.1 w'.

Ilustración 41 - FreePBX Configuración 3 SIP



The screenshot shows the 'Transport Settings' for '0.0.0.0 (udp)'. It has four rows of settings: 'Port to Listen On' with a text input field containing '5060', 'Domain the transport comes from', 'External IP Address', and 'Local network'. A red rectangular box highlights the 'Port to Listen On' field.

Ilustración 42 - FreePBX Configuración 4 SIP

Una vez que sabemos los dos puertos de los dos protocolos, vamos a crear las extensiones. En el menú superior vamos a APPLICATIONS-EXTENSIONS

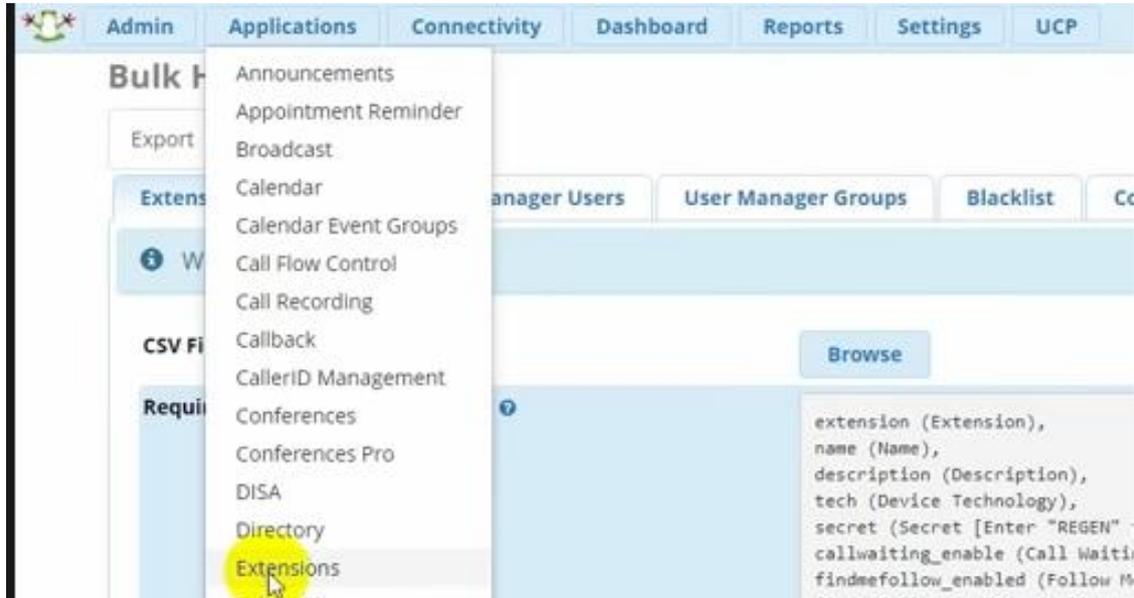


Ilustración 43 - FreePBX Extensión



Ilustración 44 - FreePBX Extensión2

Para añadir simplemente le damos a añadir y seleccionamos el tipo de protocolo con el que queremos añadir la extensión.

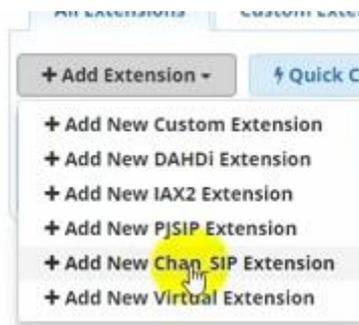


Ilustración 45 - FreePBX Añadir Extensión

Se nos abrirá un menú en el que tendremos que introducir los datos de la extensión a añadir.

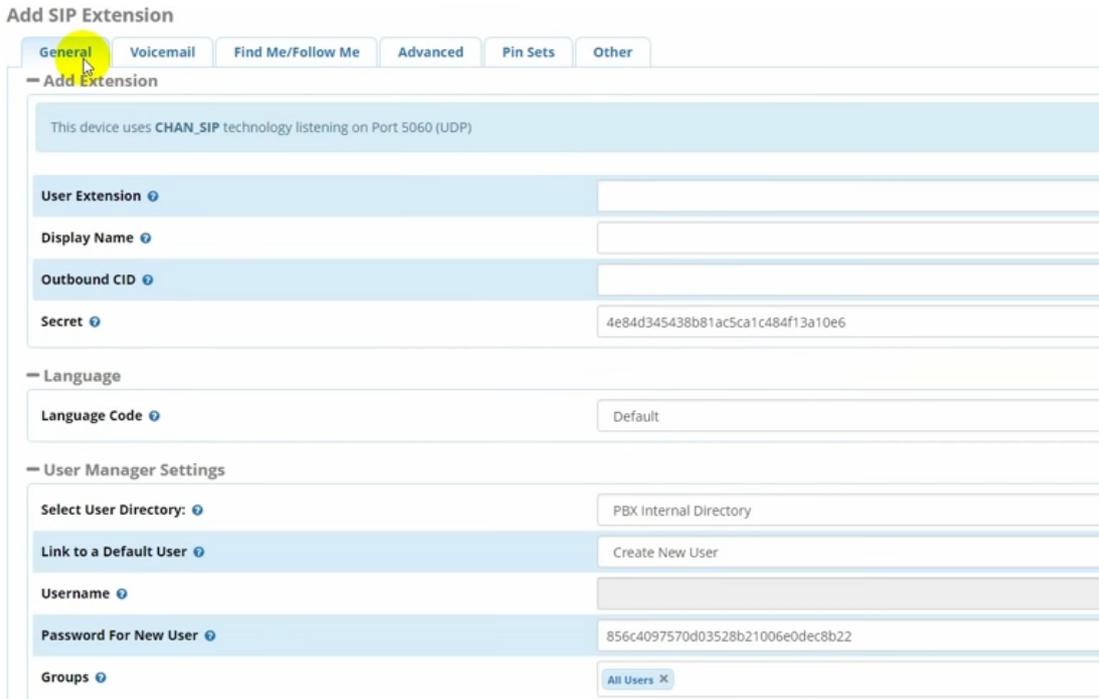


Ilustración 46 - FreePBX Configurar Extensión

Una vez rellenado tendremos que quedarnos con el número de la extensión y la contraseña, ya que la tendremos que utilizar para enlazar el teléfono.

Ahora vamos a asignar una IP fija a nuestro teléfono fijo. En la configuración del propio teléfono encontraremos la IP que nuestro router le está proporcionando, y la introduciremos en el navegador.

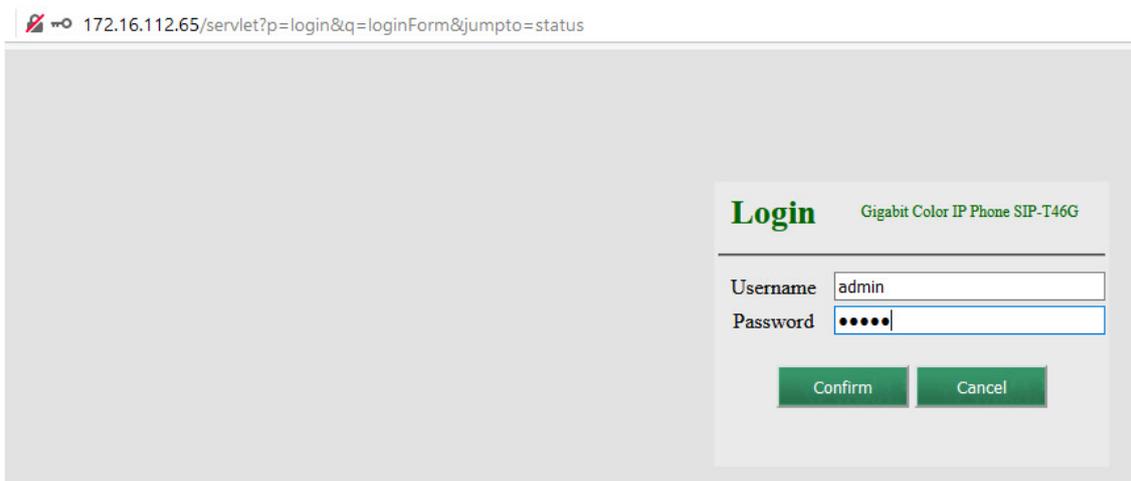


Ilustración 47 - Tlf2

Al igual que en 3CX, buscaremos el usuario y la contraseña por defecto en Internet, en este caso es “admin” y “admin”.

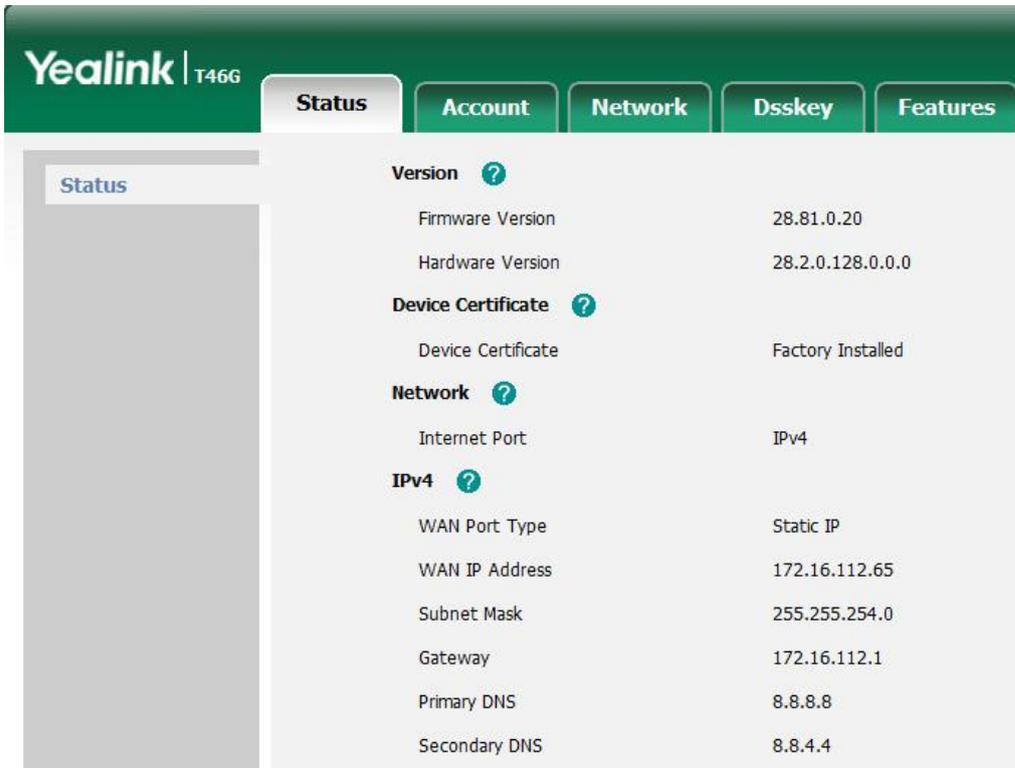


Ilustración 48 - Tlf2 Status

En la sección de Network, podremos cambiar de DHCP a IP Estática.

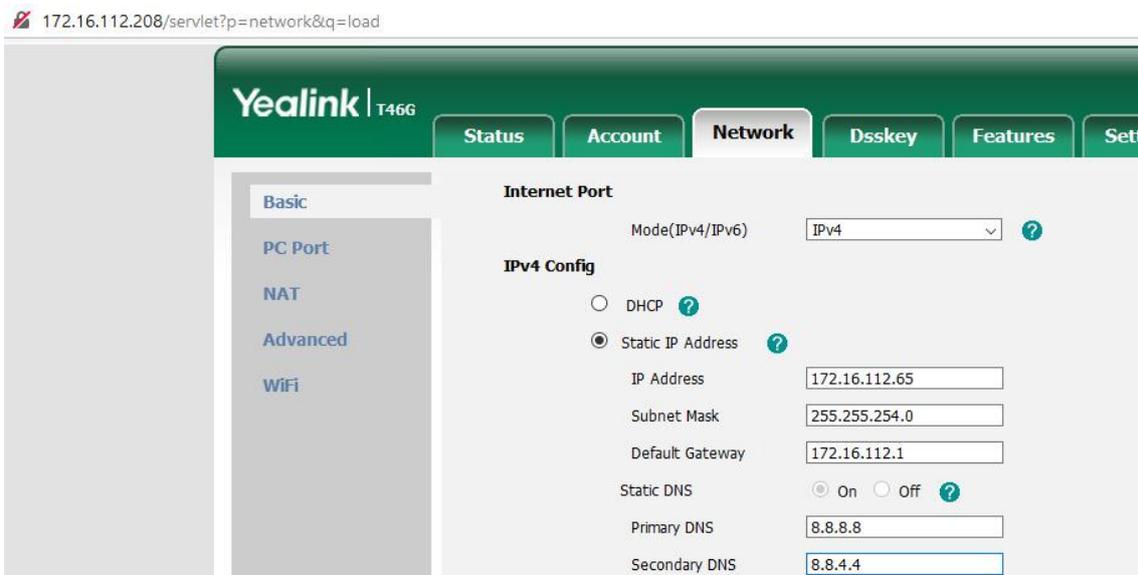
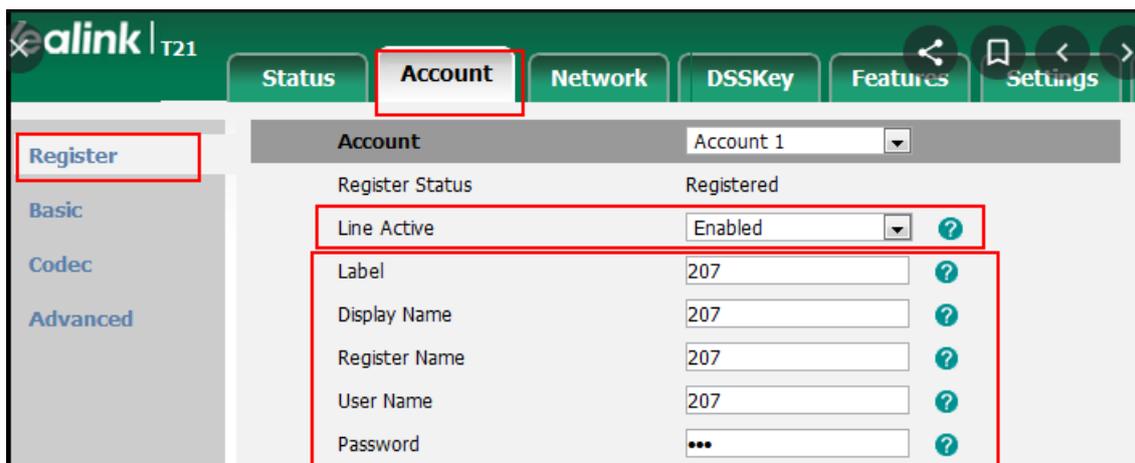


Ilustración 49 - Tlf2 configuración

Al guardar y aplicar la configuración se reiniciará el teléfono.

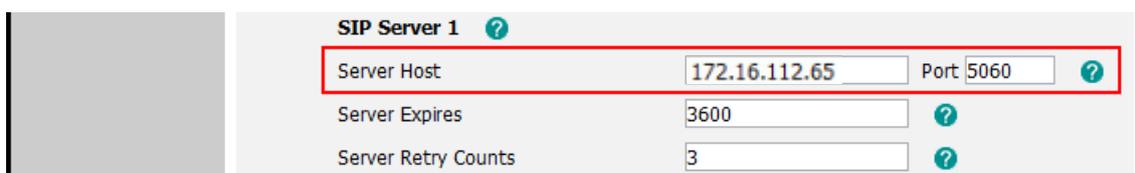
Volvemos a entrar con las mismas credenciales, y esta vez vamos al menú de ACCOUNT.



Account		Account 1
Register Status	Registered	
Line Active	Enabled	
Label	207	
Display Name	207	
Register Name	207	
User Name	207	
Password	...	

Ilustración 50 - Tlf2 Account 1

En primer lugar, tendremos que poner el apartado de LINE ACTIVE en ENABLE, después en los apartados de LABEL, DISPLAY NAME, REGISTER NAME y USER NAME pondremos la extensión que previamente hemos creado en FreePBX, y después la contraseña que hemos guardado anteriormente correspondiente a la extensión.



SIP Server 1			
Server Host	172.16.112.65	Port	5060
Server Expires	3600		
Server Retry Counts	3		

Ilustración 51 - Tlf2 SIP Server 1

Después en la parte de SIP SERVER 1 añadimos la dirección IP de nuestro servidor y el puerto correspondiente al protocolo que hemos utilizado. Cuando hayamos rellenado estos campos, le daremos a guardar y aplicar. Si ha tenido éxito en el apartado de REGISTER STATUS nos tendría que aparecer REGISTERED

Para añadir un móvil necesitaremos una aplicación móvil que nos enlace con FreePBX, nosotros hemos elegido ZOIPER una aplicación móvil gratuita.

Antes de pasar a configurar la aplicación vamos a crear otra extensión que enlazaremos al móvil. Seguimos los pasos mencionados anteriormente, pero poniendo una extensión distinta. Una vez hecho esto vamos a la aplicación y nos pedirá registrarnos.



Ilustración 52 - Zoiper

En el apartado USERNAME, pondremos el número de extensión junto con la IP de nuestro servidor de la siguiente manera:

[Nº Extensión]@[IP SERVIDOR]

Al darle a CREATE AN ACCOUNT, nos pedirá de nuevo la IP de nuestro servidor, pero esta vez añadiremos seguidamente el puerto del protocolo con el que hemos creado la extensión:

[IP SERVIDOR]:5060

Le daremos a NEXT, y nos saldrá otra ventana que dejaremos en blanco

Automáticamente se iniciará un proceso en el cual, la aplicación tratará de localizar nuestro servidor.

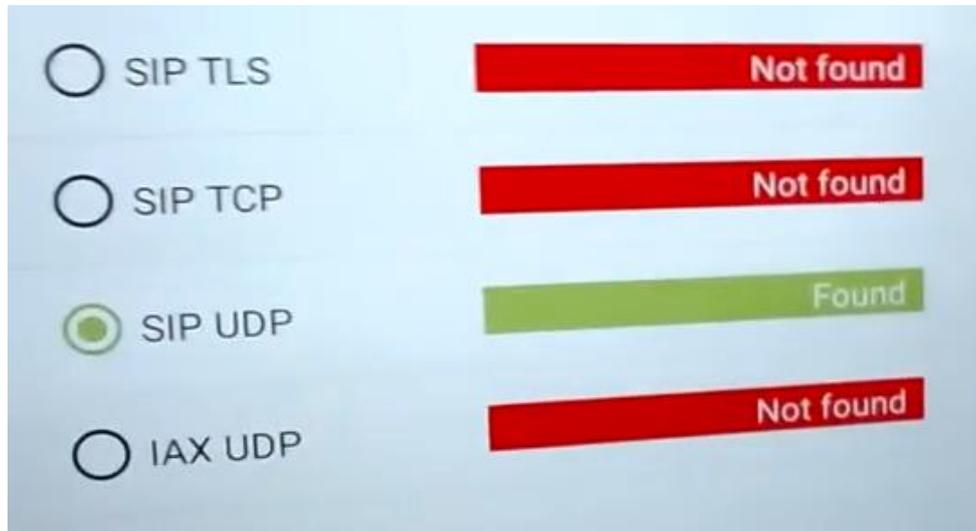


Ilustración 53 - Zoiper SIP UDP

Cuando nos lo detecte le seleccionaremos y le daremos a FINISH. Con esto ya tendríamos nuestra aplicación enlazada con FreePBX, y podremos recibir y realizar llamadas a las otras extensiones que configuremos.

Nosotros hemos querido ir un poquito más lejos, y hemos pensado que para una empresa es interesante tener un registro de llamadas con el que ver el uso que hacen sus empleados de los teléfonos. Algunas empresas también pueden incorporar un tarifador a este registro de llamadas, y los empleados tienen que ser capaces de consultar este consumo. Para esto, FreePBX incorpora un módulo con el que exporta el registro de llamadas a una base de datos MYSQL. Sin embargo, esta base de datos está almacenada localmente en el servidor, por lo que a nivel de seguridad y accesibilidad no sería adecuado dejar acceder a todos los empleados al servidor.

Para solucionar este problema hemos instalado el servicio de Apache para que todos los ordenadores de la red puedan acceder desde el propio terminal a esta información. Al hacer esto hacemos más accesible la base de datos a todos nuestros empleados, pero no todo el mundo sabe manejar un servidor de base de datos como es MYSQL. Dejar que cualquier persona pueda acceder a la base de datos, podría conllevar problemas de seguridad, aparte de que al no tener conocimientos acerca del servidor podrían acabar dañando la base de datos. Por esto hemos escrito unos archivos .php con los que los empleados pueden acceder mediante el numero de la extensión y una contraseña al registro de sus llamadas únicamente, sin la posibilidad de modificar, eliminar o añadir nada.

Accede a tu cuenta

Inserta tu extensión:

Contraseña:

Ilustración 54 - Login base de datos



Bienvenido!

Cerrar Sesión

Registro de llamadas de la extensión: 5713

Fecha llamada	Numero Origen	Nombre	Numero Destino	Contexto	Duracion	Resultado
2021-03-11 18:23:24	5713	Movil	5709	from-internal	58	ANSWERED
2021-03-11 18:31:56	5713	Movil Sergio	5714	from-internal	16	ANSWERED
2021-03-11 19:18:22	5713	Movil Sergio	5709	from-internal	35	ANSWERED

Ilustración 55 - Registro de llamadas

5. Caso Real

5.1. Requisitos cliente

Para este apartado se va a llevar a cabo el diseño de una infraestructura de red acorde con la solicitud del cliente. Este solicita el diseño de una red con un servidor de VoIP para un hotel, el cual constará de una primera planta en el que se implantará la recepción, la cual tendrá un teléfono IP y un ordenador. En esta primera planta también estará el cuarto de servidores, en el que solamente tendrá acceso el administrador. En este cuarto se guardará un servidor en el que se realizará toda la instalación de VoIP explicada anteriormente, junto con un router y un Switch Core de capa 3, desde el cual se distribuirá toda la red. A parte habrá un PC para poder manejar y administrar toda la instalación. Desde este PC se podrá conectarse a todos los dispositivos mediante el protocolo de SSH.

En la segunda y la tercera planta constarán de 3 habitaciones con sus respectivos teléfonos, por el contrario, en la cuarta planta constará de 4 habitaciones con sus respectivos teléfonos. En conclusión, el hotel constará de 4 plantas, con 11 habitaciones, y, por tanto, 11 teléfonos IP y un ordenador en la recepción. Como medida complementaria a la solicitud del cliente, se instalarán 3 ordenadores más para la administración de la red.

5.2. Equipamiento

En cuanto al equipamiento requerido para este proyecto, consistirá en un servidor en el que se instalarán los servicios y protocolos necesarios para que el servicio de VoIP funcione correctamente, esos servicios y necesidades están explicadas anteriormente. Será necesario un router para poder conectar todos los dispositivos a la red. Conectado a ese router, estará conectado un Switch Core de capa 3, el cual se encargará del enrutamiento de la red mediante un direccionamiento lógico. Este Switch conectará entre ellos a los diversos Switch de capa 2 de cada planta, distribuyendo las Vlan correspondientes a cada una de las plantas. Para ello cada planta tendrá una Vlan correspondiente, siendo la vlan200 la administrativa, a la cual estará conectada directamente al Switch Core de capa 3 el ordenador. Cada planta, como se ha mencionado anteriormente, constará de un Switch de capa 2 y un PC para poder realizar las gestiones de ese dispositivo, no obstante, desde el PC del administrador situado en la primera planta se podrá acceder vía protocolo SSH a todos los dispositivos para su posible configuración. A los dispositivos anteriores hay que sumarle los diferentes teléfonos IP solicitados por el cliente, así como un ordenador en la recepción.

5.3. Diseño de la solución

En cuanto al diseño de la solución es el expuesto en la siguiente imagen.

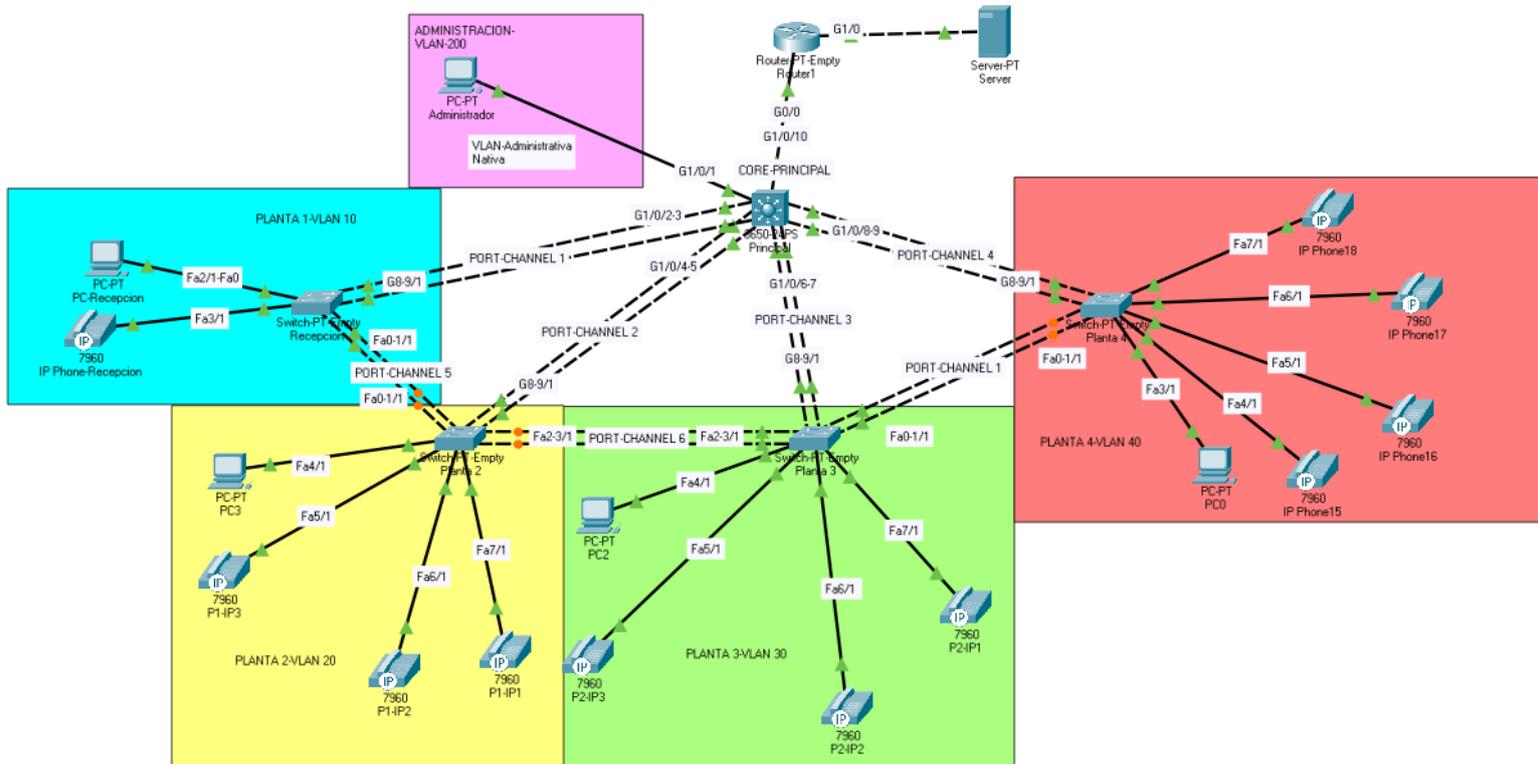


Ilustración 56 - Diseño de la red

Teniendo en cuenta la solicitud del cliente, desde esta perspectiva el diseño que se encuentra en la imagen anterior (Ilustración 56) se considera que es la mejor forma de tener una red apropiada para el problema que expone el cliente, así como una red segura y con posibilidad de ampliar en el futuro si fuera necesario. Este tipo de distribución se ha considerado la mas apropiada debido a la estructura del edificio dividido en 4 plantas. Con un Switch Core de capa 3 el cual realiza el enrutamiento y la distribución de IPs mediante el protocolo DHCP.

La empresa está distribuida de la siguiente manera, hay 4 plantas, en la planta inferior o Planta 1 se encuentra la recepción en la cual consta de un ordenador y un teléfono IP de cara al cliente, en cuanto a la parte administrativa, en el cuarto del administrador hay un servidor para controlar y manejar toda la tecnología de VoIP.

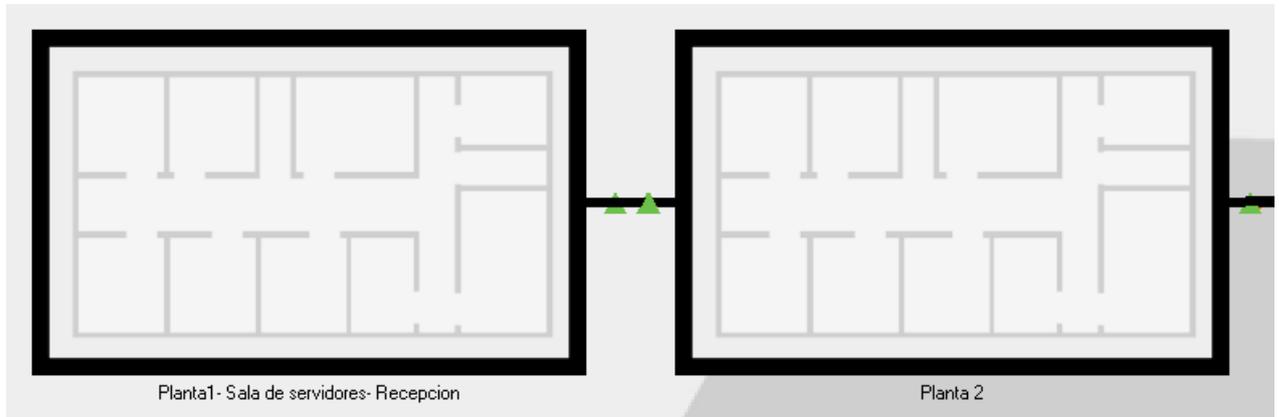


Ilustración 57- Distribución Recepción y planta 2

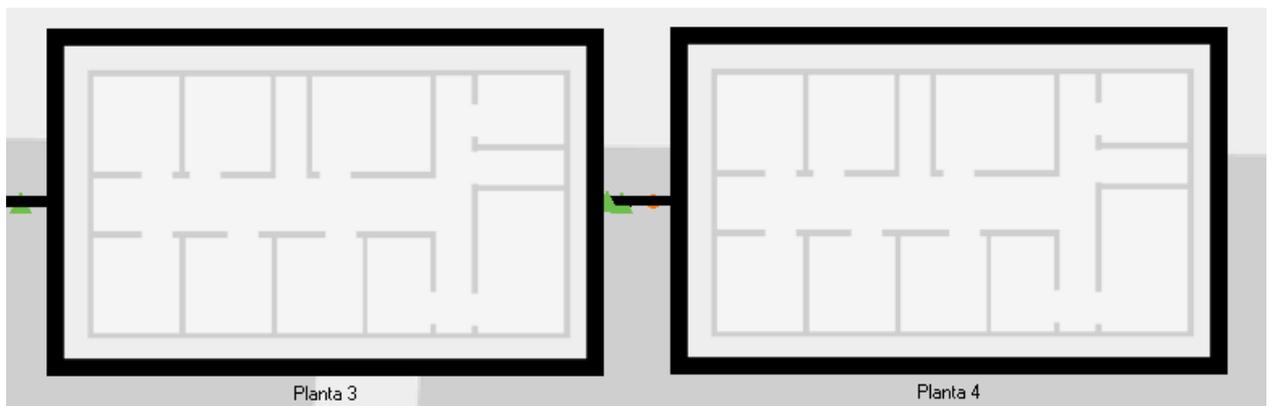


Ilustración 58 - Distribución planta 3 y 4

5.4.Descripción de la solución

La solución propuesta ha sido la creación de varias partes dentro de la misma red mediante VLAN, en este caso al existir diferentes plantas no ha sido muy complicado a la hora de la distribución de estas VLAN puesto que se le ha asignado una por planta, quedando el reparto de la siguiente manera:

Planta	VLAN	Dirección IP	Mascara subred
Nativa-Administrador	VLAN 200	192.168.200.0	255.255.255.0
Planta 1	VLAN 10	192.168.10.0	255.255.255.0
Planta 2	VLAN 20	192.168.20.0	255.255.255.0
Planta 3	VLAN 30	192.168.30.0	255.255.255.0
Planta 4	VLAN 40	192.168.40.0	255.255.255.0

Al comenzar con la configuración hay que configurar el vtp de modo que el Switch Core será de modo server, en cambio el resto de Switch serán en modo cliente. Se configurarán como troncales los puertos del Switch Core, es decir en el rango de puertos G1/0/2-9. Para que haya conectividad entre plantas será necesario realizar varios Port-Channel, en los Switch de capa 2 el número máximo de Port-Channel son de 6. La tabla de Port-Channel queda de la siguiente manera:

Dispositivo	Interfaz	Port-Channel	Dispositivo destino	Interfaz destino
Switch Core	G1/0/2-3	1	SW-Planta1	G8-9/1
	G1/0/4-5	2	SW-Planta2	G8-9/1
	G1/0/6-7	3	SW-Planta3	G8-9/1
	G1/0/8-9	4	SW-Planta4	G8-9/1
SW-Planta 1	Fa0-1/1	5	SW-Planta2	Fa0-1/1
SW-Planta 2	Fa2-3/1	6	SW-Planta3	Fa2-3/1
SW-Planta 3	Fa0-1/1	1	SW-Planta4	Fa0-1/1

5.5. Protocolos de Seguridad

Los protocolos de seguridad de la res son un tipo de protocolo de res que garantiza la seguridad y la integridad de los datos en tránsito a través de una conexión de red como internet. Están diseñados principalmente para evitar que usuarios, aplicaciones, servicios o dispositivos no autorizados accedan a los datos de la red. Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin.

Cuando se lleva a cabo la comunicación entre ordenadores conectados a una misma red, los datos se parten en paquetes de datos más pequeños, normalmente tienen una longitud de 1500 byte, ya que es el típico MTU (Maximum Transfer Unit) que se suele utilizar en las redes. Existen varios tipos de protocolos dependiendo de la zona a la que afecten, y dependiendo de lo que se quiera proteger.

El **protocolo ARP** para redes PIPv4 es uno de los protocolos fundamentales de Internet y de las redes locales, puesto que este protocolo también trabaja junto con el protocolo IP para mapear direcciones IP en relación con las direcciones de hardware utilizados por un protocolo de enlace datos. El principal objetivo es conocer la dirección física de una tarjeta de interfaz de red correspondiente a una dirección IP.

Cada equipo conectado a una red tiene un número de 46 bits que le identifica. Esta dirección es única para cada dispositivo. La comunicación por Internet no utiliza directamente esta dirección (MAC), sino que utiliza direcciones IP, es decir, que tiene que haber relación entre direcciones físicas (MAC) y lógicas.

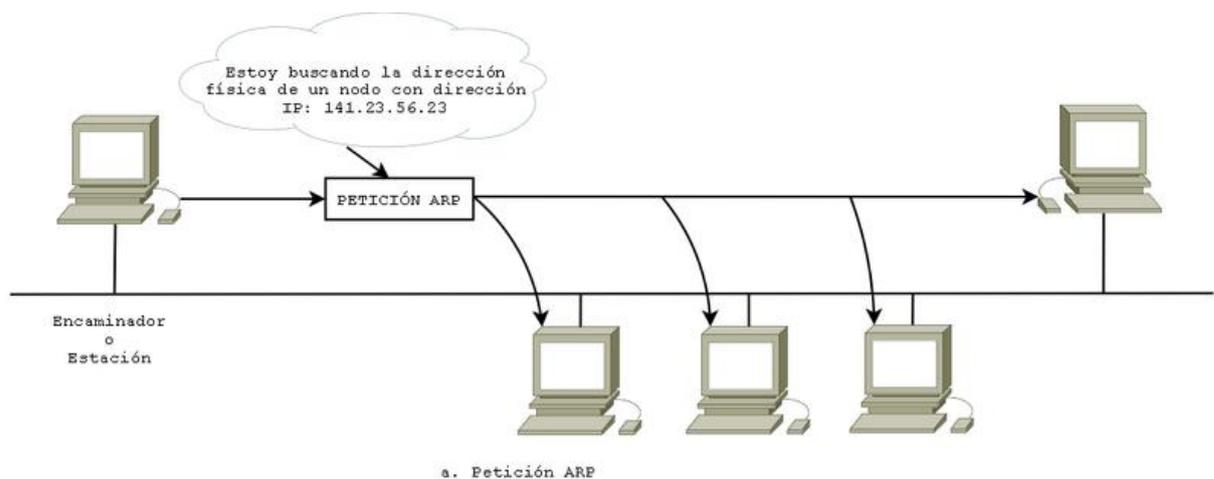


Ilustración 59 - Protocolo ARP petición

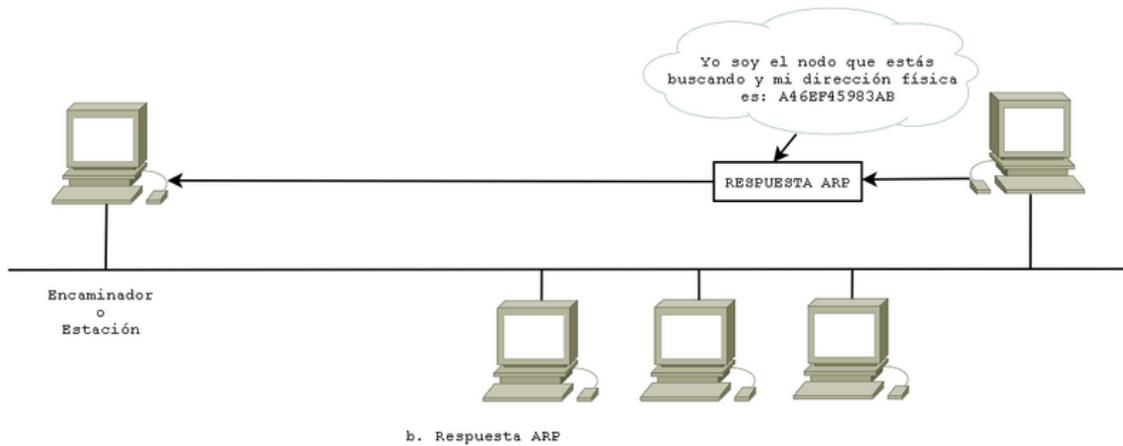


Ilustración 60 - Protocolo ARP respuesta

Uno de los protocolos utilizados en este proyecto es el **protocolo SSH** (Secure Socket Shell) proporciona una forma segura de acceder a internet a través de un ordenador remoto. SSH proporciona una autenticación y encriptación entre dos dispositivos, de esta forma se puede realizar la configuración de diferentes dispositivos vía remota desde un solo ordenador.

En la capa de transporte en este proyecto se ha utilizado el **protocolo TCP** el cual garantiza que los datos se transmiten de manera adecuada a través de Internet. Su función principal es asegurar que el tráfico llegue al destino de una manera fiable. Esta característica de fiabilidad no es posible lograrla únicamente mediante IP. Otras funciones de TCP son:

- Asegurarse de que no se pierdan los paquetes de datos.
- Control del orden de los paquetes de datos.
- Control de una posible saturación que se llegue a experimentar.
- Prevención de duplicado de paquetes.

En cuanto a la capa de protección el protocolo HTTP (Hypertext Transfer Protocol) permite que los navegadores y servidores web se comuniquen adecuadamente. Este es utilizado por navegadores web para solicitar archivos HTML de parte de los servidores remotos. Así, los usuarios podrán interactuar con dichos archivos mediante la visualización de las páginas web que cuentan con imágenes, música, videos, texto, etc. El protocolo HTTP tiene como base TCP, el cual implementa un modelo de comunicación cliente-servidor. Existen tres tipos de mensajes que HTTP utiliza:

- HTTP GET: se envía un mensaje al servidor que contiene una URL con o sin parámetros. El servidor responde retornando una página web al navegador, el cual es visible por el usuario solicitante.
- HTTP POST: Se envía un mensaje al servidor que contiene datos en la sección <body> de la solicitud. Esto es hecho para evitar el envío de datos a través de la propia URL.
- HTTP HEAD: Aquí se hace énfasis en la respuesta por parte del servidor. Este mensaje restringe lo que el servidor responde para que solamente responda con la información de la cabecera.

Como protocolo para transferencia de archivos está el **protocolo TFTP** (Trivial File Transfer Protocol) es un protocolo cliente servidor muy simple que regula la transferencia de archivos en redes informáticas. Por defecto, este protocolo se basa en el mínimo nivel de transporte UDP, que ofrece la posibilidad de transmitir datos sin necesidad de una conexión fija entre los miembros de la comunicación. No obstante, es posible implementar el protocolo TFTP basándose en otros protocolos diferentes.

Por último, el **protocolo NTP** (Network Time Protocol) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de del enrutamiento de paquetes en redes con latencia variable. El demonio NTP de Unix es un proceso de nivel de usuario que se ejecuta continuamente en la máquina que soporta NTP, y la mayor parte del protocolo está implementando en este proceso de usuario. Para obtener el mejor rendimiento NTP, es importante tener un reloj NTP estándar con lazo de seguimiento de fase implementado en el kernel del Sistema Operativo, en vez de usar solo la intervención de un demonio NTP externo.

6. Conclusiones

La finalidad de este proyecto ha sido llevar a cabo los conocimientos adquiridos durante el curso expuestos al inicio del documento.

Se ha conseguido diseñar e implementar en un caso práctico y realista una red con centralita de VoIP basado en las peticiones de un cliente ficticio utilizando la infraestructura de la escuela para poder llevar a cabo la instalación real de los diferentes servicios expuestos con anterioridad. Se ha conseguido involucrar diversas áreas durante el proyecto consiguiendo mezclar desde la configuración de una red hasta el desarrollo de una página para que el usuario de cada extensión pueda realizar una visualización del registro de sus llamadas. Pasando por la administración de una base de datos y la configuración de un Sistema Operativo basado en raspbx sin interfaz gráfica.

Durante el desarrollo del proyecto se han sumado conocimientos no vistos durante el curso referente a los protocolos de señalización (SIP y H323), así como la investigación de todo lo relacionado con el sistema de VoIP, siendo esto algo novedoso. De igual modo se han afianzado conocimientos sobre redes, en cuanto a configuración de router y Switch, así como de configuración de seguridad en esta.

Como líneas futuras a este proyecto se propone complementar las funcionalidades de ambas opciones propuestas de VoIP, así como la ampliación de la infraestructura de voz con un sistema de atención al usuario que dirija las llamadas automáticamente a un departamento determinado.

De forma adicional se puede evolucionar la infraestructura hacia entornos de colaboración en los que se integra la voz con el video de una forma más natural.

7. Bibliografía

3CX. (s.f.). *3CX*. Obtenido de <https://www.3cx.es/>

3cx. (s.f.). *H-323*. Obtenido de <https://www.3cx.es/voip-sip/h323/>

3CX. (s.f.). *SIP*. Obtenido de <https://www.3cx.es/voip-sip/sip/>

Anura. (s.f.). *FreePBX*. Obtenido de <https://www.anura.com.ar/soporte/empresas/tutoriales/configuracion-troncal-sip-freepbx/>

Asterisk. (s.f.). *Asterisk*. Obtenido de <http://www.raspberry-asterisk.org/>

Clinic cloud. (s.f.). *Procolos de seguridad*. Obtenido de <https://clinic-cloud.com/blog/protocolos-de-seguridad-de-la-informacion/>

Digital Guide IONOS. (s.f.). *Protocolo TFTP*. Obtenido de <https://www.ionos.es/digitalguide/servidores/know-how/tftp/>

FreePBX. (s.f.). *FreePBX*. Obtenido de <https://www.telefacil.com/wiki/index.php/FreePBX>

FreePBX. (s.f.). *FreePBX*. Obtenido de <https://www.freepbx.org/>

Gil, D. (s.f.). *saranet*. Obtenido de <https://blog.sarenet.es/ventajas-voip-telefonía-analógica/>

RedesZone. (s.f.). *Protocolos de redes*. Obtenido de <https://www.redeszone.net/tutoriales/internet/protocolos-basicos-redes/>

voipalia. (s.f.). *Historio voip*. Obtenido de <http://www.voipalia.com/project/historia-voip/>

Wikipedia. (s.f.). *SIP*. Obtenido de https://es.wikipedia.org/wiki/Protocolo_de_iniciaci%C3%B3n_de_sesi%C3%B3n

wikipedia. (s.f.). *wikipedia*. Obtenido de <https://es.wikipedia.org/wiki/Softphone>

xataka. (s.f.). *voip como funciona*. Obtenido de <https://www.xataka.com/basics/voip-que-como-funciona>