Institución Universitaria
Reacreditada en Alta Calidad
80 Años

Editorial ITM
25 Años

Comunicación unificada de voz sobre Protocolo de Internet

Leonardo Serna Guarín
Juan David Grajales Bustamante
Miguel Alberto Becerra Botero

Comunicación unificada de voz sobre Protocolo de Internet

Comunicación unificada de voz sobre Protocolo de Internet

Leonardo Serna Guarín

Juan David Grajales Bustamante

Miguel Alberto Becerra Botero

ITM Institución Universitaria
Reacreditada en Alta Calidad
80 Años

Colección Línea Profesoral

Serna Guarín, Leonardo, autor | Grajales Bustamante, Juan David, autor, | Becerra Botero, Miguel Alberto, autor.

Comunicación unificada de voz sobre Protocolo de Internet / Leonardo Serna Guarín, Juan David Grajales Bustamante, Miguel Alberto Becerra Botero (autores). Medellín : Institución Universitaria ITM, Editorial ITM 2025. | Primera edición.

152 páginas ; 22 x 22 cm. | Ilustraciones.

1. Computación | 2. Tecnología de la información | 3. Redes | 4. Comunicaciones informáticas | 5. Normas y protocolos de red | I. Tít. II. Serie

384.6

Primera edición: febrero de 2025
Leonardo Serna Guarín, Juan David Grajales Bustamante, Miguel Alberto Becerra Botero (autores).

Sello Editorial ITM
Calle 75 75-101 - Medellín, Colombia
Teléfono: 604 440 51 00 ext. 5197
http://catalogo.itm.edu.co
editorialitm@itm.edu.co

ISBN DIGITAL 978-628-7751-13-2
DOI http://doi.org/10.22430/reporte.6682

Corrección de estilo
Olga Lucía Muñoz
Diseño y diagramación
Mauricio Raigosa Álvarez
Diseño de cubierta
Mauricio Raigosa Álvarez
Ilustraciones
Mauricio Raigosa Álvarez
Marcela Londoño Agudelo

Contenido

Lista de recursos gráficos

Figuras

Tablas

Lista de siglas y acrónimos

ADSL	Asymmetric Digital Subscriber Line (Línea de abonado digital asíncrona)
CODEC	Coder/decoder (codificador/decodificador)
DoS	Denial of Service (Ataque de denegación de servicio)
DSLAM	Digital Subscriber Line Access Multiplexer (Multiplexor de acceso de línea de abonado digital)
DSP	Digital Signal Processing (Procesamiento digital de señales)
GoS	Grade of Service (Grado de servicio)
IAX	Inter-Asterisk eXchange protocol
ICT	Information and Communications Technology (Tecnologías de la Información y las Comunicaciones)
IP	Internet Protocol (Protocolo de Internet)

MPLS	Multiprotocol Label Switching (Conmutación de etiquetas multiprotocolo)
NAT	Network Address Translation (Traducción de direcciones de red)
PABX	Private Automatic Branch Exchange (Central privada automática)
BPS	Bits per Second (bits por segundo)
QoS	Quality of Service (Calidad del servicio)
RTP	Real-Time Transport Protocol (Protocolo de transporte en tiempo real)
SIP	Session Initiation Protoco (Protocolo de iniciación de sesión)
TCP	Transmission Control Protocol (Protocolo de control de transmission)
UDP	User Datagram Protocol (Protocolo de datagramas de usuario)
VoIP	Voice over IP (Voz sobre IP)
VPN	Virtual Private Network (Red privada virtual)
WAN	Wide Area Network (Red de área amplia)
WLAN	Wireless Local Area Network (Red de área local inalámbrica)

UC	Unified communications (Comunicaciones unificadas)
IA	Artificial Intelligence (Inteligencia artificial)
ML	Machine Learning (Aprendizaje automático)
IM	Instant Messaging (Mensajería instantánea)
CRM	Customer Relationship Management (Gestión de relaciones con el cliente)
ERP	Enterprise Resource Planning (Sistema de planificación de recursos empresariales)
NLP	Natural Language Processing (Procesamiento de lenguaje natural)

Sobre los autores

Leonardo Serna Guarín

Es magíster en Automatización y Control Industrial, especialista en Redes de Datos, ingeniero de Sistemas y tecnólogo en Electrónica. Cuenta con una amplia trayectoria en redes de comunicaciones y ciberseguridad.

Juan David Grajales Bustamante

Es magíster en Seguridad Informática e ingeniero de Telecomunicaciones. Cuenta con una amplia trayectoria en redes, Internet de las cosas y ciberseguridad.

Miguel Alberto Becerra Botero

Es doctor en Modelación y Computación Científica, magíster en Automatización y Control Industrial, especializado en Estadística Aplicada y Pedagogía Virtual, y cuenta con formación en Ingeniería Electrónica.

Introducción

El sistema de comunicación telefónico fue el primero en operar en un medio guiado. Su infraestructura inicia en el usuario básico (abonado) y va hasta su enlace con cualquier persona a quien llegue el medio en el mundo. Abarca miles de hogares donde los accesos a Internet crecen rápidamente y se convirtió en una herramienta fundamental en la implementación de nuevos desarrollos para el intercambio de la información. Dicho intercambio se fundamenta en varios aspectos, como escuchar sonidos (la voz) a largas distancias en tiempo real y transmitir información adicional como archivos, imágenes, texto, video y navegación web, entre otros.

Este libro presenta la fundamentación teórica de base para la comprensión, el diseño y la implementación de una solución de comunicación telefónica sobre una red IP, teniendo presente la optimización de recursos existentes con un mínimo impacto y preservando el buen desempeño de las funciones básicas de toda la plataforma de comunicaciones existente y, en general, de todas las funciones que repercuten en beneficio de la prestación de un servicio de telefonía.

En el primer capítulo se aborda el conocimiento general de los sistemas de comunicación telefónica, sus elementos, medios utilizados y los requisitos mínimos para entablar una conversación por medio de un sistema telefónico. En el segundo capítulo se relacionan las características de un sistema telefónico sobre una red de datos que lo soporte, gracias al conjunto de protocolos TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet).

En el tercer capítulo se analiza el conjunto de protocolos involucrados en la comunicación de voz sobre una red IP dotada de características de optimización de tráfico mediante Calidad de Servicio (QoS) y un esquema básico de

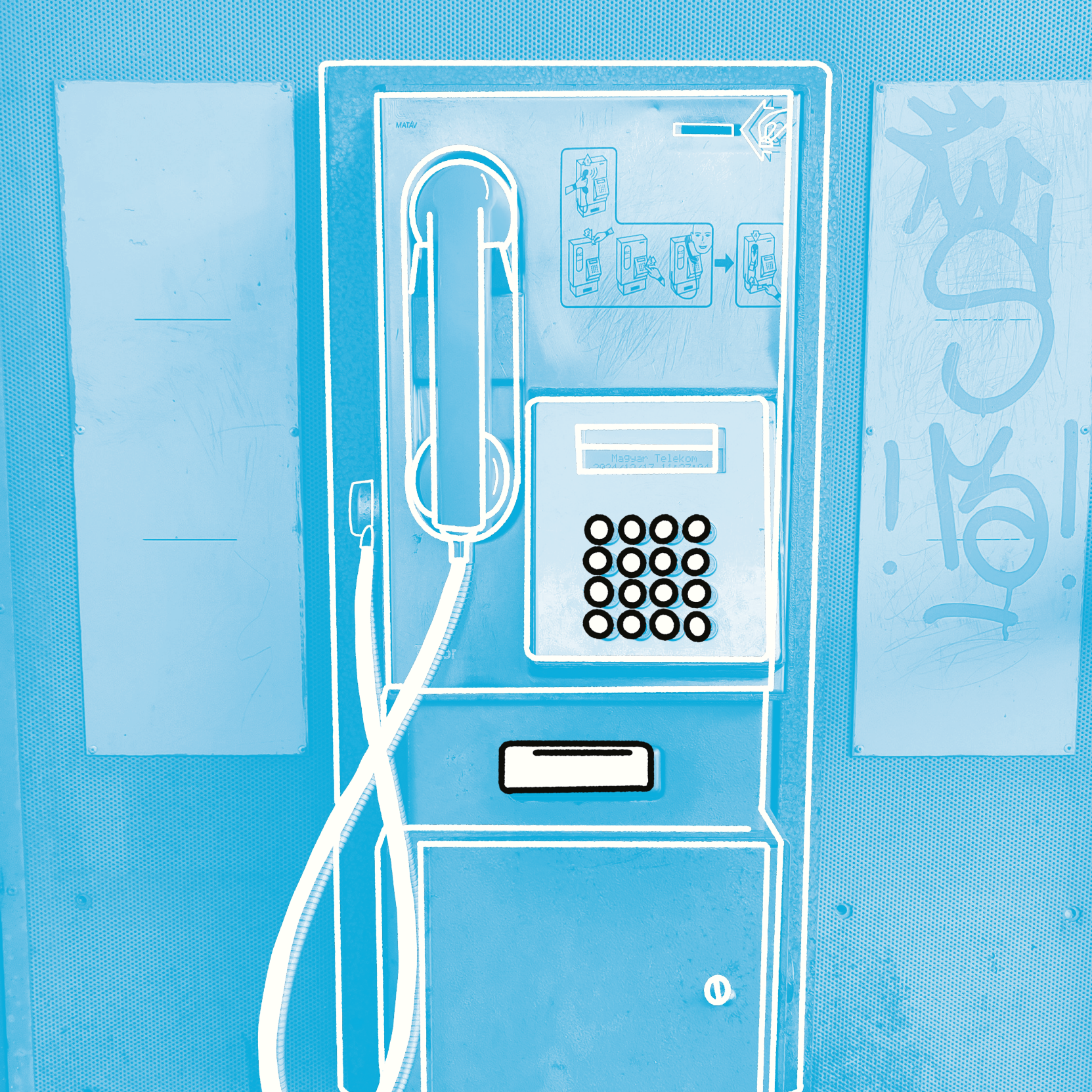
seguridad que permite una funcionalidad estable y privada, aun dentro de una red pública.

En el capítulo cuatro se desarrolla una implementación práctica utilizando herramientas de libre uso (open source), desde la elección del sistema operativo, la virtualización de una planta telefónica y la implementación de una solución de comunicación unificada de voz sobre el protocolo de Internet. La elección de los recursos utilizados se realiza con criterios de facilidad de implementación, estabilidad del servicio y accesibilidad para cualquier usuario del nivel de tecnología en las áreas de TI en un ambiente académico, e incluso en un contexto productivo o empresarial.

El capítulo cinco aborda los principales aspectos de seguridad que hay que tener en cuenta en un proceso de comunicaciones. En él se presenta una configuración básica que debe tenerse en cuenta al brindar cualquier tipo de servicio, especialmente la comunicación de voz sobre IP, donde los atacantes pueden intervenir en la comunicación, acceder a las credenciales de usuario e intervenir en los planes de minutos, entre otros aspectos.

Finalmente, el capítulo seis aborda nuevas tendencias y soluciones en procesos de comunicación, donde la integración de recursos no solo permite optimizarlos, sino también acceder a soluciones que mejoran los procesos en entornos organizacionales e incluso en contextos de uso personal.

En conclusión, este libro ofrece una guía integral para entender y aplicar soluciones de comunicación telefónica sobre redes IP, haciendo hincapié en la optimización de recursos y la seguridad en las comunicaciones. A través de sus capítulos, se ofrece un recorrido detallado que abarca desde los fundamentos teóricos hasta la implementación práctica, abordando tanto los aspectos técnicos como las tendencias emergentes en el campo. Esta obra se convierte así en una herramienta esencial para profesionales y académicos interesados en el desarrollo y mejora de sistemas de comunicación eficientes y seguros.


MATÁV
Magyar Telekom

CAPÍTULO 1.

Introducción a las comunicaciones telefónicas

Introducción

Este capítulo explora la evolución del sistema telefónico desde sus inicios analógicos hasta la transmisión digital actual. Se analizan los componentes clave de una comunicación telefónica desde el nivel local hasta la interconexión global. Se abordarán los siguientes aspectos:

- Historia de la telefonía: se revisará la transformación del sistema telefónico a lo largo del tiempo.
- Componentes básicos: se describirán los elementos de una central telefónica y el dispositivo base de comunicación telefónica.
- Telefonía mundial: se explica cómo funciona la red telefónica y se analizarán los dos métodos principales de conmutación (por circuitos y por paquetes).

Este apartado proporciona una base sólida para comprender la evolución y el funcionamiento de las comunicaciones telefónicas, un elemento fundamental en la interconectividad global.

1.1. Breve historia de las comunicaciones telefónicas

Las redes telefónicas funcionan basándose en la conmutación de circuitos y junto con la conmutación por paquetes forman parte del proceso para establecer una conexión de comunicación entre un punto origen y un

La primera llamada telefónica la hizo Alexander Graham Bell el 10 de marzo de 1876: «Sr. Watson, haga el favor de venir, le necesito». El 7 de enero de 1927 se realizó la primera llamada transatlántica entre Nueva York y Londres con un radioteléfono. Y el 3 de abril de 1973, Martin Cooper hizo la primera llamada con un celular: «Joel, aquí está Marty. Solo te estoy llamando desde un teléfono celular, un teléfono móvil real, portátil, de mano» (Parra, 2023). Actualmente ha disminuido la utilización de las comunicaciones telefónicas y estas se han integrado a sistemas de comunicación unificados a través de la red de internet.

punto destino; la conmutación de circuitos establece un canal dedicado durante el proceso de una sesión, mientras la conmutación por paquetes ensambla la información en tramos para transmitirla por diferentes rutas.

Un circuito conmutado tiene como característica la reserva de un canal para usarse en forma exclusiva en una sola tarea de comunicación: un usuario origen toma («descuelga») su teléfono, espera una señal y marca un número de abonado, mientras en el usuario destino (al otro extremo) se genera una señal sonora y se coge («descuelga») el teléfono. De esta forma, el sistema telefónico establece un enlace dedicado de punto a punto, en ambos extremos, y lo mantiene separado todo el tiempo de la conversación.

Estos sistemas de comunicación realizan la transmisión de la señal de voz en forma análoga y, aunque evolucionaron a sistemas digitales, ya no son apropiados para las necesidades actuales de comunicación (transmitir datos, realizar *streaming* de audio y video). Por tanto, se han desarrollado estándares y se han establecido acuerdos a escala mundial para migrar los sistemas telefónicos antiguos a plataformas avanzadas como la Red Digital de Servicios Integrados (RDSI) y la Línea de abonado digital asíncrona (ADSL, por sus siglas en inglés), y actualmente se llegó a la convergencia por medio de las redes que utilizan el set de protocolos de TCP/IP.

En 1873 Alexander Graham Bell se interesó por el estudio de la telegrafía, con la idea de poder ser capaz de enviar varios mensajes simultáneamente por un solo cable: para ello utilizó pares de resortes de acero e inició así la materialización del sistema telefónico. Luego en 1876 se patenta el teléfono electromagnético, con el cual se dieron grandes desarrollos en comunicación por medios guiados; y hoy en la actualidad operan los sistemas de comunicación inalámbricos que permiten la transmisión de la voz y datos por algunas de las soluciones de comunicación, como la telefonía móvil o celular.

Algunas etapas de la evolución de la telefonía y su tecnología asociada se resumen en la tabla 1.1., en la cual se detallan algunos eventos relevantes y su año de ocurrencia (Escobar Cristiani, 2012):

Tabla 1.1. La evolución de la telefonía y su tecnología

1876	Invención del teléfono
1889	Se descubren las ondas electromagnéticas, base para la comunicación inalámbrica
1909	Transmisión de radio
1919	La interconexión de centrales
1924	Aparece el teletipo
1936	Transmisión por TV
1938	Se presenta la Modulación por impulsos codificados
1940	Cables trasatlánticos para comunicación mundial
1946	Aparece el ENIAC (Electronic Numerical Integrator and Computer/Computador e Integrador Numérico Electrónico)
1947	Aparece el transistor
1948	Enlace microondas
1957	Primer satélite artificial
1960	Creación del circuito integrado
1967	Aparece Internet
1975	La fibra óptica
1977	Transmisión por fibra óptica
1978	Diseño de TCP/IP
1979	Modelo OSI
1983	El Departamento de Defensa de EU adopta TCP/IP (base de internet)
1987	Circuito integrado con un millón de transistores
1988	El cable trasatlántico submarino con fibra óptica
1989	Aparece la SDH (Synchronous Optical Networking/Jerarquía digital síncrona)
1989	El CERN libera la World Wide Web (www)

Fuente: elaboración propia.

1.2 Sistema básico de comunicación telefónica

La información se origina en una «fuente», cuando se transmite llega a un «destino» y se transporta como un mensaje en un medio llamado «canal de comunicación». En teoría no hay límite de distancia, debido a que puede recorrer desde una corta distancia hasta grandes trayectos, características que se detallan en la figura 1.1.

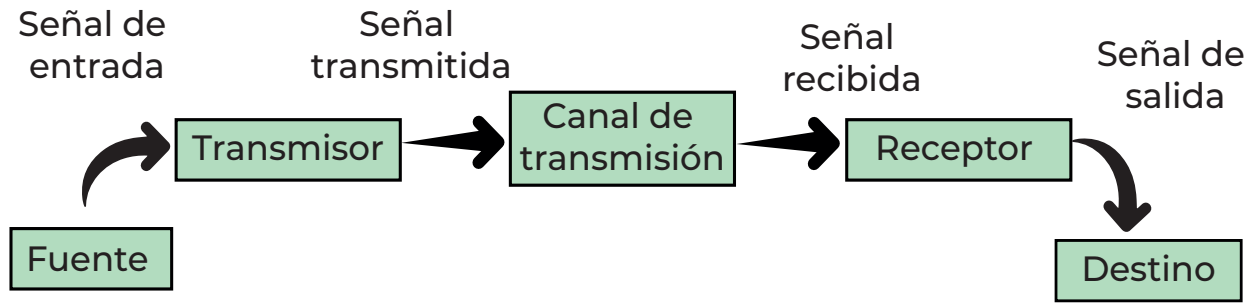
El sistema básico de comunicaciones debe tener las siguientes características:

- Rapidez. Deben desarrollarse en tiempo real, porque a pesar de la distancia los tiempos de retraso disminuyen la validez de la información.
- Seguridad. La información se debe entregar solo a quien corresponda, de manera integral.
- Veracidad. Su contenido debe conservarse intacto.
- Accesibilidad en costos. Debe garantizar la transmisión de la información a un costo viable.

1.3. Transformación del sistema telefónico

En sus inicios, las centrales telefónicas eran controladas manualmente por operadores. Posteriormente se desarrollaron los sistemas de control y señalización para lograr la automatización del sistema, que mejora la rapidez del

Figura 1.1. Sistema básico de comunicación

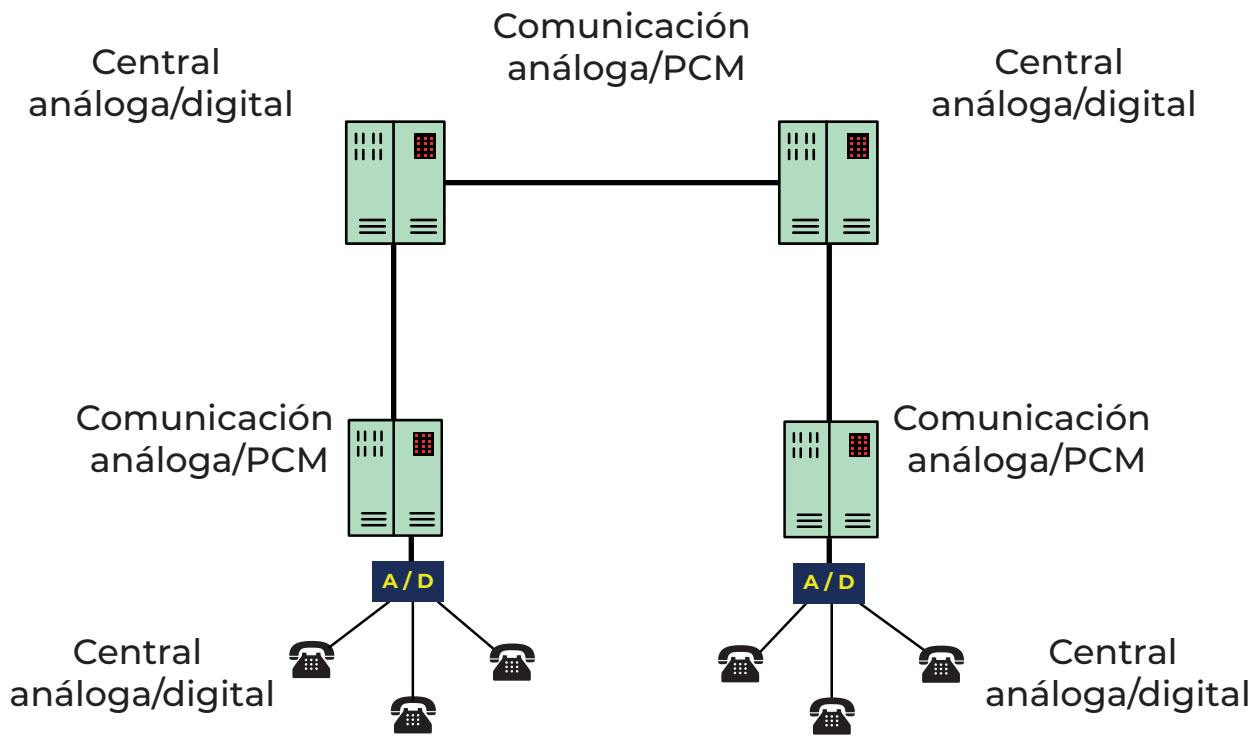


Fuente: elaboración propia.

servicio, ahorra costos y ofrece así mejores ventajas para los usuarios. Alrededor de los años 70 los conmutadores fueron analógicos y su transmisión totalmente análoga, la cual posteriormente evolucionó hacia la transmisión digital como solución para mitigar el ruido y la pérdida de señal en largas distancias (Hill, 2007).

Las centrales automáticas eran electromecánicas, compuestas de elementos eléctricos y mecánicos como el relé. Más tarde evolucionaron a las centrales semielectrónicas, con elementos de control electrónicos que permitieron desarrollar nuevas capacidades en los sistemas: nuevos servicios, aumento del tráfico telefónico y de la capacidad de señalización, ahorro de costos y mejora de los recursos por consumo energético y por tamaño de los equipos. En la red de la figura 1.2. se ilustra la red telefónica análoga y su evolución a un sistema digital.

Figura 1.2. Evolución de la red telefónica



Fuente: elaboración propia a partir de Escobar Cristiani (2012).

La industria telefónica permitió establecer una red mundial para la transmisión de la voz constituida por sistemas análogos y digitales que, a la par de la evolución tecnológica del circuito digital y de los sistemas de cómputo generaron grandes cambios en los sistemas de comunicaciones, entre los cuales se destacan la automatización y los nuevos modos de transmisión. Seguidamente se suplieron nuevas necesidades de comunicación diferentes a la voz, como la transmisión de datos e imágenes, surgiendo redes alternativas o de nueva generación para permitir la interconexión con otras redes a escala global, regida por normas y estándares internacionales que integran gran variedad de servicios (Cabezas Pozo, 2007).

En general, estas redes telefónicas se clasifican en dos tipos:

- Redes públicas, que pueden ser fijas y móviles.
- Redes privadas, constituidas por un conmutador.

Las redes públicas se diferencian de las privadas en que se comunican entre dos o más abonados, mientras que las privadas son utilizadas por las compañías en sus requerimientos de comunicación (Fernández García y Barbado Santana, 2008).

1.4 Componentes básicos de una central telefónica

Los principales elementos que constituyen una central telefónica son:

1. Las galerías subterráneas que interconectan los cables de los usuarios con la central.
2. Los MDF (repartidores principales). En estos repartidores finaliza el cable del abonado y se unen a los servicios contratados por cada usuario terminal.
3. Los equipos de conmutación (analógicos o digitales). Soportan la red básica telefónica (RTB) y los equipos Digitales de Servicios Integrados RDSI.
4. El multiplexor (DSLAM). Utilizado para brindar servicios de banda ancha a los usuarios que lo requieren. Este equipo opera como un módem: por un lado se conecta al usuario y por el otro a Internet.
5. Los equipos de transmisión interconectan centrales utilizando fibra óptica u otro tipo de medio; conducen la comunicación hacia su destino, donde se integran servicios con las redes de datos.
6. Los bancos de baterías sirven para alimentar los equipos telefónicos con 48V de C.C.

7. Los generadores de energía aseguran el funcionamiento continuo de las baterías, evitando que se descarguen.

1.5. Dispositivo base de comunicación telefónica

En todo sistema telefónico se distinguen tres subsistemas: la conmutación encargada de la conexión entre abonados, la transmisión como transporte de energía por algún medio y la distribución como la conexión hasta el punto final con el usuario. La distribución inicia en un nodo troncal y finaliza en un equipo terminal, está conformada por dos hilos conductores que unen la central de conmutación y el teléfono terminal.

El teléfono o aparato terminal es el elemento de comunicación empleado por los usuarios. Inicialmente, estos dispositivos debían enlazarse a las líneas telefónicas y no se movían fácilmente; actualmente, con el teléfono inalámbrico puede haber desplazamiento de decenas de metros, brindando mayor libertad a los abonados. En el mismo sentido, con la aparición de la telefonía celular el usuario puede comunicarse desde cualquier sitio gracias a los nuevos sistemas de comunicación y al desarrollo de nuevos protocolos.

En la figura 1.3. se detallan los componentes básicos que constituyen un teléfono convencional, incluyendo los circuitos que operan en conjunto para realizar una llamada: el circuito de conversación formado por la parte analógica del dispositivo y el circuito de marcación para manejar el marcado de las llamadas realizadas.

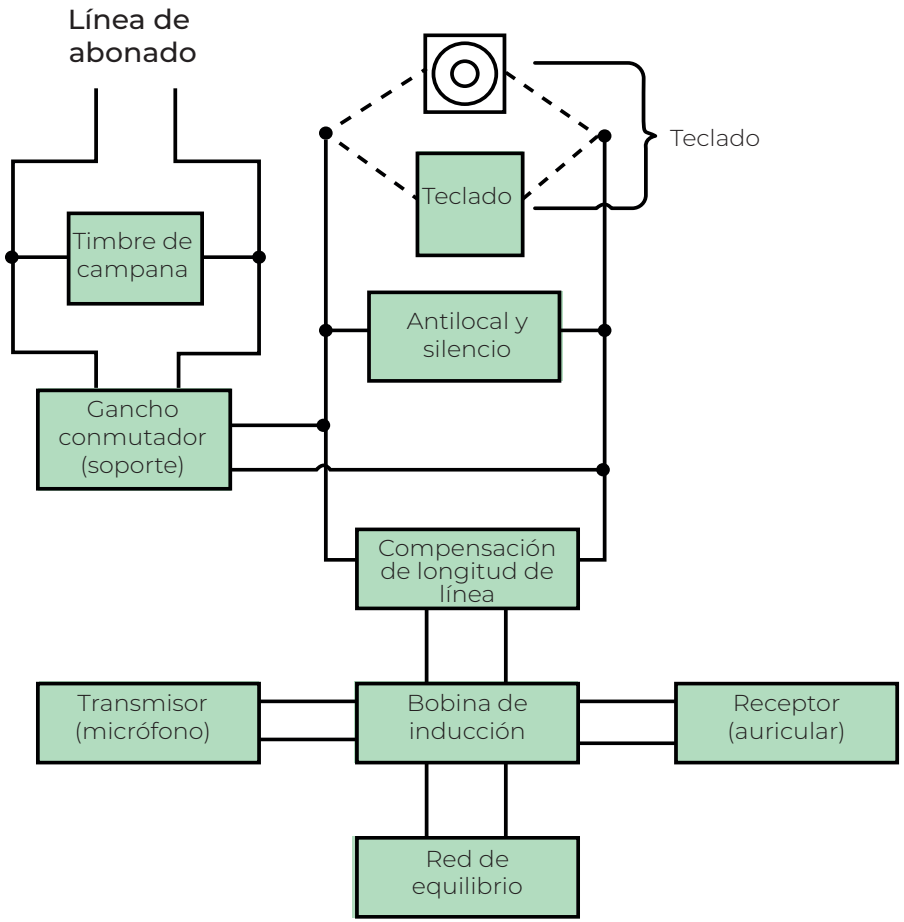
En función del tipo de marcación se distinguen los siguientes tipos de teléfono:

- Disco giratorio con diez orificios: realiza cortes de corriente generando pulsos de llamada entre el usuario y la central. Con el número de pulsos se determina el número a marcar.
- Teclado decádico: utiliza un teclado numérico que lo hace más seguro para marcar, pero funciona igual que el sistema de disco giratorio.
- Teclado multifrecuencia DTMF: basado en la utilización de tonos o señales. Al pulsarse una tecla se envían dos tonos correspondientes respectivamente a la fila y a la columna de una matriz.

1.6. La telefonía en el ámbito mundial

Actualmente, el sistema telefónico alrededor del mundo sigue siendo analógico, sobre todo en la última milla de conexión al usuario. La modulación utilizada emplea señales eléctricas

Figura 1.3. Componentes del teléfono convencion



Fuente: elaboración propia a partir de González Parrón y González Martínez (2019).

que viajan en un par de hilos, generalmente de cobre, para el transporte de la voz. La transmisión analógica ofrece la ventaja de ser un sistema simple, con un retardo en la transmisión relativamente bajo y es económico para pocos usuarios que hablan al tiempo sin estar muy distantes; y una desventaja relevante en el sistema analógico es la utilización de un par de hilos para una conversación, lo cual no es práctico y lo hace muy costoso.

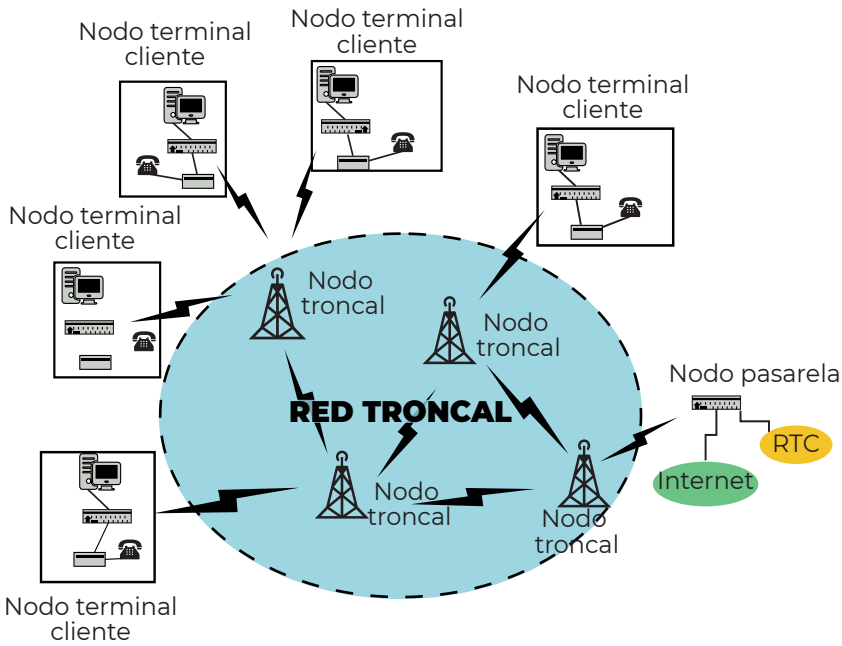
La mayoría de los países usan tecnología digital en su red telefónica principal, donde la línea del usuario es análoga pero la señal es transformada en un flujo de datos digitales en la primera central local: se realiza una multiplexación de muchos canales de voz mediante Multiplexación por División en el Tiempo (TDM) para una señal digital o por División en la Frecuencia (FDM) para el caso de ambas señales, análoga o digital (Ahson & Ilyas, 2009).

La red o planta externa está constituida por los elementos que establecen el enlace de la central telefónica con los usuarios; esta red se compone de cables de cobre o fibra óptica, cajas de empalme y bobinas. Las partes que forman la red telefónica a escala global se detallan en la figura 1.4.

Puede observarse la jerarquía de redes que constituyen el sistema:

- La red local de un usuario compuesta de líneas de extensión conectadas a una central automática privada, como un PABX para telefonía o datos en una LAN.

Figura 1.4. Red telefónica global



Fuente: elaboración propia a partir de Hill (2007).

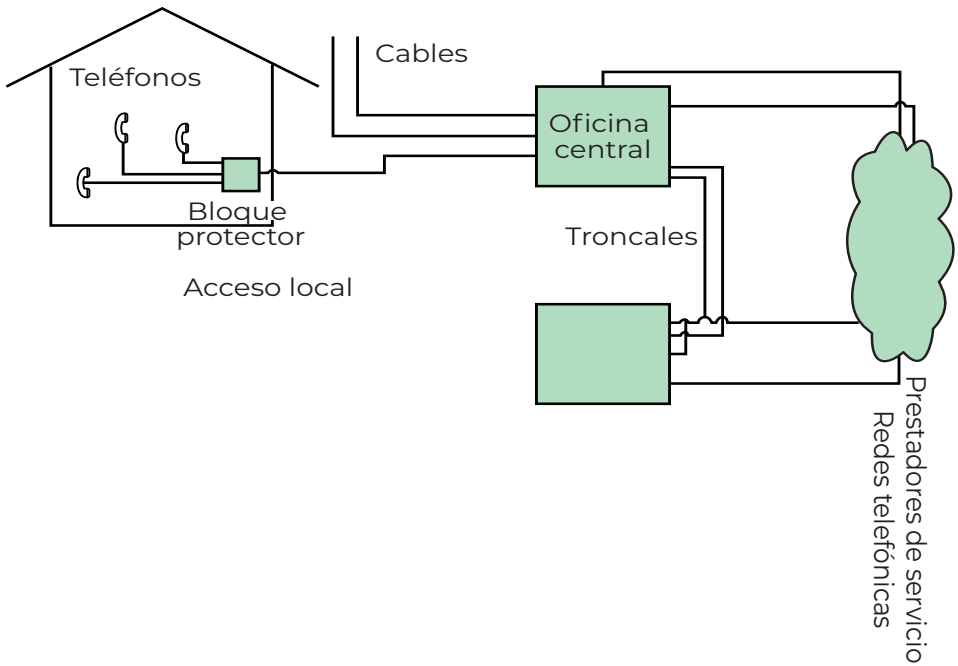
- La red de distribución de los usuarios denominada «red de acceso», la cual interconecta a un intercambiador local o prestador de servicios.
- La red que interconecta un grupo de centrales locales a un centro local primario.
- La red troncal que interconecta centros primarios en todo el país y, a su vez, con otras redes a escala global por medio de un *gateway* internacional de intercambio.

En la figura 1.5. se observan los componentes básicos de una red de telefonía que se involucran desde el usuario hasta el proveedor de servicios PSTN.

1.7. La red telefónica

La red de telefonía ha sido la de mayor alcance geográfico con el más grande número de usuarios; de igual forma, es un sistema complejo que permite realizar una llamada entre dos

Figura 1.5. Componentes básicos de la red telefónica

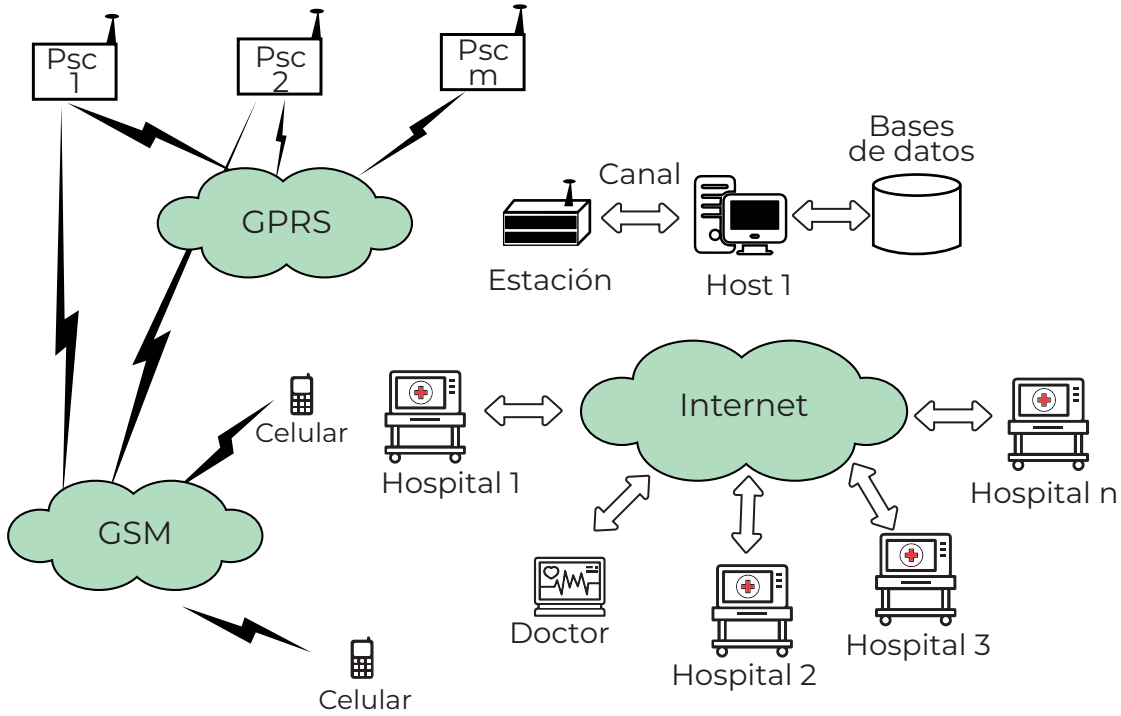


Fuente: elaboración propia a partir de Noll (1998).

usuarios en sitios distantes o en cualquier lugar del planeta. Los teléfonos instalados alrededor de la Tierra se interconectan por una red mundial formada por trayectorias que interconectan nodos de conmutación. Las trayectorias de comunicación son establecidas por los conmutadores cada vez que se hace una llamada y finalizan la trayectoria cuando el enlace no es requerido; asimismo se realizan funciones analógicas en cada trayectoria y se determina automáticamente la tarificación o el cobro correspondiente por la utilización del sistema. La figura 1.6. detalla los componentes de una red telefónica y su vinculación a otras redes (Dornheim, 2020).

El canal de comunicación establecido entre un origen y un destino utiliza fundamentalmente dos técnicas de conmutación: conmutación de circuitos y conmutación de paquetes (cabe anotar que la conmutación de mensajes funciona en las redes telegráficas). La conmu-

Figura 1.6. Red telefónica unida a otras redes



Fuente: elaboración propia (2023).

tación evolucionó desde su origen de la forma manual a la forma automática analógica, posteriormente a TDM digital y actualmente sobre IP. En la figura 1.7. se resumen las tecnologías usadas por las centrales de conmutación.

En el funcionamiento del sistema telefónico se conforman varios planes técnicos, como se detalla a continuación:

1. La red de telefonía: constituida por todos los elementos físicos entre terminales, cables y dispositivos de control.

2. El plan de conmutación: establece los diferentes tipos de control que utilizará para transmitir la señal de voz entre la entrada y la salida del sistema de comunicación.

3. El plan de transmisión: define las características de la señal, su atenuación permisible, rangos de frecuencia de operación, niveles de ruido tolerables y niveles de potencia para establecer la comunicación de terminal a terminal.

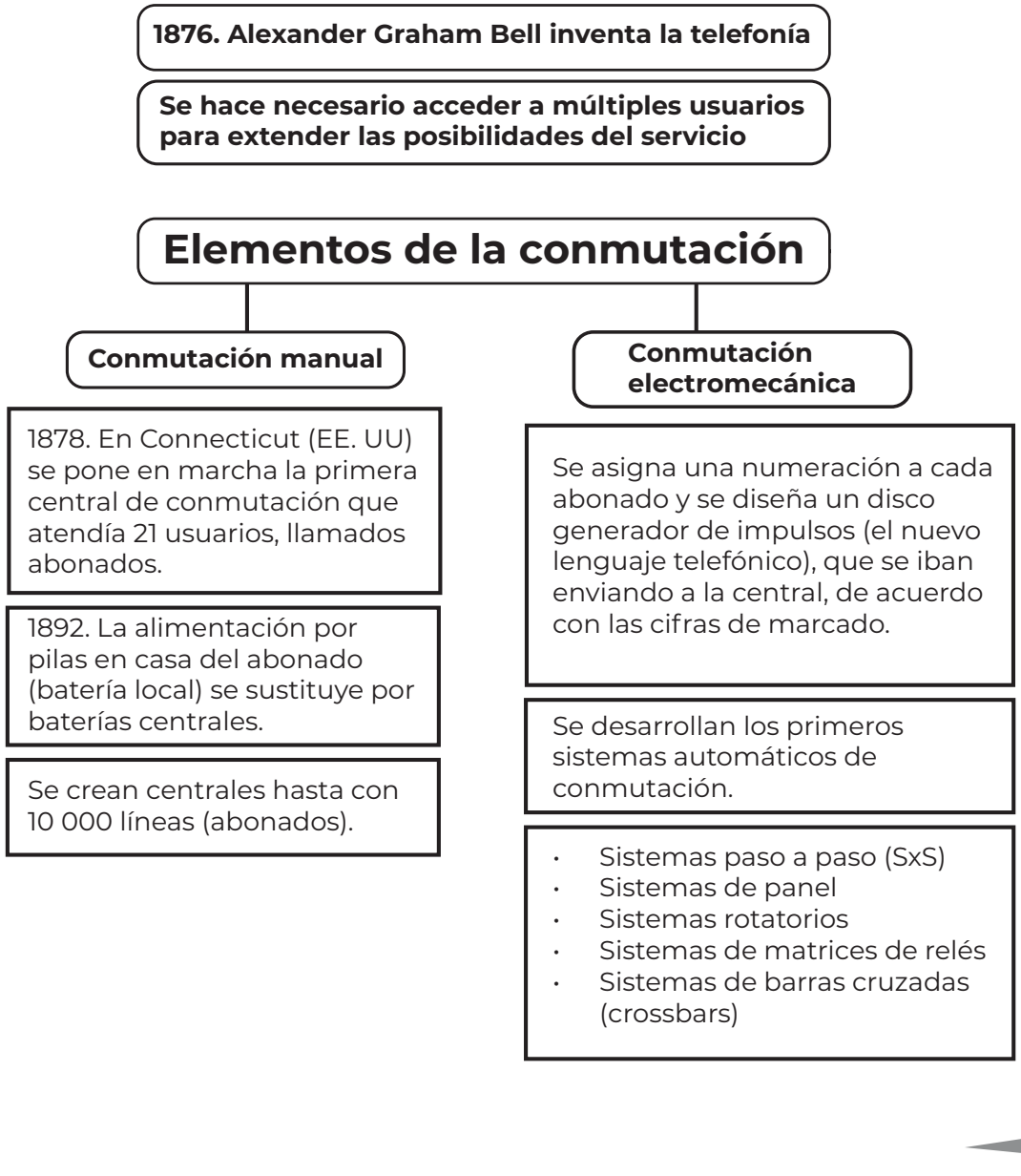
4. El plan de tasación: comprende los controles de tiempo y la cuantificación o tarifas de los procesos de comunicación telefónica. Determina el costo de una comunicación telefónica basado en el tiempo de actividad.

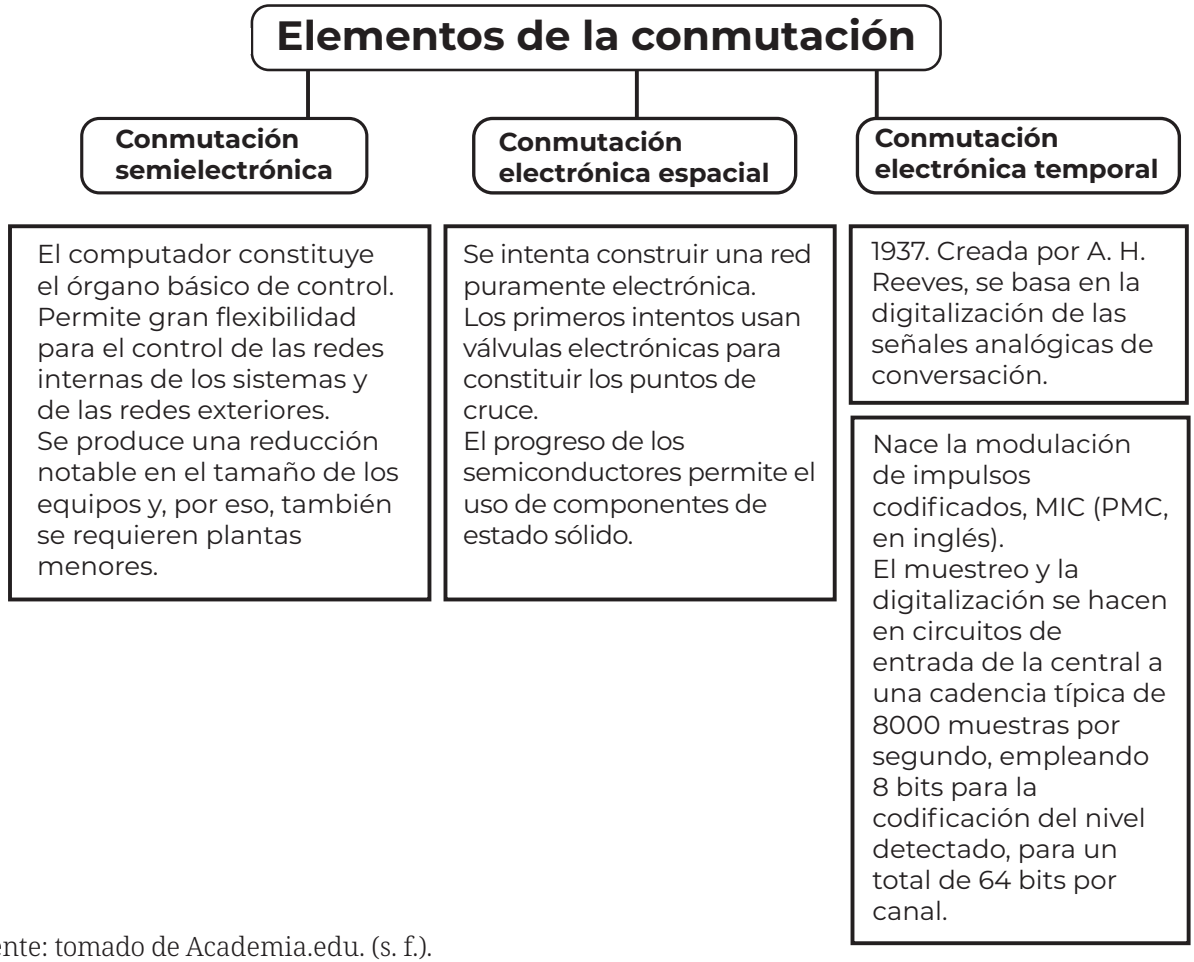
5. El plan de señalización: comprende el conjunto de reglas y protocolos que gobiernan la comunicación desde que se inicia hasta que finaliza. Hay un conjunto de señales entre la terminal y la central, y a su vez entre distintas centrales. La señalización se puede realizar por canal asociado CAS (Channel Asociated Signaling) donde esta viaja por el mismo canal que utiliza la voz o por canal común CCS (Common Channel Signaling) para la transmisión digital a mayor velocidad y por un canal específico o diferente al utilizado por la voz.

6. Dentro de una red telefónica, cada usuario se identifica con un número telefónico. Al levantar la bocina se da un tono de invitación a marcar, el conmutador que lo atiende espera instrucciones del número telefónico para suministrar a la conmutadora la información respectiva para el enrutamiento y los costos asociados a la llamada. El número telefónico es una dirección jerárquica que permite conmutar la llamada, al establecer la comunicación entre el origen y el destino entre regiones, ciudades o países (Noll, 1998).

7. El plan de numeración: este plan asigna un número a cada usuario o terminal para permitir su identificación, encaminando sin error las llamadas que transitan en la red. De igual forma incluye los números de ser-

Figura 1.7. Evolución de las centrales de conmutación





Fuente: tomado de Academia.edu. (s. f.).

vicios especiales y suplementarios, como los números de emergencia, servicio de hora, policía o larga distancia; además de las combinaciones numéricas de 0 a 9, este plan también incluye códigos como el asterisco y el numeral en servicios como la transferencia de llamadas. Este plan se desarrolla conforme a normas internacionales.

Dentro del plan de numeración se definen varios criterios para la asignación del número al usuario, haciendo que este sea único dentro de un contexto local y fijando de esta forma varios números (estructura del número identificador):

- Número de abonado: determina la posición del suscriptor y puede estar planea-

do acorde a la distribución geográfica. El número telefónico tiene las funciones de enrutar la llamada por la red y activar el tarificador (control de tiempo y cobro).

- Número de central: identifica cada central en un área geográfica.
- Número local: conjunto de dígitos marcados por el usuario para comunicarse con su destino local (código central + número de abonado).
- Código de área: indicativo nacional, identifica un área geográfica con un grupo de centrales locales dentro de un país.
- Número nacional: conjunto de dígitos que identifica un usuario en un país (código área + número local).
- Código país: indicativo internacional que identifica un país.
- Número internacional: identifica los usuarios entre países (código país + número nacional).

El plan de numeración también define los códigos de acceso nacional e internacional para cada país y permite seleccionar el operador que realizará el enrutamiento de las llamadas de larga distancia. La recomendación E.164 de la UIT-T define el indicativo de los países. La estructura del número nacional o internacional se detalla en la tabla 1.2.

Los sistemas de conmutación tienen una limitante referente al número máximo de usuarios que puede atender cada unidad. Cada país define un plan de numeración que puede ser abierto cuando el número del usuario es de longitud variable por no estar estandarizado y cerrado cuando los números de los usuarios son fijos. Este último caso se da en países pequeños donde no son necesarios prefijos regionales y permite repartir más números de usuario sin alargar su longitud.

De forma general, las principales funciones de la central telefónica son las siguientes:

- Identificar la central a la que está conectado el usuario destino.
- Encaminar la llamada hacia la central y generar enrutamiento. El plan de encaminamiento tiene en cuenta las rutas directas, las alternativas y la congestión.
- Reservar trayectorias entre usuarios para realizar la comunicación.
- Manejar servicios digitales y analógicos.
- Realizar tarificación para las llamadas de cada usuario.

Tabla 1.2. Estructura del número nacional e internacional

		Número nacional	
PI	**CC**	**NDC**	**SN**
Prefijo internacional. Código de acceso	Código de país. De 1 a 2 cifras	Indicativo nacional de destino. De 1 a 3 cifras	Número de suscriptor. De 5 a 7 cifras
	Número internacional		

Fuente: elaboración propia (2023).

- Realizar la señalización entre centrales y usuarios.
- Establecimiento y verificación de protocolos que se ejecutan en los nodos y centrales.
- Transmisión. Los nodos se encargan de adaptar la información al canal de comunicación.
- Interfaz. Cada nodo proporciona al canal las señales que serán transmitidas según el medio utilizado.
- Recuperación de fallas. El sistema debe recuperarse y reanudar la transmisión de los mensajes que no fueron enviados.
- Formateo. En una interconexión entre diferentes redes puede haber diferentes protocolos; por ello puede ser necesario modificar en los nodos el formato en que se reciben los mensajes.
- Ruteo. El mensaje contiene información acerca de los usuarios origen y los usuarios destino.
- Repetición. Muchos protocolos utilizan reglas por medio de las cuales el nodo receptor detecta si hubo algún error en la transmisión.
- Direccionamiento. Los nodos identifican direcciones para llevar los mensajes a su destino.
- Control de flujo. El canal tiene una capacidad máxima de manejo de mensajes, una vez se satura no envía más mensajes hasta que los ya enviados se entreguen de forma satisfactoria al destino.

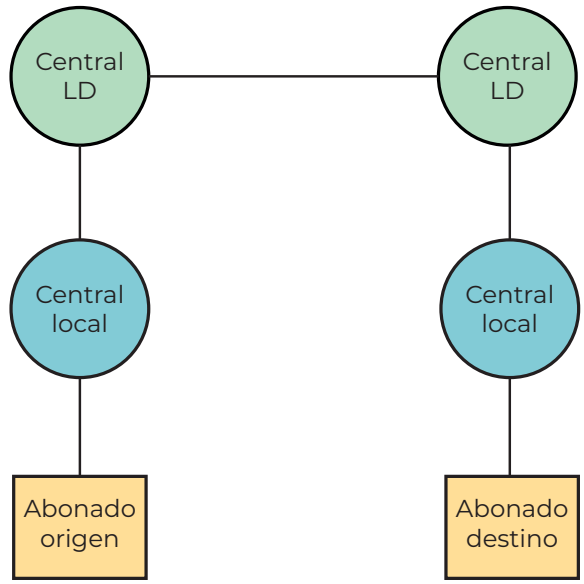
1.8. Conmutación por circuitos

La central telefónica identifica el destino y enruta la llamada, indicando con un tono que alguien lo quiere contactar; una vez identificado el destino, reserva una trayectoria entre origen y destino durante todo el tiempo que tarde la comunicación. En esta conmutación se establece una ruta o circuito físico previo a la transferencia de información en la comunicación entre el origen y el destino (figura 1.8.), el uso de este circuito permanece continuo y es exclusivo. Una vez termina la comunicación se desconecta el circuito y se liberan los enlaces entre los nodos, de manera que estos enlaces queden disponibles para utilizarlos posteriormente en otras conexiones.

Sus principales características son:

- Ancho de banda fijo e invariable.
- Bajo retardo en el establecimiento de la comunicación.
- Comunicación en tiempo real.
- Retardos pequeños y constantes, siendo ideal para voz y video.
- Recursos usados de forma ineficiente.

Figura 1.8. Conmutación por circuitos



Fuente: elaboración propia a partir de Escobar Cristiani (2012).

1.9. Conmutación por paquetes

Esta técnica fue desarrollada para utilizar de manera eficiente el medio de transmisión. La comunicación que establecen diferentes usuarios puede compartir una misma trayectoria física; la información se segmenta en pequeños pedazos o paquetes, y cada uno contiene datos de control en un encabezado, como las

direcciones origen y destino, el número de paquete y una secuencia de bits para verificación de errores. Cada paquete viaja entre nodos y algunas veces por rutas diferentes.

El sistema acepta paquetes de un nodo, los almacena en un búfer y los retransmite a otro conmutador, en el cual se repite la secuencia de almacenamiento y retransmisión. Este proceso se repite hasta que todos los paquetes llegan al nodo de destino.

Las principales características de este sistema son:

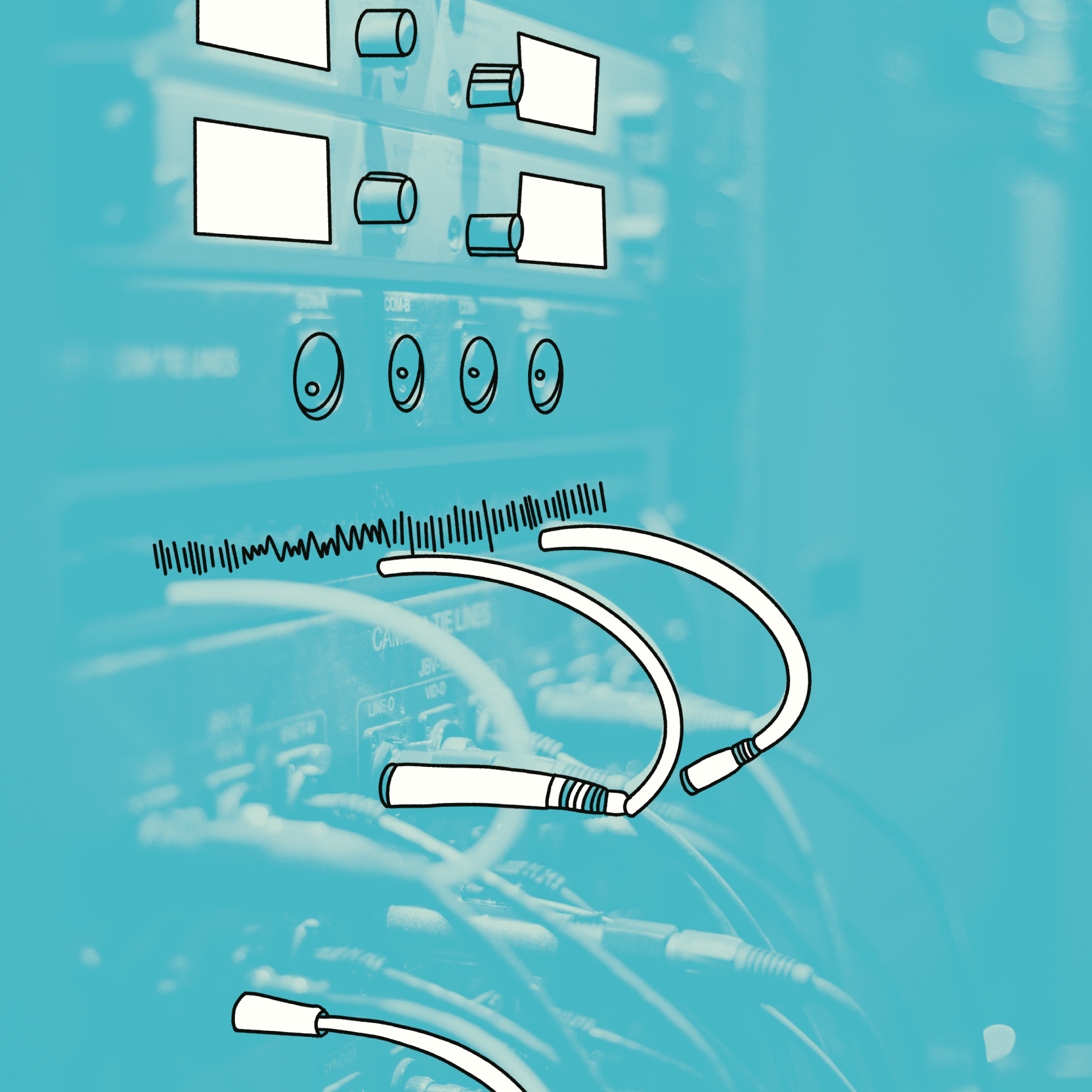
- En comparación con la conmutación por circuitos, optimiza los métodos y medios empleados para la transferencia de información.
- Tiene diferentes velocidades o capacidades de transferencia; las tasas de origen pueden ser diferentes en el destino.
- Puede ofrecer rutas alternativas.
- Ancho de banda asignado dinámicamente.
- El retardo de propagación no es constante y es mayor que el de circuitos.
- Apropiado para tráfico interactivo.
- Diversos paquetes y destinos utilizan el mismo medio para transmitir.
- Probabilidad de pérdida de paquetes transmitidos, por saturación o por congestión.
- La tarificación se hace por tráfico.
- Es necesario el mensaje de recibo entre conmutadores para indicar que los paquetes llegaron; en caso contrario, los paquetes serán retransmitidos.

Conclusiones

La evolución y la transformación histórica del sistema telefónico ha sido sorprendente, desde los primeros experimentos de Alexander Graham Bell hasta las complejas redes de telecomunicaciones actuales. La transformación del sistema telefónico ha permitido una comunicación más rápida, segura y eficiente, adaptándose a las necesidades crecientes de la humanidad. El desarrollo de nuevas tecnologías y la digitalización de los sistemas han sido cruciales para esta evolución, destacándose la capacidad del sistema telefónico para innovar y mejorar continuamente.

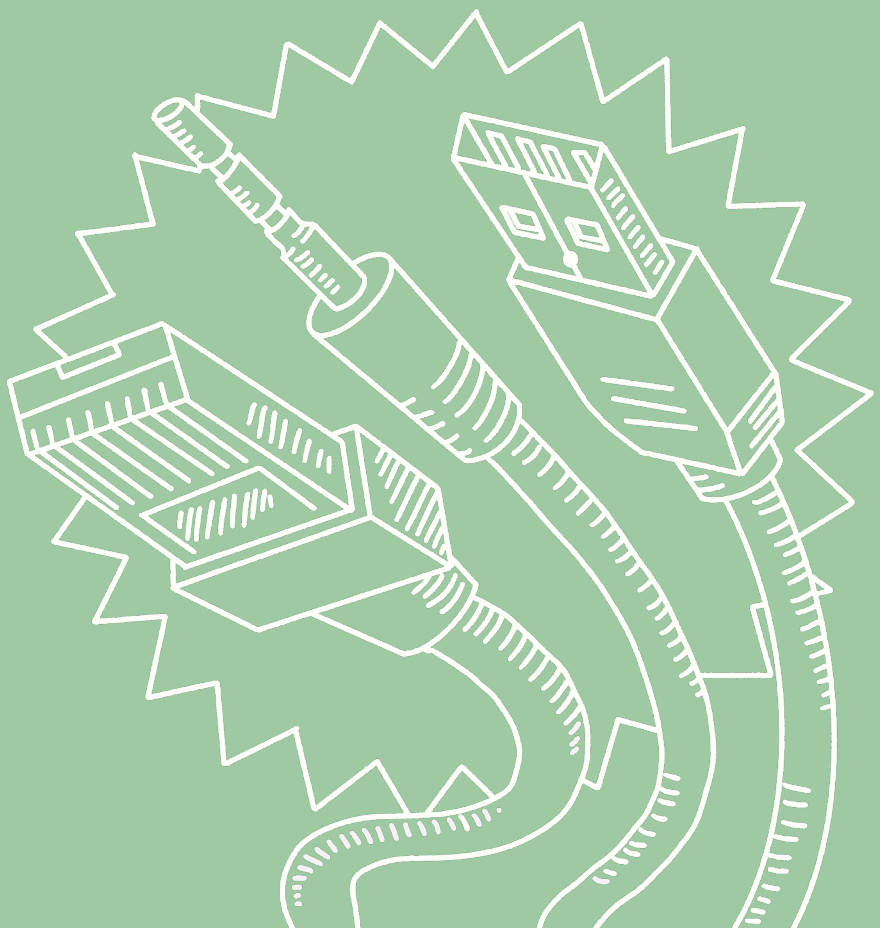
Los componentes y el funcionamiento de las centrales telefónicas son esenciales para el funcionamiento efectivo de las comunicaciones telefónicas; estos incluyen el equipo de conmutación que permite la conexión de llamadas y los dispositivos de transmisión que facilitan la transferencia de voz y datos. La central telefónica actúa como un *hub* (concentrador o nodo) que gestiona y dirige el tráfico de llamadas, asegurando que la comunicación se realice de manera eficiente. Entender estos componentes es fundamental para cualquier estudio sobre sistemas de comunicación.

La importancia de la conmutación en la red telefónica, tanto por circuitos como por paquetes, es fundamental en la operación de esta red. La conmutación por circuitos establece una conexión dedicada durante toda la duración de una llamada, proporcionando una comunicación continua y estable. En contraste, la conmutación por paquetes divide los datos en paquetes que se envían independientemente y se reensamblan en el destino; esta última ha ganado preeminencia en las redes modernas debido a su eficiencia y capacidad para manejar grandes volúmenes de tráfico. Comprender estas técnicas es vital para apreciar cómo se mantiene la calidad y fiabilidad en las comunicaciones telefónicas actuales.



CAPÍTULO 2.

Redes de comunicaciones orientadas a VoIP



Introducción

En este capítulo se explora la tecnología de Voz sobre Protocolo de Internet (VoIP), una innovación que ha revolucionado la manera de realizar las comunicaciones de voz. Este segmento abarca una variedad de temas esenciales para entender la telefonía IP, desde su definición y funcionamiento hasta su arquitectura básica y los diferentes tipos de arquitecturas empleadas. Se examinan también los códecs utilizados en la comunicación VoIP, fundamentales para la codificación y decodificación de la voz en formato digital. Además, se profundiza en los protocolos empleados en VoIP (como SIP, H.323, IAX) y las comparaciones entre ellos (H.323 vs. SIP, IAX vs. SIP); estos subtemas proporcionan un conocimiento integral sobre cómo se establecen, gestionan y optimizan las comunicaciones de voz a través de Internet.

La telefonía IP o VoIP es la realización de conversaciones telefónicas a través de una red de ordenadores en un entorno local o a través de Internet, usando el Protocolo IP (Dornheim, 2020). Este sistema de comunicaciones permite utilizar la plataforma de Internet como un canal telefónico que permite llevar la voz a cualquier destino sobre la red IP, proporcionando una base que agrega aplicaciones unificadas de comunicaciones más avanzadas –incluidas conferencias web y videoconferencias–, que transforman la forma en que se presta un servicio. El sistema de voz IP cumple tres funciones básicas: empaquetar la voz, digitalizar la voz y enrutar los paquetes utilizando Internet (Joskowicz, 2013).

En 1995 unos jóvenes en Israel desarrollaron el primer *softphone* (Internet Phone Software). Entre 2010 y 2018 la voz sobre redes IP incrementó siete veces su uso en el ámbito empresarial, ahorrando costos entre 20 y 30 dólares mensuales y reduciendo la tarifa internacional en un 90 %; adicionalmente, se logró un ahorro de 32 minutos en llamadas telefónicas por día (Willing, 2024).

En la tabla 2.1. se detallan algunas diferencias entre la telefonía tradicional y la telefonía IP, con el fin de identificar la opción de mayor beneficio operativo y económico para el desempeño de las actividades empresariales (Ockay, 2018).

Tabla 2.1. Telefonía tradicional vs. telefonía IP

Características	Telefonía tradicional	Telefonía IP
Ancho de banda	Menos ancho de banda	Mayor ancho de banda
Medio de transmisión	Cable de pares (línea telefónica)	Cable UTP (línea de Internet)
Calidad de servicio	No hay que cumplir unos requisitos de calidad del servicio	La latencia tiene que estar entre 2000ms-3000ms
Servicios ofrecidos	Tarificación por tiempo Se establece llamada Ancho de banda fijo	Tarificación por ancho de banda No se establece llamada sino autenticación Ancho de banda variable
Tiempo de establecimiento	Aceptable para voz Muy largo para datos	No existe fase de establecimiento
Retardo de transmisión	Despreciables	Retardos de milisegundos en todas las llamadas
Asignación de circuitos	Único y exclusivo para cada comunicación	Compartido por otras comunicaciones simultáneas
Identificación del destino	Solo en la fase de establecimiento	Se incluye un identificador en cada paquete
Necesidad de almacenar en la red	No	Sí, en los nodos de la red
Flexibilidad de la red	Encaminamiento alternativo	Gran flexibilidad

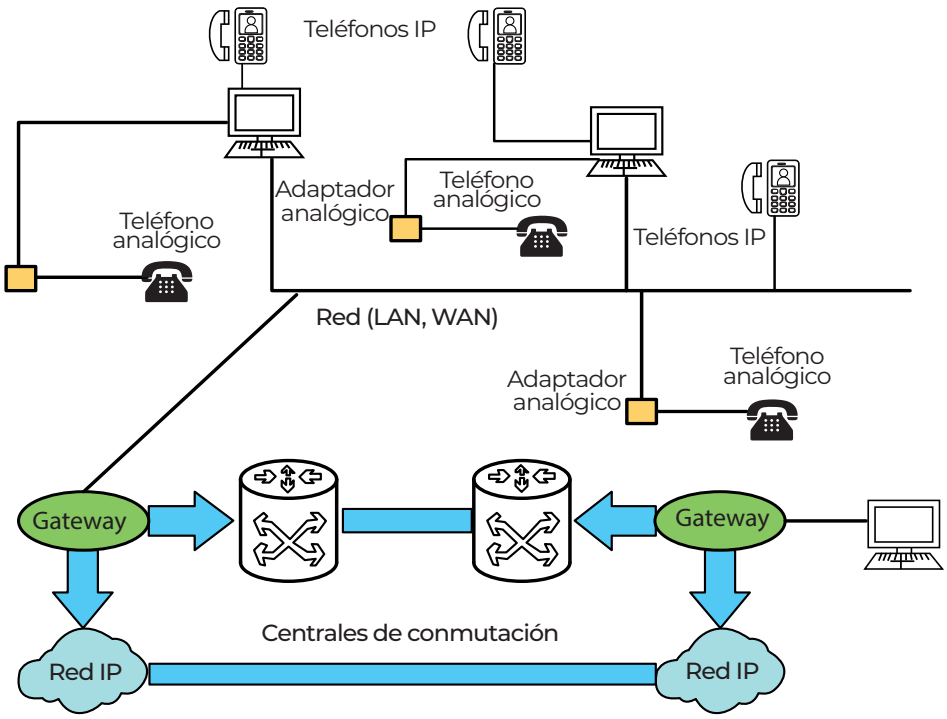
Fuente: elaboración propia (2023).

La ventaja que sobresale en el sistema de comunicación de voz sobre IP es su bajo costo cuando se realizan llamadas fuera de un paquete convencional de la telefonía común, incluidos los sistemas de telefonía móvil; además permite la integración de voz y datos en un mismo sistema, utilizando recursos existentes como la plataforma de cómputo y los canales de acceso dedicado. Por otra parte, debe tenerse presente que su calidad de voz es inferior y presenta más riesgos de seguridad comparado con la telefonía tradicional (Hersent, 2011).

2.1 Arquitectura básica de un sistema VoIP

Los elementos que conforman un sistema general de VoIP se detallan en la figura 2.1.

Figura 2.1. Sistema unificado de VoIP



Fuente: elaboración propia a partir de García (2008).

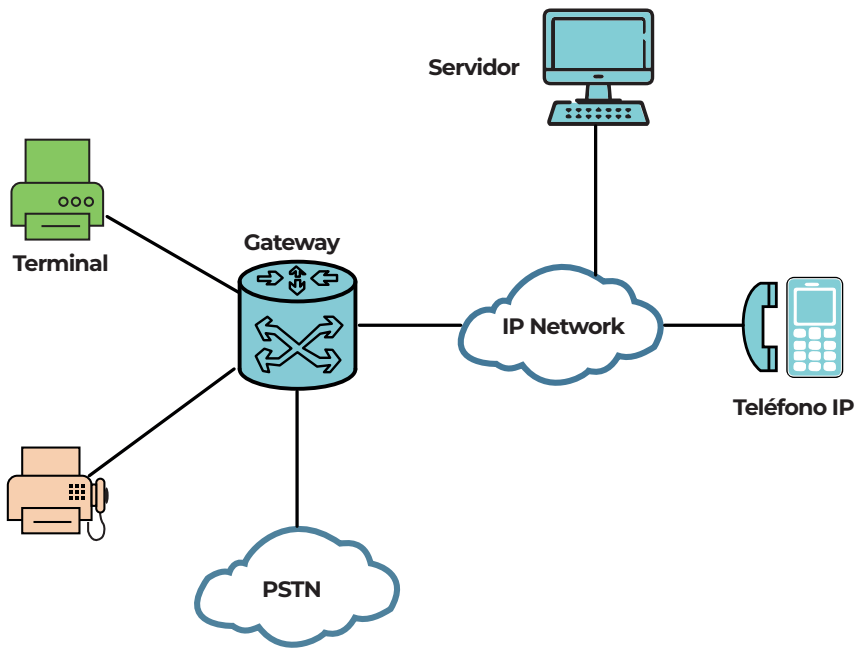
Entre los elementos de un sistema VoIP se destacan:

1. Equipos terminales: teléfonos IP encargados de ofrecer el servicio al usuario. Incluye elementos que pueden ser *hardware* conectado directamente a una red IP o *software* mediante aplicaciones que simulan un teléfono con soporte VoIP.

2. Servidor de VoIP: provee los servicios y funciones para soportar el enrutamiento de llamadas en la red. El servidor recibe distintos nombres según el protocolo de señalización utilizado: en un sistema H.323 recibe el nombre de *gatekeeper* y en un sistema SIP se conoce como servidor SIP.

3. *Gateway:* es el equipo que hace la traducción de la telefonía fija tradicional a la red VoIP. Está constituido por elementos de *hardware* o *software*, y actúa de forma transparente al usuario. En la figura 2.2. se detalla un *router* (enrutador) haciendo las veces de *gateway*.

Figura 2.2. Arquitectura de un sistema VoIP



Fuente: elaboración propia a partir de Duarte Domingo (2014).

4. Red IP o de ordenadores: provee conectividad LAN entre todos los terminales, incluso a nivel WAN. Esta red puede ser privada o pública.

5. Centrales de conmutación para VoIP: estos elementos son opcionales y su función es optimizar el tráfico de telefonía IP.

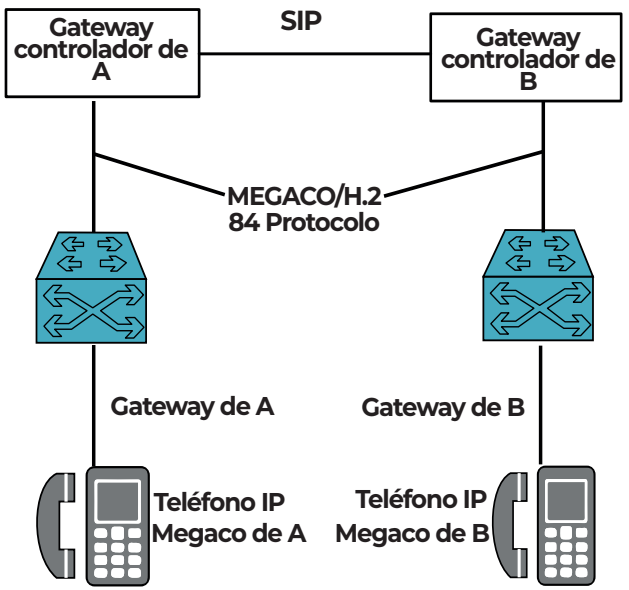
2.2. Tipos de arquitectura de VoIP

Un sistema VoIP puede construirse utilizando una arquitectura centralizada o distribuida. De esta forma se pueden construir redes de administración simple con diversos tipos de terminales que dependen del protocolo empleado.

2.2.1. Arquitectura de VoIP centralizada

Inicialmente las redes de voz tenían una arquitectura centralizada con teléfonos controlados por conmutadores centralizados, tal como se detalla en la figura 2.3. Esta arquitectura utiliza los protocolos MGCP y MEGACO, diseñados para un dispositivo central llamado Call Agent o Controlador Media Gateway que maneja el control de llamadas y la lógica de conmutación; la inteligencia, el provisionamiento, el control y la administración de la red es centralizada. En esta configuración los dispositivos finales (*endpoints*) tienen características limitadas, porque se suprimen innovaciones de los teléfonos cuando se construyen servicios fuera de las características de la voz.

Figura 2.3. Arquitectura centralizada en VoIP



Fuente: elaboración propia (2023).

2.2.2. Arquitectura de VoIP distribuida

En esta solución se utilizan los protocolos H.323 y SIP, los cuales permiten que la inteligencia de la red se distribuya entre dispositivos de control de llamadas y puntos terminales. La

inteligencia se basa en establecer las llamadas, brindar características, enrutamiento, provisionamiento, tarificación, entre otros aspectos de la comunicación. Los puntos terminales pueden ser *gateways*, teléfonos IP o dispositivos que inician y finalizan una llamada VoIP. Los dispositivos para el control de llamadas son los *gatekeepers* con H.323 y los servidores Proxy (o *redirect*) con SIP.

Esta arquitectura es flexible por permitir que las aplicaciones VoIP sean tratadas como cualquier aplicación IP distribuida; además, agrega inteligencia al dispositivo de control de llamadas de acuerdo con las necesidades tecnológicas y comerciales del sistema de VoIP.

2.3. Códecs utilizados en la comunicación de VoIP

El códec es un estándar para convertir el sonido a señal digital y viceversa. Existen ocho códecs muy utilizados, con una tasa de bits diferente derivada del tamaño de muestreo del códec / intervalo muestreo de códec; el muestreo es el número de bytes capturados por el *DSP* (Procesador Digital de Señal) en cada intervalo de muestreo (Valverde Balbuena, 2018). En la tabla 2.2. se detallan algunos códecs de audio y sus características

2.4. Protocolos utilizados en VoIP

2.4.1. SIP

Session Initiation Protocol (SIP) es un protocolo de señalización que tiene las funciones de crear, modificar y terminar sesiones a través de redes IP; permite localizar los usuarios e intercambiar información de los medios implicados en la sesión. Independiente del tipo de sesión a establecer, se utiliza para realizar conversaciones de voz, videoconferencias y aplicaciones compartidas, entre otras. Es independiente de los protocolos UDP, TCP, TLS/TCP y del protocolo SDP (Session Description Protocol), el cual negocia los parámetros de la sesión (Johnston, 2016).

2.4.2. Principales características

Las sesiones de SIP incluyen conferencias multimedia de Internet o de cualquier red IP, llamadas telefónicas y la difusión multimedia. Los integrantes de una sesión se comunican a través de *multicast*, unidifusión o combinados. El protocolo SIP soporta descripciones de la sesión, lo que permite a los participantes llegar a un acuerdo sobre un conjunto compatible de tipos de medios. De igual forma es compatible con movilidad del usuario, representando y redirigiendo las peticiones a la localización de este. No está ligado a ningún protocolo de control de conferencia y opera a nivel de capa de aplicación del modelo OSI (figura 2.4.).

Tabla 2.2. Códecs

Nombre	Estándar	Tasa de bits (kb/s)	Muestreo (kHz)	Tamaño Trama (ms)	Puntuación
G.711	UIT-T	64	8	Muestreada	4.1
G.721	UIT-T	32	8	Muestreada	
G.722	UIT-T	64	16	Muestreada	
G.722.1	UIT-T	24/32	16	20	
G.723.1	UIT-T	5.6/6.3	8	30	3.8 - 3.9
G.726	UIT-T	16/24/32/40	8	Muestreada	3.85
G.727	UIT-T	Variable		Muestreada	
G.728	UIT-T	16	8	2.5	3.61
G.729	UIT-T	8	8	10	3.92
GSM	ETSI	13	8	22.5	3.5 - 3.7
LPC10	Gob.USA	2.4	8	22.5	
iLBC		8	13.3	30	4.1

Fuente: elaboración propia a partir de Sierra Rodríguez (2011).

SIP garantiza la comunicación a su destino y la realización de cualquier asignación de información descriptiva de la información de ubicación. Con esto, el grupo involucrado en la llamada se pone de acuerdo sobre las funciones admitidas, reconociendo que no todas las partes involucradas pueden soportar el mismo nivel de características. Al gestionar una llamada, el participante puede invitar a unos usuarios a participar en la misma o cancelar las conexiones a otros; adicionalmente, puede transferir o poner en espera a los demás usuarios.

El usuario puede cambiar las características de la llamada durante su curso. Una llamada es creada con la característica de voz, pero en el transcurso se puede habilitar una función de video; asimismo, otro usuario puede unirse a una llamada y necesitar diferentes características para ser habilitado y participar en la conversación.

Algunas direcciones de usuarios SIP se asocian al correo electrónico: el usuario es identificado con una dirección URL jerárquica, cons-

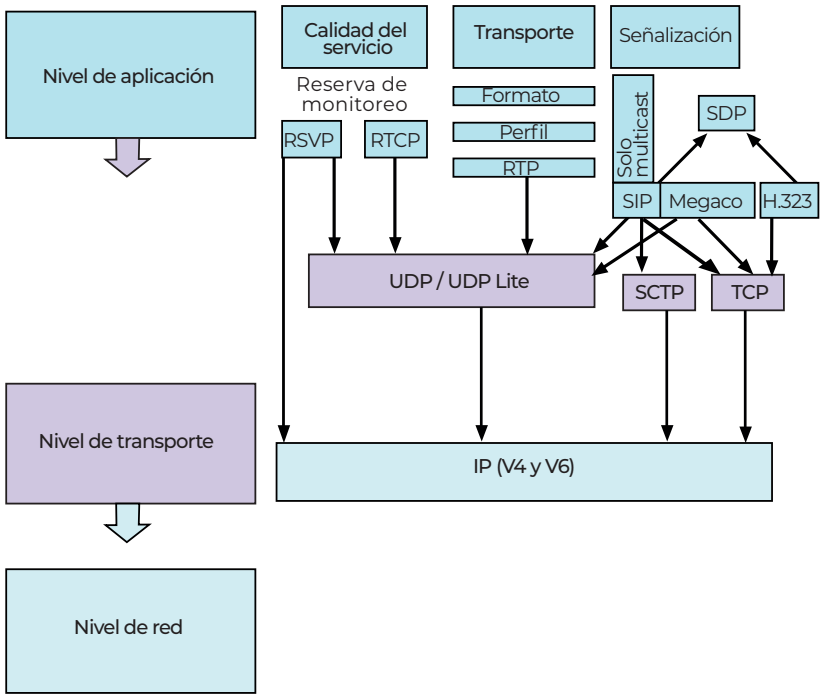
truida alrededor de elementos como el número de teléfono o el nombre del *host* (sip:usuario@compañia.com). Es un proceso sencillo para redirigir a un usuario a otro teléfono, funciona como una redirección a una página web.

2.4.3. Solicitudes en SIP

Se tiene una línea de solicitudes para establecer la comunicación (figura 2.5.). El protocolo SIP utiliza mensajes para la conexión y control de llamadas, definiendo seis procesos:

- REGISTER: deja un registro de la ubicación del usuario actual, dirección IP y el puerto por el cual ha realizado el registro de mensajes.
- INVITE: indica que un usuario está siendo invitado a participar en la llamada.
- ACK: mensaje que confirma la recepción del proceso INVITE.
- BYE: es utilizado para finalizar las sesiones multimedia.

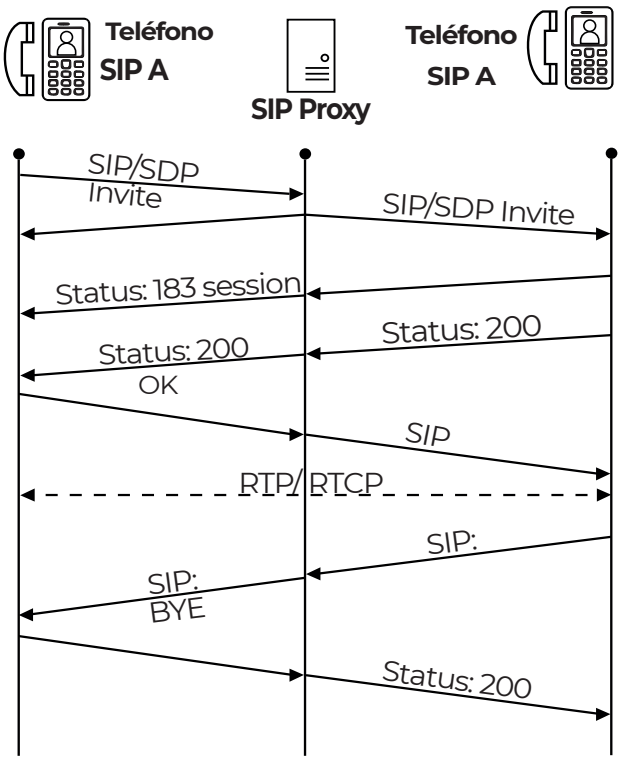
Figura 2.4. Ubicación de SIP en protocolos sobre IP



Fuente: elaboración propia (2023).

- CANCEL: cancela una sesión no establecida en su totalidad, cuando el destinatario no confirma.
- OPTIONS: revisa la información de las capacidades de envío y recepción de los teléfonos SIP.

Figura 2.5. Solicitudes SIP



Fuente: elaboración propia a partir de Znaty et al. (2005).

2.4.4. Respuestas en SIP

El agente de usuario o el servidor Proxy reciben una solicitud, entonces proceden a envíar una respuesta. Toda solicitud es respondida, excepto las ACK. Las respuestas se identifican con un código de tres dígitos y dependiendo del primer dígito tienen un significado distinto. Pueden ser respuestas provisionales (1xx) y finales (2xx-6xx). La transacción está formada por ninguna o por varias respuestas provisionales y una sola respuesta final; el código respuesta es un número entero de 100 a 699 que indica el tipo de respuesta. Se identifican seis clases de respuesta:

1xx: provisional, no finaliza una transacción.

2xx: de éxito.

3xx: de redirección a otra dirección.

4xx: de error del cliente que hace la petición.

5xx: de error del servidor que atiende la petición.

6xx: de errores globales a toda la red.

2.4.5. Problemas en SIP 1-NAT

El protocolo SIP fue creado sin tener en cuenta el mecanismo NAT (Network Adress Translation), donde los equipos tienen una IP pública. Con NAT se presentan dos dificultades:

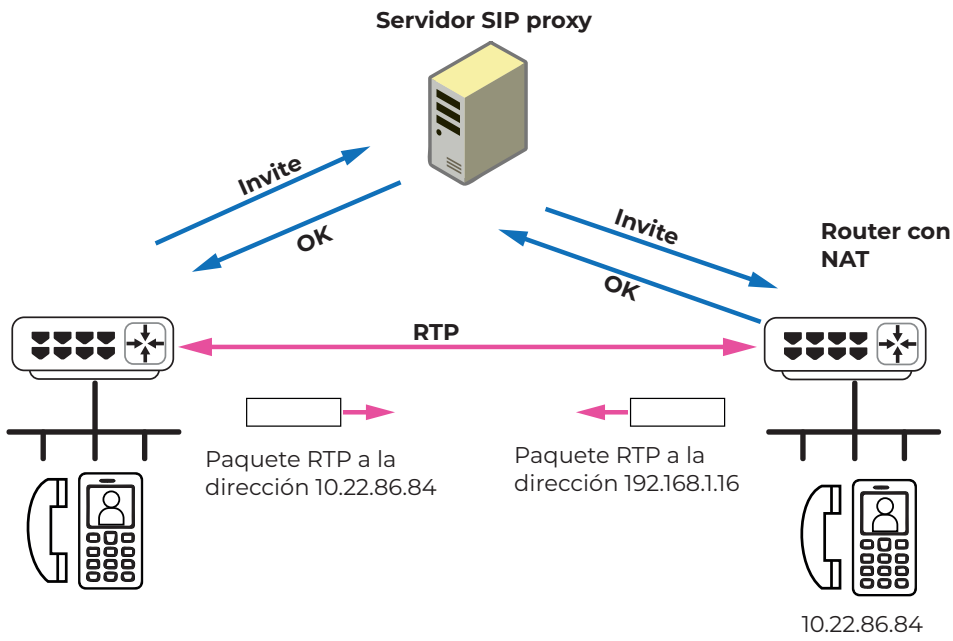
- Dos teléfonos IP no se pueden enviar paquetes de voz a través de la WAN con IP privadas. El RTP debe ir dirigido hacia IP públicas del lado WAN de los *routers* (enrutadores).

- Un paquete RTP no pasa a través de NAT y no llega al teléfono de destino si no tiene en el NAT una asociación IP privada-puerto/IP pública-puerto. Debe haber una conexión saliente a través de NAT. Esta dificultad se ilustra en la figura 2.6.

2.4.6. Dos problemas de SIP debidos a NAT

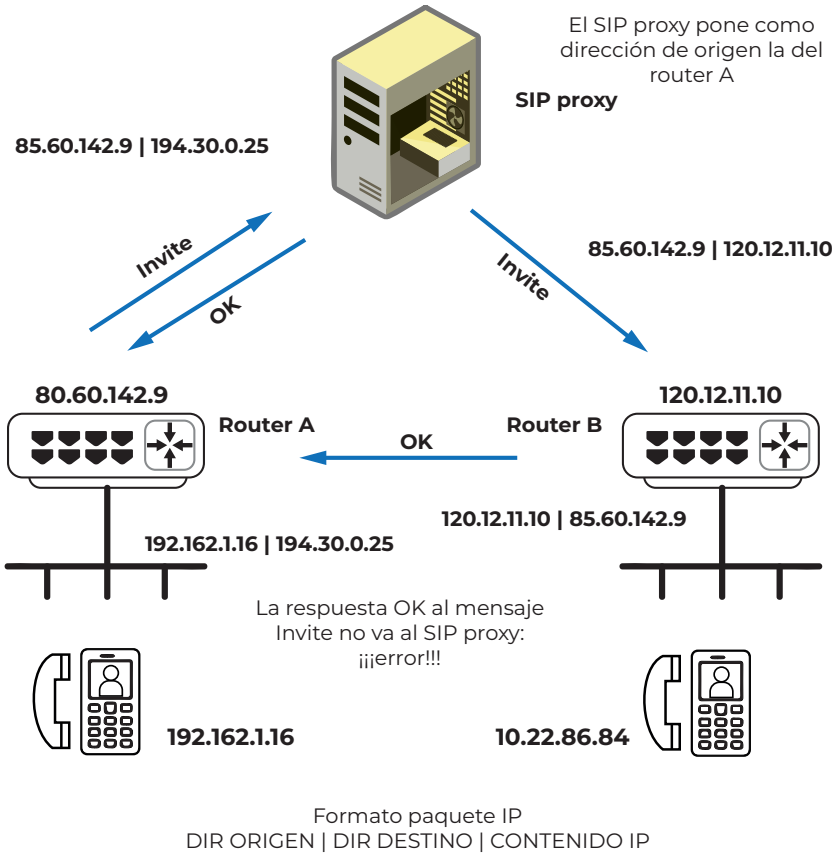
El primer problema podría solucionarse si durante la fase de señalización el SIP Proxy informa a cada teléfono la IP pública y puerto para enviar los paquetes RTP de voz. Esto exige modificar el contenido de los paquetes SIP y no es posible hacerlo mediante modificación de direcciones IP en la cabecera de los paquetes por parte del SIP Proxy, tal como se ilustra en la figura 2.7.

Figura 2.6. Conexión a través de NAT



Fuente: elaboración propia a partir de Znaty et al. (2005).

Figura 2.7. Proxy SIP



Fuente: elaboración propia a partir de Znaty et al. (2005).

El SIP Proxy hace retransmisión de mensajes SIP entre los extremos, pero no los modifica: en la figura 2.7. el SIP Proxy intenta informar al teléfono B la IP pública del teléfono A colocando el valor en DIR IP ORIGEN del paquete enviado, entonces la señalización SIP falla porque el mensaje de respuesta OK al mensaje INVITE no llega a quien envió el paquete. La IP pública y puerto al cual se dirigen los paquetes RTP de voz deben colocarse en el interior de los mensajes SIP de INVITE de los teléfonos que intervienen en la conversación. Para hacer esto se requiere que los teléfonos conozcan los valores de la IP pública y puerto con los que

salen a la WAN, lo cual se logra utilizando los Servidores STUN (Session Traversal Utilities for NAT) como se ilustra en la figura 2.8.

Los teléfonos participantes en la comunicación deben acceder a un servidor STUN para identificar su IP y puerto con los que sale a la WAN. Los servidores STUN se encuentran en direcciones IP públicas. Por medio del servidor STUN, el *softphone* encuentra la IP pública para enlazarse al exterior y utiliza ese valor para informar al teléfono SIP del otro extremo la dirección y puerto al cual debe enviar los paquetes RTP. Aunque el protocolo STUN es simple y efectivo, debe haber una asociación creada en el NAT para que entren paquetes de voz RTP desde la WAN hacia un teléfono situado en la LAN. De acuerdo con el NAT utilizado, se tienen dos soluciones posibles:

- NAT tipo Full Cone. El paquete RTP de voz con destino a la IP pública-puerto utilizado para la comunicación con el SIP Proxy o con el servidor STUN será enviado por NAT al teléfono correspondiente. Aunque los paquetes RTP de voz provengan de una IP diferente, NAT *Full Cone* no examina dirección IP de origen de los paquetes ni puerto (figura 2.9.).

- NAT tipo Restricted Cone, Port Restricted Cone o Symmetric. Es necesario que los paquetes de voz RTP tengan como dirección de origen la propia del SIP Proxy o la del servidor STUN; este tipo de NAT solo deja pasar paquetes hacia el lado LAN si provienen de la IP pública del lado WAN con la que se ha establecido la conexión de salida. Los paquetes de voz atraviesan el SIP Proxy o el servidor STUN. En la figura 2.10 se observa un ejemplo de esta solución.

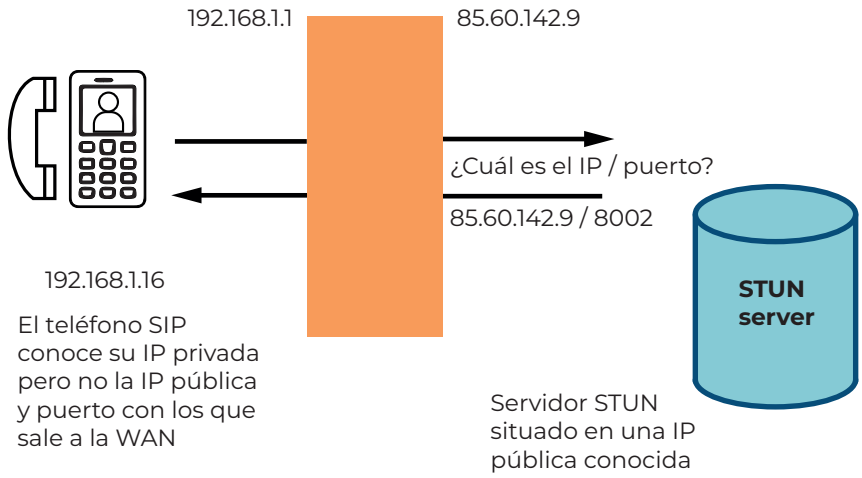
2.4.7. Firewalls o cortafuegos

Los *firewalls* o cortafuegos (sistema de seguridad de red de los computadores) casi siempre impiden a los equipos SIP la recepción de tráfico RTP entrante o saliente o la señalización SIP. La solución para que VoIP funcione es identificar qué puertos TCP/UDP deben ser abiertos o permitidos. Para la señalización SIP se utilizan puertos conocidos como 5060 UDP. Para los paquetes de voz el problema dependerá de la PBX IP utilizada para la comunicación. Se debe evitar abrir todos los puertos TCP y UDP.

2.4.8.Encriptación en las comunicaciones

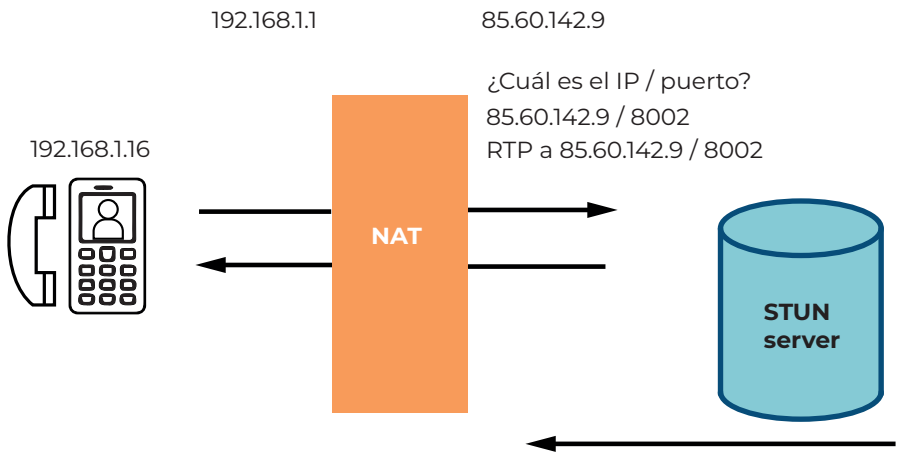
En la comunicación SIP es necesario proteger la fase de señalización y la fase de transporte A con el protocolo RTP. Lo primero se garantiza con el protocolo TLS (Transient Layer Security), utilizado en las comunicaciones mediante

Figura 2.8. Funcionamiento del servidor STUN



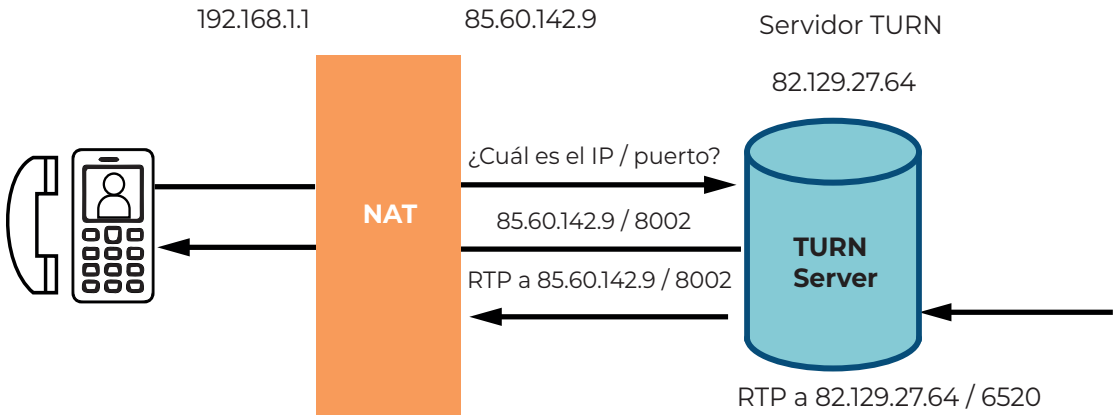
Fuente: elaboración propia a partir de Znaty et al. (2005).

Figura 2.9. NAT de tipo *Full Cone*



Fuente: elaboración propia a partir de Znaty et al. (2005).

Figura 2.10. Los otros tres tipos de NAT



Fuente: elaboración propia a partir de Znaty et al. (2005).

caciones SIP porque el protocolo es complejo y algunas veces no hay compatibilidad entre diferentes fabricantes de equipos SIP.

2.5. El H.323

Este estándar precisa las exigencias para sistemas de comunicaciones multimedia en escenarios donde el transporte de la información se realiza en una red basada en paquetes (Packet Based Network-PBN) que no puede garantizar la Calidad de Servicio (QoS); los terminales H.323 pueden proporcionar servicios de audio y video (opcionalmente) en tiempo real y servicio de comunicación de datos. En H.323 los paquetes de voz son encapsulados con RTP y transportados en UDP. Para gestionar la calidad de la comunicación de voz en la red se utiliza el protocolo RTCP (Real-Time Control Protocol).

2.5.1. Protocolos de transporte en tiempo real (RTP y RTCP)

El RTP es un protocolo de transporte cuyo objetivo es proporcionar un servicio de entrega extremo para transmitir datos como el audio y el video en tiempo real. El RTCP (Real Transporte Control Protocol) se basa en la transmisión periódica de paquetes de control para los participantes de una sesión, utilizando los mismos mecanismos de distribución de los paquetes de datos; este paquete contiene información im-

portante para la monitorización de la entrega de los paquetes de audio, como *jitter* entre llegada de paquetes, número de paquetes perdidos, número total de paquetes y octetos transmitidos, y otros datos útiles para el diagnóstico, seguimiento y corrección de algunos tipos de condiciones de error en la red.

2.5.2. La calidad de servicio (QoS) en H.323

La calidad del servicio puede definirse como la capacidad de la red para garantizar y mantener ciertos niveles de rendimiento para cada aplicación de acuerdo con las necesidades específicas de cada usuario. Aunque el concepto de *calidad* (QoS) usualmente se refiere a la fidelidad de la señal de voz recibida, también se aplica a otros aspectos como disponibilidad de la red, probabilidad de bloqueo, existencia de servicios especiales (conferencias, identificación del usuario que llama, etc.), escalabilidad y penetración.

2.5.3. La calidad de la señal de voz en H.323

Esta calidad de voz en la red telefónica es fundamentalmente subjetiva, aunque las medidas estándar hayan sido desarrolladas por la Unión Internacional de Telecomunicaciones (UIT). Para la transmisión de voz sobre redes de paquetes hay cuatro factores principales que influyen en la calidad del servicio (mencionados anteriormente): ancho de banda, retardo (de extremo a extremo) del paquete, retraso *jitter* y pérdida de los paquetes.

2.5.4. Ancho de banda en H.323

El ancho de banda mínimo necesario para la transmisión de la señal de voz es una función de la técnica de codificación utilizada. El ancho de banda disponible en la red y el mecanismo de compartimiento de este ancho de banda entre varias aplicaciones tienen influencia directa en el retraso por el paquete y consecuentemente en la calidad del servicio resultante.

2.5.5. Retraso de paquetes en H.323

El retraso del paquete se define formalmente como la diferencia de tiempo en segundos entre el instante en que el terminal que llama envía el primer bit del paquete y el instante en que el terminal llamado recibe este bit. Su comportamiento es aleatorio dependiendo de la carga en la red.

2.5.6. Pérdida de paquetes en H.323

Las redes IP no garantizan la entrega de los paquetes y debido a los fuertes requisitos de retardo impuestos por las aplicaciones interactivas

en tiempo real, no se pueden utilizar protocolos de transporte fiables como TCP. La pérdida de paquetes es inevitable y puede influir significativamente en la QoS de VoIP.

2.5.7. Mejorar la QoS de VoIP

Para alcanzar una QoS adecuada para el tráfico de VoIP se puede adoptar una serie de medidas: garantizar el ancho de banda requerido para la transmisión de paquetes de voz (protocolo de reserva de recursos); minimizar los retrasos sufridos por los paquetes en la red y que sean lo más constantes posible (utilización de mecanismos de priorización de paquetes de voz, utilizar técnicas de enrutamiento que favorezcan las rutas con menos retardo, utilizar los mecanismos más eficientes para el enrutamiento de paquetes en los *routers* o enrutadores); y eliminar o minimizar la fluctuación (*jitter*) de retardo sufrido por los paquetes (usar *dejitter* búfer).

2.5.8. Clasificación o identificación del tráfico en H.323

La clasificación del tráfico se puede hacer paquete a paquete (analizando las características del tráfico de cada uno), o sesión a sesión (cuando el transmisor negocia un cifrado de extremo a extremo, previo a la transmisión). La política de clasificación de paquetes es fijada por el operador de red y puede basarse en varios criterios, como tipo de tráfico contenido en el paquete, la dirección de la puerta física, dirección MAC, dirección IP de la fuente o destino, puerta de aplicación, etc.

2.5.9. La disciplina de despacho en H.323

El almacenamiento temporal de paquetes y la disciplina de despacho definen cómo servirá el nodo de red los paquetes almacenados en las colas. Cuando la red transporta simultáneamente tráfico de voz y datos, deben asociarse niveles de prioridad diferentes para ambos tipos de tráfico, con la disciplina de despacho priorizando el tráfico de voz para minimizar el retraso que estos paquetes sufren en cada nodo de la red.

2.5.10. Técnicas de control de congestión de tráfico en H.323

Las técnicas de control de congestión supervisan el tráfico en la red para anticipar y prevenir la ocurrencia de congestión, generalmente mediante el descarte de paquetes. Las dos técnicas principales que operan con este objetivo son la Random Early Detection (RED) y su versión con ponderación la Weight Random Early Detention (WRED).

- Random Early Detection (RED): cuando sucede un *timeout* en el transmisor TCP, el protocolo reduce el tamaño de la ventana

de transmisión y empieza el proceso de inicio lento (*slow start*), donde el tamaño de la ventana se aumenta gradualmente a medida que el transmisor recibe acuses de recibo positivos desde el receptor.

- Weigth Random Early Detention (WRED): en el algoritmo WRED la probabilidad de desechar un paquete entrante se define por la tasa de ocupación de la cola y una pesa asociada al flujo (o clase de flujo) a la que pertenece el paquete. Con el WRED se busca que los paquetes de mayor prioridad tengan menos probabilidades de descartarse. Un gran flujo de tráfico de voz puede causar desbordamiento en una cola WRED y, como consecuencia, una tasa alta de pérdida de paquetes.

2.5.11. Las arquitecturas para la QoS en H.323

El modelo de servicios integrados propone dos clases de servicios, más allá del servicio habitual de mejor esfuerzo:

- Servicio garantizado: para aplicaciones en tiempo real como VoIP, que requieren un ancho de banda límite garantizado para evitar el retraso.

- Servicio de carga controlada: en aplicaciones que requieren servicio «mejor que mejor esfuerzo», pero sin garantía de ancho de banda o límite de demora.

2.5.12. Otros requisitos para la VoIP en H.323

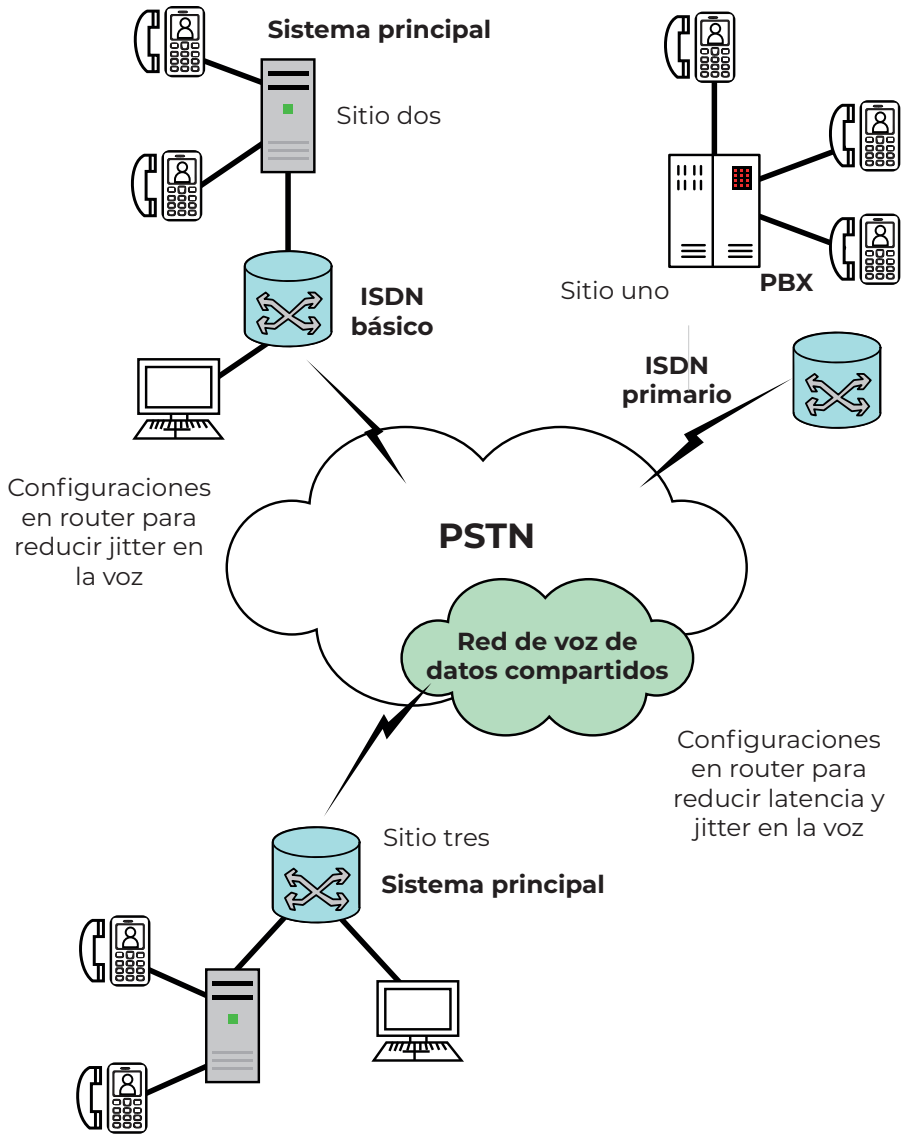
El uso de la Voz IP constituye una buena alternativa para la implementación de redes multimedia corporativas o incluso de *backbones* con capacidad para la integración de tráfico de las empresas proveedoras de servicios de telecomunicaciones. La figura 2.11. detalla un ejemplo de una solución con H.323.

2.6. H.323 vs. SIP

Se realizan comparaciones entre ambas soluciones, identificando diferencias, similitudes y ventajas (Comparison of VOIP Signaling Protocol H.323 vs. SIP).

1. Teleconferencia o videoconferencia. El H.323 ha sido referente durante mucho tiempo. No obstante, con SIP hay mejoras ante la existencia de una serie de factores que limitan a H.323 como un protocolo para las grandes masas. H.323 se extendería hacia SS7, con total compatibilidad con los estándares anteriores, bien para conmutación de circuitos o de paquetes. Además, pretendía llevar la telefonía convencional hacia redes IP. La integración de H.323 con Internet se obstaculiza por

Figura 2.11. VoIP en H.323



Fuente: elaboración propia a partir de Sosa (2016).

características propias de esta tecnología, como no usar ninguno de los estándares aprobados por el IETF para Internet: no proporciona servicios complementarios ni aprovecha el trabajo hecho.

2. Seguridad. En H.323 se definen mecanismos de seguridad y facilidades de negociación con H.235, puede utilizar SSL en la capa de transporte. SIP soporta mecanismos de autenticación vía HTTP.

3. Arquitectura. En H.323 hay capacidad de intercambio, control de conferencia, señalización básica, QoS, registro, etc. Por su parte, SIP cubre servicios de señalización de llamadas, localización y registro de usuarios. Los componentes en una red H.323 incluyen *gateways*, terminales, puentes de comunicación junto a un *gatekeeper*; la arquitectura para este protocolo es *peer-to-peer,* soportando comunicación de usuario-por-usuario. SIP incluye los *user agents,* análogos a los terminales de H.323 que operan como cliente o servidor. La solución SIP requiere un Servidor Proxy para enrutar las llamadas a otras entidades y un servidor de registro, no se requieren más componentes para hacer una llamada.

4. Videoconferencia. El H.323 soporta la conferencia de datos y la de video, hay lugar para el control de la conferencia y la sincronización de los *streams* de audio y video. El SIP no soporta el protocolo T.120 para la conferencia de datos, no tiene mecanismos de sincronización ni de control para la conferencia.

5. Codificación de mensajes. Para H.323 los mensajes son codificados en formato binario compacto, apropiado para conexiones de banda ancha y banda angosta; esta codificación reduce el tamaño de la transmisión y conserva el ancho de banda. El SIP solo entiende mensajes de forma URL y los mensajes son codificados en texto en lugar de lenguaje binario, lo cual facilita su entendimiento pero aumenta el tamaño del mensaje a enviar.

6. Estabilidad. En H.323 no hay direccionamiento, se utiliza «zona H.323», con problemas de escalabilidad y direccionamiento entre zonas; hay dificultades en los componentes de red y en el soporte de múltiples conversaciones en zonas H.323 grandes, porque el *gatekeeper* tiene que conocer el estado de cada llamada. En SIP cuando la carga de llamadas en la red se eleva, usa los servidores de redirección, sin estado; SIP funciona sobre UDP (User Datagram Protocol).

7. Funcionabilidad. Ambos manejan la configuración de llamadas y el control de llamadas y de medios de diversas maneras.

En H.323 está la definición de cada uno de ellos. En SIP se define por separado la configuración de llamadas y el uso de protocolos para controlarlas. Hay capacidad de intercambio. En la llamada de H.323 los terminales anuncian la capacidad que tienen para compresión y video, porque las variables pueden cambiar la configuración durante la llamada. En SIP estos parámetros solo pueden cambiarse al iniciar una nueva llamada.

2.7. IAX

Inter-Asterisk eXchange protocol (IAX), desarrollado por Digium, es un servidor de código abierto, una central telefónica para comunicar servidores VoIP; soporta muchos códecs y gran número de canales (*streams*), por lo cual se puede utilizar para transportar señalización y cualquier tipo de datos entre puntos finales mediante el puerto UDP 4569. Este protocolo es binario, diseñado y organizado para reducir la carga en flujos de datos de voz.

IAX permite el envío de señalización y datos por varios canales. Los datos de varias llamadas se encapsulan en un conjunto de paquetes y se añaden a un datagrama IP, reduciendo el retardo y el *overhead* asociado a los canales individuales, lo cual ayuda a mejorar la utilización del ancho de banda y a reducir los tiempos de procesamiento. El protocolo IAX proporciona control y transmisión de flujos multimedia sobre IP, como videoconferencias y presentaciones remotas, es transparente a los cortafuegos y es eficaz para trabajar en redes internas.

IAX establece sesiones internas que utilizan cualquier códec para transmitir voz o video, y se basa en los estándares SIP, MGCP y RTP; fue diseñado para transmitir voz, pero puede transportar cualquier *MediaStream*, incluyendo video. Actualmente IAX es un protocolo abierto.

2.7.1. Descripción del protocolo IAX

IAX es un protocolo par a par orientado a VoIP que incluye funciones de control y de media, diseñado para describir y transportar llamadas multimedia mediante IP. Su diseño permite la multiplexación de señales y llamadas multimedia sobre un mismo puerto UDP asociado entre dos pares. La señalización unificada de IAX y la trayectoria de medias logran transparencia sobre NAT, lo cual es una ventaja de IAX sobre otros protocolos similares. IAX es un protocolo binario cuyos principales beneficios son la eficiencia en la asignación del ancho de banda, robustez contra ataques y facilidad de implementación. La unidad elemental de comunicación entre pares IAX es una trama (*frame*).

2.7.2. Arquitectura del IAX

Es diseñado para conexiones VoIP entre servidores Asterisk, pero también sirve para cone-

xiones entre clientes y servidores que soporten el protocolo. Sus objetivos son: minimizar el ancho de banda, evitar problema con NAT y transmitir planes de marcación.

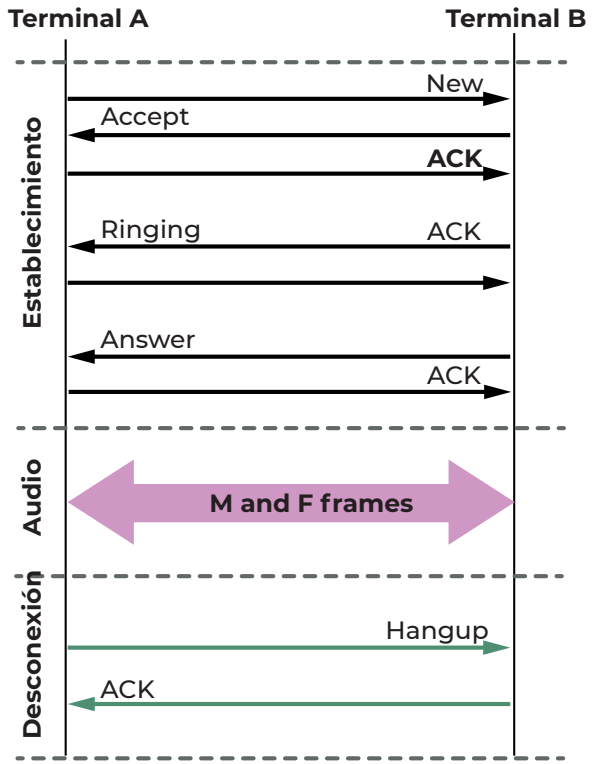
IAX o IAX2 es un protocolo binario y esto hace que los mensajes usen menos ancho de banda. Para resolver los problemas con NAT usa UDP como protocolo de transporte sobre el puerto 4569, y tanto la información de señalización como los datos viajan conjuntamente (a diferencia de SIP); debido a esto es menos proclive a problemas de NAT para pasar los *routers* (enrutadores) y *firewalls* (cortafuegos) más fácilmente.

2.7.3. Funcionamiento del IAX

En la figura 2.12. se detalla el flujo de datos de una comunicación IAX2. Esta comunicación IAX o IAX2 tiene tres fases:

- Realización de una llamada: un terminal A inicia una conexión y manda el mensaje «New». El terminal al que se llama responde con un «Accept» y A le responde con un «ACK». Seguidamente, el terminal al que se llama da las señales de «ringing» y quien hace la llamada contesta con un «ACK» para confirmar la recepción del mensaje. Finalmente, el receptor acepta la llamada con un «Answer» y quien llama lo confirma.

Figura 2.12. Llamada IAX o IAX2



Fuente: elaboración propia a partir de Joskowicz (2013).

- Flujo de datos o de audio: los *frames* M y F se envían en ambos sentidos con la información de voz. Los M son *miniframes* que contienen una cabecera de cuatro *bytes* que reduce el uso del ancho de banda. Los F son *frames* completos que incluyen información de sincronización. En IAX este flujo utiliza el mismo protocolo UDP que

utilizan los mensajes de señalización, con lo cual evita los problemas de NAT.

- Liberación de la llamada o desconexión: la conexión se libera con el envío de un mensaje de «Hangup» y confirmando dicho mensaje.

2.7.4. La seguridad en AIX

El protocolo soporta tres procesos de autentificación: (1) texto plano (*plaintext*), (2) *hash* MD5 (Message- Digest algorithm 5) y (3) contraseña RSA de intercambio. Estos procesos no consideran el cifrado de medias (*media path*) ni de las cabeceras entre puntos finales, ya que para ello existen soluciones como el uso de una VPN o de *software* para encriptar el canal con túneles configurados y funcionales.

Como formas de negación de servicio (DoS, Denial of Service), existen dos alternativas:

- Sobrecargando a los pares con peticiones falsas: se evita identificando sobrecargas y emitiendo una alarma o una acción de protección.

- Ataque ingenioso: se realiza mediante la inyección de medias con el fin de ocasionar un exceso de procesamiento al insertar paquetes fuera de orden y enviando órdenes como «Hangup» o «Transfer». Esto requiere desactivar la supervisión del canal binario, ya que el número de secuencia de los mensajes necesita sincronizarse con el intercambio del protocolo.

Es motivo de investigación que IAX pueda cifrar los canales entre los puntos finales mediante el intercambio de llaves RSA o de una llave dinámica en el establecimiento de la llamada, cuya aplicación representa una solución para acoplamiento. El protocolo IAX2 fue diseñado para trabajar con NAT. Utilizar un puerto normal UDP para señalización y transmisión de comunicación mantiene los requisitos de los cortafuegos, lo que facilita la implementación de IAX en redes seguras.

2.8. IAX vs. SIP

Con IAX se solventan diferentes problemas o inconvenientes que tiene SIP con VoIP. Sus principales diferencias son:

- Ancho de banda. EL protocolo IAX utiliza menor ancho de banda y los mensajes son codificados de forma binaria, mientras en SIP son mensajes de texto. De igual forma, IAX reduce la información de las cabeceras de los mensajes bajando el consumo de ancho de banda.

- NAT. En IAX la señalización y los datos viajan juntos, con lo cual se evitan las dificultades de NAT que aparecen en SIP. En SIP la señalización y los datos viajan de

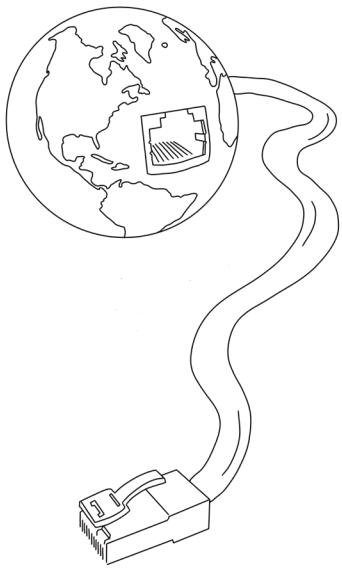
forma separada, por lo que aparecen problemas de NAT para el flujo de audio entre los *routers* (enrutadores) y los *firewalls* (cortafuegos). SIP soluciona este problema con un servidor STUN.

- La estandarización. El protocolo SIP está estandarizado por la IETF y es ampliamente implementado por todos los fabricantes de equipos y *software*. El protocolo IAX está en proceso de estandarización y no se encuentra frecuentemente en los dispositivos del mercado.

- La utilización de puertos. EL protocolo IAX usa el puerto 4569 para enviar la información de señalización y los datos de las llamadas, utilizando un mecanismo de multiplexión. En SIP se utiliza un puerto 5060 para señalización y dos puertos RTP por cada conexión de audio (en total tres puertos).

- El flujo de audio con un servidor. En el protocolo SIP la señalización de control pasa por el servidor y la información de audio (RTP) viaja de extremo a extremo sin pasar por el servidor SIP. En IAX la señalización y los datos viajan de forma conjunta y todo el tráfico de audio pasa por el servidor IAX, con lo cual aumenta la utilización del ancho de banda que soportan los servidores IAX cuando hay mucho flujo simultáneo de llamadas.

- Otras diferencias. El protocolo IAX es desarrollado para VoIP y transmisión de video, y presenta funcionalidades como la posibilidad de enviar o recibir planes de marcado (*dialplans*) al usarlo juntamente con servidores Asterisk. Por su parte, SIP es de propósito general y puede transmitir cualquier información diferente al audio o al video.



Conclusiones

La comprensión y aplicación de la telefonía IP ha transformado las comunicaciones tradicionales al utilizar Internet como medio de transmisión para las llamadas de voz, ofreciendo una mayor flexibilidad y reducción de costos. Al reemplazar las líneas telefónicas convencionales con conexiones de datos, VoIP permite integrar múltiples servicios de comunicación como voz, video y datos en una sola red. Esta convergencia no solo optimiza los recursos de comunicación, sino que también facilita la implementación de soluciones de comunicación más avanzadas y adaptables a las necesidades actuales.

Tanto los códecs como los protocolos desempeñan un papel crucial en la comunicación VoIP ya que son responsables de la compresión y descompresión de las señales de voz, lo que permite su transmisión eficiente a través de redes de datos. Protocolos como SIP, H.323 e IAX son esenciales para el establecimiento, control y finalización de las llamadas VoIP. Cada protocolo tiene sus propias ventajas y aplicaciones específicas, destacándose SIP por su simplicidad y flexibilidad, H.323 por su robustez en redes de gran escala e IAX por su eficiencia en el manejo de múltiples llamadas en una única conexión. La comprensión y correcta implementación de estos códecs y protocolos son fundamentales para garantizar una comunicación clara y confiable en sistemas VoIP.

Las arquitecturas de sistemas VoIP y su impacto en la eficiencia de la red pueden variar desde soluciones *peer-to-peer* simples hasta configuraciones de servidor-cliente más complejas. La elección de la arquitectura adecuada depende de factores como el tamaño de la red, los requisitos de Calidad del Servicio (QoS) y la escalabilidad. Una arquitectura bien diseñada puede mejorar significativamente la eficiencia de la red y la calidad de las llamadas, al tiempo que facilita la gestión y el mantenimiento del sistema. Además, las arquitecturas avanzadas permiten la integración de funcionalidades adicionales como la grabación de llamadas y conferencias, que pueden ser vitales para aplicaciones empresariales y servicios de atención al cliente.

CAPÍTULO 3.

Telefonía sobre redes IP

Introducción

Este capítulo se adentra en aspectos fundamentales para la implementación y optimización de la v en redes IP. En este apartado se abordan temas fundamentales como el ancho de banda requerido para VoIP, aspectos que determinan la calidad y la capacidad de las llamadas de voz, y se examinan las técnicas de optimización del tráfico de VoIP para mejorar la eficiencia y Calidad del Servicio (QoS). También abarca el enrutamiento con QoS, incluyendo los protocolos WSP (*Weighted Scheduling Protocol*) y SWP (*Shortest Weighted Path*), que son esenciales para priorizar el tráfico de voz en la red. La seguridad es otro punto crucial tanto en redes IP generales como en plataformas abiertas de VoIP, y se exploran las tecnologías de VPN (Redes Privadas Virtuales) para asegurar las comunicaciones. Estos apartados proporcionan una comprensión integral de los desafíos y soluciones para implementar VoIP de manera efectiva y segura en redes IP.

3.1. El ancho de banda requerido en VoIP

De acuerdo con el modelo OSI, la información atraviesa diferentes capas donde hay empaquetamiento de los datos en la red. El audio codificado es encapsulado en paquetes RTP. Asimismo, RTP es empaquetado en segmentos UDP y posteriormente estos son encapsulados dentro de paquetes IP. En Ethernet, para referirse al empaquetamiento, se utiliza el

La primera red Arpanet en 1969 interconectó cuatro instituciones: Universidad de California en Los Ángeles y la Universidad de California en Santa Bárbara, el Stanford Research Institute (RSI) en Menlo Park, California, y la Universidad de Utah en Salt Lake City, Utah. Actualmente, la clasificación del tráfico de internet a nivel global está compuesto por un 60.6 % para *streaming*, en *web* representa un 13.1 %, para *gaming* un 8.0 %, en redes sociales un 6.1 % y para compartir archivos representa un 4.2 % (Liébana Carrascosa, 2020).

término colectivo «sobrecarga» (*overhead*); sin importar el códec utilizado, la sobrecarga introducida en el paquete es fija (Rivero et al., 2006). La sobrecarga se detalla de la siguiente forma:

- RTP: 4.8 kbps.
- UDP: 3.2 kbps.
- IP: 8 kbps.
- Ethernet (sin QoS): 15.2 kbps.
- La sobrecarga (*overhead*): 31.2 kbps.

La comunicación de VoIP necesita un ancho de banda para operar adecuadamente: esto se conoce como la tasa de transferencia de datos y es medida en bits por segundo (bps). La fórmula para el cálculo del ancho de banda necesario por llamada es:

$$\textbf{\textit{Ancho de banda}} = \textbf{\textit{tamaño total de paquetes x PPS}}$$

donde ***PPS*** es «paquetes por segundo» y se obtiene:

$$\textbf{\textit{PPS}} = \frac{\textbf{\textit{(tasa de bits de códec)}}}{\textbf{\textit{(tamaño de la carga útil de voz)}}}$$

El otro elemento para calcular el ancho de banda es el tamaño total del paquete:

$$\textbf{\textit{Tamaño total del paquete}} = \textbf{\textit{(cabecera de capa 2)}} + \textbf{\textit{(cabecera IP/UDP/RTP)}} + \textbf{\textit{(tamaño de la carga útil de voz)}}$$

3.2. Optimización del tráfico de VoIP

Diferentes aspectos afectan las comunicaciones de VoIP y de videoconferencia IP (Alarcón Quigua, 2008):

- La latencia: los servicios sobre IP como audio y video son sensibles a la latencia por ser aplicaciones de tiempo real. Para el caso de VoIP, al exceder la latencia en los 250ms (milisegundos), la calidad de la llamada es deficiente.

- La pérdida de paquetes: esta se ocasiona en una trayectoria de la señal por una tasa de error (la cual debe ser inferior al 5 %), pero también por la congestión del búfer de una interfaz que provoca un efecto de voces robóticas durante la llamada.

- El *jitter*: la voz se convierte en paquetes de datos divididos y toman diferentes caminos entre el emisor y el receptor; de esta forma pueden llegar a su destino en desorden y producir el efecto *jitter* que imposibilita la comunicación, porque las velocidades de llegada no son homogéneas.

Para garantizar la calidad del servicio, controlar la pérdida de paquetes, la latencia y el *jitter* se pueden emplear las siguientes medidas (Duarte Domingo, 2014):

- Garantizar el ancho de banda: la calidad en la comunicación VoIP requiere un canal dedicado o ancho de banda garantizado. De esta forma se evitan la congestión y la pérdida de paquetes.

- La elección del códec: esto facilita la optimización del ancho de banda.

- Priorización de paquetes: dar prioridad a los paquetes de voz disminuye las demoras en la transmisión, lo que garantiza una latencia dentro los parámetros recomendados. La calidad de la red VoIP está relacionada con la calidad que tendrán las comunicaciones del *Contact Center*.

3.3. Enrutamiento con QoS: WSP y SWP

El enrutamiento basado en QoS es motivo de investigación desde tiempo atrás. Selecciona rutas que tengan la QoS requerida y logra una eficiencia global en la utilización de los recursos. Un ejemplo es Shortest-Widest-Path (WSP), que usa el ancho de banda como métrica y selecciona la mejor ruta de mayor ancho de banda. Para el caso de dos caminos con el mismo ancho de banda, se selecciona el de la mínima cantidad de saltos (Frikha, 2013).

Los algoritmos de enrutamiento de CBR y su complejidad dependen del tipo y número de métricas incluidas en el cálculo de la ruta. El ancho de banda y los saltos son restricciones más útiles que el ***delay*** y el ***jitter***, porque pocas aplicaciones son sensibles a la violación de estas restricciones; como el ***delay*** y el ***jitter*** se calculan con el ancho de banda asignado y el número de saltos, esto se mapea por restricciones de ancho de banda y número de saltos. De igual forma, hay aplicaciones en tiempo real que requieren un ancho de banda específico y el número de saltos determina más consumo de recursos.

En el esquema de CBR hay un balance y equilibrio entre la conservación de recursos y el balanceo de carga. Para una solución viable de CBR se tienen las siguientes opciones:

- Shortest-Distance Path (SDP): método utilizado en el enrutamiento dinámico. Preserva los recursos seleccionando las rutas más cortas.

- Widest-Shortest Path (WSP): este método balancea la carga mediante la elección de rutas con más ancho de banda. Selecciona caminos con mínimo número de saltos y cuando hay varios elige el de mayor ancho de banda.

- Shortest-Widest Path (SWP): este método hace intercambio entre los extremos: elige el camino más corto cuando la carga es alta y al camino más «ancho» cuando la carga es baja. Determina la ruta con el

mayor ancho de banda y en caso de varias rutas elige la de menor cantidad de saltos.

Los dos últimos métodos consumen más recursos, lo cual es ineficiente para un alto requerimiento de la red; por esto hay que compensar la conservación de recursos y el balanceo de carga.

3.4. Seguridad en las redes

La seguridad de la información no se refiere solamente a eliminar virus sino también a otros tipos de ataques, ya sean activos como el enmascaramiento, la retrasmisión y denegación del servicio, entre otros, o pasivos como el análisis de tráfico, la divulgación de contenido y la obtención de parámetros, entre otros, donde los delincuentes informáticos pueden acceder a la red. En las empresas debe garantizarse la protección de los datos sensibles y los sistemas frente a las amenazas, donde la prioridad es salvaguardar la disponibilidad, confidencialidad e integridad de los datos (Franco Romero, 2019).

3.5. Seguridad en VoIP para plataformas abiertas

Esta clase de tecnología tiene una gran demanda en la actualidad; debido a este auge se detectan diferentes tipos de ataques y vulnerabilidades (Thermos & Takanen, 2008). En la tabla 3.1. se presentan los más comunes.

La seguridad en un sistema de comunicación de VoIP consiste en proteger todos sus componentes sobre una infraestructura de datos segura, que proporcione tolerancia a fallos, estabilidad y escalabilidad (Uzcategui, 2015). Entre los elementos fundamentales se encuentran:

- Las redes Ethernet o de entorno local.
- Las redes WLAN.
- El control de tráfico en diferentes zonas y perimetrales.
- Utilización de diferentes tipos de VPN.

La implementación de VoIP requiere políticas para asegurar el sistema de comunicaciones; esta tecnología requiere apoyo de las otras capas y protocolos de las redes. De igual forma, la telefonía IP hereda problemas ya existentes, como las amenazas comunes de seguridad que tienen las redes de datos. En la tabla 3.2. se presentan los temas de seguridad a tener en cuenta y las tecnologías referentes al modelo OSI que intervienen en la comunicación y que son sensibles para garantizar un ámbito de VoIP seguro (Chakraborty et al., 2019).

Tabla 3.1. Ataques y vulnerabilidades

Capa	Ataques y vulnerabilidades
Políticas y procedimientos	No concientizar al personal Uso inadecuado de roles y permisos Contraseñas débiles y predeterminadas
Seguridad física	Infraestructura física inadecuada No contar con controles de acceso Acceso al personal no autorizado Pérdida de energía
Seguridad de red	Suplantación de direcciones IP Suplantación de enrutamiento SYN *floods* Escaneo de puertos
Seguridad en los servicios	Suplantación por nombre de dominio Envenenamiento de ARP Inyección de SQL Denegación de servicio
Seguridad en el S.O.	Desbordamiento de búfer Sistemas operativos sin actualizar Configuraciones mal realizadas
Seguridad en las aplicaciones y protocolos de VoIP	*Sniffing* Suplantación de páginas web Secuestro de sesiones Redirección de llamadas Reproducción de llamadas

Fuente: elaboración propia (2023).

Tabla 3.2. Seguridad en VoIP

Seguridad aplicaciones y protocolos VoIP
Seguridad en el sistema operativo
Seguridad en los servicios
Seguridad de red
Seguridad física
Política y procedimientos

Aplicación	Elastix
Presentación	G.729/G.711
Sesión	SIP
Transporte	UDP/RTP/RTCP
Red	IP
Enlace	Ethernet
Física	Ethernet

Fuente: elaboración propia (2023).

3.6. Las VPN

Son redes privadas virtuales formadas dentro de una infraestructura privada o pública para el caso de un entorno local o cuando se hace necesario cruzar una red como Internet. Se puede usar una red VPN para conexión segura entre oficinas y usuarios remotos por medio de un acceso a Internet a través de un ISP. De esta forma se evitan enlaces WAN dedicados o conexión telefónica de larga distancia (Mairs, 2002).

La utilización de una VPN reduce costos por ancho de banda en una WAN y permite el incremento de la velocidad de conexión a Internet por el ancho de banda, como puede ocurrir en DSL, Ethernet o cable Módem. Una VPN proporciona enlace seguro al utilizar túneles VPN (SSL: Secure Sockets Layer) y Seguridad IP Cifrada (IPSec). Estas redes protegen los datos del acceso no autorizado, permiten aprovechar la infraestructura de Internet existente y extienden el alcance de la red sin ampliar con bajos o sin cambios en la infraestructura.

Las redes VPN-IPSec y VPN-SSL son soluciones de conexión para oficinas remotas y

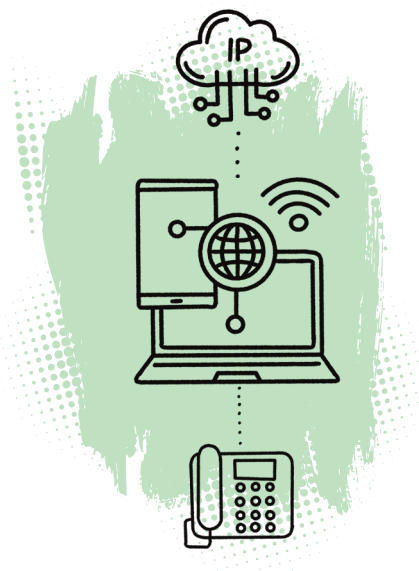
partners comerciales que buscan mejorar la seguridad en la comunicación, conservando derechos de acceso específicos en el caso de empleados, contratistas o aliados; su utilización incrementa la productividad, la reducción de costos en infraestructura y aumenta la flexibilidad. Varios tipos de VPN cifradas son:

- VPN IPSec sitio a sitio: es una alternativa a las redes WAN de línea alquilada que permite extender los recursos de la red de una oficina a sus sucursales, al hogar y los sitios de *aliados* comerciales.

- VPN acceso remoto: mediante esta solución se lleva cualquier aplicación de voz, video y datos al escritorio remoto, con acceso a los datos alojados en el escritorio de la oficina principal y en la nube. Esta red virtual puede instalarse con IPSec, SSL o ambas, dependiendo de los requerimientos de implementación.

- *Tunneling:* en este método hay un canal donde viajan los paquetes y estos van cifrados al usuario autorizado, quien deberá descifrar su contenido para acceder a ellos. Este método es uno de los más utilizados en las VPN y comprende el proceso de encapsulación (encapsula el paquete original dentro de uno nuevo, el paquete puede contener nueva información de direccionamiento y enrutamiento), enrutamiento y desencapsulación. Los mecanismos más comunes para realizar *tunneling* son:

- GRE (Generic Routing Encapsulation)
- L2PT
- PPTP
- *Tunneling* entre origen y destino.
- *Router* a *router*



Conclusiones

La importancia del ancho de banda y de la optimización del tráfico en VoIP radica en que constituyen un recurso vital para las comunicaciones VoIP, ya que afectan directamente la calidad de las llamadas. Una gestión adecuada del ancho de banda asegura que las llamadas sean claras y sin interrupciones. Y la optimización del tráfico en VoIP por medio de técnicas como la compresión de datos y la priorización de paquetes de voz, es esencial para maximizar la eficiencia de la red; estas técnicas permiten manejar de manera efectiva el tráfico de voz incluso en redes congestionadas, garantizando una experiencia de usuario satisfactoria.

El enrutamiento con Calidad de Servicio (QoS) mediante protocolos como WSP y SWP es crucial para asegurar que las comunicaciones de voz tengan prioridad sobre otros tipos de tráfico en la red. Estos protocolos permiten asignar diferentes niveles de prioridad a los paquetes de datos, asegurando que el tráfico de voz reciba el tratamiento necesario para mantener una alta calidad de llamada. La correcta aplicación de QoS en el enrutamiento de VoIP no solo mejora la calidad de las llamadas, sino que también optimiza el uso de los recursos de red al reducir la latencia y la pérdida de paquetes.

La seguridad en VoIP y el uso de redes VPN es una preocupación primordial, especialmente en plataformas abiertas donde las amenazas suelen ser más frecuentes. La implementación de medidas de seguridad como el cifrado de datos y la autenticación robusta es fundamental para proteger las comunicaciones de voz contra ataques y accesos no autorizados. Las redes VPN ofrecen una capa adicional de seguridad con la creación de canales de comunicación cifrados, protegiendo los datos de voz durante su transmisión a través de redes públicas; el uso de estas redes en sistemas VoIP garantiza la confidencialidad e integridad de las comunicaciones, mitigando los riesgos de interceptación y fraude.

CAPÍTULO 4.

Caso práctico de voz sobre IP

Introducción

A lo largo de este capítulo, centrado en la implementación práctica de una solución de Voz sobre IP (VoIP), se abordarán las consideraciones y pasos necesarios para elegir los terminales adecuados, seleccionar el sistema y el proveedor de servicios más idóneos, y virtualizar una planta telefónica en sistemas operativos como Windows o Linux. Asimismo, se explorará la configuración de la máquina virtual, la instalación y configuración inicial del sistema operativo (FreePBX) y la creación de extensiones telefónicas y troncales. Este caso práctico proporciona una guía detallada para establecer una infraestructura de VoIP robusta y eficiente, adaptada a las necesidades específicas de una entidad.

La implementación de voz sobre IP requiere evaluar varios aspectos dentro de una organización, como el funcionamiento de la red de comunicaciones, la infraestructura existente de dispositivos, los servicios requeridos y los elementos necesarios para implementar una solución de comunicaciones de telefonía sobre IP (Sierra Rodríguez, 2011).

Inicialmente se evaluará el estado de los dispositivos en cuanto a actualización y obsolescencia, así como la capacidad de la red LAN. La velocidad y el ancho de banda son determinantes en el rendimiento del sistema de telefonía IP. La capacidad y vigencia de los suiches y enrutadores (*routers*) permite optimizar el ancho de banda con Calidad de Servicio (QoS), a fin de obtener un servicio satisfactorio.

El primer computador de propósito general, el ENIAC (Electronic Numerical Integrator And Computer), se desarrolló entre 1943 y 1945 en la escuela Moore de la Universidad de Pensilvania (EU), pero antes se había construido la primera computadora mecánica programable, la Z1 alemana, entre 1935 y 1936 por Konrad Zuse (Jaimovich, 2019). Hoy existen entornos virtuales donde se ejecuta *software* en un ambiente aislado que puede gestionar varias máquinas simultáneamente sin recursos físicos adicionales, obteniendo alta disponibilidad de recursos, administración centralizada y aumento de la productividad, entre otras (Ramírez, 2020).

Para una infraestructura de VoIP permanente se recomienda utilizar la red con teléfonos físicos VoIP. También se incluye el segmento inalámbrico mediante wifi como parte de la Red de Área Local (LAN); en esta circunstancia se tendrán presentes los enrutadores (*routers*) o dispositivos wifis que sean capaces de priorizar el tráfico VoIP para evitar la latencia y la falta de calidad de la voz (Hersent, 2011).

4.1. Elección de terminales de acuerdo con los requerimientos

- Los teléfonos físicos (*hardphones*). Un hardphone básico de escritorio cuenta con un teclado estándar y botones para las funciones adicionales como transferencia de llamada, y uno más avanzado como central que recibe y distribuye las llamadas. Es más costoso al contar con funcionalidades avanzadas para gestionar múltiples líneas, agilizar y facilitar la administración de la comunicación.

- Los *softphones* o *software* de teléfono. Utilizados en ordenadores, portátiles, *smartphones* y tabletas. Consumen mayor procesamiento, puesto que para transmitir la voz procesa miles de muestreos por segundo.

- Los adaptadores ATA (Analog Telephone Adaptor). Estos adaptadores habilitan los teléfonos analógicos para utilizar VoIP.

- Los terminales convencionales operan conectados a una central telefónica con capacidad IP. La central se encarga de realizar todas las funciones IP soportadas por los terminales.

4.2. Elección del sistema

- Los dispositivos físicos PBX IP. Localizados, instalados y gestionados en la oficina, soportan conectividad tradicional e IP, tanto en extensiones como en líneas telefónicas.

- PBX en la nube o por software. La central telefónica se encuentra en la nube o en una aplicación instalada en un ordenador. Se pueden obtener alquilando extensiones a un proveedor o instalando la central en un centro de datos; en este caso el costo se puede conseguir con una financiación vía *renting* de la central, dependiendo de las dimensiones de la centralita a contratar (Meggelen et al., 2013).

4.3. Elección del servicio y proveedor

El servicio de Internet en función del número de extensiones, líneas utilizadas simultáneamente, códec utilizado y topología elegida podrá ir desde un servicio asimétrico (ADSL)

compartido o de uso exclusivo para la VoIP, hasta un servicio simétrico con una reserva de canal para la VoIP. También se puede adquirir directamente por medio de un servicio de telefonía por Internet. Las llamadas van directamente de la oficina a la red mediante troncales SIP sin intermediarios, y es posible disponer de números de teléfono internacionales que se pueden conectar a la nueva central IP. Según la topología empleada, hay que considerar las políticas de seguridad necesarias que deben implementarse.

4.4. Virtualizando la planta telefónica

La virtualización de sistemas operativos permite configurar y aprovechar al máximo los recursos para la instalación de aplicaciones y servicios esenciales en una infraestructura de comunicaciones. Las máquinas virtuales (VM) permiten la ejecución de sistemas operativos como si se tuviera otro computador o *hardware* real, lo cual permite optimizar y ejecutar simultáneamente servidores en un mismo equipo; de esta forma se obtiene una infraestructura ágil y flexible, una reducción de costos, administración centralizada, continuidad del negocio y uso eficiente de los recursos. Estos sistemas virtuales son gestionados con aplicaciones especializadas de escritorio como VirtualBox de Oracle (https://www.virtualbox.org) y Vmplayer de Vmware (https://www.vmware.com).

4.4.1. ¿Windows o Linux?

Windows es un sistema operativo de Microsoft y un estándar en equipos de hogar y empresariales, con una interfaz gráfica GUI que ha facilitado su aprendizaje y su popularidad (Tanenbaum, 2009). Por su parte, Linux es uno de los sistemas operativos más fiables y eficientes que se puedan encontrar y en su evolución gráfica se asemeja a Windows. Existen muchas distribuciones diferentes basadas en GNU/Linux, las hay para toda clase de ordenadores y dispositivos electrónicos: portátiles o de escritorio, *smartphones* o PDA, puntos de acceso de redes inalámbricas, etc. La naturaleza de su código abierto permite que cualquiera pueda tomarlo y desarrollarlo hasta el momento, y adaptarlo a sus propias necesidades; cada vez más empresas y usuarios eligen sistemas basados en Linux por sus elevadas prestaciones y la cantidad de *software* disponible.

A continuación se implementará una solución de Voz sobre IP en una plataforma *open source* bien conocida como Asterisk (Meggelen et al., 2019; Sierra Rodríguez, 2011). Esta centralita cuenta con varias versiones implementadas y preconfiguradas en sistemas operativos Linux como FreePBX (https://www.freepbx.org) e Issabel (https://www.issabel.org), en las cuales se podrá acondicionar desde una solución muy básica hasta una de nivel empresarial o productivo. Inicialmente se realizará la instala-

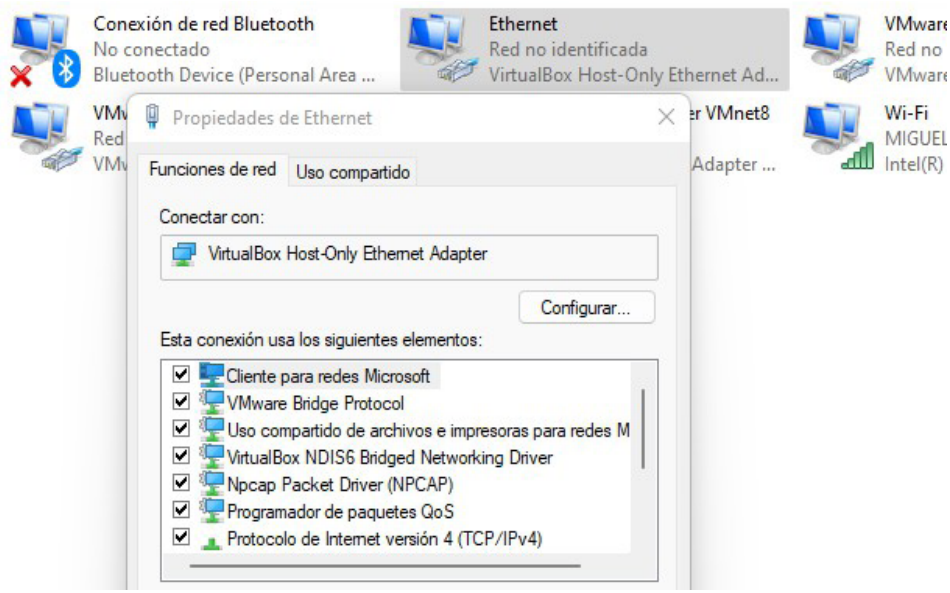
ción de una máquina virtual por medio de Virtualbox, cuya descarga se obtiene del siguiente enlace: https://www.virtualbox.org/wiki/Downloads.

4.5. Instalación de la aplicación para virtualizar

Antes de realizar la instalación de la herramienta se deben verificar los adaptadores disponibles en el sistema operativo, toda vez que al instalar VirtualBox se adiciona una conexión de red virtual para comunicar los equipos en una red interna o establecer la comunicación entre máquinas virtuales y dispositivos externos. En Panel de control/Conexiones de red se verifican los adaptadores de red instalados. Como se observa en la figura 4.1., se adicionó un adaptador llamado VirtualBox Host Only.

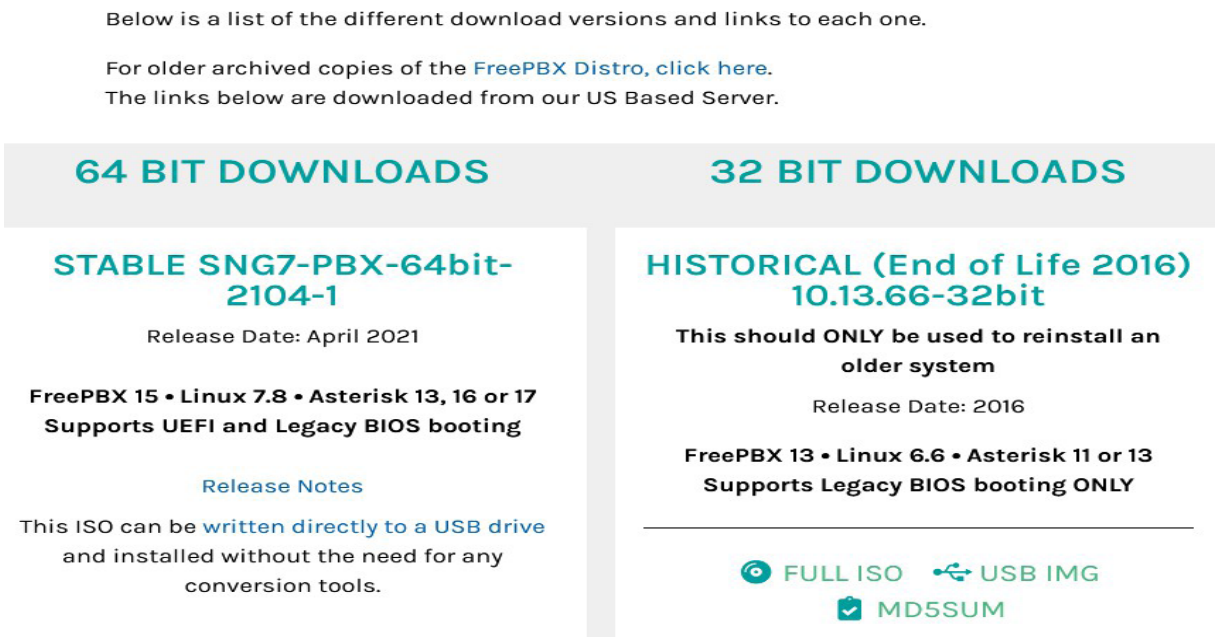
Luego se descarga el sistema operativo (imagen xxx.iso) con la centralita preconfigurada; para este caso se utilizará FreePBX que se obtiene del siguiente enlace: https://www.freepbx.org/downloads/. En la figura 4.2. se detallan las alternativas de descarga, como versión del sistema operativo y plataforma de 32 o 64 bits.

Figura 4.1. Adaptadores de red de VirtualBox



Fuente: elaboración propia (2023).

Figura 4.2. Versión del S.O. VoIP en máquina virtual (VM)



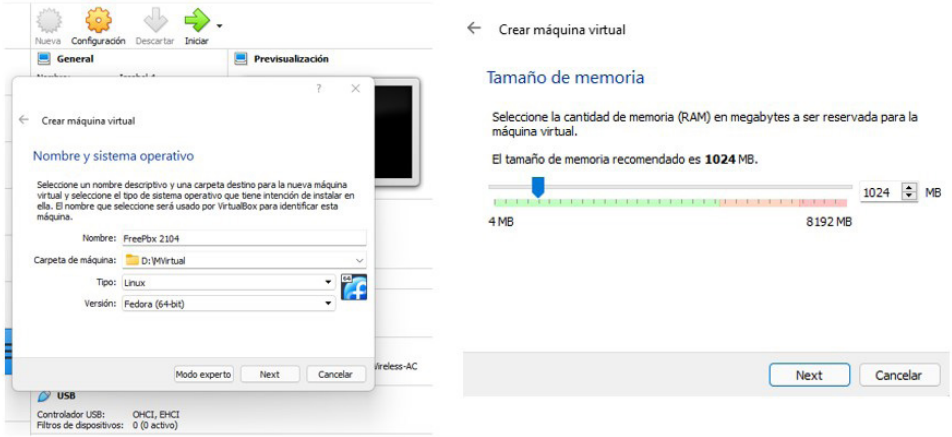
Fuente: elaboración propia (2023).

Se recomienda crear una carpeta en la raíz del sistema: c:\DiscoVirtual (o una carpeta no protegida por el sistema operativo) y copiar allí la imagen descargada FreePBX xxx.iso que corresponde al sistema operativo para instalar como máquina virtual.

4.6. Configurando la máquina virtual

Inicie VirtualBox y haga clic en «Nueva» para crear una máquina. Tal como se ilustra en la figura 4.3., se define el nombre, la ubicación y el tipo de plataforma: para este caso se selecciona Linux (Fedora o RedHat), debido a que FreePBX está desarrollado sobre la plataforma Centos de la familia RedHat. Después de hacer clic en «Next» se establecen otras configuraciones, como el tamaño de la memoria RAM cuyo mínimo requerimiento es de 1024 GB.

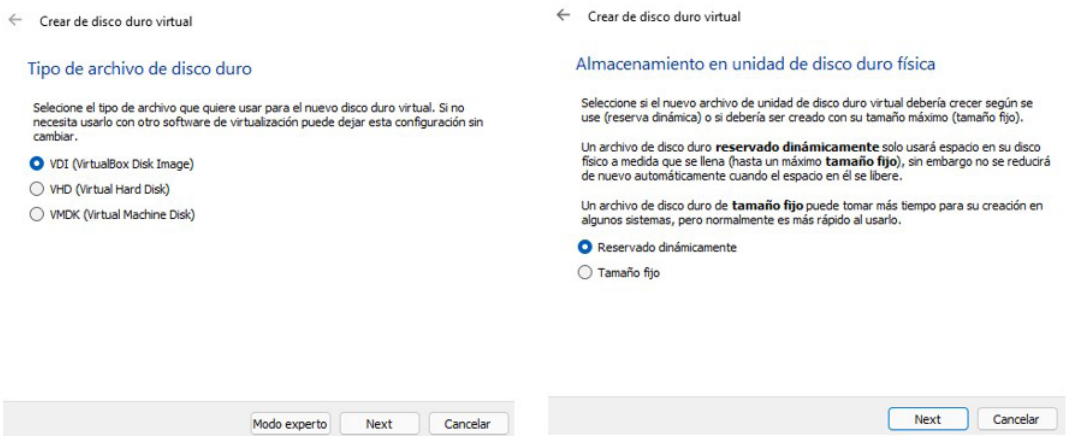
Figura 4.3. Nombre y ubicación de la máquina virtual (VM)



Fuente: elaboración propia (2023).

En la figura 4.4. se ilustra la elección del tipo de disco duro a utilizar en la máquina FreePBX. Posteriormente se define si el espacio del disco duro se utilizará de manera fija o ajustado dinámicamente.

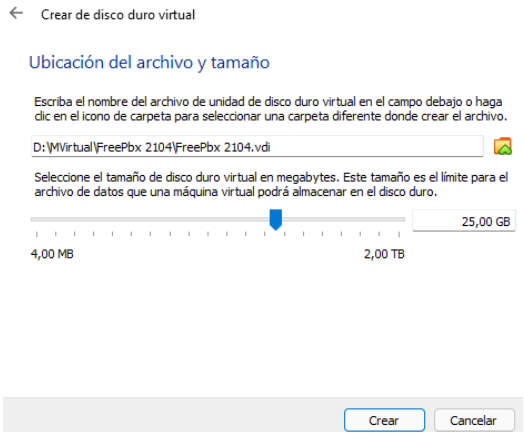
Figura 4.4. Tipo de disco en la máquina virtual (VM)



Fuente: elaboración propia (2023).

Seguidamente se elige el tamaño del disco y su ubicación, como se detalla en la figura 4.5.

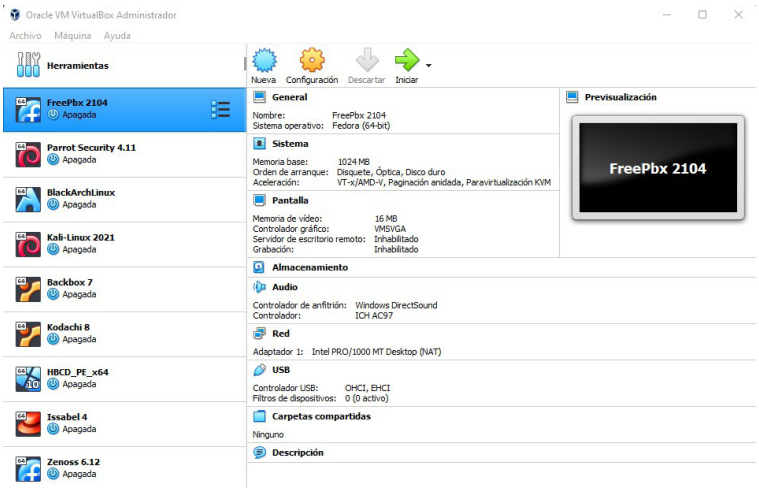
Figura 4.5. Tamaño del disco en la máquina virtual (VM)



Fuente: elaboración propia (2023).

En la figura 4.6. se puede observar la nueva máquina virtual creada, con un resumen de sus características en el panel derecho de la figura.

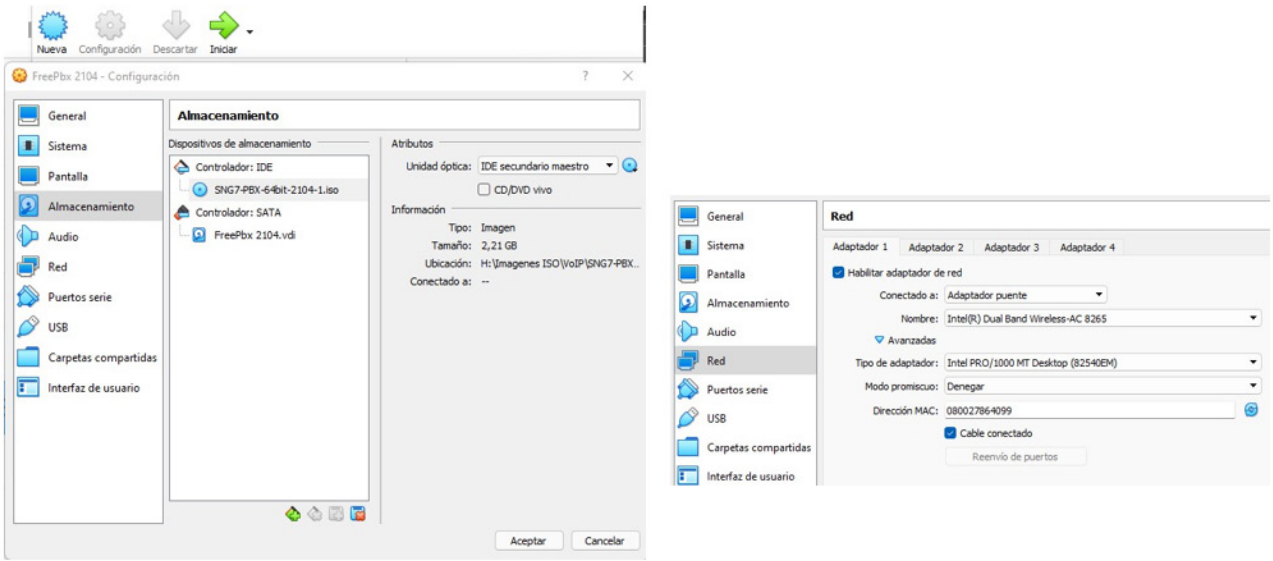
Figura 4.6. Máquina virtual (VM) creada



Fuente: elaboración propia (2023).

Finalmente, en la parte de almacenamiento se configura el primer inicio de la máquina con el acceso al archivo ***.iso* ubicado en la carpeta establecida al comienzo de la instalación del sistema operativo virtual. En la figura 4.7. se observa la asignación de la imagen a la unidad óptica virtual. Se recomienda configurar el adaptador de red como puente, para que la nueva máquina forme parte de la red local y se acceda a ella fácilmente desde cualquier dispositivo requerido como parte del sistema de comunicación de voz IP.

Figura 4.7. Características de la máquina virtual (VM) creada

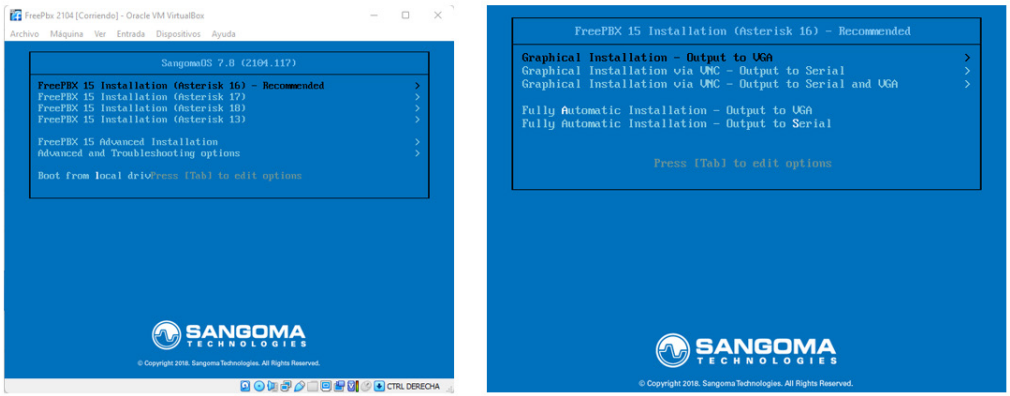


Fuente: elaboración propia (2023).

4.7 Instalando la nueva máquina virtual

Una vez establecida la configuración detallada anteriormente, se puede iniciar la máquina donde se instalará el sistema operativo con la central Asterisk preconfigurada. La figura 4.8. muestra las opciones disponibles para la instalación y por defecto se selecciona la recomendada. La primera opción que se detalla en la imagen derecha indica el tipo de salida para la instalación gráfica del sistema.

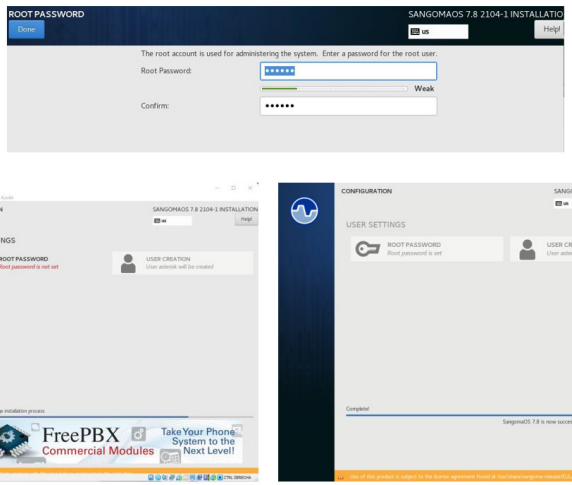
Figura 4.8. Instalación del S.O. en la máquina virtual (VM)



Fuente: elaboración propia (2023).

Posteriormente, en la figura 4.9. se detalla el inicio de la instalación del nuevo sistema operativo: en esta parte se define la contraseña de súper usuario de Linux. Una vez terminada la instalación, se procede a reiniciar el sistema (*reboot*).

Figura 4.9. Inicio de sesión en la máquina virtual (VM) creada



Fuente: elaboración propia (2023).

Una vez terminado el proceso de instalación de la máquina virtual y de haberla reiniciado, esta pedirá el acceso al sistema: las credenciales son para el usuario *root* y su contraseña la definida en el proceso de instalación. En la figura 4.10. se observa la dirección IP registrada de la red local donde se podrá acceder por medio de algún navegador web. En este ejemplo aparece la dirección y un cuadro de mensaje referente a la necesidad de activar la máquina.

Figura 4.10. Consola de FreePBX

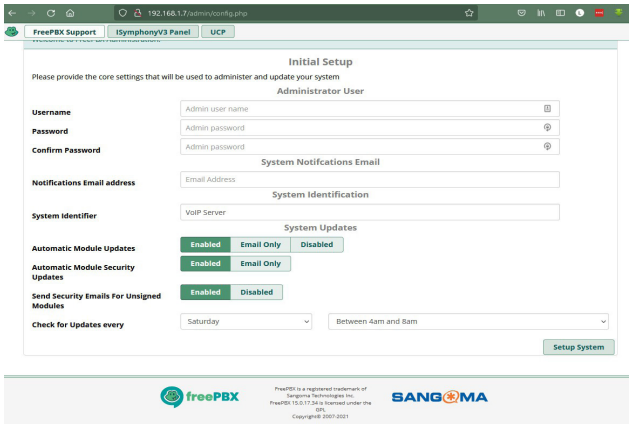
Fuente: elaboración propia (2023).

4.8. Configuración inicial del sistema operativo (FreePBX)

Se procede a iniciar sesión en la interfaz gráfica de usuario del PBX («GUI»). Utilizando otra máquina en la misma red se abre un navegador web y se ingresa la dirección IP del PBX detallado en la figura 4.10. de este ejemplo. Si desconoce la dirección IP de la máquina, se puede consultar desde la consola o símbolo del sistema de Linux. Se inicia sesión en la consola de Linux utilizando el nombre de usuario *root* sin comillas y la contraseña de *root* seleccionada durante la instalación; seguidamente se mostrará la dirección IP.

En la figura 4.11. se ilustran los parámetros iniciales a configurar que solicita la plataforma, como nombre de usuario, contraseña y actualizaciones automáticas.

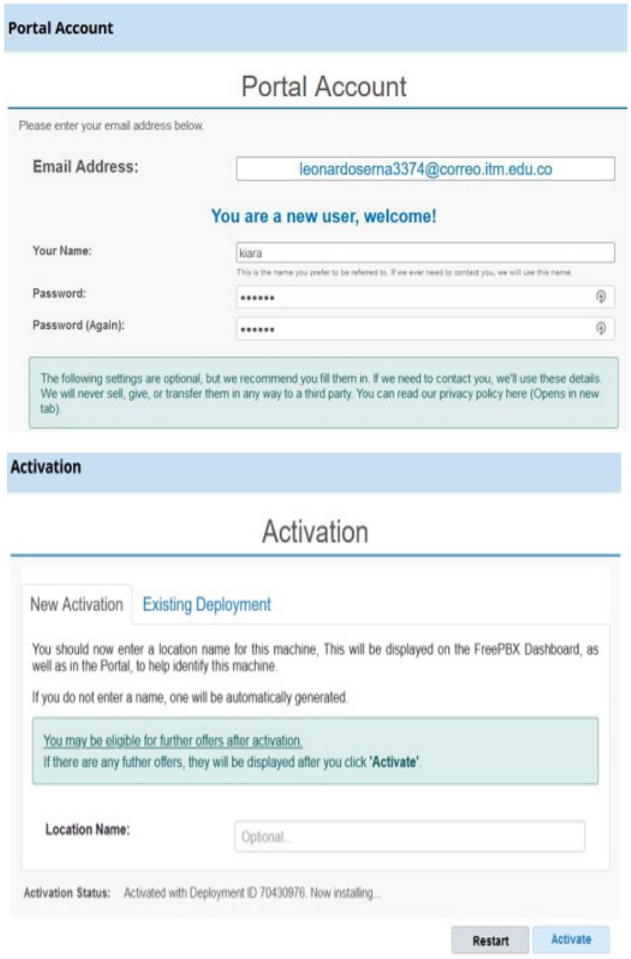
Figura 4.11. Parámetros iniciales para configurar en FreePBX



Fuente: elaboración propia (2023).

Seguidamente, en la figura 4.12. se ilustra la creación de un usuario en el portal y se procede a la activación de la máquina para que pueda operar de manera totalmente funcional.

Figura 4.12. Creación de usuarios



Fuente: elaboración propia (2023).

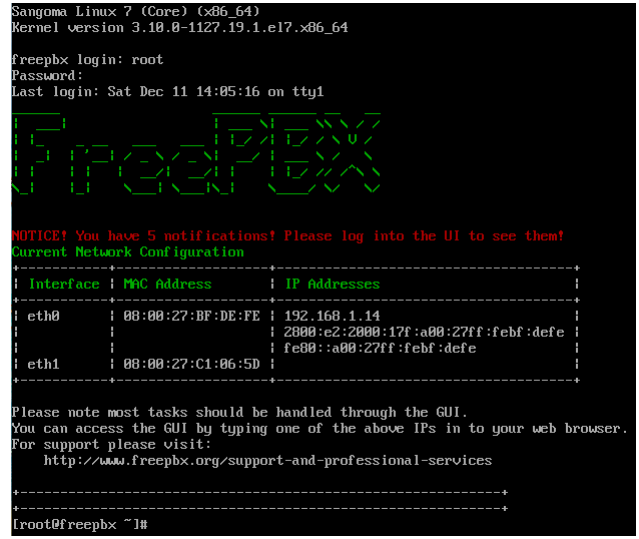
En ocasiones la configuración inicial puede arrojar un error de parametrización, por lo que se recomienda ejecutar en la consola de Linux (FreePBX):

[root@ FreePBX] # fwconsole ma install sysadmin

[root@ FreePBX] # fwconsole ma enable sysadmin

En la figura 4.13. se presenta el estado de la activación de la máquina y su nueva dirección de acceso.

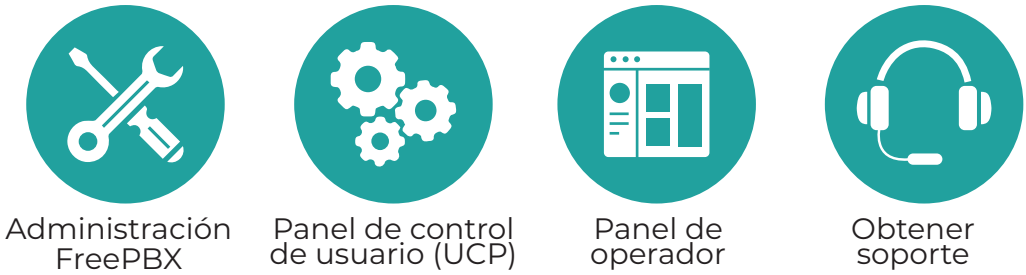
Figura 4.13. Activación de la consola de FreePBX



Fuente: elaboración propia (2023).

Al ingresar por el navegador web, se mostrarán los módulos de acceso ilustrados en la figura 4.14.

Figura 4.14. Módulos de acceso a FreePBX



Fuente: elaboración propia (2023).

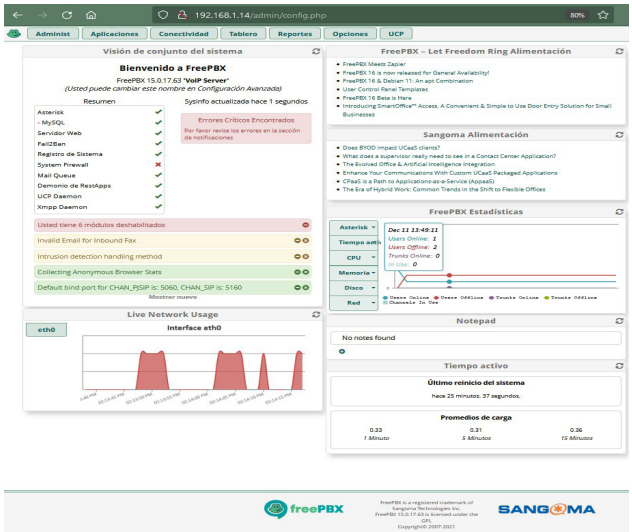
- FreePBX Administration permitirá configurar el PBX. Se utiliza el nombre de usuario y la contraseña de administrador configurada en el paso anterior para iniciar sesión. Esta sección es lo que la mayoría de la gente llama « FreePBX».

- Panel de Control de Usuario (UCP). Lugar donde un usuario puede iniciar sesión para hacer llamadas web, configurar los botones de su teléfono, escuchar mensajes de voz, enviar y recibir faxes, usar mensajes SMS y XMPP, ver conferencias y más, dependiendo de las funcionalidades que haya habilitado para el usuario.

- Panel de Operador. Es una pantalla que permite al operador controlar las llamadas.

- Obtener Soporte. Lleva a una página web con varias opciones de soporte oficial para FreePBX. Al ingresar por el primer módulo aparece el tablero inicial donde se muestra el estado de la conexión y estadísticas de uso de la plataforma, como se detalla en la figura 4.15.

Figura 4.15. Consola web del FreePBX

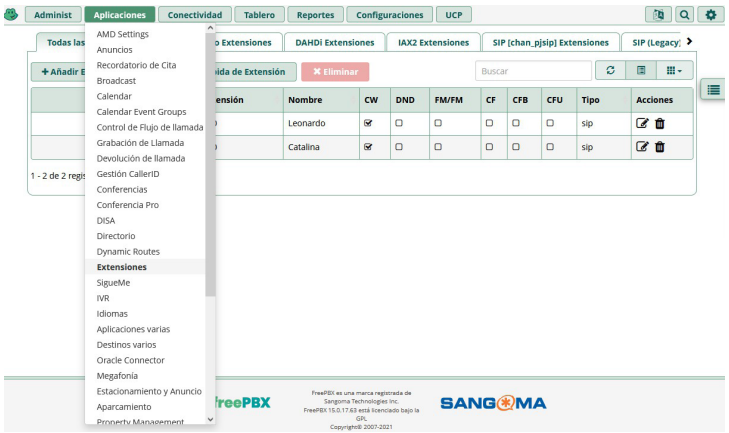


Fuente: elaboración propia (2023).

4.9. Configuración de las extensiones telefónicas

Se ingresa por la pestaña de *Aplicaciones* y se selecciona el enlace de *Extensiones* para agregar las terminales telefónicas. En la figura 4.16. se detalla el menú de acceso a esta parte de la configuración.

Figura 4.16. Configuración del FreePBX



Fuente: elaboración propia (2023).

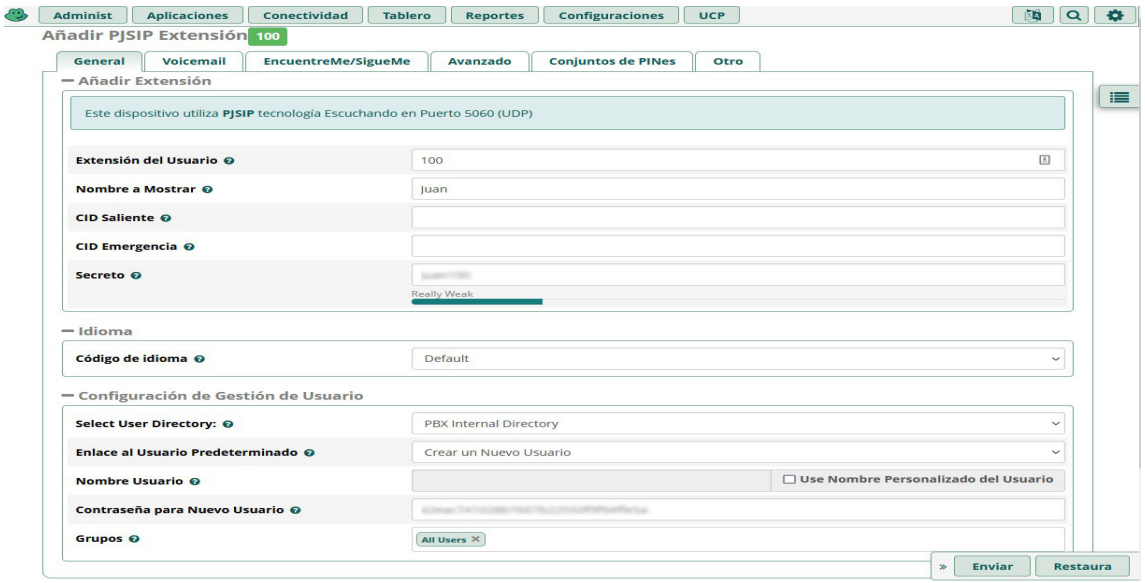
Al agregar la extensión, tal como está ilustrado en la figura 4.17., se puede elegir entre los diferentes tipos que ofrece el sistema.

Figura 4.17. Agregar extensiones en FreePBX

Fuente: elaboración propia (2023).

Cada extensión se puede configurar con unos parámetros básicos como el número (extensión del usuario), nombre a mostrar en la identificación de la llamada y una clave de autenticación de usuario (secreto) ante la planta PBX. Posteriormente, en Avanzado se pueden configurar parámetros adicionales como el tipo de conexión y puertos NAT, entre otros. En la figura 4.18. se detalla la creación del nuevo usuario y el puerto asociado de escucha utilizando el protocolo UDP.

Figura 4.18. Creación del usuario en FreePBX



Fuente: elaboración propia (2023).

4.10. Instalación del cliente telefónico (*softphone*)

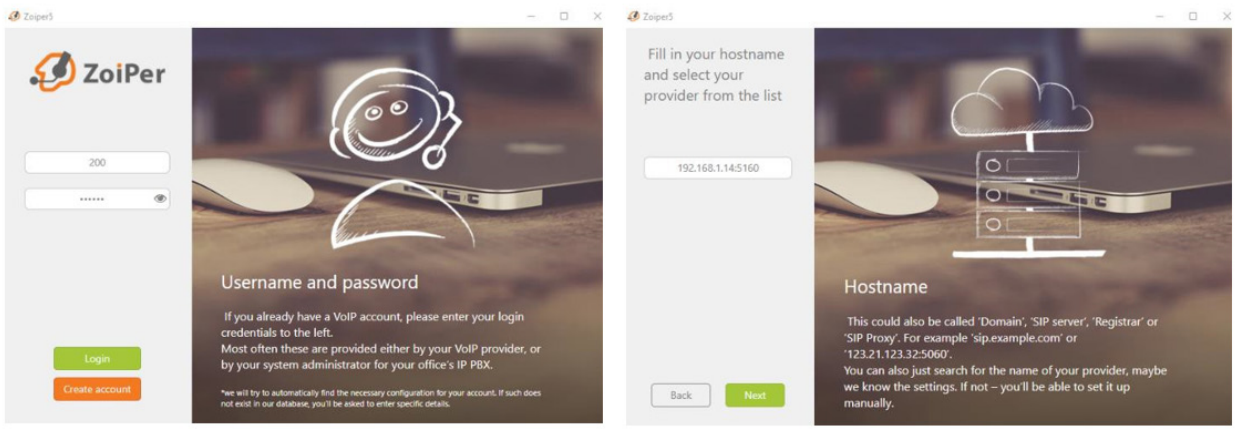
Ya se tiene configurada de manera básica la planta telefónica y lista para su uso. Se elige un terminal físico de voz IP o en este caso se instalará una aplicación que permite autenticar el usuario y establecer enlace con otros equipos en la red; esta aplicación permite la comunicación desde cualquier computador, tableta o *smartphone* como si se tuviera un terminal telefónico físico, al poder realizar llamadas, videoconferencias o mensajes de chats por la misma aplicación.

El *softphone* es versátil en su instalación y su utilización. Está constituido por una interfaz intuitiva de fácil comprensión y por un teclado virtual parecido al de los teléfonos convencionales. Se utiliza la aplicación Zoiper (https://www.zoiper.com) que contiene una parte libre para su utilización y muchas funciones restringidas orientadas a la parte comercial; es multiplataforma, pudiéndose instalar en sistemas Linux, Windows y Android.

Otra aplicación utilizada en la práctica para emular dos o más terminales en el mismo equipo es Linphone (https://www.linphone.org), una aplicación también multiplataforma y totalmente libre o de código abierto (open source).

Una vez instalada la aplicación cliente, en la figura 4.19. se detalla la configuración inicial del *softphone.*

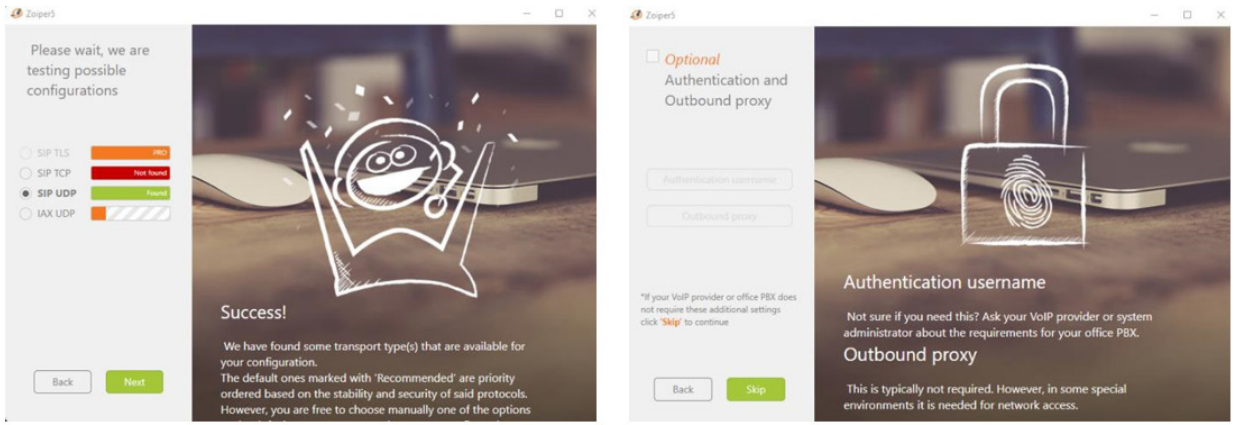
Figura 4.19. Aplicación de usuario



Fuente: elaboración propia (2023).

Dentro de la configuración se puede verificar la conexión con la planta telefónica por UDP y una configuración opcional como credenciales de autenticación y proxy adicionales, detallados en la figura 4.20.

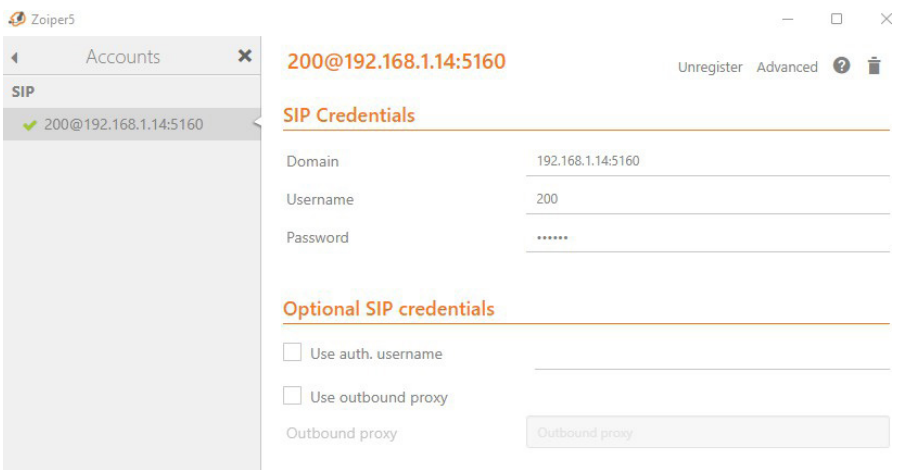
Figura 4.20. Autenticación de usuario desde el *softphone*



Fuente: elaboración propia (2023).

Nótese la configuración básica en la figura 4.21., como dirección del servidor, número de extensión, puerto utilizado y la contraseña de usuario asignada (*Secreto*).

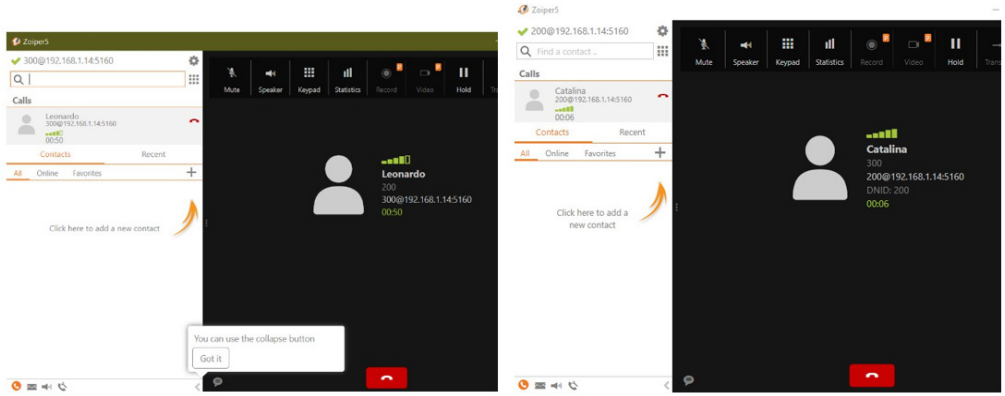
Figura 4.21. Cuenta asignada en FreePBX



Fuente: elaboración propia (2023).

Desde otro equipo, y habiendo instalado el mismo cliente, en la red se realiza el proceso de marcado, tal como se detalla en la figura 4.22.

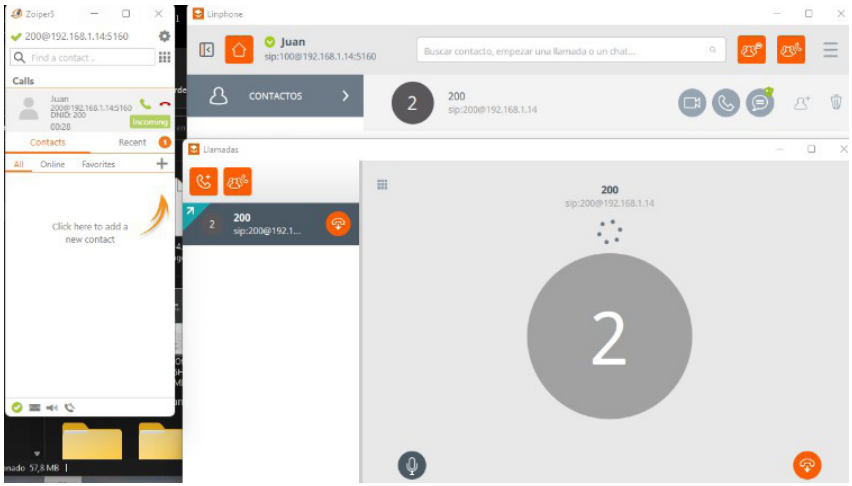
Figura 4.22. Proceso de marcado y conectividad en FreePBX



Fuente: elaboración propia (2023).

Finalmente, en la misma estación se utilizan dos extensiones con diferentes *softphones* para la prueba de la tercera extensión, detallado en la figura 4.23.

Figura 4.23. Conexión de diferentes usuarios en FreePBX

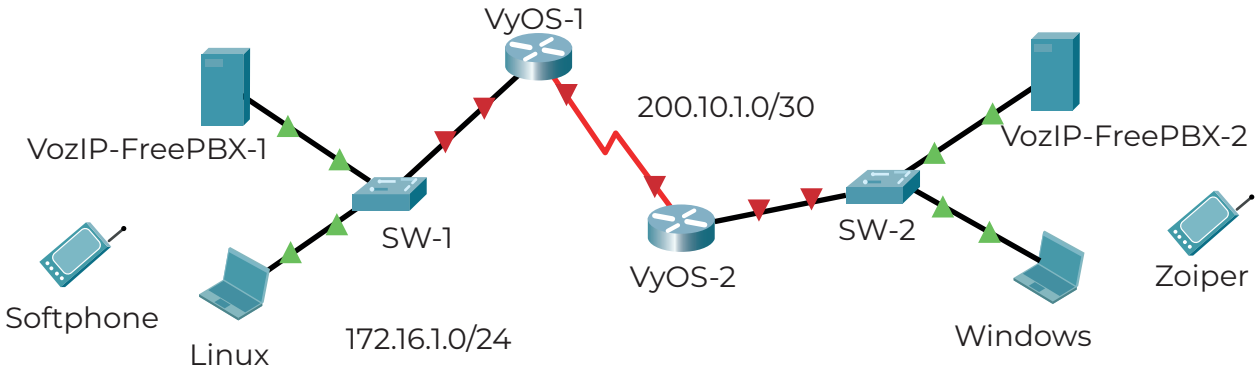


Fuente: elaboración propia (2023).

4.11. Construcción de una troncal telefónica

Una solución de comunicaciones extendida a varias sedes requiere la formación de enlaces troncales y la interconexión al exterior se realiza por esta misma técnica. En el ejemplo práctico de la figura 4.24., se configurará en un ambiente virtualizado el siguiente esquema entre una estación remota (sistema virtual) y una estación local (sistema real), unidas mediante un enlace troncal que en la mayoría de los casos constituye un ambiente WAN enrutado de dos servidores de VoIP.

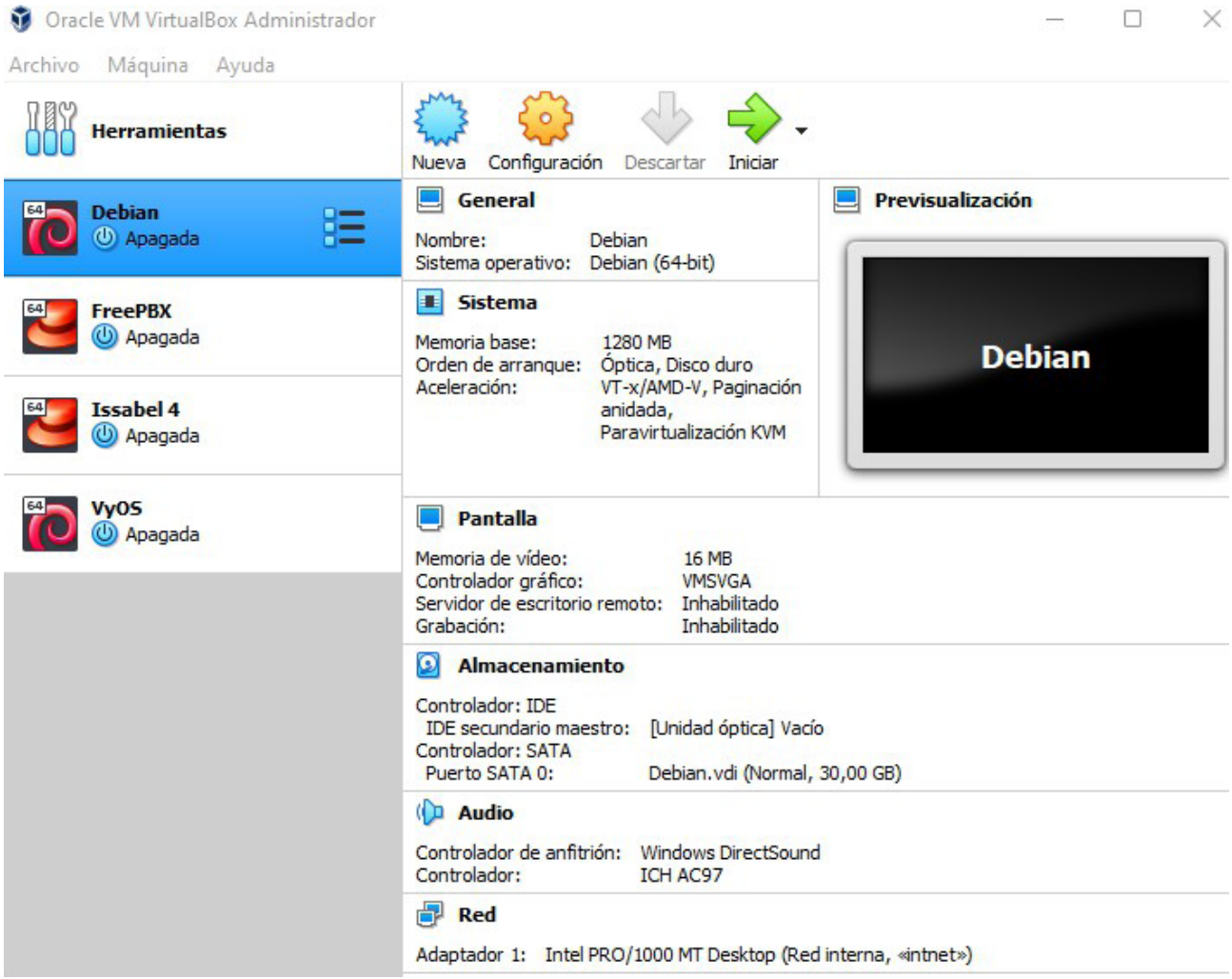
Figura 4.24. Esquema de red WAN



Fuente: elaboración propia (2023).

Se instala Debian como sistema virtual (se instalará cliente VoIP). Se procede a obtener una versión actualizada del sistema operativo y se puede descargar de la siguiente dirección: https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid. En seguida, se configura la plataforma VirtualBox para instalar Debian; esta configuración inicial se detalla en la figura 4.25.

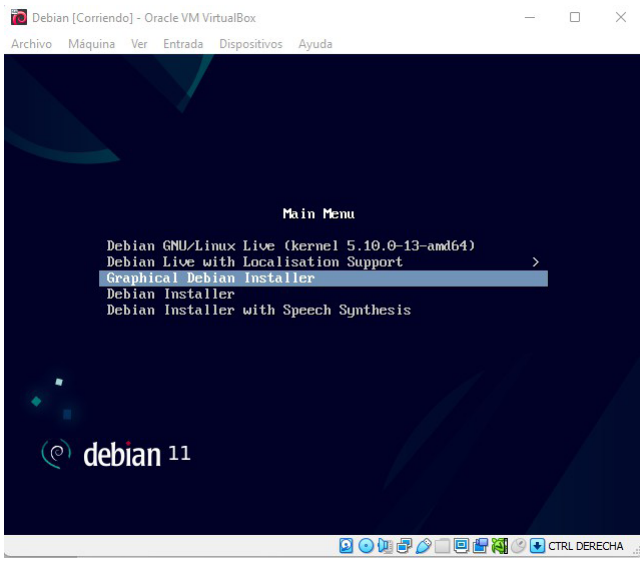
Figura 4.25. Configuración de la VM Linux



Fuente: elaboración propia (2023).

En la figura 4.26. se indica «Seleccionar» el instalador gráfico.

Figura 4.26. Selección del modo instalador Linux



Fuente: elaboración propia (2023).

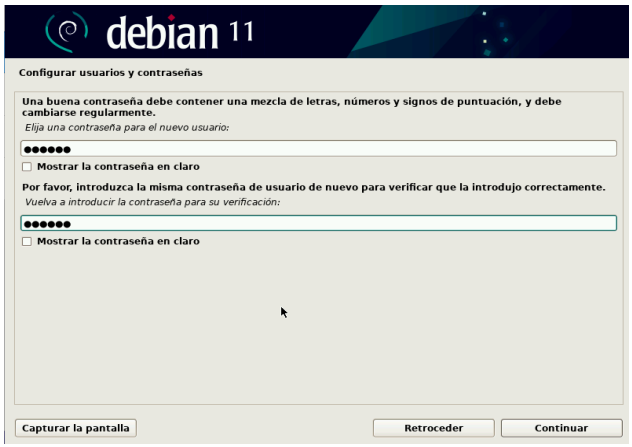
Luego se debe ubicar idioma, región y distribución de teclado, tal como se ilustra en la figura 4.27.

Figura 4.27. Parámetros iniciales en Linux

Fuente: elaboración propia (2023).

En la figura 4.28., se muestra la configuración adicional como parámetros de red y usuario.

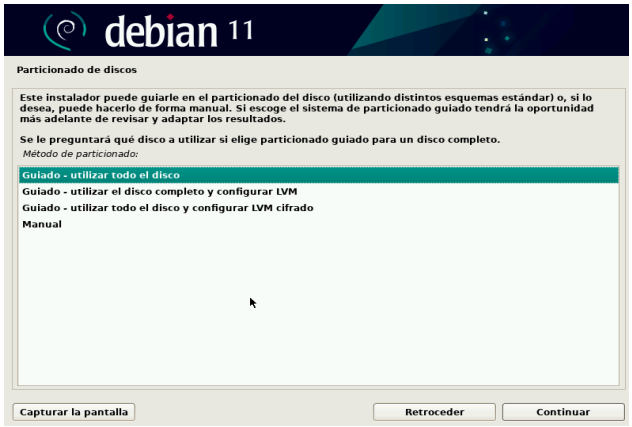
Figura 4.28. Configuración de contraseñas



Fuente: elaboración propia (2023).

En la figura 4.29., se indica seleccionar «utilizar por defecto» el particionado automático de discos.

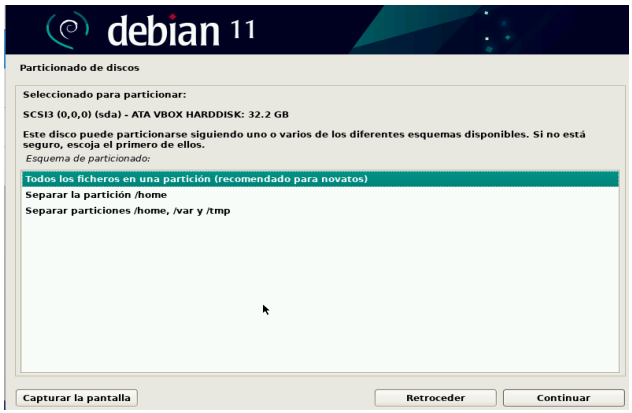
Figura 4.29. Particionado de discos



Fuente: elaboración propia (2023).

En la figura 4.30. se observan todos los archivos en la misma ubicación.

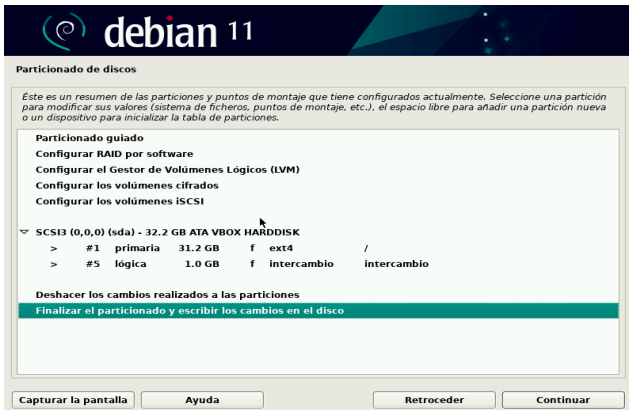
Figura 4.30. Selección del modo de particionado de disco



Fuente: elaboración propia (2023).

Finalmente, la figura 4.31. muestra el proceso final de configuración para la instalación del sistema operativo.

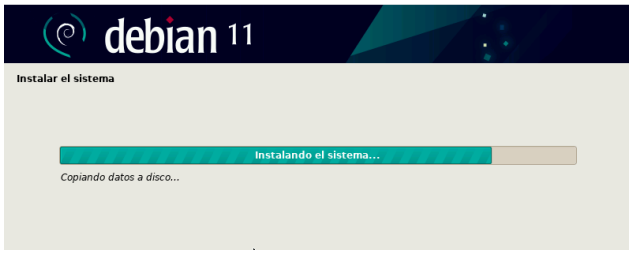
Figura 4.31. Resumen de particiones



Fuente: elaboración propia (2023).

Posteriormente se inicia el proceso de instalación que se detalla en la figura 4.32.

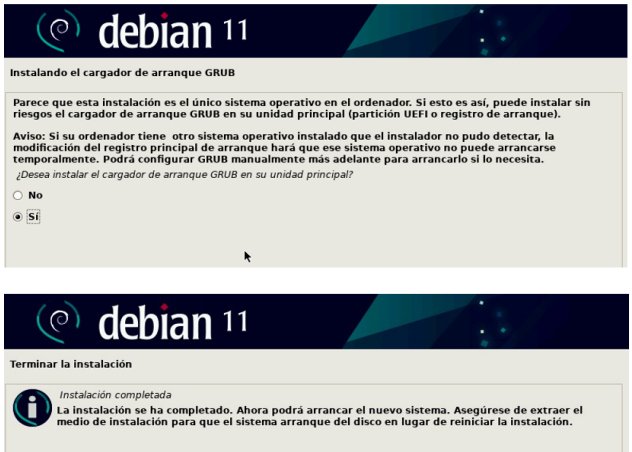
Figura 4.32. Inicio de la instalación



Fuente: elaboración propia.

En la figura 4.33. se muestra la selección de «No utilizar réplica de red» y seleccionar «Sí» para la instalación del GRUB en la unidad principal, ubicando la unidad /dev/sda.

Figura 4.33. Instalación del arranque y fin de la instalación



Fuente: elaboración propia (2023).

Entre las diferentes versiones de escritorio pueden cambiar un poco los diálogos o pantallas de presentación (figura 4.34.). Por ejemplo, el escritorio XFCE https://ftp.acc.umu.se/debian-cd/current-live/amd64/iso-hybrid/debian-live-12.9.0-amd64-xfce.iso

Figura 4.34. Instalación con escritorio en Linux

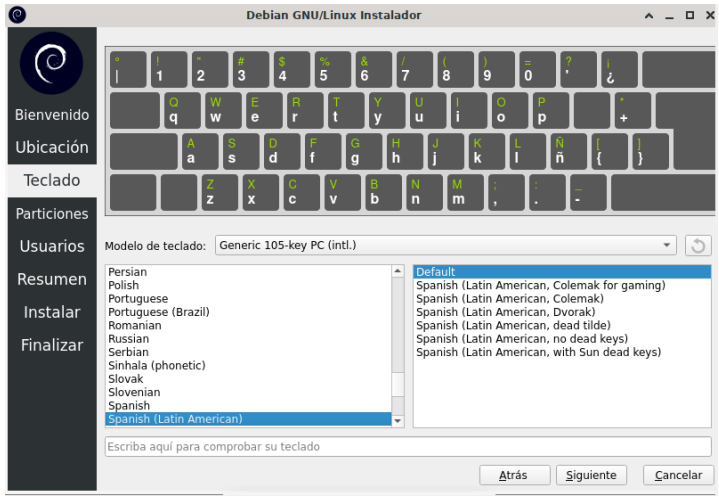
Se hace selección de región, tal como se muestra en la figura 4.35.

Figura 4.35. Selección de zona

Fuente: elaboración propia (2023).

Luego se debe seleccionar el teclado y el idioma, como se ve en la figura 4.36.

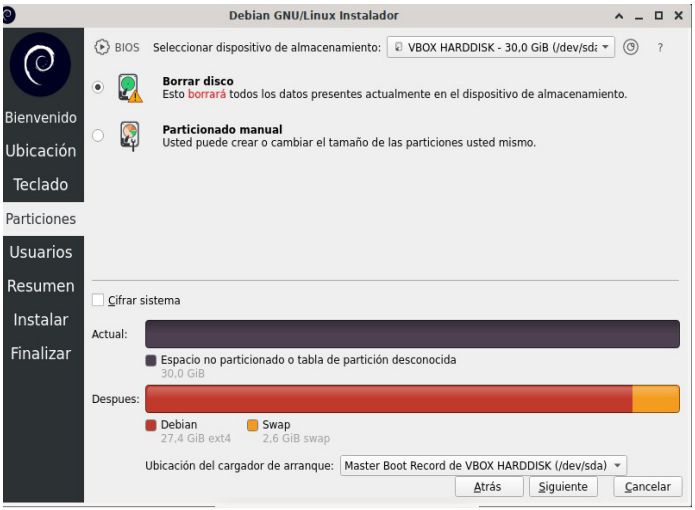
Figura 4.36. Selección de teclado



Fuente: elaboración propia (2023).

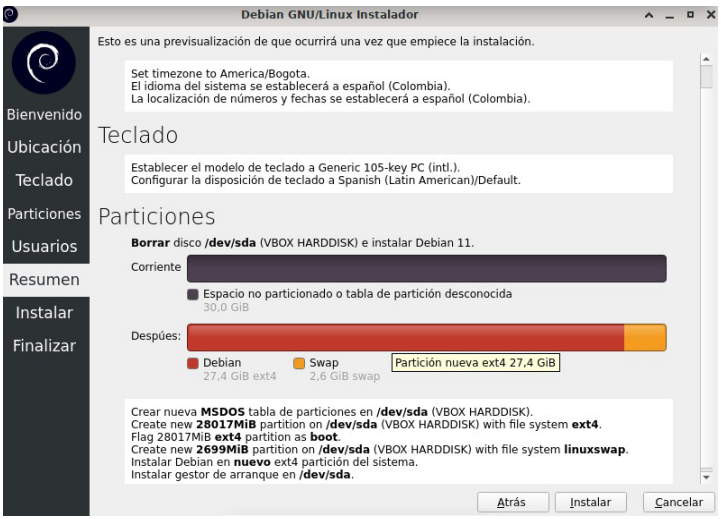
En la figura 4.37. se muestra la configuración de los parámetros del disco duro.

Figura 4.37. Configuración de disco



Por último, en la figura 4.38. se detalla el resumen de la configuración recomendada.

Figura 4.38. Resumen particionado

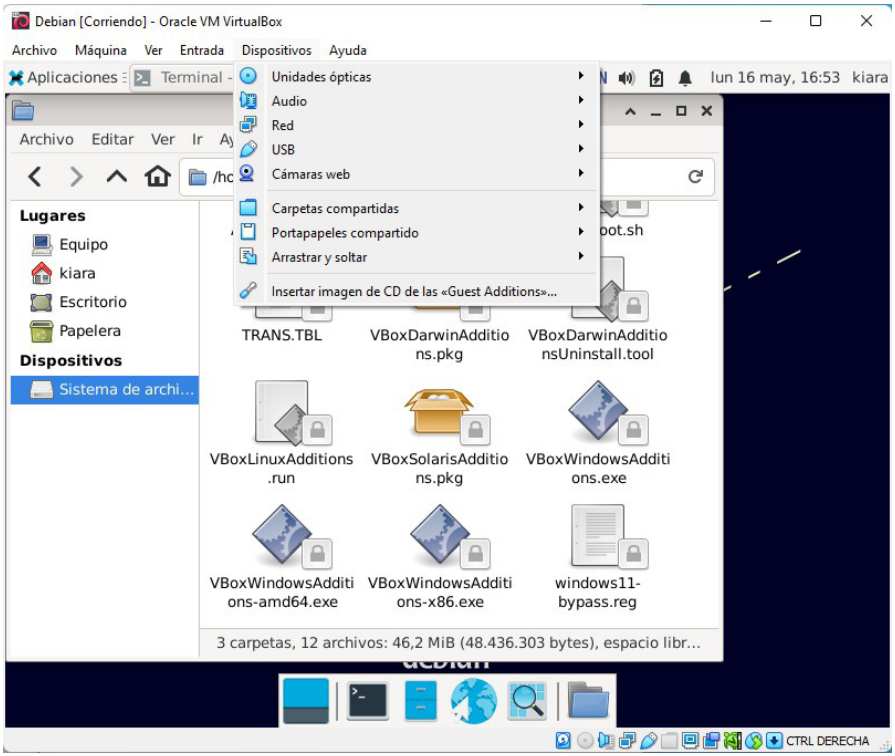


Fuente: elaboración propia (2023).

Una vez finalizada la instalación se debe actualizar el sistema desde una terminal *apt update & upgrade. Se recomienda* instalar los *Guest Additions* para tener una mejor integración entre el sistema operativo real y el de la máquina virtual (figura 4.39).

En el menú «Dispositivos» se habilitará la unidad con el instalador de los controladores y se copiará el contenido del CD virtual a una carpeta dentro de la máquina Linux.

Figura 4.39. Instalación de herramientas adicionales

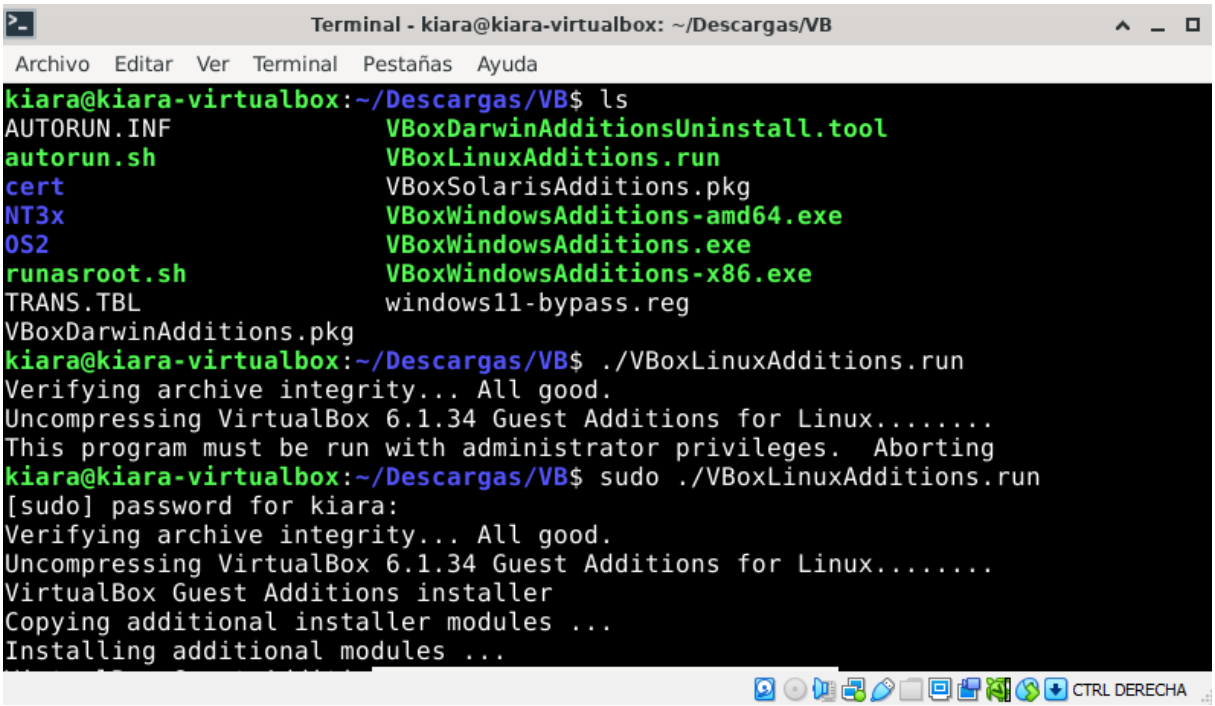


Fuente: elaboración propia (2023).

Desde una terminal y ubicados en la carpeta, se han de instalar los controladores (figura 4.40):

$ sudo ./VBoxLinuxAdditions.run

Figura 4.40. Ubicación de archivos



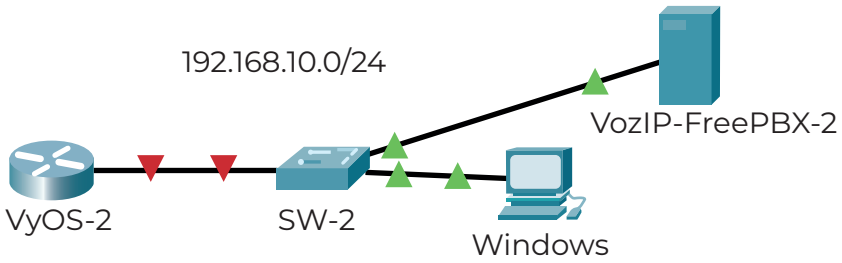
Fuente: elaboración propia (2023).

Una vez finalizada la instalación se reinicia la máquina virtual y se tendrá una mejor integración entre ambos sistemas operativos.

4.12. Acceso a la planta telefónica de cada sede

Inicialmente se configura la sede con la planta FreePBX. Para la estación Windows se ubica en Conexiones de red y se configura la red interna, con adaptador en Virtualbox solo como anfitrión; el adaptador en Windows se configura en el segmento de red para que se establezca comunicación entre la máquina real Windows y el servidor IP FreePBX. En la figura 4.41. se detalla la configuración de la sede 2.

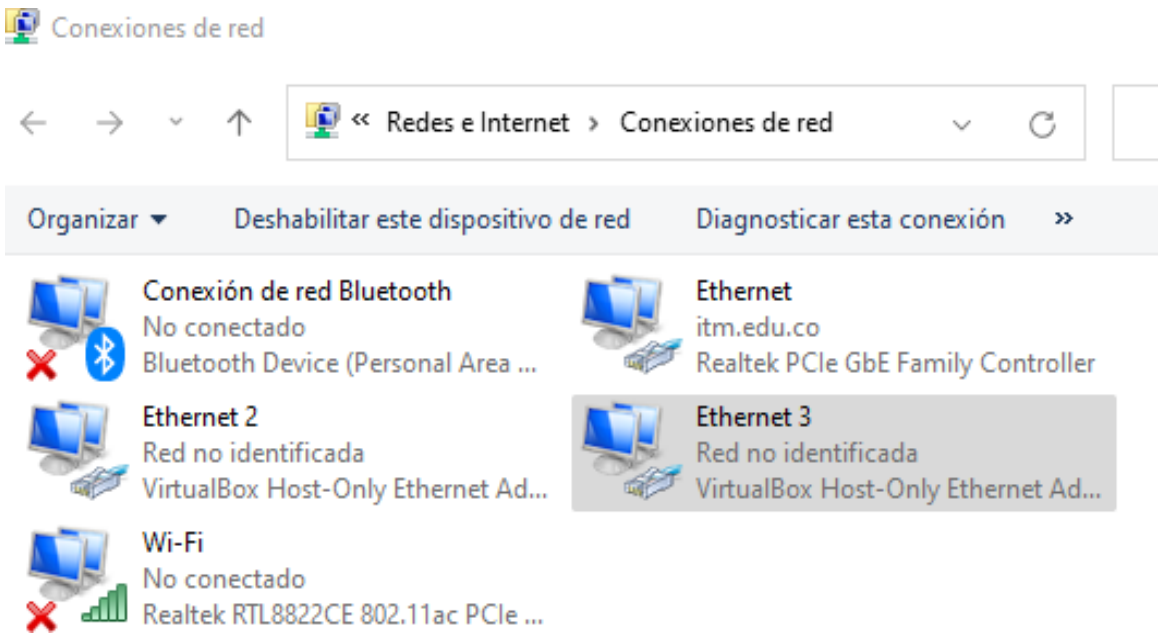
Figura 4.41. Sede local 2



Fuente: elaboración propia (2023).

En la figura 4.42. se muestran los adaptadores que deben configurarse para la máquina virtual.

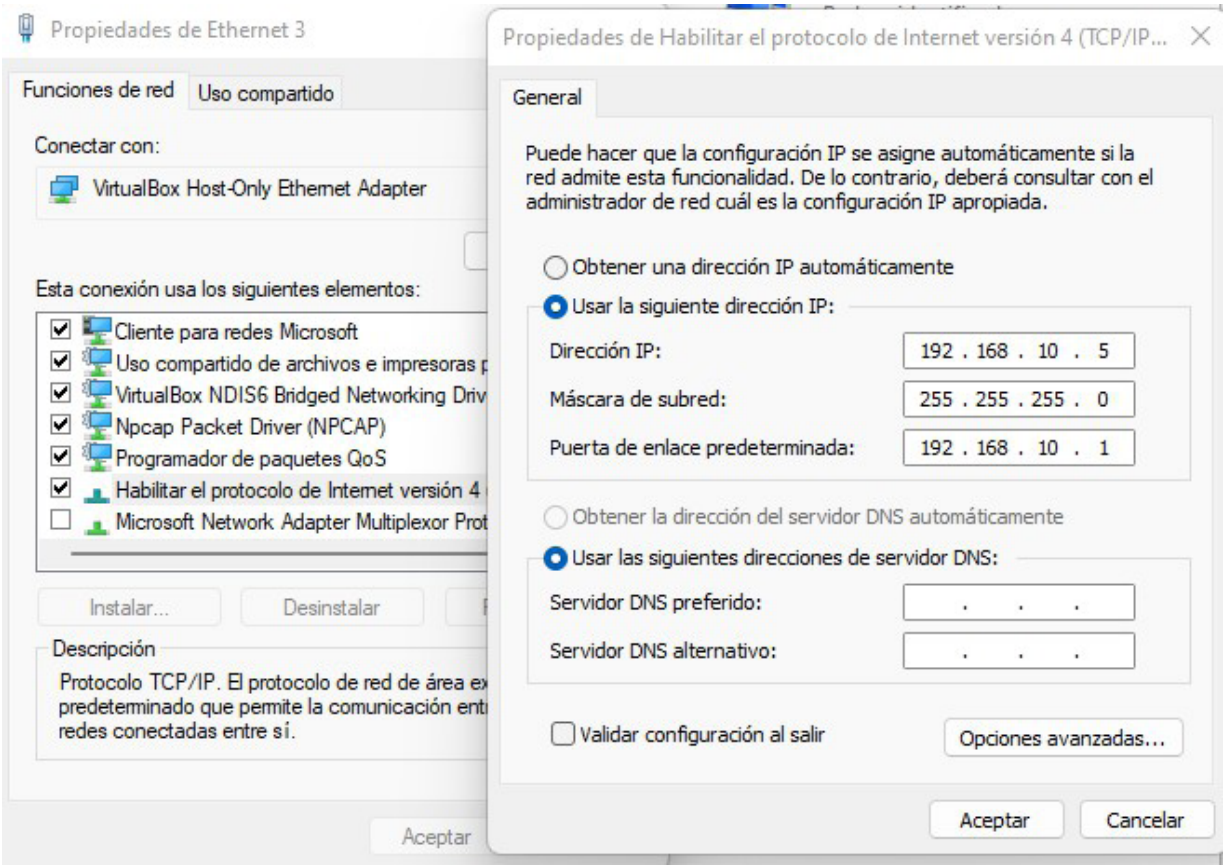
Figura 4.42. Estado de los adaptadores de red



Fuente: elaboración propia (2023).

En la figura 4.43., se detalla la configuración IP del adaptador de red.

Figura 4.43. Direccionamiento del adaptador

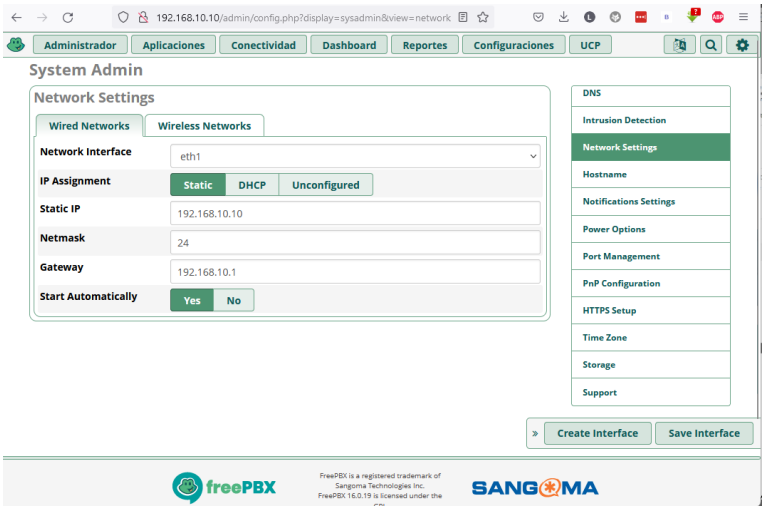


Fuente: elaboración propia (2023).

En FreePBX de la sede 2, ingresando por el módulo Administrador, Configuración del Sistema, se configura la dirección IP estática entre el segmento del adaptador virtual en Windows y la FreePBX con el *router* VyOS (figura 4.44.).

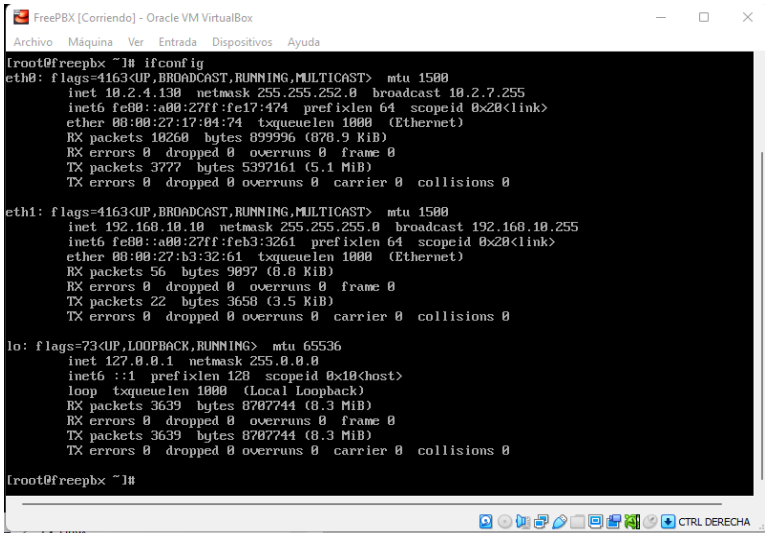
Una vez realizada la configuración se verifica el direccionamiento asignado a la planta FreePBX de la sede 2, tal como se aprecia en la figura 4.45.

Figura 4.44. Direccionamiento en la planta 2



Fuente: elaboración propia (2023).

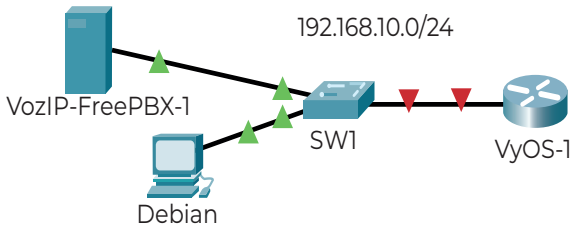
Figura 4.45. Estado del direccionamiento en la planta en sede 2



Fuente: elaboración propia (2023).

Finalmente, en la planta FreePBX-1 de la sede 1 también se debe configurar el respectivo direccionamiento para acceder a la planta desde la estación Linux en el mismo segmento de red (figura 4.46.).

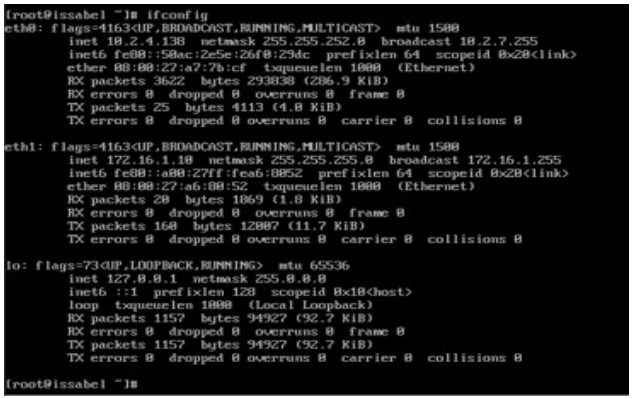
Figura 4.46. FreePBX de la sede local 1



Fuente: elaboración propia (2023).

Posteriormente se verifica el estado del direccionamiento en la FreePBX-1, cuyos resultados se aprecian en la figura 4.47.

Figura 4.47. Estado del direccionamiento en la planta en sede 1



Fuente: elaboración propia (2023).

Nótese que las plantas telefónicas de cada sede contienen un adaptador adicional en modo puente que permite el acceso a ellas, inicialmente desde una máquina real, para establecer las configuraciones iniciales; una vez configurada la red interna con sus respectivos segmentos de red ya no se requieren dichos adaptadores y se pueden desactivar. En este punto y para el ejemplo propuesto, verifique que la planta Issabel es accesible desde Linux y la planta FreePBX es accesible desde la máquina Windows.

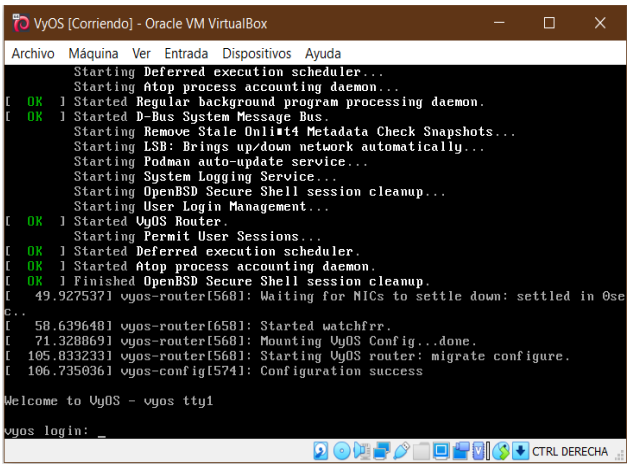
4.13. Instalación de los enrutadores (*routers*)

VyOS es un sistema operativo basado en Linux, específicamente en Debian, diseñado con el propósito de reemplazar las versiones comerciales de Cisco. VyOS es un sistema totalmente configurable que ofrece gran variedad de servicios: entre los más importantes están los más típicos en redes como DNS, DHCP, TELNET, SSH, firewall, etc. También se pueden configurar los protocolos de enrutamiento avanzado OSPF, RIP, BGP, como se hace en Cisco. Primero se deben habilitar dos adaptadores de red, uno para configurar los enlaces (preferible como modo anfitrión) y el segundo para las redes locales (preferible como modo puente). La figura 4.48. muestra la pantalla inicial del programa.

Luego de iniciar VyOS, se debe «loguear» en el sistema. Por defecto el usuario y contraseña

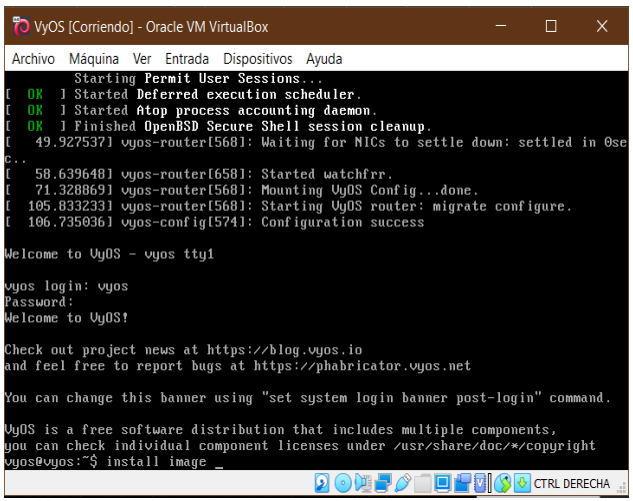
son *username* y *password:* vyos:vyos. Luego se debe ejecutar el comando *install image* para instalar VyOS en el disco duro (figura 4.49.).

Figura 4.48. Inicio VyOS



Fuente: elaboración propia (2023).

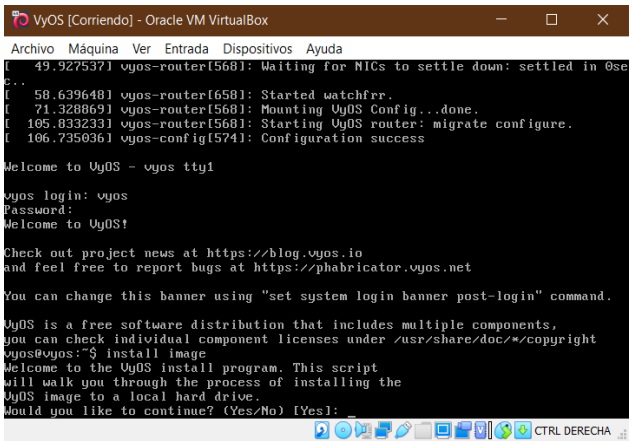
Figura 4.49. Instalación de VyOS



Fuente: elaboración propia (2023).

El sistema pregunta si se desea continuar, se selecciona «Sí» (figura 4.50), y luego se selecciona el tipo de particionado a realizar. VyOS requiere por defecto 2GB de disco duro (recomendable modo dinámico) y 1024 MB de memoria RAM.

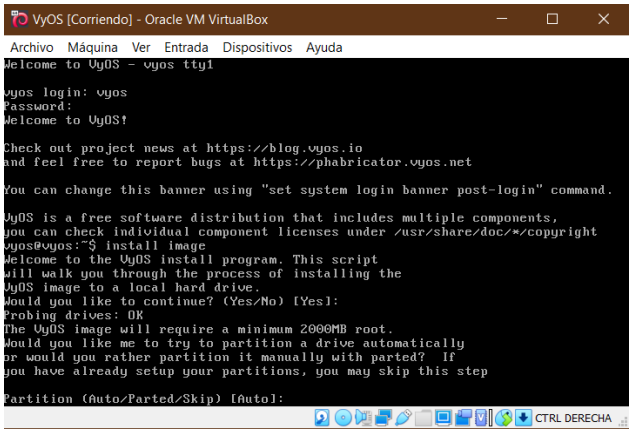
Figura 4.50. Particionado de disco



Fuente: elaboración propia (2023).

Luego VyOS solicita confirmar la instalación en el disco duro del sistema, tal como se ilustra en la figura 4.51.

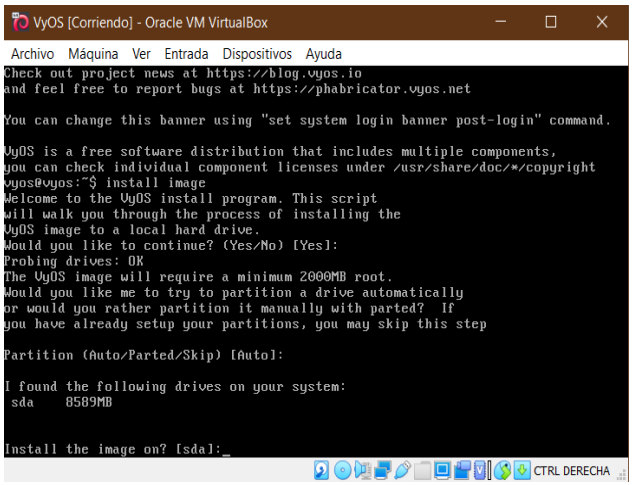
Figura 4.51. Sitio de instalación



Fuente: elaboración propia (2023).

Debe configurar el tamaño que desea utilizar en el disco duro del sistema. Luego de todo lo anterior, el asistente inicia el proceso de copia del sistema en el computador (figura 4.52.).

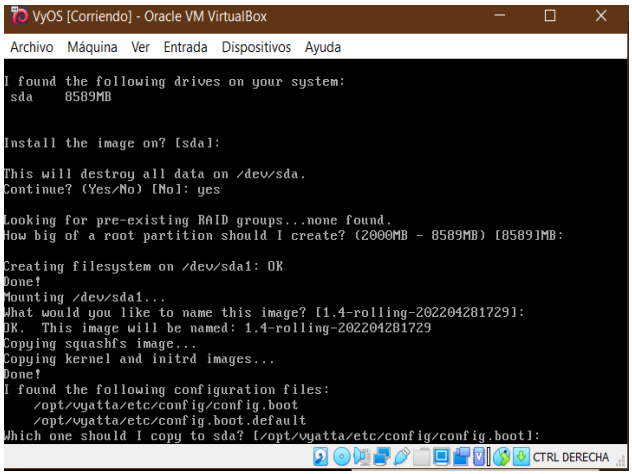
Figura 4.52. Confirmación de instalación



Fuente: elaboración propia (2023).

Luego el sistema solicita confirmar el disco donde se instalará la imagen y solicita el nombre de la imagen. Una vez finalizado el proceso de copia, el sistema solicita una nueva contraseña diferente a la que VyOS tiene por defecto, para el nuevo usuario. Debe indicarse la partición donde se instalará el gestor de arranque GRUB: VyOS usa GRUB para inicio o arranque del sistema (figura 4.53.).

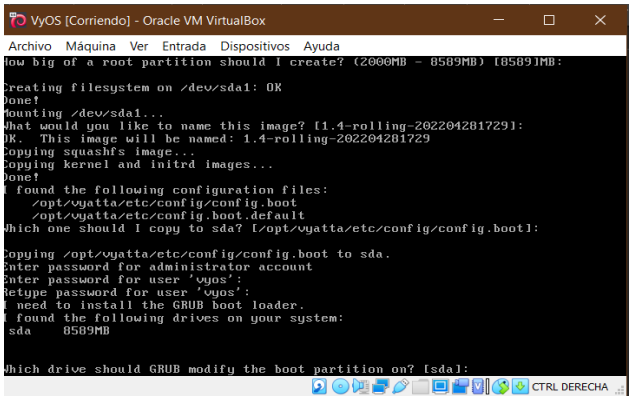
Figura 4.53. Instalación del arranque del sistema



Fuente: elaboración propia (2023).

Finalizado el proceso de instalación se debe reiniciar el sistema, ejecutando el comando *Reboot* o *Poweroff* para apagar. Luego se debe cambiar el orden de *booteo* (figura 4.54) en Virtualbox y quitar el *iso* de instalación de la unidad de cd virtual.

Figura 4.54. Finalización de la instalación



Fuente: elaboración propia (2023).

VyOS tiene varios modos de operación:

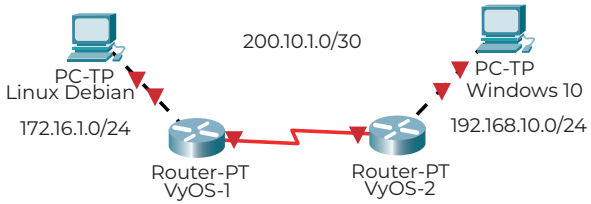
Configure -------- modo *router*

$ y # ----------modo operación básica y con privilegios de una terminal Linux.

4.14. Enrutamiento para interconexión de las sedes

La figura 4.55. detalla el esquema de enrutamiento planteado entre sedes.

Figura 4.55. Enrutamiento WAN



Fuente: elaboración propia (2023).

Para la interconexión de las sedes se tendrá en cuenta el esquema de direccionamiento planteado en la tabla 4.1.

Tabla 4.1. Direccionamiento

Dispositivo	Dirección IP	Máscara	*Gateway*
PC Debian, enp0s8	172.16.1.5	255.255.255.0	172.16.1.1
VozIP-Issabel, eth1	172.16.1.10	255.255.255.0	172.16.1.1
VyOS-1, eth1	172.16.1.1	255.255.255.0	N/A
VyOS-1, eth0 (inet)	200.10.1.1	255.255.255.252	N/A
PC Windows, Virtualbox host only	192.168.10.5	255.255.255.0	192.168.10.1
Voz Ip-FreePBX, eth1	192.168.10.10	255.255.255.0	192.168.10.1
VyOS-2, eth1	192.168.10.1	255.255.255.0	N/A
VyOS-2, eth0 (inet)	200.10.1.2	255.255.255.252	N/A

Fuente: elaboración propia (2023).

Se procederá a configurar RIP como protocolo de enrutamiento dinámico. Para ingresar en el modo configuración del *router*, ejecute el comando *Configure*. El comando *Show interfaces* despliega las interfaces disponibles. Configure las direcciones y para aplicar cualquier cambio ejecute *Commit.* Para guardar permanentemente utilice la instrucción *Save* (figura 4.56.).

Luego se verifica la configuración de ambas interfaces, tal como se aprecia en la figura 4.57.

Figura 4.56. Estado de las interfaces

```
vyos@vyos:~$ configure
[edit]
vyos@vyos# show interfaces
 ethernet eth0 {
     hw-id 08:00:27:a8:7d:a0
 }
 ethernet eth1 {
     hw-id 08:00:27:b0:c6:1f
 }
 loopback lo {
 }
[edit]
vyos@vyos# set interfaces ethernet eth0 address 200.10.1.1/30
[edit]
vyos@vyos# commit
[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos# _
```

Fuente: elaboración propia (2023).

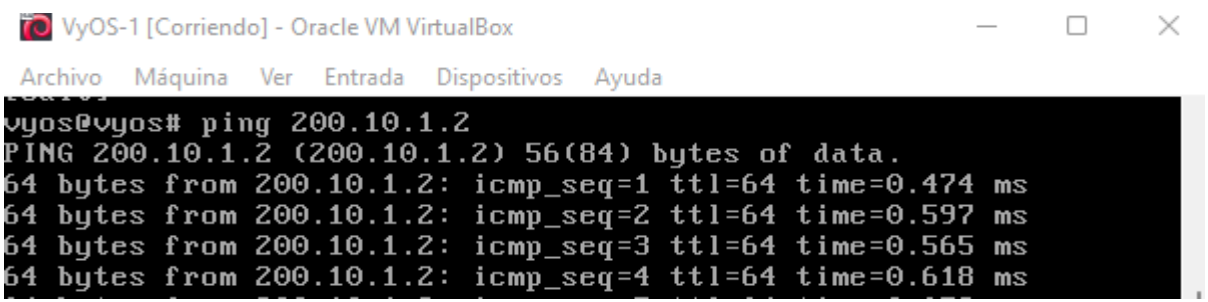
Figura 4.57. Direcciones en las interfaces

```
vyos@vyos# show interfaces
 ethernet eth0 {
     address 200.10.1.1/30
     hw-id 08:00:27:a8:7d:a0
 }
 ethernet eth1 {
     address 172.16.1.1/24
     hw-id 08:00:27:b0:c6:1f
 }
 loopback lo {
 }
[edit]
vyos@vyos#
```

Fuente: elaboración propia (2023).

Se realiza la misma configuración en el *router* VyOS-2 y se prueba la conectividad entre ambos enrutadores o *routers* (figura 4.58.).

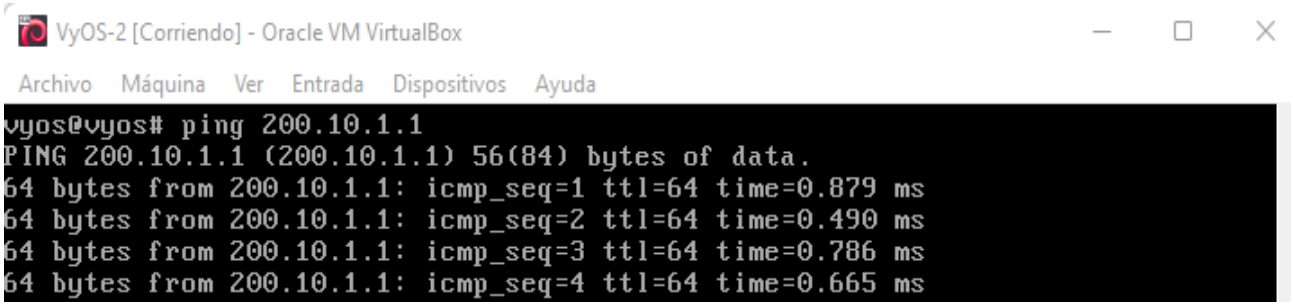
Figura 4.58. Conectividad *router* de sede 1



Fuente: elaboración propia (2023).

En ambas sedes se prueba la conectividad (figura 4.59.).

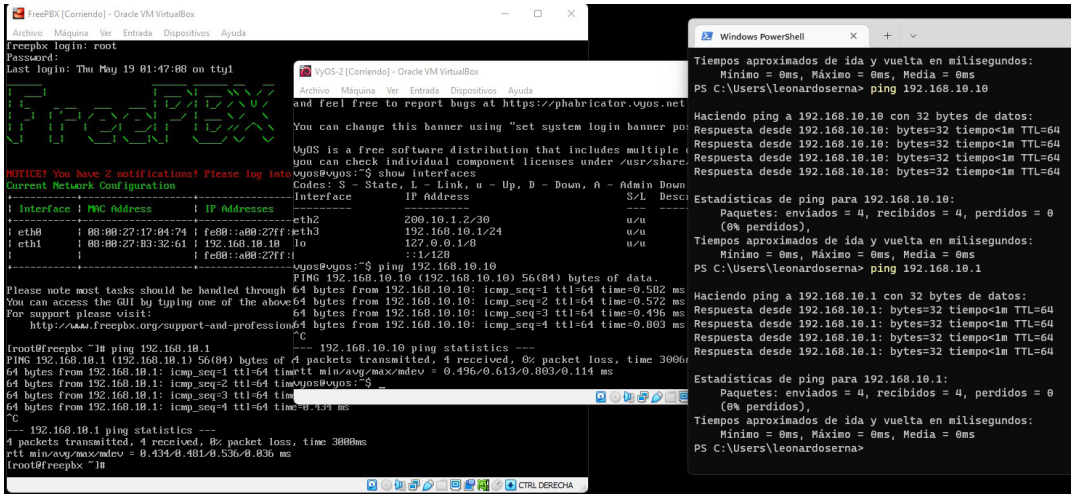
Figura 4.59. Conectividad *router* de sede 2



Fuente: elaboración propia (2023).

Se procede a configurar las demás interfaces y para que ambas sedes se puedan ver, se enrutará el tráfico entre los enrutadores o *routers.* En esta práctica se utiliza el protocolo RIP. Al configurar cada sede (VyOS-1 y VyOS-2), se prueba la conectividad entre cada dispositivo y el *router* (figura 4.60).

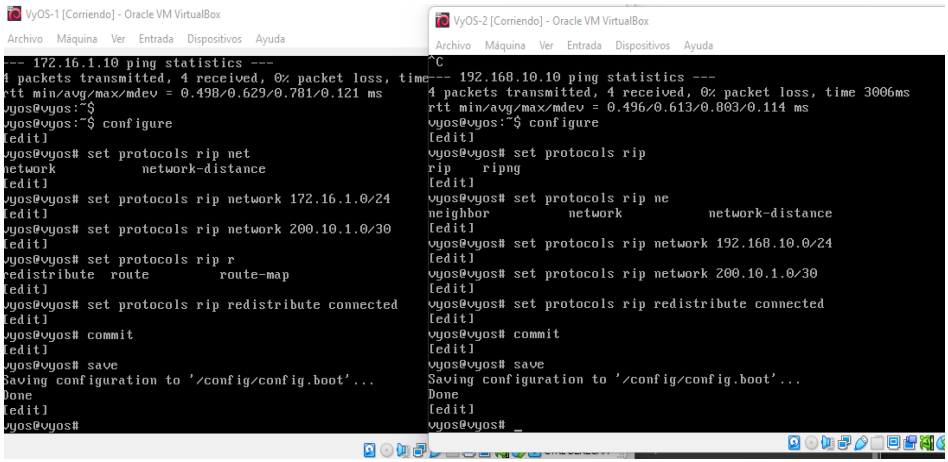
Figura 4.60. Conectividad con el *router*



Fuente: elaboración propia (2023).

Ahora se procede a configurar el protocolo de enrutamiento y a divulgar las redes, tal como se aprecia en la figura 4.61.

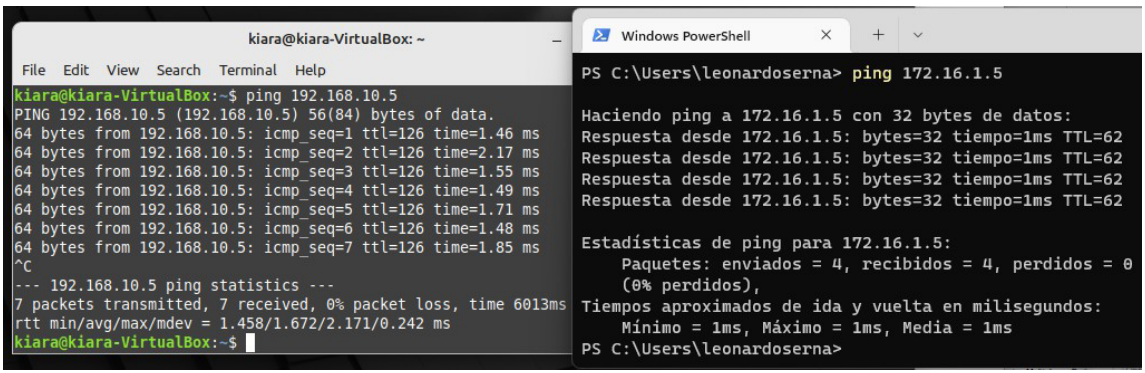
Figura 4.61. Enrutamiento entre los *router*



Fuente: elaboración propia (2023).

Adicionalmente, ya se puede verificar conectividad entre las sedes, lo que garantizará que los clientes de VoIP se puedan comunicar al haber conectividad entre las plantas telefónicas de sede 1 y sede 2 (figura 4.62.).

Figura 4.62. Conectividad entre sedes

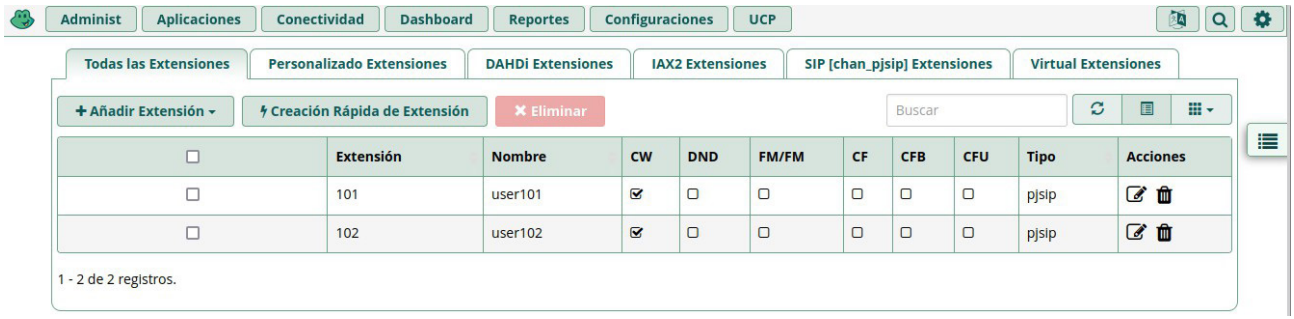


Fuente: elaboración propia (2023).

4.15. Configuración de la troncal

Inicialmente se verifica que cada planta tenga acceso, para lo cual se crean dos extensiones (figura 4.63.) y se realizan pruebas de comunicación.

Figura 4.63. Interfaz en sede 1

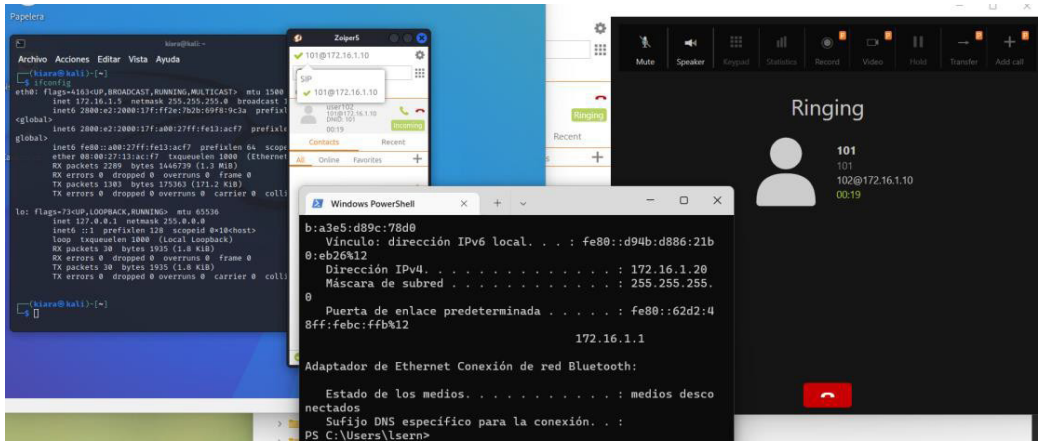


Fuente: elaboración propia (2023).

En este caso se han configurado dos estaciones de la sede 1 con la dirección 172.16.1.15 y 172.16.1.120, y se ha instalado el cliente en la estación Linux # dpkg -i Zoiper***.deb

En la figura 4.64. se puede observar la conexión entre ambas terminales.

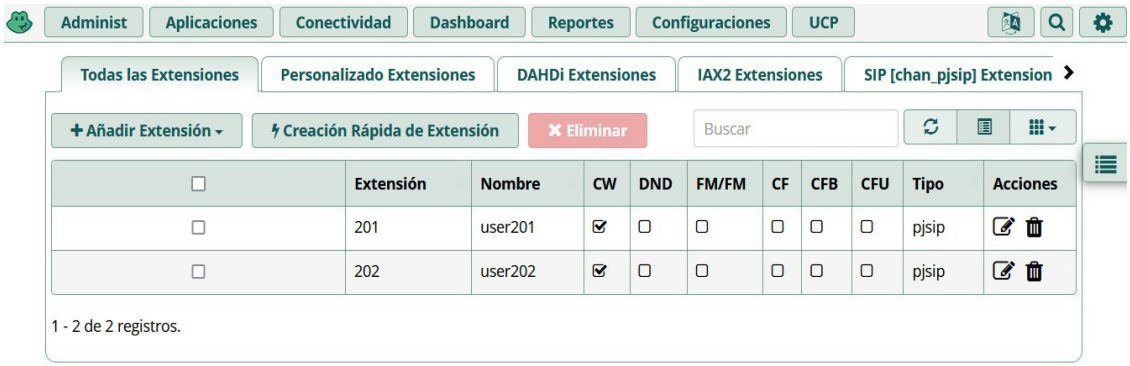
Figura 4.64. Conectividad entre clientes



Fuente: elaboración propia (2023).

En la sede 2 se realiza el mismo procedimiento (figura 4.65.) y se verifica el acceso a la planta telefónica.

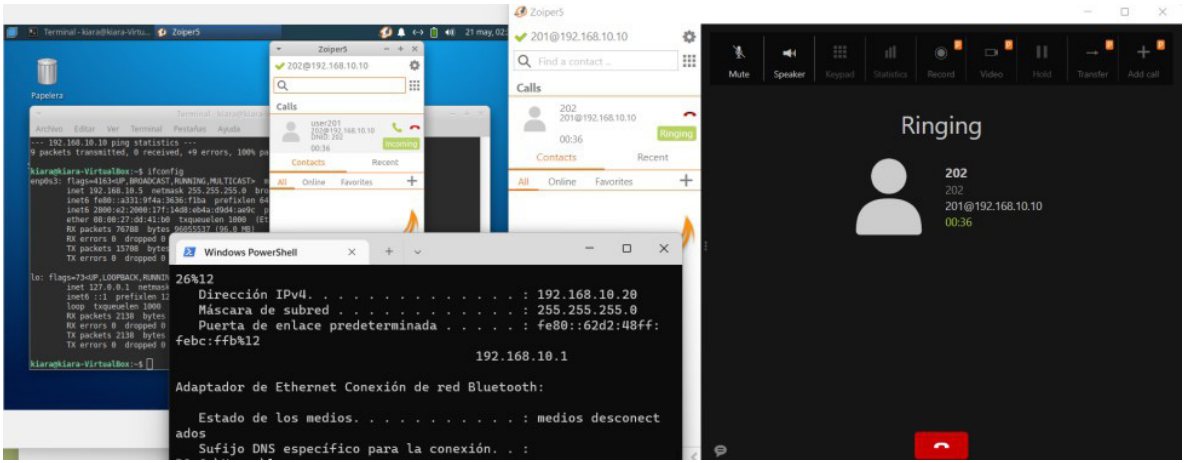
Figura 4.65. Interfaz en sede 2



Fuente: elaboración propia (2023).

En la figura 4.66. se visualiza la conectividad entre usuarios.

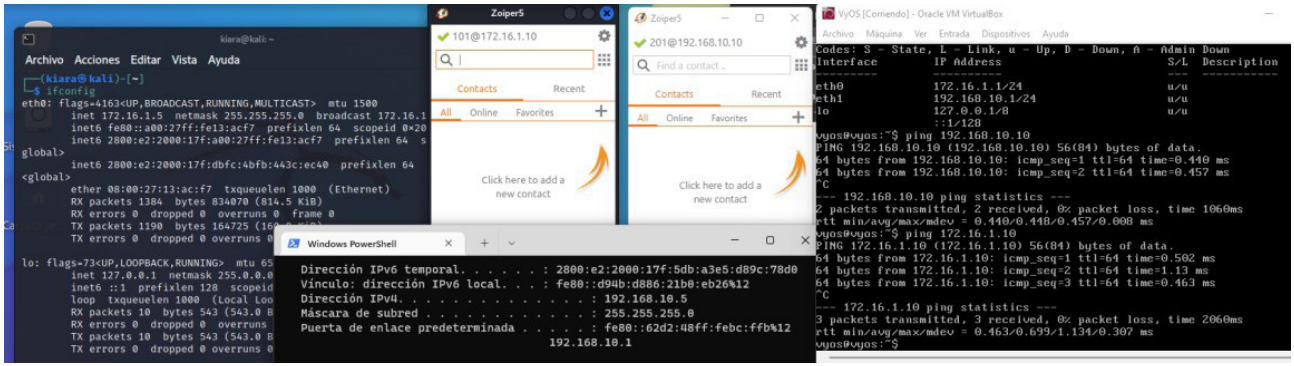
Figura 4.66. Conectividad entre clientes



Fuente: elaboración propia (2023).

En la figura 4.67. se detalla la conectividad entre todas las plantas y el equipo.

Figura 4.67. Resumen de conectividad



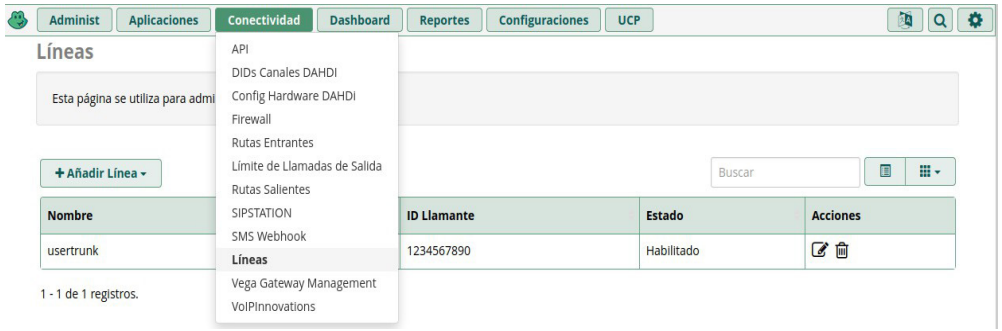
Fuente: elaboración propia (2023).

Al configurar las plantas con FreePBX para que funcionen con el servicio SIP Trunking, deben realizarse cambios de configuración en tres áreas:

- Conectividad→ Líneas (troncales)
- Conectividad→ Rutas entrantes
- Conectividad→ Rutas de salida

Se procede a la creación de la troncal en cada una de las plantas correspondientes de sede. Ingresando por el menú Conectividad / Líneas (*trunk*), se creará la troncal con su respectivo nombre (figura 4.68.)

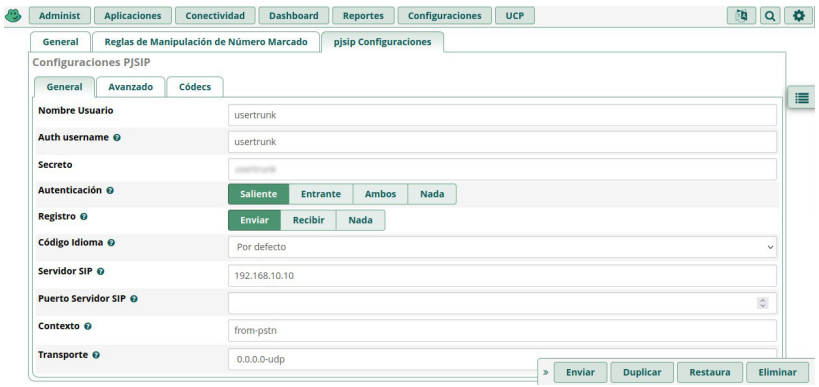
Figura 4.68. Menú conectividad



Fuente: elaboración propia (2023).

Por el menú Configuraciones PJSIP / General, se agrega el usuario con su respectiva contraseña. De igual forma se debe ingresar la dirección del servidor de Voz IP con el cual establecerá la troncal (figura 4.69.). Nótese que para el ejemplo, la sede 1 está direccionada al servidor de la sede 2.

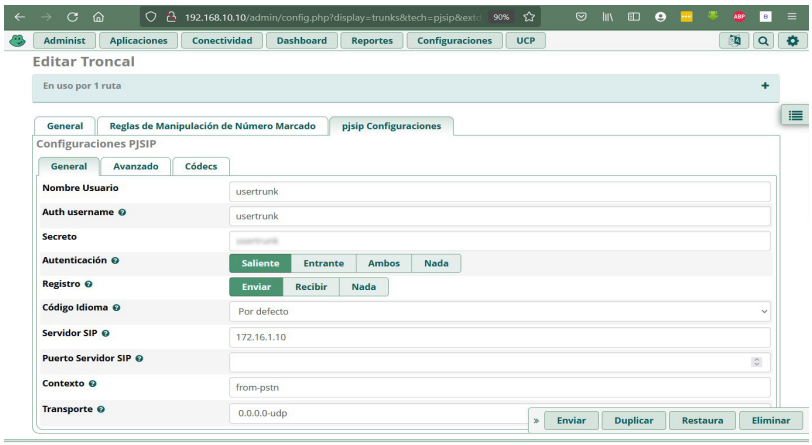
Figura 4.69. Configuración de conectividad



Fuente: elaboración propia (2023).

En la sede 2 deberá aparecer relacionada la dirección del servidor de Voz IP, tal como se aprecia en la figura 4.70.

Figura 4.70. Configuración general



Fuente: elaboración propia (2023).

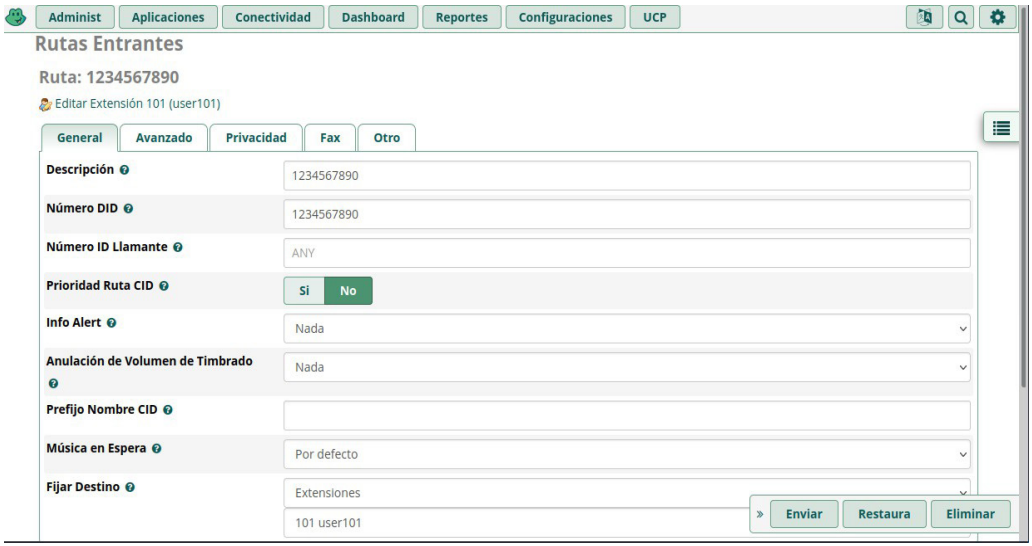
Seguidamente, en la figura 4.71 se ilustra la configuración de las rutas entrantes donde se ha de agregar.

Figura 4.71. Conectividad y rutas

Fuente: elaboración propia (2023).

Se define un identificador y el grupo de extensiones a las que llegarán las llamadas (figura 4.72.).

Figura 4.72. Menú general



Fuente: elaboración propia (2023).

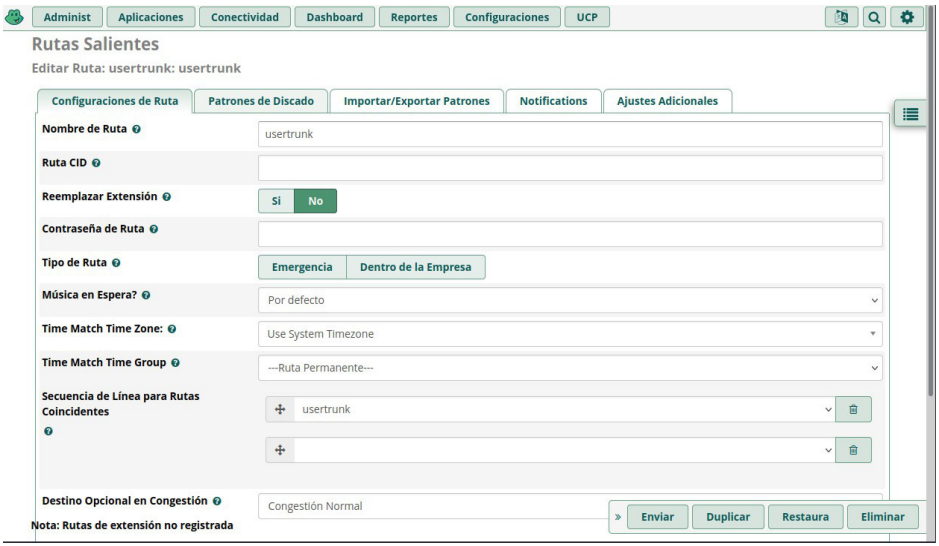
Posteriormente han de configurarse las rutas salientes, como se muestra en la figura 4.73.

Figura 4.73. Rutas salientes

Fuente: elaboración propia (2023).

Acá es necesario definir el nombre de la ruta y seleccionar la secuencia de líneas donde debe aparecer el nombre de la troncal, y seleccionarla (figura 4.74.).

Figura 4.74. Configuración de rutas

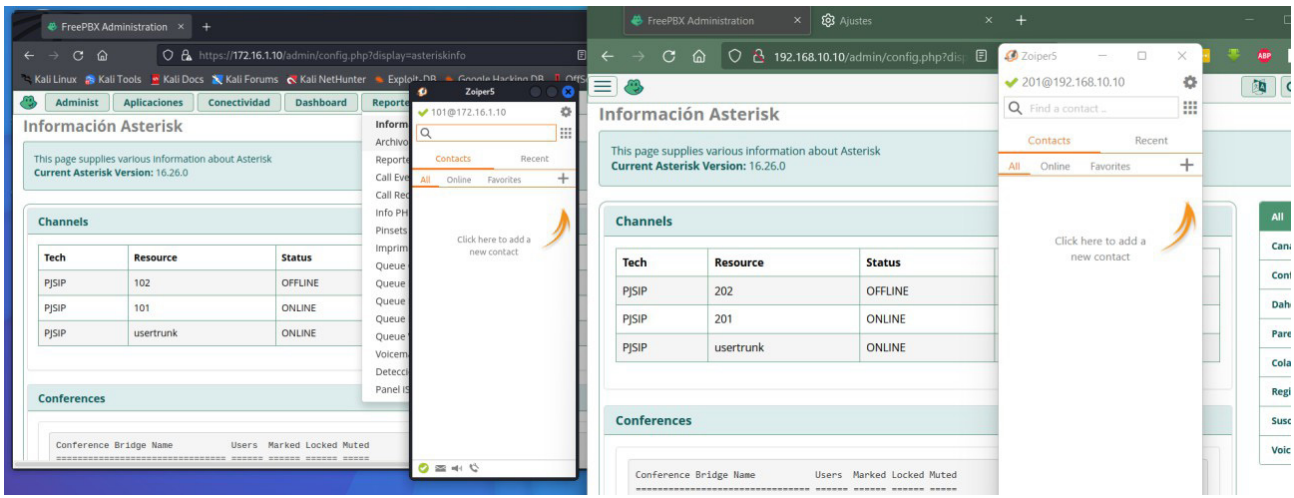


Fuente: elaboración propia (2023).

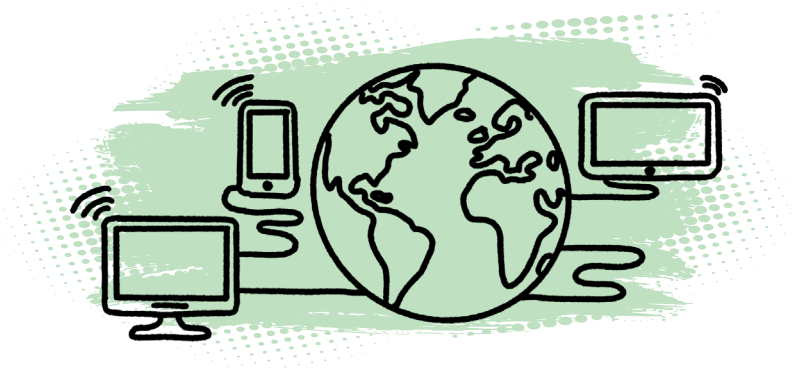
Una vez realizados cada uno de los cambios, dar clic en «Enviar» y posteriormente en «Aplicar configuración» que aparece resaltado en rojo en el menú superior.

Finalmente, en la figura 4.75. se puede observar el estado de la troncal en línea y el estado de las extensiones, ingresando por Reportes / Información de Asterisk.

Figura 4.75. Estado de la troncal entre ambas sedes



Fuente: elaboración propia (2023).



Conclusiones

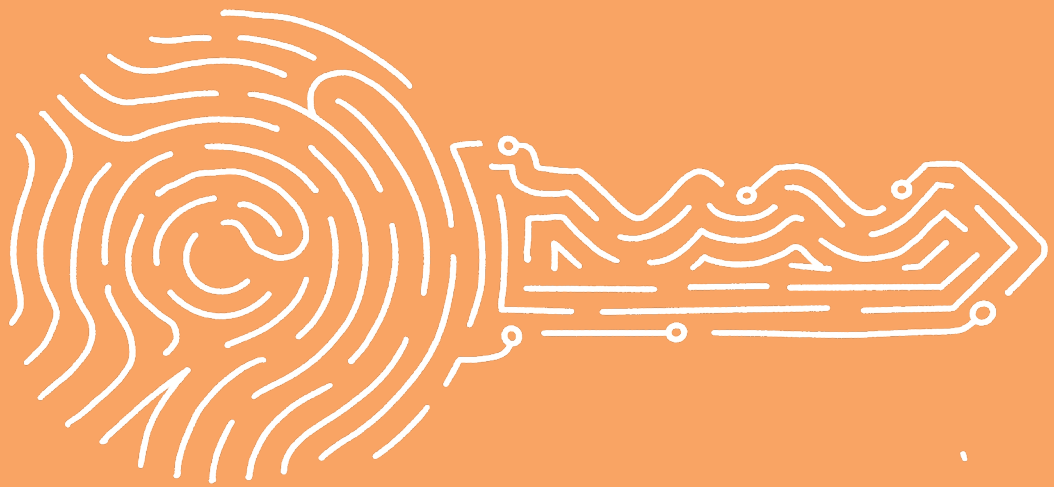
La correcta selección de terminales y sistemas VoIP es crucial para asegurar la calidad y fiabilidad del servicio. Es importante considerar las necesidades específicas de la organización, incluyendo el tipo de terminales (*hardware* o *software*), el sistema operativo para la virtualización y la capacidad de los terminales en términos de funcionalidades y compatibilidad con otros componentes de la red (Blokdyk, 2019).

En este sentido, la configuración y virtualización eficiente de la planta telefónica junto con la adecuada configuración de la máquina virtual y del sistema operativo permiten una mayor flexibilidad y escalabilidad en la gestión de la infraestructura VoIP. La elección entre Windows y Linux para la virtualización debe basarse en los requerimientos de seguridad, estabilidad y costos operativos. La implementación de FreePBX como sistema operativo de gestión facilita la administración de extensiones y troncales, optimizando el flujo de comunicaciones dentro de la organización.

Por último, la construcción y gestión de troncales telefónicas es esencial para garantizar una comunicación fluida y efectiva entre diferentes sedes de la organización. Un adecuado acceso y configuración de las troncales permite una mejor administración del tráfico de llamadas, reduciendo posibles puntos de falla y mejorando la continuidad del servicio. La integración de troncales también facilita la centralización de las comunicaciones, optimizando recursos y mejorando la eficiencia operativa.

CAPÍTULO 5.

Seguridad de la aplicación de FREEPBX (Voz sobre IP)



Introducción

En este capítulo se aborda la seguridad en la implementación de FreePBX, una aplicación de VoIP. En este contexto la seguridad se convierte en un tema indispensable ante la creciente prevalencia de amenazas informáticas que pueden comprometer la integridad y la confidencialidad de las comunicaciones. A medida que las tecnologías de comunicación basadas en *software* ganan popularidad, es fundamental implementar soluciones de seguridad robustas para los sistemas que manejan información sensible. Esta etapa detalla los procedimientos para auditar y fortalecer la seguridad de un sistema FreePBX, incluyendo la implementación de *firewalls* (cortafuegos), el escaneo de puertos y la configuración de reglas específicas para mitigar posibles amenazas.

Como se describió en el capítulo 3 sobre generalidades de la seguridad en el entorno VoIP, la seguridad se está convirtiendo en un tema cada vez más importante en el entorno de las comunicaciones actuales, se está volviendo vital considerar cómo proteger un sistema antes de incorporarlo en las operaciones de implementación cotidiana. Debido al creciente interés en la comunicación de medios basada en *software* (por ejemplo, la aplicación VoIP), se necesitan soluciones de seguridad que hagan que estas tecnologías sean lo suficientemente confiables para transportar información sensible (Orebaugh y Pinkard, 2008).

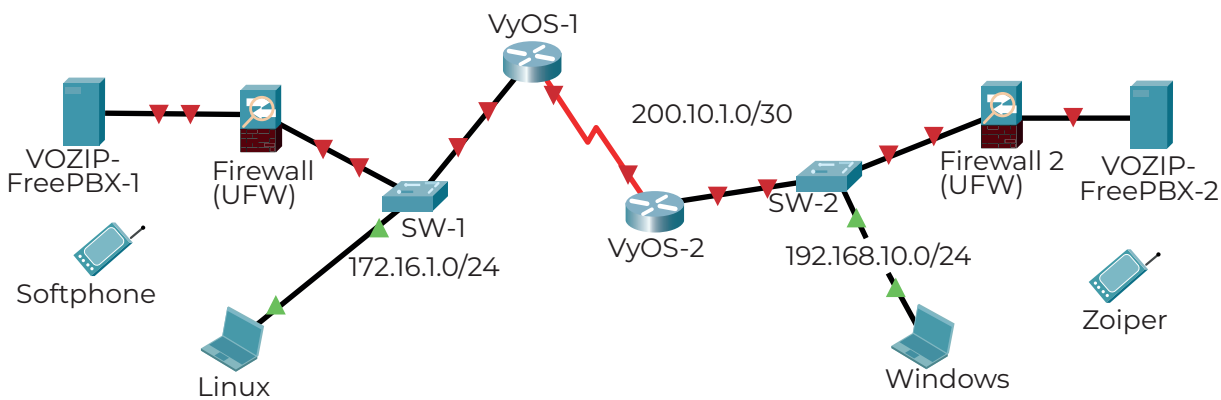
El 2 de noviembre de 1988 la historia de Internet y la seguridad informática cambiaron radicalmente a causa del «gusano Morris» que hizo el mayor daño informático hasta ese momento, con un ataque a 6 000 computadoras de las 60 000 que estaban conectadas a Internet. El primer ciberataque ocurrió en Francia en 1834, cuando dos banqueros franceses, François y Joseph Blanc, utilizan un telégrafo óptico para sus propios fines consiguiendo información antes que sus competidores (Sardanyés, 2024).

El sistema VoIP debería ser más seguro que otros sistemas informáticos. Estas aplicaciones cuentan con su propio sistema operativo, lo que significa que existe la posibilidad de que tenga algún tipo de vulnerabilidad y debería ser parcheado lo antes posible. Los delincuentes informáticos pueden producir muchos ataques en la red VoIP, como DoS y DDOS, descifrado de contraseñas, rastreo, SQL-Injection, modificación de datos, etc. Hay más problemas de seguridad disponibles que deberían ser seguros en la red VoIP (Sisalem et al., 2009), como gestión de registros, seguridad de red interna, ataque de *malware*, etc., haciendo la salvedad de que si bien no son previsibles todos los riesgos, estos al menos deben ser considerados para adelantar los controles requeridos para su mitigación (Suthar & Rughani, 2020).

Se propone una solución para contrarrestar las posibles amenazas para la protección de la red VoIP propuesta (figura 5.1.), consistente en agregarle a cada sistema un *firewall* (UFW) y la aplicación FreePBX para brindarle seguridad a la máquina FreePBX 172.16.1.10

Lo primero es hacer una auditoría a cada sistema para observar posibles vulnerabilidades, con herramientas para detectar puertos abiertos, servicios y protocolos, etc. En este caso práctico se implementó la aplicación NMAP (Network Mapper), una herramienta de código abierto para la exploración de redes y la auditoría de seguridad (Orebaugh y Pinkard, 2008), diseñada para escanear rápidamente grandes redes, aunque funciona bien contra *hosts* individuales. NMAP utiliza paquetes de IP sin

Figura 5.1. Red troncal con firewall



Fuente: elaboración propia (2023).

procesar de forma novedosa para determinar qué *hosts* están disponibles en la red, qué servicios (nombre y versión de la aplicación) ofrecen esos *hosts*, qué sistemas operativos (y versiones de SO) están ejecutando, qué tipo de filtros de paquetes/cortafuegos están en uso y muchas otras características.

Al realizar un escaneo de puertos de la dirección IP del sistema operativo, se encontró que muchos puertos estaban abiertos y podían ser susceptibles a algún tipo de amenaza, como se observa en la figura 5.2.

Figura 5.2. Escaneo de puertos

```
kiara@kiara-vmwarevirtualplatform:~$ nmap -p 1-65535 172.16.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-30 17:46 -05
Nmap scan report for 172.16.1.10
Host is up (0.0100s latency).
Not shown: 65515 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
81/tcp   open  hosts2-ns
82/tcp   open  xfer
83/tcp   open  mit-ml-dev
84/tcp   open  ctf
111/tcp  open  rpcbind
443/tcp  open  https
3306/tcp open  mysql
5000/tcp open  upnp
5222/tcp open  xmpp-client
6002/tcp open  X11:2
6006/tcp open  X11:6
6081/tcp open  geneve
6082/tcp open  p25cai
8001/tcp open  vcom-tunnel
8003/tcp open  mcreport
8088/tcp open  radan-http
```

Fuente: elaboración propia (2023).

Después de verificar por medio de un escaneo de puertos y vulnerabilidades, se hace un *hardening* (endurecimiento o reforzamiento) del sistema operativo para que funcione de manera más segura con las reglas del *firewall* UFW.

El primer paso es activar el *firewall* (UFW) con *sudo ufw enable*; luego de que esté habilitado se implementan las reglas para que el sistema operativo quede más protegido de las diferentes amenazas, como se puede visualizar en la figura 5.3.

Figura 5.3. Implementar reglas de *firewall* (UFW)

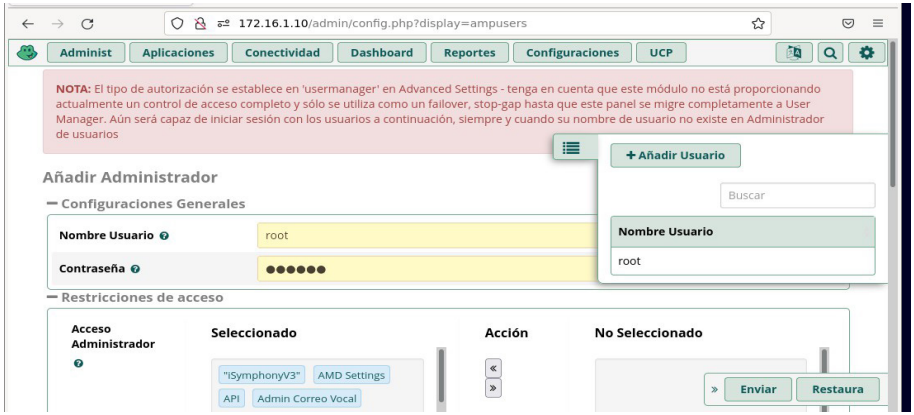
```
[root@freepbx ~]# sudo ufw deny 100:10000/tcp
Rule added
Rule added (v6)
[root@freepbx ~]# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp (SSH)               ALLOW IN    Anywhere
224.0.0.251 5353/udp (mDNS) ALLOW IN    Anywhere
21/tcp                     DENY IN     Anywhere
53/tcp                     DENY IN     Anywhere
100:10000/tcp              DENY IN     Anywhere
22/tcp (SSH (v6))          ALLOW IN    Anywhere (v6)
ff02::fb 5353/udp (mDNS)   ALLOW IN    Anywhere (v6)
21/tcp (v6)                DENY IN     Anywhere (v6)
53/tcp (v6)                DENY IN     Anywhere (v6)
100:10000/tcp (v6)         DENY IN     Anywhere (v6)

[root@freepbx ~]# S
```

Fuente: elaboración propia (2023).

5.1. Instalar *firewall* en FreePBX

Lo primero es entrar a la consola de Administración de la PBX con la dirección IP (en este caso la 172.16.1.10). Pide el usuario y la contraseña para trabajar en el entorno gráfico donde se encuentran todas las herramientas necesarias para hacer una buena gestión de los procesos (figura 5.4.).

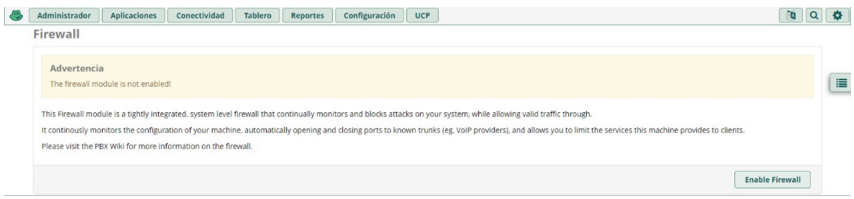
Figura 5.4. Entorno web de FreePBX

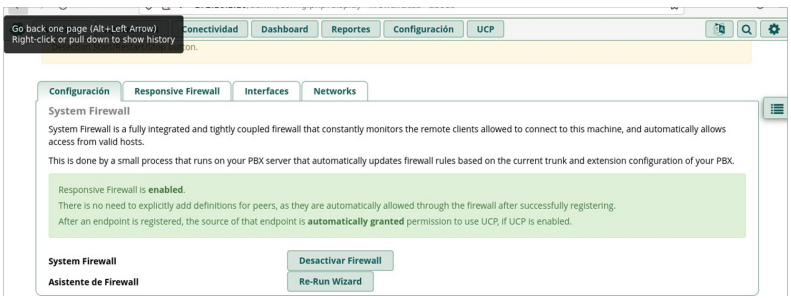


Fuente: elaboración propia (2023).

Luego se accede a la pestaña «Conectividad» y se ubica en *firewall* para habilitarlo (figura 5.5.).

Figura 5.5. Habilitar *firewall*

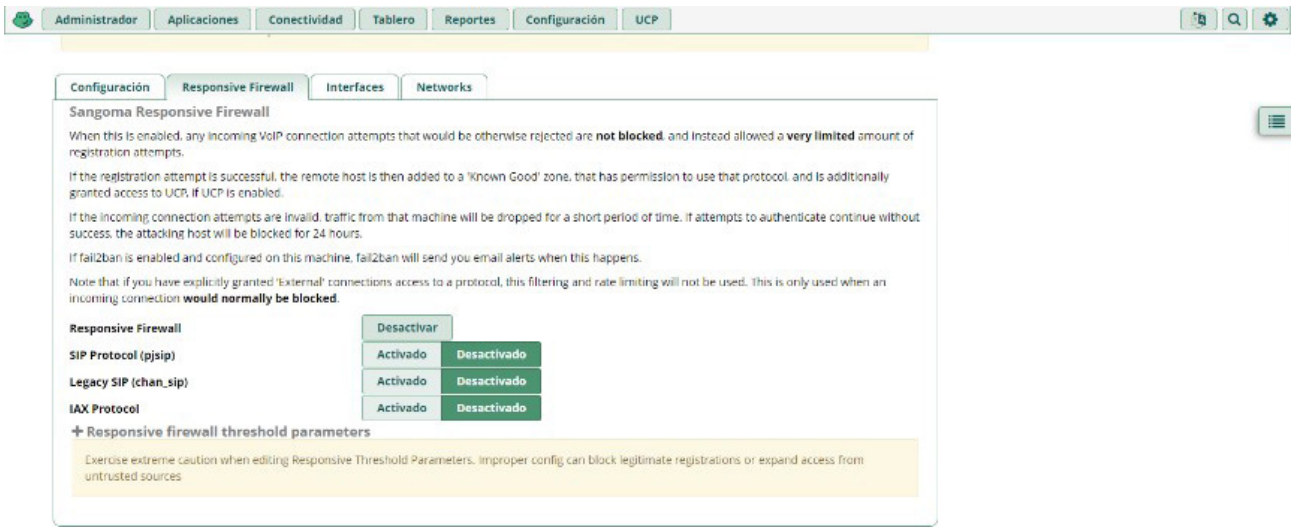




Fuente: elaboración propia (2023).

Después se continúa habilitando las funciones *«Responsive/Firewall»*. Esta función agrega dinámicamente una dirección IP al *firewall* una vez que el teléfono se ha conectado con éxito desde la IP. Esta IP se eliminará automáticamente cuando el teléfono se desconecte (figura 5.6). Se habilitan todas las pestañas de los tres servicios indicados para inhabilitar conexiones entrantes desconocidas y bloquearlas durante un tiempo determinado.

Figura 5.6. Habilitar reglas del firewall



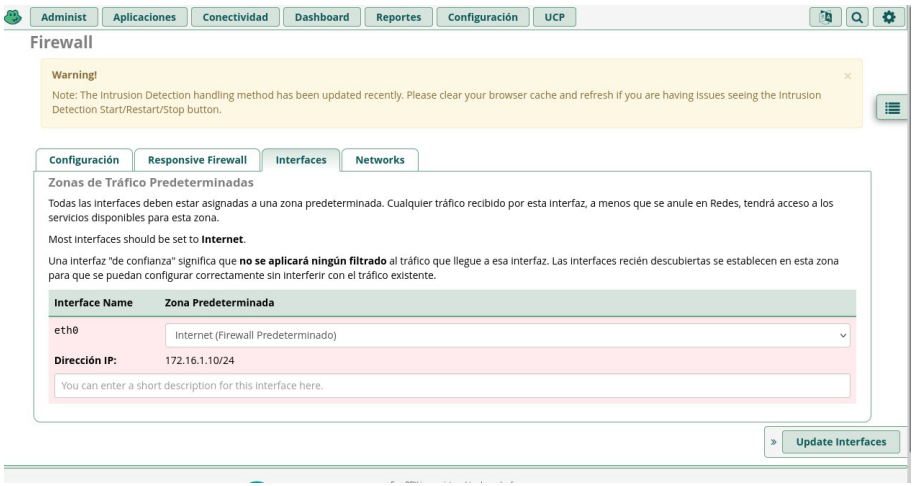
Fuente: elaboración propia (2023).

Luego se da clic en la pestaña «Interfaces» (figura 5.7.) para cambiar la zona de la interfaz de red de la PBX.

Es necesario cambiar «eth0» de la zona «Confiable» a la zona «Internet», seleccionándola del menú desplegable debajo de «Zona predeterminada». Haga clic en «Actualizar interfaces» en la parte inferior derecha para confirmar el cambio.

Importante**:** para aplicar sus cambios a un sistema en ejecución de inmediato, deshabilite/vuelva a habilitar el *firewall* o reinicie la FreePBX.

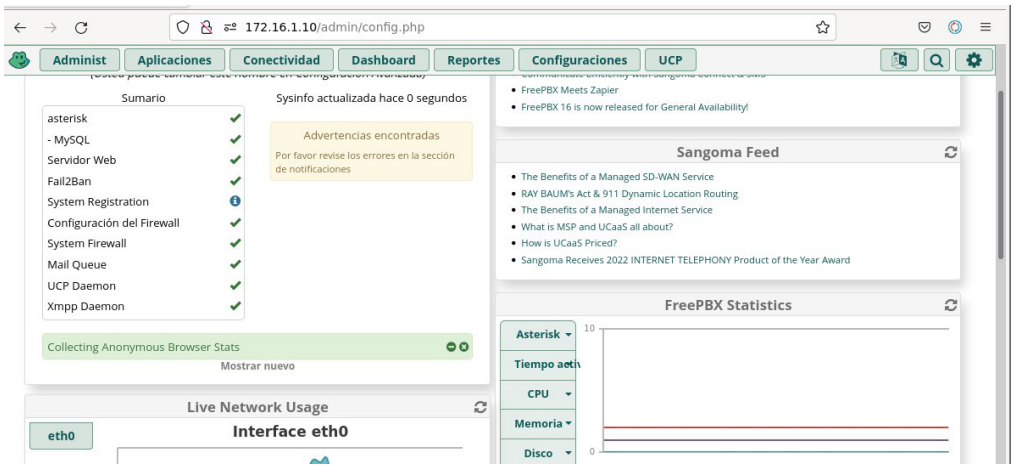
Figura 5.7. Interfaces activas



Fuente: elaboración propia (2023).

Cuando se configura correctamente el *firewall*, la interfaz aparece como se evidencia en la figura 5.8., fortaleciendo el sistema con mayor protección para reducir los intentos de amenazas.

Figura 5.8. Sistema firewall activado



Fuente: elaboración propia (2023).

De acuerdo con Uzcategui (2015), las estrategias generales contra el riesgo asociado a la red VoIP son:

- Contar con una buena política de seguridad para toda la organización, ofreciendo una formación continua a los empleados sobre los tipos de riesgos y sus protocolos para prevenirlos. Es necesario generar una cultura organizacional orientada a la gestión de los riesgos que permita cumplir con los objetivos de negocio de la mejor manera posible, previendo los riesgos a los que se está expuesto constantemente.
- Mantener actualizado el *firmware* del dispositivo.
- Mantener actualizado el *software* de la aplicación.
- Mantener separado el tráfico de TI y VoIP en las redes de la organización.
- Asegurar físicamente los dispositivos siempre que sea posible.
- Utilizar protocolos de mensajería y cifrados seguros.
- Interactuar con el personal de seguridad de la red dentro de la organización.
- Usar contraseñas seguras en ordenadores, teléfonos móviles, tabletas y cualquier otro dispositivo que esté conectado a la red.

Conclusiones

Reconocer la importancia de la auditoría inicial del sistema y la aplicación de medidas de *hardening* son pasos fundamentales para asegurar la infraestructura VoIP. Utilizar herramientas como NMAP y OpenVAS para identificar vulnerabilidades y puertos abiertos permite una evaluación precisa de los riesgos. Posteriormente la configuración de *firewalls,* tanto en el sistema operativo como en la aplicación FreePBX, proporciona una capa adicional de protección contra ataques como DoS, DDoS y otras intrusiones.

A este respecto, la correcta implementación de un *firewall* tanto en la máquina que ejecuta FreePBX como en la red troncal, es crucial para la seguridad del sistema. El uso de Universal Firewall (UFW) en el sistema operativo y su configuración específica dentro de FreePBX, incluyendo la habilitación de funciones como *«Responsive Firewall»*, ayudan a bloquear conexiones no autorizadas y a proteger contra amenazas dinámicas. La configuración adecuada de las interfaces de red y la gestión de zonas aseguran que solo el tráfico legítimo pueda acceder al sistema.

En síntesis, además de las estrategias generales de seguridad para redes VoIP y de las configuraciones técnicas, es esencial contar con políticas de seguridad bien definidas y una cultura organizacional orientada a la gestión de riesgos. Son prácticas recomendadas mantener actualizados tanto el *firmware* de los dispositivos como el *software* de la aplicación, segregar el tráfico de TI y VoIP, asegurar físicamente los dispositivos y utilizar protocolos de cifrado robustos. La formación continua del personal y la interacción con los equipos de seguridad de red, también son elementos clave para mantener un entorno VoIP seguro y resiliente (Hasan, 2024)


5G

CAPÍTULO 6.

Introducción a las comunicaciones unificadas

Introducción

En este último capítulo se realiza una breve introducción a las comunicaciones unificadas (UC), resaltando sus características y su evolución como respuesta a la necesidad de desarrollar mayores servicios frente a la dinámica cambiante de la tecnología, en aras de realizar tareas con mayor eficiencia y con el mejor aprovechamiento de recursos.

6.1. Comunicaciones unificadas (UC)

Las comunicaciones unificadas (UC) hacen referencia a los servicios de comunicación de voz, mensajería, video, conferencia web, correo electrónico, entre otros, de forma integrada. Estos servicios se han vuelto muy populares por su utilización empresarial y organizacional, en especial para el trabajo remoto. Se evidenció la popularización de su uso durante la pandemia de COVID-19, destacándose herramientas como Teams, Cisco Webex, entre otras, que facilitan a los usuarios acceder y administrar todas sus comunicaciones desde un único lugar

Las UC permite mejorar la productividad al integrar múltiples servicios de comunicación en una única plataforma, lo que conlleva un trabajo en equipo más eficaz y una globalización a la que puede accederse desde un portátil (*laptop)*, un teléfono inteligente (*smartpone)* o una tableta (*tablet).* Por otro lado, las UC se destacan por sus costos más bajos comparados con los de sistemas de comunicación tradicionales. Adicionalmente, facilita la gestión a

De los tres últimos cambios tecnológicos relevantes, el primero ocurre en 2006 con la consolidación del protocolo SIP como protocolo de comunicaciones y se suma la aparición de soluciones de código abierto; el segundo es la aparición de la tecnología WebRTC (Web Real Time Comunication) que abre nuevos canales multimedia; y el tercer cambio se vive actualmente con la demanda de soluciones de comunicación diferentes acompañadas de nuevas tecnologías como 5G, Inteligencia Artificial y el *Machine Learnig*, entre otros, que marcan una nueva revolución en los procesos de comunicaciones (Quobis, 2023).

los administradores de red y comunicaciones o al equipo de TI dentro de las organizaciones.

6.2. Componentes de las UC

- VoIP (Voice over IP): hace referencia a los servicios de voz a través de redes IP, lo que permite realizar y recibir llamadas telefónicas por medio de Internet.
- Videoconferencia y conferencia web: permite la comunicación por medio de video y audio en tiempo real entre dos o más usuarios, además de compartir pantalla, presentaciones, entre otros.
- Mensajería instantánea (IM): permite la comunicación por medio de mensajes de texto en tiempo real.
- Presencia: hace referencia al estado de conexión de los usuarios y su disponibilidad (ocupado, disponible...).
- Correo electrónico y calendarios: integra correo electrónico y calendario.
- Movilidad: acceso a servicios de comunicación desde dispositivos móviles, facilitando el trabajo remoto y la movilidad de los empleados.
- Integración con aplicaciones empresariales: conexión con otras aplicaciones empresariales como CRM (Customer Relationship Management) y ERP (Enterprise Resource Planning).

6.3. Inteligencia artificial en las UC

La integración de Inteligencia Artificial (IA) y *Machine Learning* (ML) en las comunicaciones unificadas vienen transformando la forma en que las organizaciones gestionan sus comunicaciones, mejorando la eficiencia, la seguridad y la experiencia del usuario. Estas tecnologías permiten una gestión más inteligente y proactiva de las comunicaciones, facilitando la colaboración y optimizando los procesos empresariales.

De acuerdo con Al-shawabka et al. (2020) y Mauro et al. (2024), la inteligencia artificial y el *Machine Learning* juegan un papel crucial en la mejora y optimización de las Comunicaciones Unificadas (UC) al ampliar sus capacidades por medio de *chatbots*, asistentes virtuales, procesamiento de lenguaje natural para el análisis de sentimientos, transcripción de voz a texto, traducción en tiempo real, análisis de uso para optimizar los recursos de red, detección de anomalías, mejora de la seguridad con autenticación biométrica, sistemas de recomendación y gestión de proyectos, pronóstico de demanda de datos, entre otros.

Un ejemplo representativo del uso de la IA es la herramienta Teams de Microsoft, que busca mejorar la seguridad y la experiencia del usuario. A continuación se presentan las características de esta herramienta:

- Transcripción y subtítulos en tiempo real. Teams utiliza tecnología de reconocimiento de voz y procesamiento de lenguaje natural (NLP) para proporcionar transcripciones y subtítulos en tiempo real durante las videoconferencias. Esto ayuda a los usuarios a seguir la conversación, especialmente en entornos ruidosos o para personas con problemas auditivos.

- Traducción automática. Teams ofrece traducción automática de mensajes de chat y subtítulos, lo que facilita la comunicación entre equipos internacionales que hablan diferentes idiomas. Esta funcionalidad es impulsada por IA para traducir el texto en tiempo real.

- Análisis de sentimientos. Mediante técnicas de procesamiento de lenguaje natural, Teams puede analizar el tono y el sentimiento de los mensajes de chat. Esto puede ser útil para identificar problemas potenciales en la moral del equipo o para detectar conflictos que podrían necesitar atención.

- Reconocimiento de patrones y sugerencias inteligentes. Teams utiliza algoritmos de *Machine Learning* para reconocer patrones en el comportamiento del usuario y hacer recomendaciones inteligentes para:

- Sugerencias de archivos. Basado en el contexto de una conversación, Teams puede sugerir archivos relevantes que podrían ser útiles para los participantes.

- Sugerencias de mensajes. Al escribir un mensaje, Teams puede ofrecer sugerencias para completar frases o palabras basadas en el contexto y el historial de mensajes.

- Optimización de la calidad de las llamadas. Se utiliza IA y ML para monitorizar y optimizar la calidad de las llamadas y videoconferencias en Teams. Los algoritmos pueden ajustar dinámicamente la calidad del audio y el video en función de la conexión a Internet del usuario para asegurar una experiencia fluida.

- Detección de objetos y reconocimiento de imágenes. Teams puede utilizar IA para detectar y reconocer objetos en imágenes compartidas durante las reuniones. Esto es útil para funcionalidades como la pizarra virtual, donde la IA puede mejorar la

legibilidad de los diagramas y notas escritas a mano.

- Seguridad y detección de fraude. Se aplica IA y *Machine Learning* para mejorar la seguridad en Teams. Esto incluye la detección de actividades sospechosas, prevención de fraudes y protección contra ataques cibernéticos. Los algoritmos pueden identificar patrones anómalos en el comportamiento del usuario y alertar a los administradores de seguridad.

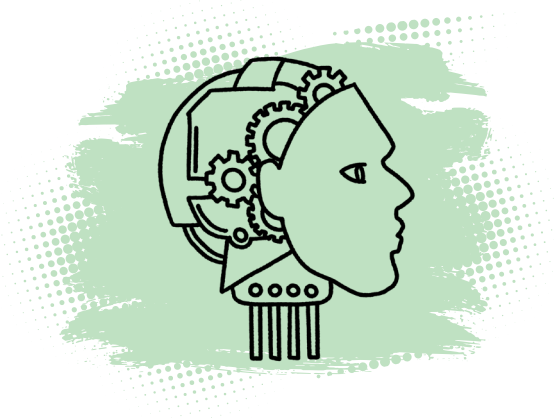
- Asistentes virtuales y *bots*. Teams integra asistentes virtuales y *bots* que utilizan IA para automatizar tareas rutinarias y proporcionar asistencia a los usuarios. A continuación, presentamos algunos ejemplos:

  ◊ Microsoft Cortana. Integrado en Teams, puede ayudar a programar reuniones, buscar información y realizar otras tareas administrativas.

  ◊ *Bots* Personalizados. Las organizaciones pueden crear *bots* personalizados que utilicen IA para interactuar con los empleados, responder preguntas frecuentes y gestionar tareas específicas.

  ◊ Desenfoque de fondo y reemplazo. Durante las videollamadas, Teams utiliza técnicas de visión por computadora impulsadas por IA para desenfocar o reemplazar el fondo detrás del usuario. Esto ayuda a mantener la privacidad y reducir distracciones durante las reuniones.

  ◊ Subtítulos en tiempo real y traducción. Útil donde los participantes hablan diferentes idiomas. Teams puede proporcionar subtítulos en tiempo real y traducir esos subtítulos al idioma preferido de cada participante.



Conclusiones

La evolución de las comunicaciones telefónicas ha sido proporcional al avance del desarrollo tecnológico; desde la comunicación entre pares hasta la actualidad se han adicionado una gran cantidad de tecnologías y servicios en una solución integrada de comunicaciones tanto para pequeñas como para grandes organizaciones. Paralelo a este desarrollo se hicieron indispensables medidas de protección para esa comunicación que evolucionó a complejos sistemas, incluidos aquellos de soluciones criptográficas.

Las instituciones de formación superior juegan un rol fundamental en el desarrollo tecnológico, y mediante implementaciones prácticas en los desarrollos curriculares permiten que la generación actual comprenda de manera integral no sólo el principio e inicio de la comunicación, sino aquellos aspectos fundamentales a tener en cuenta para despertar la curiosidad y desarrollar nuevas soluciones que impacten con nuevas formas de comunicación.

Este texto que forma parte de la formación base de los programas de tecnología permite llegar al estudiante de manera práctica con actividades experimentales sencillas, para llegar a la construcción de sistemas más complejos orientados al logro de un perfil profesional integral y de manera específica en las áreas de electrónica y telecomunicaciones.

REFERENCIAS

Acosta Martell, R. W., Caballero Hernández, G. L., y Mena Sosa, E. L. (2016). *Integración de voz, video y datos sobre FRAME RELAY, ATM E IP* [Trabajo de grado, Universidad Don Bosco]. http://hdl.handle.net/11715/998

Ahson, S., & Ilyas, M. (2009). *VoIP Handbook. Applications, Technologies, Reliability, and Security*. CRC Press.

Alarcón Quigua, A. (2008). *Estudio, implementación y análisis de tráfico de una red VoIP bajo el protocolo SIP* [Trabajo de grado, Universidad Pontificia Bolivariana]. http://hdl.handle.net/20.500.11912/735

Al-shawabka, A., Restuccia, F., D'Oro, S., & Melodia, T. (2020). Massive-Scale I/Q Datasets for WiFi Radio Fingerprinting. *Computer Networks*, *182*, 107566. https://doi.org/10.1016/j.comnet.2020.107566

Blokdyk, G. (2019). *VoIP A Complete Guide- 2019 Edition*. 5STARCooks.

Cabezas Pozo, J. D. (2007). *Sistemas de telefonía: sistemas de telecomunicación e informáticos*. Editorial Paraninfo.

Chakraborty, T., Misra, I. S., & Prasad, R. (2019). *VoIP Technology: Applications and Challenges*. Springer.

Dornheim, S. (2020). *Managing the PSTN Transformation. A Blueprint for a Successful Migration to IP-Based Networks*. CRC Press.

Duarte Domingo, L. (2014). *Diseño de aplicaciones sobre VoIP con mecanismos de geoposicionamiento* [Trabajo de grado, Universidad Politécnica de Cataluña]. http://hdl.handle.net/2099.1/20826

Escobar Cristiani, M. J. (2012). *Telefonía y conmutación*. RED Tercer Milenio. https://www.aliat.click/BibliotecasDigitales/sistemas/Telefonia_y_conmutacion.pdf

Evolución de la comunicación telefónica. (s. f). *Academia.edu.* https://www.academia.edu/11076871/Evoluci%C3%B3n_de_la_conmutaci%C3%B3n_telef%C3%B3nica

Fernández García, C., y Barbado Santana, J. A. (2008). *Instalaciones de telefonía. Prácticas*. Editorial Paraninfo.

Franco Romero, G. A. (2019). *Análisis de vulnerabilidades de seguridad en sistemas de VoIP, con el uso de herramientas de hacking ético* [Trabajo de grado, Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/39259

Frikha, M. (2013). *Ad Hoc Networks: Routing, Qos and Optimization*. Wiley. https://doi.org/10.1002/9781118557747

González Parrón, J. J., y González Martínez, A. (2019). *Montaje y mantenimiento de instalaciones de telefonía y comunicación interior (MF0121).* Cano Pina.

Hasan, M. (2024, March 27). VoIP Security: How it Works, Encryption and Best Practices. *REVE Systems*. https://www.revesoft.com/blog/cloud-telephony/voip-security/

Hersent, O. (2011). *IP Telephony: Deploying VoIP Protocols and IMS Infrastructure*. John Wiley & Sons.

Hill, G. (2007). *The Cable and Telecommunications Professionals' Reference. Volume 1. PSTN, IP and Cellular Networks, and Mathematical Techniques*. Focal Press.

Jaimovich, D. (2019, 14 de octubre). Cuál fue la primera computadora de la historia. *Infobae*. https://www.infobae.com/america/tecno/2019/10/14/cual-fue-la-primera-computadora-de-la-historia/

Johnston, A. B. (2016). *SIP: Understanding the Session Initiation Protocol*. Artech House.

Joskowicz, J. (2013). *Voz, video y telefonía sobre IP*. Universidad de la República. https://www.fing.edu.uy/iie/ense/asign/ccu/material/docs/Voz%20Video%20y%20Telefonia%20sobre%20IP.pdf

Landivar, E. (2011). *Comunicaciones unificadas con Elastix. Vol. 1*. (n. d.).

Liébana Carrascosa, Á. D. (2020). *Nuevas técnicas para optimizar el tráfico de red utilizando Big Data* [Trabajo de grado, Universidad Politécnica de Valencia]. https://riunet.upv.es/handle/10251/157712

Mairs, J. (2002). *VPNs: A Beginner's Guide*. McGraw-Hill/Osborne Media.

Mauro, M. D., Galatro, G., Postiglione, F., Song, W., & Liotta, A. (2024). Multivariate Time Series Characterization and Forecasting of VoIP Traffic in Real Mobile Networks. *IEEE Transactions on Network and Service Management*, *21*(1), 851-865. https://doi.org/10.1109/TNSM.2023.3295748

Meggelen, J., Bryant, R., & Madsen, L. (2013). *Asterisk: The Definitive Guide: Open-Source Telephony for the Enterprise*. O'Reilly.

Noll, A. M. (1998). *Introduction to Telephones and Telephone Systems*. Artech House.

Ockay, M. (2018). *Cisco Unified Communications Manager Express a Hands-On Approach*. CreateSpace.

Orebaugh, A., & Pinkard, B. (2008). *Nmap in the Enterprise: Your Guide to Network Scanning*. Syngress.

Parra, S. (2023, 3 de abril). Martin Cooper hizo la primera llamada en un móvil hace 50 años: ¿qué dijo? *National Geographic España*. https://www.nationalgeographic.com.es/ciencia/martin-cooper-hizo-primera-llamada-movil-hace-50-anos-que-dijo_19726

Porter, T. (2006*). Practical VoIP Security*. Elsevier.

Quobis. (2023). *Libro blanco. El futuro de las comunicaciones unificadas*. Quobis:. https://quobis.com/es/2023/04/27/quobis-presenta-el-libro-blanco-del-futuro-de-las-comunicaciones-unificadas/

Ramírez, I. (2016, 25 de julio). Máquinas virtuales: qué son, cómo funcionan y cómo utilizarlas. *Xataca.* https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

Rivero, S., Delfino, A., y San Martín, M. (2006). *Ingeniería de Tráfico en Redes MPLS*. https://www.academia.edu/120776072/Ingenier%C3%ADa_de_tr%C3%A1fico_en_Redes_%20MPLS

Sardanyés, E. (2024, 30 de junio). Primer ciberataque de la historia y los ciberataques que han perdurado en el tiempo. *ESED*. https://www.esedsl.com/blog/primer-ciberataque-historia-y-ciberataques-que-han-perdurado

Sierra Rodríguez, A. (2011). *Instalación de un sistema VoIP corporativo basado en Asterisk* [Tesis de maestría, Universidad Politécnica de Cartagena]. http://hdl.handle.net/10317/737

Sisalem, D., Kuthan, J., Abend, U., Floroiu, J., & Schulzrinne, H. (2009). *SIP Security*. Wiley. https://doi.org/10.1002/9780470516997

Suthar, D., & Rughani, P. H. (18-19 de diciembre de 2020). A Comprehensive Study of VoIP Security. *Proceedings on the 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India*, 812-817. https://doi.org/10.1109/ICACCCN51052.2020.9362943

Tanenbaum, A. S. (2009). *Sistema operativos modernos*. Pearson.

Thermos, P., & Takanen, A. (2008). *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures*. Pearson.

Thu, K. M. (2009). Comparison of VOIP signaling protocol H.323 Vs SIP. *Proceedings of World Academy of Science, Engineering and Technology*, *38*, 2070-3740. https://www.researchgate.net/publication/294865196

Uzcategui, L. (2015). *Seguridad en VoIP*. https://www.academia.edu/43430300/Seguridad_en_VoIP

Valverde Balbuena, O. (2018). *Las redes informáticas y la VoIP*. (n. d.).

Willing, N. (2024, 26 de mayo). *21 estadísticas sobre VoIP que las empresas deben conocer en 2025*. https://www.techopedia.com/es/estadisticas-voip

Znaty, S., Dauphin, J.-L., & Geldwerth, R. (2005). *SIP: Session Initiation Protocol*. Effort. https://silo.tips/download/sip-session-initiation-protocol

Comunicación unficada de voz
sobre Protocolo de Internet

•

Las fuentes tipográficas empleadas son Noto serif 11 puntos,
para texto corrido, y Sora bold en títulos.

Línea Profesoral

El objetivo de esta obra es conocer e implementar una solución de comunicación unificada basada en una plataforma de voz sobre el Protocolo de Internet. El desarrollo se centra en aprovechar los recursos mediante el uso de herramientas de código abierto con tecnologías de bajo coste. Para infraestructuras de comunicaciones existentes, se priorizan requisitos de implementación orientados a optimizar recursos y garantizar niveles mínimos de seguridad.

El libro también se presenta como una herramienta de apoyo y refuerzo en cursos de la estructura curricular de programas de tecnologías de la información, especialmente en el área de tecnología e ingeniería en telecomunicaciones de la Facultad de Ingenierías del ITM. Los cursos en los que se apoya su desarrollo forman parte de los planes de estudio de grado en redes de computadoras, servicios en red, redes de telecomunicaciones y teoría de teletráfico.

@ITMFondoEditorial

@editorial_itm

Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación