

Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

GENERACIÓN Y MONITOREO DE TRÁFICO IP, MARCACIÓN DE PAQUETES Y
OPTIMIZACIÓN DEL ANCHO DE BANDA CON POLÍTICAS DE CALIDAD DE SERVICIO

Proyecto Integrador

Previo la obtención del Título de:

INGENIERO EN TELECOMUNICACIONES

Presentado por:

Ochoa Chávez Gabriela Beatriz

Rumipamba Guacho Miguel Angel

Guayaquil - Ecuador

Año: 2023

Dedicatoria

El presente proyecto lo dedico a Dios y a toda mi familia.

Principalmente, a mi esposo Richard Estrada que no permitió que me rindiera, y ha estado a mi lado en todo momento, mostrándome su amor incondicional.

A mis hijas: Maite, Melinda y Maeve, quienes me llenan energía y amor.

A mis padres Williams Orrala y Grecia Chevez quienes son pilares fundamentales en mi vida en compañía de mis hermanos William y Giuliana.

Y a todas las personas que han pasado por mi vida y me han ayudado cuidando de mis niñas para poder culminar con éxito mi carrera.

Gabriela Ochoa Ch.

Dedicatoria

El presente proyecto se lo dedico a Dios por ser mi guía en los momentos difíciles, a mi madre Dora Guacho que desde el cielo sigue guiando mis pasos y fue fundamental en mi educación universitaria, te amo mamá y aprecio todo el sacrificio realizado, logrando juntos el éxito de hoy. También, agradezco a mi padre Jorge Rumipamba por sus consejos y valores, así como a mis hermanos Marisol, Diego, Gabriel y Jorge, y a mi cuñado José Navarrete, por su confianza y apoyo constante. Finalmente, agradezco a mis sobrinos Angelina, Mike, Maite, Valentina y Sofía por su aliento y cariño.

Miguel Angel Rumipamba Guacho

Agradecimientos

Agradezco a Dios por permitirme culminar mi carrera. A mi esposo porque hacemos un gran equipo, logrando muchas metas, una de ellas, el presente proyecto. A mis padres por su continuo cuidado y atención en todo momento.

A mis compañeras del colegio que estuvieron pendiente y me ayudaron a ingresar a la universidad, en particular Kimberlyn Moran.

También, un especial agradecimiento a Jenny Flores, Madelyne Estrada, Hilbert Burgos, Ruth Ajo, Betty Flores, Silvia Gómez, Teresita, Andrea Suarez por cuidar de mis niñas permitiéndome continuar con mis estudios y convirtiéndose en parte de mi familia.

Agradezco a las profesoras: Verónica Soto y María Álvarez por su guías y paciencia brindada para terminar este documento.

Gabriela Ochoa Ch.

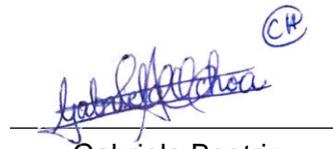
Agradecimientos

Agradezco primeramente a Dios, a mi madre Dora Guacho, en el cielo, cuya sabiduría y amor continúan siendo mi fuente de orientación y consuelo. Dedico este proyecto como un tributo a su legado y como una manera de mantener viva su memoria en mi corazón. También, quiero agradecer sinceramente a mi profesora y tutora de la materia integradora, quienes desempeñaron un papel fundamental en la realización de este proyecto. Les agradezco por todas las enseñanzas brindadas. Además, quiero extender mi agradecimiento a todos los maestros que formaron parte de mi educación, así como a mis compañeros que siempre estuvieron allí para apoyarme y ofrecerme su amistad.

Miguel Angel Rumipamba Guacho

Declaración Expresa

"Los derechos de titularidad y explotación, nos corresponde conforme al reglamento de propiedad intelectual de la institución; Gabriela Beatriz Ochoa Chevez y Miguel Angel Rumipamba Guacho y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



Gabriela Beatriz
Ochoa Chévez



Miguel Angel
Rumipamba Guacho

Evaluadores

Ph.D. María Antonieta
Álvarez Villanueva
Profesor de Materia

M.Sc. Verónica Alexandra
Soto Vera
Tutor de proyecto

Resumen

En este proyecto se considera cuando una red detecta sobrecarga ya que conduce a la congestión, afectando negativamente el rendimiento de los servicios y aplicaciones en la red. Se toma en cuenta que las simulaciones son más económicas al construir una red real para realizar pruebas y experimentos. El objetivo es simular el funcionamiento de servicio de telefonía IP mediante el monitoreo del flujo de tráfico de señalización y datos, en un sistema programable de generación y marcación de paquetes IP para la optimización del ancho de banda con sus respectivas políticas de calidad de servicio implementadas en una red. Para las simulaciones presentes se investigó programas de licencias libre, GNS3 como simulador de la red, Asterisk como servidor de VoIP, se generó tráfico de correo a través de Scapy y se utilizó WinSCP para la transferencia de archivos, la calidad de servicio se basó en clasificar el tráfico por protocolos y se gestionó las colas por WFQ. Se captó paquetes de diferentes tipos de tráfico y se implementó configuraciones en los routers para clasificar diversos paquetes a través de asignación de categorías de ancho de banda.

Palabras Clave: Simulaciones, licencias libres, gestión, WFQ.

Abstract

In this project, we consider the scenario where a network detects overload, as it leads to congestion, negatively impacting the performance of services and applications on the network. It is taken into account that simulations are more cost-effective than building a real network for testing and experiments. Our objective is to simulate the operation of an IP telephony service by monitoring the flow of signaling and data traffic, using a programmable system for generating and marking IP packets to optimize bandwidth with their respective quality of service policies implemented in a network. For the current simulations, we researched free license programs, using GNS3 as the network simulator, Asterisk as the VoIP server, generating mail traffic through Scapy, and employing WinSCP for file transfer. Quality of service was based on classifying traffic by protocols, and queues were managed using WFQ. Packets of different types of traffic were captured, and configurations on the routers were implemented to classify various packets through bandwidth category assignments

Keywords: Simulations, open-source licenses, management, WFQ.

Índice general

Resumen	I
<i>Abstract</i>	II
Índice general	III
Abreviaturas.....	V
Índice de figuras	VII
Índice de tablas.....	VIII
Índice de anexos.....	IX
Capítulo 1	1
1. Introducción.....	2
1.1 Descripción del problema	3
1.2 Justificación del problema	3
1.3 Objetivos	4
1.3.1 Objetivo general.....	4
1.3.2 Objetivos específicos	5
1.4 Marco teórico.....	5
1.4.1 Red VoIP	5
1.4.2 Generación de tráfico de red.....	7
1.4.3 Mecanismos para configuraciones de QoS en los routers y el manejo de colas	8
Capítulo 2	11
2. Planificación del desarrollo de un sistema para generación de tráfico, marcación de paquetes IP y monitoreo de tráfico de VoIP.....	12
2.1 Etapas del procedimiento	12
2.2 Descripción del proyecto	13

Capítulo 3	17
3. Implementación y pruebas.....	18
3.1 Escenario 1-Red VoIP	18
3.1.1 Implementación Red VoIP	18
3.1.2 Análisis de los resultados Red VoIP	19
3.2 Escenario 2-Red VoIP con QoS	22
3.2.1 Implementación Red VoIP con QoS.....	22
3.2.2 Análisis de los resultados Red VoIP con QoS.....	25
Capítulo 4	28
4. Conclusiones y recomendaciones	29
4.1 Conclusiones	29
4.2 Recomendaciones	30
Referencias.....	31
Anexos.....	33

Abreviaturas

ESPOL Escuela Superior Politécnica del Litoral

IP Internet Protocol
Protocolo De Internet

VoIP Voice Over Internet Protocol
Voz Sobre Protocolo De Internet

GLP General Public License
Licencia Pública General

LAN Local Area Network
Red De Area Local

WAN Wide Area Network
Red De Area Amplea

PDA Personal Digital Assistant
Asistente Personal Digital

TCP Transmission Control Protocol
Protocolo De Control De Transmisión

UDP User Datagram Protocol
Protocolo De Datagramas De Usuario

FTP File Transfer Protocol
Protocolo De Transferencia De Ficheros

AF Assured Forwarding
Reenvío Seguro

EF Expedited Forwarding
Reenvío Acelerado

QoS	Quality Of Service Calidad De Servicio
PBX	Private Branch Exchange Central Privada Automática
RTC	Commuted Telephone Network Red Telefónica Conmutada
QoE	Quality Of Experience Calidad De Experiencia
WFQ	Weighted Fair Queueing Espera Equitativa Ponderada
CBWFQ	Class-Based Weighted Fair Queueing Cola Justa Ponderada Basada En Clases
DiffServ	Differentiated Services Servicios Diferenciados
DSCP	Differentiated Services Code Point Punto De Código De Servicio Diferenciado
ToS	Type Of Service Tipo De Servicio
CS	Class Selector Selector De Clases
DF	Default Forwarding Reenvío Predeterminado
PC	Personal Computer Computadora Personal
SIP	Session Initiation Protocol Protocolo de iniciación De Sesión

Índice de figuras

Fig. 1. Campo ToS. [12]	9
Fig. 2. Campo DSCP. [12]	9
Fig. 3. Diagrama de flujo del presnete proyecto.....	12
Fig. 4. Topología del escenario 1 definición de IP de cada componente.	19
Fig. 5. Paquetes SIP captadas a traes de Wireshark en la red VoIP durante ja ejecución de una llamada IP.	20
Fig. 6. Se visualiza el flujo del tráfico de la red VoIP.....	21
Fig. 7. Topología del escenario 2 con sus respectivas IP.	22
Fig. 8. Paquetes TCP, correo, captados mediante Wireshark de la red VoIP con QoS.	25
Fig. 9. Se visualiza los 3 tipos de tráfico generados a través de la red VoIP con QoS mediante Wireshark y su promedio de bits/s.....	26
Fig. 10. Configuraciones del router principal de la red VoIP con QoS.....	27

Índice de tablas

Tabla 1. Cuadro comparativo entre la telefonía IP y convencional [5].....	6
Tabla 2. Cuadro comparativo de los diferentes softwares de simulación [14] [15].	13
Tabla 3. Cuadro comparativo de los diferentes softwares de simulación [16] [17].	14
Tabla 4. Cuadro comparativo de los diferentes softwares libres de simulación [18].....	15
Tabla 5. Cuadro comparativo de los diferentes servidores libres de simulación [19]....	15
Tabla 6. Cuadro comparativo de los diferentes softwares libres de simulación [20].....	16
Tabla 7. Configuraciones del Router 1.....	23
Tabla 8. Configuraciones del router PRINCIPAL.	24

Índice de anexos

Anexo 1. Guía 1-Red VoIP.....	33
Anexo 2. Guía 2-Red VoIP con QoS.....	79
Anexo 3. Configuraciones del dispositivo de red-Router Principal.....	98
Anexo 4. Configuraciones del dispositivo de red-Router 1	102

Capítulo 1

1. Introducción

Durante la década de los 90, los operadores de telefonía tradicionales, entidades educativas y empresas, empezaron a llevar voz y video a las redes IP, en particular las intranets corporativas e Internet. Estos nuevos avances son conocidos actualmente como VoIP, también llamado Voz sobre IP o Voz sobre Protocolo de Internet. Este proceso se trata de fragmentar el audio como el video en segmentos más pequeñas para luego ser enviado estos fragmentos a través de una red IP, y luego volver a ensamblarlos en el destino final. De esta forma, las personas pueden comunicarse de manera efectiva utilizando esta tecnología. En los años siguientes, hubo mejoras continuas en las redes de datos, y cercano del 2005, resultaba accesible obtener una conexión a la red de Internet que satisfaga con las condiciones básicas para proporcionar una calidad de voz adecuada y un servicio confiable. Esto minimizó las posibles pausas o cortes durante las conversaciones. Este avance significativo impulsó aún más el uso de la tecnología VoIP, lo que llevó a la creación de numerosas soluciones que la aprovechan en la actualidad. Un caso notable es Asterisk, una central telefónica de código abierto distribuida con licencia GPL. Este sistema, con respaldo comercial de Digium, ha emergido como una de las opciones IP preferidas en varios campos, incluyendo el sector empresarial y el educativo. Un ejemplo notable de sistema VoIP es Skype, desarrollado por dos estudiantes, Janus Friis y Niklas Zennström, universitarios en 2003, el cual utiliza una escritura privada, haciendo referencia a que no se basa en un protocolo estándar, lo que podría presentar limitaciones a sus usuarios en el transcurso del tiempo [1].

En la actualidad existe tres clases de redes IP: Internet, Red IP pública, Intranet. De estas, la última se refiere a la red propia de una empresa que puede estar conformada por varias LAN conectadas por WAN, esta topología es recomendada para VoIP. Un elemento importante en una Red IP es el softphone, aplicación informática que emulan capacidades de un teléfono. Estas aplicaciones permiten que dispositivos como computadoras o un asistente digital personal

(PDAs) actúen como teléfonos VoIP. No es imprescindible que el dispositivo sea de alto rendimiento para lograr esto, tan sólo se requiere de componentes de audio apropiado y la capacidad de enlazarse a una red de protocolo TCP/IP [2].

Para mantener una comunicación óptima entre usuarios dentro de una red multiservicio dada la presencia de diferentes tipos de tráficos sean estas de VoIP, videos, telefonía IP, FTP (archivos), etc., con marcaciones como AF (reenvío seguro), EF (reenvío acelerado), diferentes codificaciones, se debe monitorear dichos tráficos, aplicar QoS (calidad de servicio) mediante configuraciones en los equipos de la red para dar prioridad a la voz o al tráfico marcado como prioritario [3]. Esto permite entender con más claridad cómo ha ido evolucionando la comunicación VoIP. Por tal motivo, el propósito de este proyecto es armar una red emulada, logrando con ello un rendimiento óptimo de la red mediante la optimización del ancho de banda, reduciendo la latencia y los tiempos de respuesta, mejorando la experiencia del usuario en términos de calidad y permitiendo una administración más efectiva de los recursos de la red.

1.1 Descripción del problema

Se puede detectar sobrecarga en ciertos puntos de la red, lo que conduce a la congestión, afectando negativamente el funcionamiento de los servicios y programas en la red. En ese sentido, la propuesta de esta investigación es desarrollar recursos de formación académica para demostrar el funcionamiento de servicio de telefonía IP mediante el monitoreo del flujo de tráfico de señalización y datos utilizados en los servicios de telefonía IP. Además, diseñar e implementar un sistema programable de generación y marcación de paquetes que permita evaluar el funcionamiento de políticas de calidad de servicio implementadas en una red.

1.2 Justificación del problema

La simulación de redes IP, que también se denomina simulación de redes de computadoras, ofrece una variedad de beneficios que ayudan a mejorar el diseño, la

implementación y el rendimiento de las redes informáticas, mientras se evitan los riesgos y costos asociados con pruebas en un entorno de producción real. La simulación es más económica que construir una red real para realizar pruebas y experimentos. No es necesario adquirir hardware adicional ni implementar cambios en la infraestructura existente. Permite crear un entorno de prueba completamente controlado y predecible. Se pueden simular diversos escenarios y configuraciones para comprender mejor el comportamiento de la red bajo diferentes condiciones. Al trabajar en un entorno virtual, los errores o fallos no afectan la red real, dando garantía a la confiabilidad de los datos y la integridad de la infraestructura.

Se expone un caso de Ethio Telecom, su red IP no cumplía con la priorización del tráfico, la clasificación y rendimiento de QoS, por esto proponen mejorar la calidad de los servicios de VoIP, para ello realizan simulaciones de su red donde se aplica el modelo DiffServ, donde se implementa una clase de servicio diferente en el borde del proveedor de servicios Edge Enrutador mediante el establecimiento de políticas de tráfico, marcación y políticas basadas en clases, priorización del tráfico (cola justa ponderada basada en clases) y técnica de control de congestión (descarte temprano aleatorio ponderado) el cual permite organizar y dar prioridad al tráfico en función de la red servicio de cola [13].

Por estas razones, este proyecto emulara una red, donde brinde servicio de telefonía IP, se genere tráfico FTP y correo para evaluar el funcionamiento de políticas de calidad que nos brinda el modelo WFQ, para priorizar el tráfico VoIP.

1.3 Objetivos

1.3.1 Objetivo general

Simular el funcionamiento de servicio de telefonía IP mediante el monitoreo del flujo de tráfico de señalización y datos, en un sistema programable de generación y marcación de paquetes IP para la optimización del ancho de banda con sus respectivas políticas de calidad de servicio implementadas en una red.

1.3.2 Objetivos específicos

- Investigar los diferentes emuladores de red y generadores de tráfico, sus componentes y sus funcionamientos para el diseño de la red.
- Implementar un generador de tráfico en la red de prueba para paquetes de correo y transferencia de archivos, con su marcación de paquetes y monitoreo de tráfico.
- Aplicar políticas de gestión de QoS para la clasificación y priorización del tráfico IP.
- Realizar el análisis estadístico del flujo de paquetes durante una llamada de VOIP mediante analizador de paquetes de red.

1.4 Marco teórico

En esta sección se detallan los conceptos de una red VoIP y sus componentes como centralita y softphone; generador de tráfico y los diferentes mecanismos para aplicar calidad de servicio.

1.4.1 Red VoIP

EL nodo central de conmutación que une a diferentes teléfonos es la centralita telefónica, el cual se encuentra en un nivel lógico en una posición central de los equipos conectados a través de este. Las centralitas son programa telefónico de fuentes abiertas que permite crear sistemas de telefonía IP con características avanzada. Es altamente flexible, escalable y se utiliza para realizar llamadas a través de redes IP. Es ampliamente utilizado para desarrollar soluciones personalizadas de comunicación de voz y video, como por ejemplo Asterisk [9]. Se conforma de enlaces de diferentes terminales telefónicos o extensiones en una organización a través de una central telefónica. Este servicio puede ser proporcionado a pequeña empresa como a una gran empresa donde tenga cientos de extensiones. La transmisión analógica puede ser base de una centralita, como también, puede ser la transmisión digital a través de paquetes IP. Actualmente, se cuenta con tres clases de centralitas: centralita física en armario, software de centralitas que

se integran en un ordenador o servidor de una empresa y centralitas virtuales que se encuentran en servidores de los usuarios de telefonía IP. Están siendo superadas las centralistas virtuales de las físicas, gracias a su atractiva relación calidad-precio y variedad de opciones en sus configuraciones [4]. Sus ventajas a diferencia de una telefonía convencional son expuestas en tabla 1.

Tabla 1. Cuadro comparativo entre la telefonía IP y convencional [5]

Ventajas	Telefonía IP	Telefonía Convencional
Alta Calidad en las Llamadas	SI	SI
¿Necesita Electricidad?	SI	NO
¿Ofrece Movilidad?	SI	NO
¿Llamadas Internaciones Económicas?	SI	NO
¿Altas Cuotas Mensuales?	NO	SI
¿Numeración Basada En La Localización Física?	NO	SI
¿Llamadas De Bajo Costo?	SI	NO
¿Dependen Del Cableado?	NO	SI
¿Necesita Internet?	SI	NO

Para ejecutar las llamadas IP se requiere de un softphone, como por ejemplo Zoiper, que es una aplicación de software VoIP que permite ejecutar llamadas de video y voz a través de internet, es compatible con diferentes plataformas y proveedores de servicios VoIP, con una interfaz sencilla de usar y cualidades avanzadas utilizadas por usuarios individuales o empresas [10].

El envío de voz mediante las redes IP (VoIP) está adquiriendo cada vez más importancia y popularidad. La calidad de la experiencia (QoE) se refiere a qué tan bien un servicio de red cumple con los intereses y requerimientos que solicitan los usuarios. Con respecto a la medición del rendimiento en una red, desde una perspectiva técnica y a la capacidad de gestionarla. se relacionan a la calidad de servicio (QoS) para cumplir con los requisitos necesarios para las aplicaciones. Dificultades propias de las redes de datos son confrontado por la red VoIP, como degradación recibida por los usuarios en cuanto a la calidad del servicio. Los cuales pueden ser causadas por factores como retardos, variaciones en los retardos (jitter) y pérdida de paquetes,

entre otros. Con el fin de que los servicios dados por la red VoIP pueda ampliamente ser adoptada con fines comerciales, es fundamental asegurar un nivel de calidad de voz tolerable [6].

1.4.2 Generación de tráfico de red

Un generador de tráfico es una herramienta o dispositivo que simula y genera flujos de datos o paquetes de red, simulando el comportamiento del tráfico real dentro de una red. Se utiliza en pruebas y laboratorios para evaluar, medir y validar el rendimiento, capacidad y calidad de servicio de equipos de red. Los generadores pueden ajustar tasas, crear patrones de tráfico y proporcionar métricas detalladas para asegurar que la red esté preparada para enfrentar las demandas reales y detectar posibles problemas antes de implementar servicios en la infraestructura de producción. Algunos tipos de tráfico:

- Tráfico de datos: se utiliza en cualquier red, debido a que realiza varias actividades como navegación web, transferencia de archivos, correos electrónicos, etc.
- Transmisión de tráfico de voz a través del protocolo de internet (VoIP): la transferencia de tráfico de voz en redes fundamentadas en internet, el tráfico de voz a través de protocolos VoIP emplea redes de datos como internet o redes privadas para transportar las llamadas de voz.
- Tráfico de correo electrónico: Transferencia de mensajes y datos asociados entre diferentes servidores y clientes de correo electrónico.
- Tráfico de Streaming: Transferencia continua y en tiempo real, de datos multimedia como audio y video, a través de internet [7].

Así como, scapy que es una herramienta de código abierto en Python que accede a crear, enviar, capturar y analizar paquetes de red. Permitiendo personalizar y manipular el tráfico de la red, realizar escaneos y pruebas de seguridad, de gran beneficio para gestores de redes y profesionales de seguridad informática [11]. Una manera de ser ejecutado es a través del sistema operativo Debian, fundamentado en la colaboración abierta disponible en el núcleo Linux, es muy

utilizada por su estabilidad, seguridad y amplia selección de software de fuentes abiertas. Utiliza el gestor de herramienta de paquetes avanzado (ATP) y admite diversas arquitecturas de hardware [8].

1.4.3 Mecanismos para configuraciones de QoS en los routers y el manejo de colas

A continuación, se describe las configuraciones de QoS que se han investigado:

- **Weighted Fair Queueing (WFQ)**

Protocolo de gestión de colas avanzado, utilizado en dispositivos de red para controlar el flujo de datos de manera equitativa y eficiente. En WFQ, los paquetes se organizan en colas en función de su origen y destino, asignándole un peso proporcional a su importancia. Esto garantiza que los flujos de tráfico críticos reciban más ancho de banda sin marginar por completo los flujos de tráfico menos relevantes, el resultado es una asignación justa de recursos permitiendo una latencia reducida en la red [12].

- **Class-Based Weighted Fair Queueing (CBWFQ)**

Extensión avanzada del protocolo WFQ que permite una administración más precisa del tráfico en redes, el cual divide el tráfico en clases basadas en criterios como el tipo de aplicación, dirección IP o puerto. Cada clase tiene su propia cola y peso asignado, de esta manera se puede asignar más ancho de banda a clases de tráficos con prioridad alta como video o voz, mientras se mantiene un nivel justo de servicio para otras clases, permite la personalización de políticas de asignación de ancho de banda según las necesidades de la red [12].

- **Differentiated Services (DiffServ).**

Protocolo de gestión de calidad de servicio en redes IP, clasifica el tráfico en grupos y asigna etiquetas a los paquetes para indicar su prioridad y tratamiento. Esto permite que los dispositivos de red prioricen y manejen de manera eficiente el tráfico crítico como por ejemplo el de voz y video, sin abrumar los recursos de red del tráfico menos importante. Por lo tanto,

aumenta la satisfacción del usuario al brindar un rendimiento más estable y equitativo para una variedad de aplicaciones en la red. Se ejecuta a través de los 8 bits inicialmente utilizados para definir tipo de servicio (ToS), como se observa en la Fig.1. Este campo sufre alteraciones, como se logra visualizar en la Fig.2, para evolucionar hacia el campo Differentiated Services Code Point (DSCP), que es empleado para una categorización más precisa de los paquetes [12].

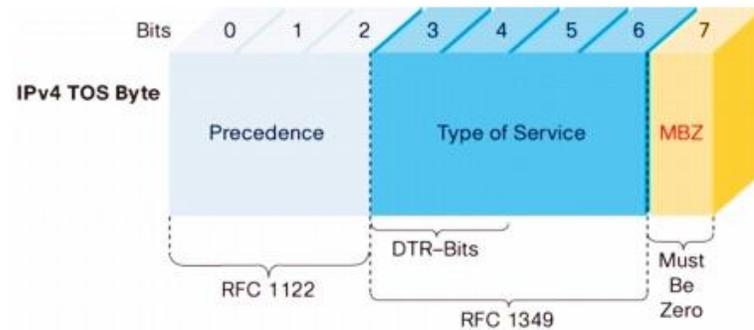


Fig. 1. Campo ToS. [12]

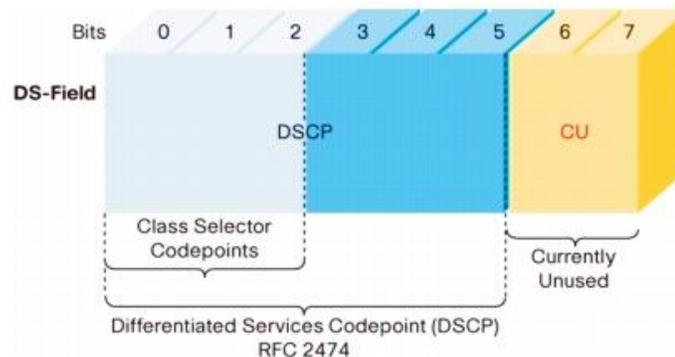


Fig. 2. Campo DSCP. [12]

El campo DSCP es un valor en el encabezado IP de un paquete que se utiliza en el enfoque de gestión de calidad de servicio (QoS) llamado DiffServ, el cual indica la prioridad y el tratamiento que se debe dar a un paquete en la red. Es un valor de 6 bits que se encuentra en el

campo de tipo de servicio (ToS) del encabezado IP. El DSCP permite clasificar el tráfico en diferentes clases o categorías con niveles de prioridad específicos. Los dispositivos de red utilizan estos valores para determinar cómo se manejará el tráfico, como la atribución del ancho de banda y la planificación de colas.

El campo DSP presenta valores que se pueden dividir en cuatro categorías:

- Expedited Forwarding (EF): la categoría de mayor prioridad posee un valor de 46, se utiliza para categorizar el tráfico que requiere garantía en sus parámetros de calidad de servicios (QoS).
- Assured Forwarding (AF): prioridad de segunda clase, en cuatro subclases es posible seccionar, definiéndoles un ancho de banda diferente de acuerdo con el tráfico que vaya a circular en la red. Cada clase tiene tres probabilidades de descarte distinta sea esta baja, media o alta.
- Class Selector (CS): esta categoría se emplea para mantener la compatibilidad con el campo ToS, consiste en ocho valores que son idénticos a los originales, con ceros al final.
- Default Forwarding (DF): prioridad baja es su categoría, que se aplica automáticamente en la creación de paquetes IP, tiene un valor de 0(000000) [12].

Capítulo 2

2. Planificación del desarrollo de un sistema para generación de tráfico, marcación de paquetes IP y monitoreo de tráfico de VoIP

En este capítulo se explica el enfoque utilizado para planificar la estructura de la red y sus componentes, partiendo desde la recopilación de información hasta la toma de decisiones para los softphone, centralitas, programa de simulación de red, máquina virtual, programa para el análisis de tráfico y mecanismo de marcación de paquetes.

2.1 Etapas del procedimiento

En la Fig. 3 se muestra los pasos a seguir para realizar el presente proyecto donde se empezó con una investigación sobre servidores y software de licencias libres a implementar en la topología de red emulada, se eligen dos escenarios a desarrollar tomando en cuenta los requerimientos planteados, para luego crear máquinas virtuales como PC y servidores con sus respectivas configuraciones y software; que serán usados en la red emulada en GNS3, configuraciones de marcación de paquetes en los ruteadores hasta llegar a pruebas de los diferentes tipos de tráfico y calidad de servicio.

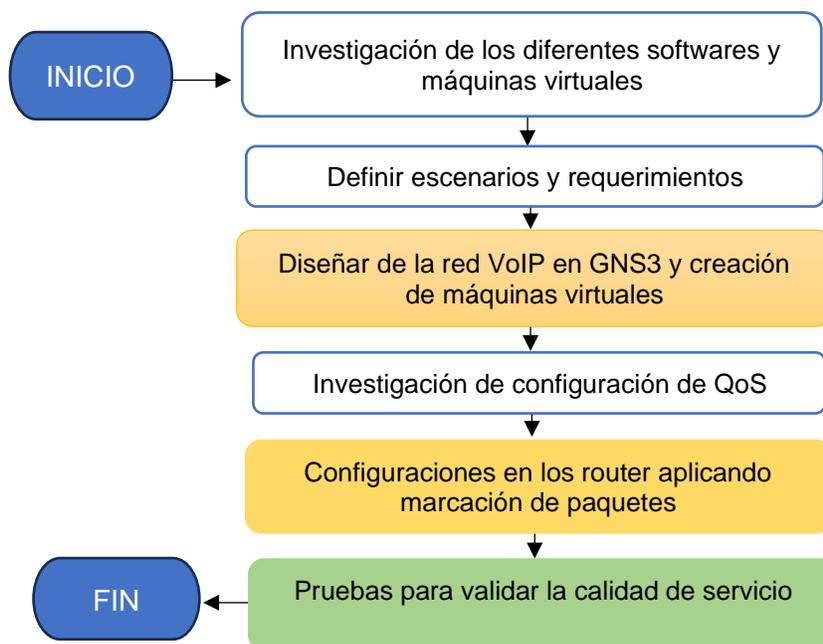


Fig. 3. Diagrama de flujo del presente proyecto.

2.2 Descripción del proyecto

En el desarrollo de este proyecto, para la llamada de voz existen software como Zoiper, 3CX y Linphone. Se seleccionó Zoiper, cuyas características principales se muestran en la tabla 2, por ser un software multiplataforma y a su vez brinda una solución de softphone SIP, eliminando hardware adicionales o teléfonos IP físicos, consolidando múltiples funciones en un solo dispositivo, ofreciendo una fácil configuración y una interfaz de usuario simple, lo que lo convierte en un complemento ideal para una centralita virtual.

Tabla 2. Cuadro comparativo de los diferentes softwares de simulación [14] [15].

Ítems	Zoiper	3CX	Linphone
Soporte IP PBX	Es una IP PBX (central telefónica privada de internet), de estándar abierto, ofrece comunicaciones unificadas completas.	Es una IP PBX (central telefónica privada de internet), de estándar abierto, ofrece comunicaciones unificadas completas.	No cuenta con estas funcionalidades.
Funcionalidades	Enrutamiento de llamadas, acceso móvil, base de datos de contacto, grabación de llamadas.	Enrutamiento de llamadas, importación y exportación de datos, colaboración entre varios usuarios.	No cuenta con estas funcionalidades.
Implementación	Utilizando la nube, entorno local.	Utilizando la nube, ambiente local.	Utilizando la nube, ambiente local.
Formación	Documentación.	En persona, en directo en línea, videos.	En vivo en la web.
Asistencia	E-mail/Help Desk, chat.	Ayuda telefónica, E-mail/Help Desk.	No cuenta con estas funcionalidades.

Para diseñar una centralita telefónica están disponibles los softwares como Asterisk, CloudTalk, Aircall, las características de estos tres softwares se encuentran descritas en la tabla 3, para el presente proyecto se escogió Asterisk por ser de código abierto y gratuito, este se

adapta a necesidades específicas y es personalizable, permite incorporar una amplia diversidad de funciones y características.

Tabla 3. Cuadro comparativo de los diferentes softwares de simulación [16] [17].

Ítems	Asterisk	CloudTalk	Aircall
Ideal para	Es de código abierto, ayuda a construir aplicaciones de comunicación.	Sistema de atención telefónica en la nube.	Pymes que utilizan el teléfono para realizar negocios.
Funcionalidades	Conexión VoIP, distribución automática de llamadas, videoconferencia.	Enrutamiento de llamadas, colas de espera personalizadas, grabación de llamadas.	Conexión VoIP, grabación de llamada, mensajería SMS.
Implementación	Utilizando la nube.	Utilizando la nube.	Utilizando la nube.
Formación	En línea, en persona, documentación.	Fácil integración con las redes sociales, videos.	Persona en vivo en la web, videos.
Asistencia	E-mail/help Desk, asistencia telefónica, chat.	Ayuda telefónica, chat.	E-mail/help Desk, ayuda telefónica, chat.

Para el desarrollo de la propuesta de red existen softwares libres como GNS3, Mininet, Cisco Packet Tracer, Boson Netsim, sus características relevantes se encuentran expuesta en la tabla 4. Para el presente proyecto se seleccionó GNS3, ya que permite la compatibilidad con múltiples sistemas operativos de enrutadores y switches, utiliza imágenes reales de dispositivos, tiene mayor flexibilidad y control en la configuración de redes complejas, permite la integración con máquinas virtuales para realizar pruebas avanzadas, ajustándose a los requerimientos solicitados y para ser utilizado en la parte académica, siempre que se cumpla con los términos de la Licencia Pública General (GPL).

Tabla 4. Cuadro comparativo de los diferentes softwares libres de simulación [18].

Parámetros de evaluación	Herramientas			
	GNS3	Mininet	Packet Tracer	Boson Netsim
Sistema Operativo	Windows, Linux y MacOS.	Linux	Windows y Linux.	Windows
Tipo de licencia	Libre/Comercial.	Libre	Comercial	Comercial
Uso Investigativo	Alto	Alto	Alto	Medio
Manejo de equipos cisco	✓	—	✓	✓
Ejecución de programas reales	✓	✓	—	—
Soporte de diferentes protocolos	✓	✓	✓	✓

Para el uso de máquinas virtuales se propone Debian 11, FreeBSD, en la tabla 5 se presentan sus principales características, se seleccionó Debian 11 por el soporte de hardware, gran cantidad de paquetes de software disponibles utiliza el sistema herramienta de paquete avanzado (APT) para la gestión de paquetes, proporcionando estabilidad y soporte.

Tabla 5. Cuadro comparativo de los diferentes servidores libres de simulación [19].

Ítems	FreeBSD	Debian	Solaris
Prioridad	Son mas útiles los rangos de menor prioridad.	Los rangos bajos de prioridad son mejores.	Su prioridad aumenta a mayores rangos.
Funcionamiento de Cola	“Activa” y “expirados” son las colas que se manejan.	“Activa” y “expirados” son las colas que se emplean.	Por CPU se maneja cola de envió.
Decisión de prioridad	El tiempo de ejecución contra el tiempo inactivo son factores para el cálculo aritmético.	El tiempo de ejecución contra el tiempo inactivo son factores para el cálculo aritmético.	En la tabla se ejecuta una indagación.
Direccionamiento	Un vmSPACE, detalla el espacio de direcciones de un procedimiento, dividiéndolo en secciones lógicas conocidas como regiones.	Hace uso de un descriptor de memoria donde se segmenta el espacio de direcciones de un proceso en regiones lógicas denominadas “áreas de memoria”.	Cada procedimiento posee un “espacio de direcciones” compuesto por “segmentos”, que son secciones lógicas.
Gestión de archivos	Utiliza el método de atracción de datos o “nodo virtual”.	Utiliza el método de atracción de datos o “nodo virtual”.	Utiliza el principio inodo.

Para el monitoreo y análisis de los diferentes tráficos generados están disponibles software como Wireshark, Tcpdump y Fiddler, en la tabla 6 se detalla sus características. Para el presente proyecto se seleccionó Wireshark por ser la más adecuada para análisis exhaustivo de tráfico de red en varios protocolos, es de código abierto y multiplataforma permitiendo analizar el flujo de datos en la red en tiempo real y de archivos de captura previamente almacenados.

Tabla 6. Cuadro comparativo de los diferentes softwares libres de simulación [20].

Herramientas	Capacidades y Características		
Wireshark	Soporte para cientos de protocolos de red.	Compatible en todo sistema operativo. (Linux, Windows, MacOS, Solaris y más).	Interoperable con muchos formatos de archivos.
	Adquisición de datos en tiempo actual desde Ethernet, IEEE 802.11, ATM y más.	Soporte de variedad de protocolos de descifrado (WPA/WPA2, etc.).	Directrices cromáticas para una inspección visual más ágil.
Tcpdump	Registro de todas las interfaces disponibles.	Registro de una de las interfaces	Registra solo paquetes fallidos.
Fiddler	Manipulación de sesiones.	Prueba de seguridad.	Prueba de rendimiento.

Finalmente, para la aplicación de marcación de paquetes y calidad de servicio en un router Cisco, están disponibles la detección temprana aleatoria ponderada (WRED), cola de baja latencia (LLQ) y los servicios diferenciados (DiffServ). Para este proyecto se implementó un esquema de calidad de servicio WFQ, donde se crean múltiples filas de tráfico, cada una con una prioridad diferente. Y se trabaja mediante clasificación de prioridad por protocolos. La cola de alta prioridad enruta el tráfico de manera inmediata, mientras que la de baja prioridad lo hace cuando hay recursos disponibles. Para evitar el bloqueo total del tráfico entre las colas, lo que lleva a la implementación de diversos modelos de gestión de colas, desde la simple priorización hasta la asignación de recursos específicos a cada cola, utilizando técnicas de clasificación de paquetes para determinar a qué cola se envía cada paquete.

Capítulo 3

3. Implementación y pruebas

En este capítulo se expone los recursos requeridos en los equipos, configuraciones y pruebas del servicio de calidad. La topología propuesta consta de varios dispositivos interconectados, incluyendo teléfonos IP, un servidor de telefonía IP, routers y switches. Los teléfonos IP actúan como puntos finales de comunicación, mientras que el servidor de telefonía IP se encarga de gestionar las llamadas y la señalización. Los routers y switches dirigen el tráfico de voz a través de la red, asegurando la calidad de servicio y la conectividad adecuada. Esta topología permite a los usuarios explorar aspectos como la configuración de QoS, la resolución de problemas de latencia y la optimización de la red para garantizar una experiencia de voz clara y sin interrupciones. Para el desarrollo de este proyecto se contó con un total de cuatro máquinas virtuales creadas en virtual box con los que se arma dos escenarios en GNS3, las cuales se detallan a continuación:

- Dos máquinas que cuentan con Windows 7 basado en Microsoft.
- Una máquina con Debian 11 basado en Linux.
- Una máquina con Elastix 2.5.0 basado en Linux.

3.1 Escenario 1-Red VoIP

En el primer escenario se diseña la red VoIP, donde se evalúa únicamente lo que es tráfico VoIP, sus respectiva configuraciones y pasos a seguir se encuentran en el Anexo 1.

3.1.1 Implementación Red VoIP

La red del escenario 1 se muestra en la Fig.4, donde se emplea un enrutador, una centralita Asterisk que opera como un servidor SIP, manejando la señalización y el control de llamadas. Las dos PC funcionan como terminales SIP, utilizando la aplicación Zoiper para registrar extensiones en la centralita. Cuando una PC inicia una llamada, Zoiper codifica la voz en paquetes RTP y los envía al enrutador. La centralita autentica la llamada y establece una

sesión de voz entre las PC involucradas. Esta red VoIP simulada en GNS3 permite la comunicación basada en protocolos SIP y RTP, donde la centralita Asterisk se encarga de la gestión y el direccionamiento de las llamadas, mientras que las PC actúan como puntos terminales que utilizan Zoiper para interactuar con la infraestructura VoIP. Dentro del router se configura la velocidad en 1000 Mbps, se le da dirección IP a la interfaz GigabitEthernet1/0 192.168.200.143 y a la interfaz GigabitEthernet0/0 192.168.100.140.

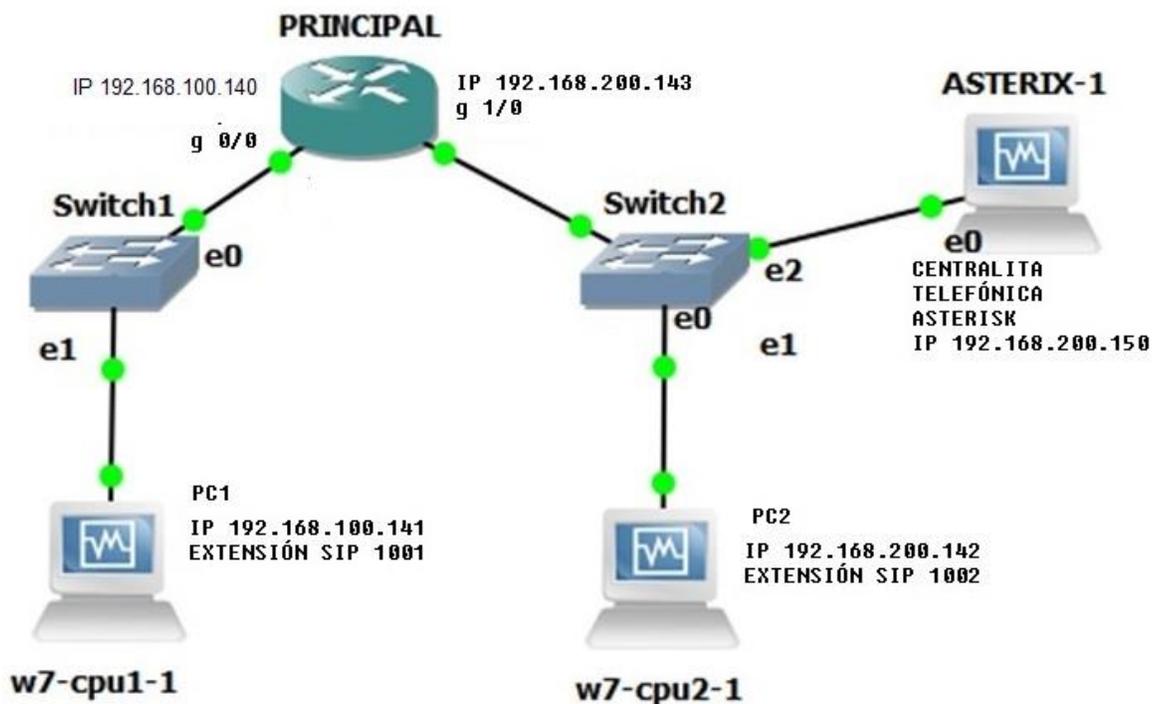


Fig. 4. Topología del escenario 1 definición de IP de cada componente.

3.1.2 Análisis de los resultados Red VoIP

En la red VoIP, al capturar el tráfico mediante Wireshark, se puede verificar que paquetes SIP han sido generados en el transcurso de una llamada IP, como se muestra en la Fig.5, donde hay paquetes con dirección IP origen y destino de las PC.

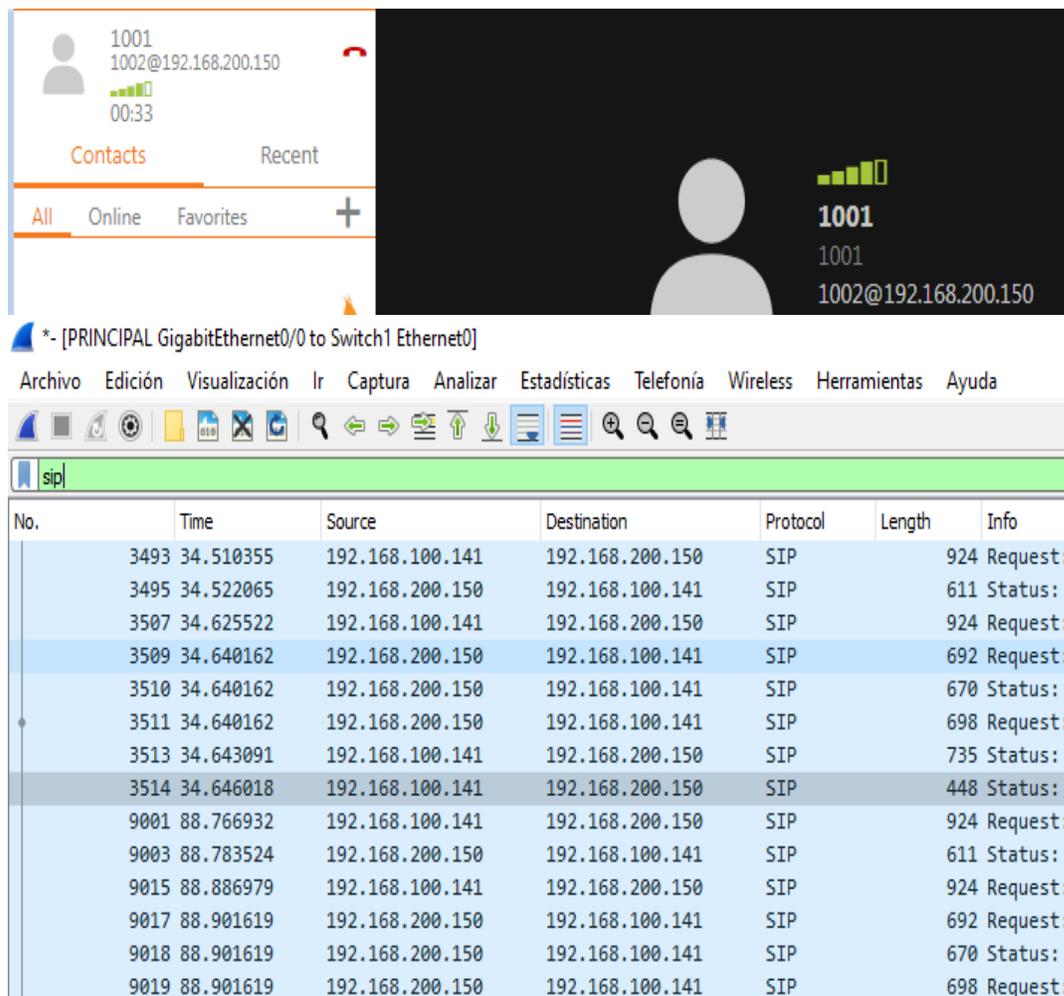


Fig. 5. Paquetes SIP captadas a traes de Wireshark en la red VoIP durante ja ejecución de una llamada IP.

En la Fig. 6 se observa el gráfico de tiempo al respecto de los bits del tráfico de voz para ver el flujo de los paquetes durante una ejecución de una llamada entre la PC1 y PC2, donde hay un alcance de 46000 Bits/seg. Con una latencia de 20 ms, por lo tanto, se puede considerar que es relativamente baja y es adecuada para una llamada IP. También, se observa un pico de 34000 Bits/seg, esto ocurre por una sincronización o problemas de conexión de la red. Confirmando que este escenario tiene un funcionamiento adecuado para realizar una red VoIP.

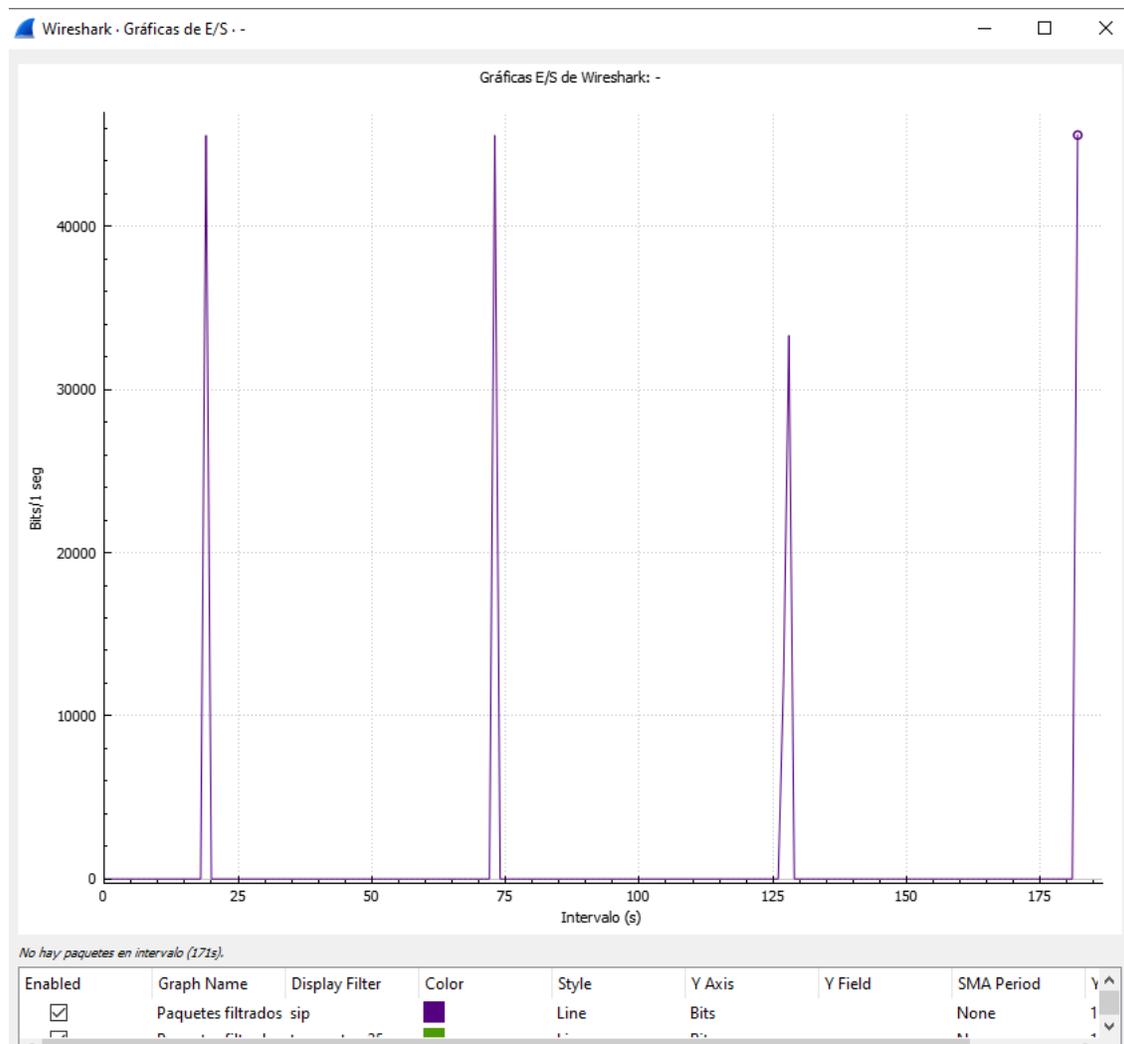


Fig. 6. Se visualiza el flujo del tráfico de la red VoIP.

3.2 Escenario 2-Red VoIP con QoS

En el segundo escenario se genera diferentes tipos de tráficos y configuraciones en los routers de calidad de servicio, sus respectivas configuraciones y pasos a seguir se encuentran en el Anexo2.

3.2.1 Implementación Red VoIP con QoS

En el entorno simulado en GNS3, se establece una red multiservicio que aborda la saturación del enlace con los tráficos de VoIP, correo y transferencia de archivo. En esta topología, como se muestra en la Fig.7, los switches segmentan y dirigen el tráfico, mientras que la centralita Asterisk actúa como el controlador central para las llamadas VoIP, gestionando la señalización y el direccionamiento. Las dos PC ejecutan Zoiper como cliente, interactuando con la centralita Asterisk. La integración de elementos Debian 11 en la red permite generar tráfico FTP, las PC cuentan con WinSCP para la transferencia de correo electrónico.

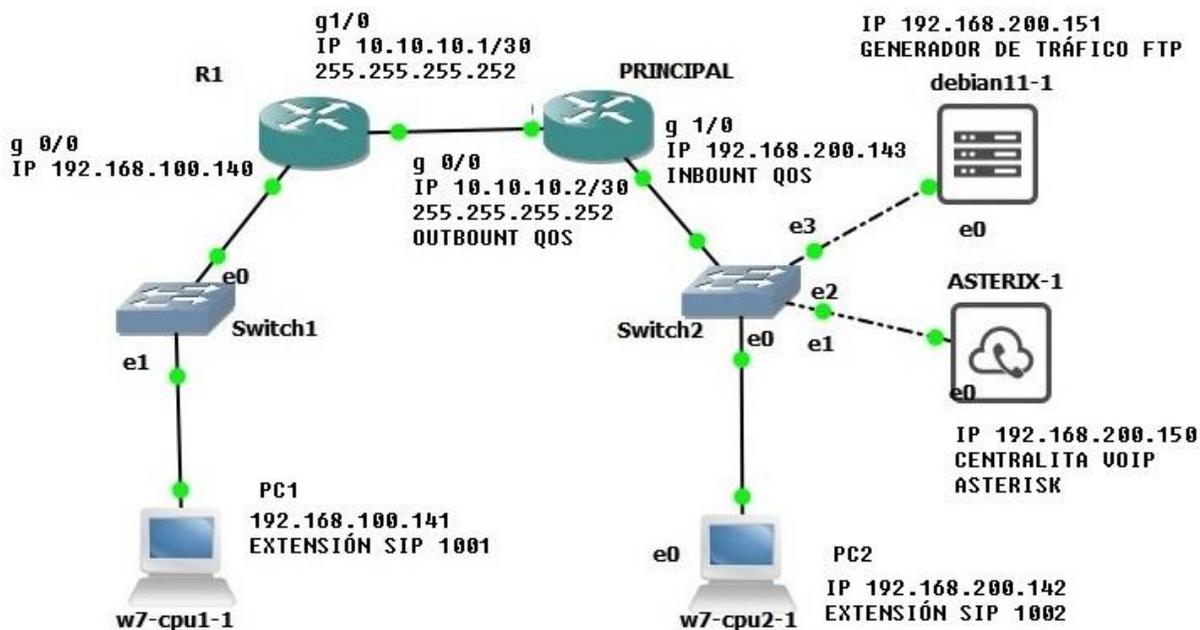


Fig. 7. Topología del escenario 2 con sus respectivas IP.

En esta red el router principal se lo configura con enrutamiento estático, reglas de acceso ACL por protocolo, marcación de paquetes QoS, asignación de prioridad con mapeo de clases QoS, el cual gestiona el enrutamiento de los paquetes mediante la asignación de niveles de servicio (DSCP), asegurando la entrega constante y predecible de la voz. Entre router principal y router R1 se utilizan técnicas de control de la velocidad del flujo de tráfico en el ancho de banda mediante el comando rate-limit en las interfaces GigabitEthernet1/0 e interfaz GigabitEthernet0/0 y configuraciones de asignación de políticas de mapeo QoS sobre dichas interfaces. Las configuraciones mencionadas se muestran en la tabla 7 del router R1 y en la tabla 8 del router PRINCIPAL.

Tabla 7. Configuraciones del Router 1.

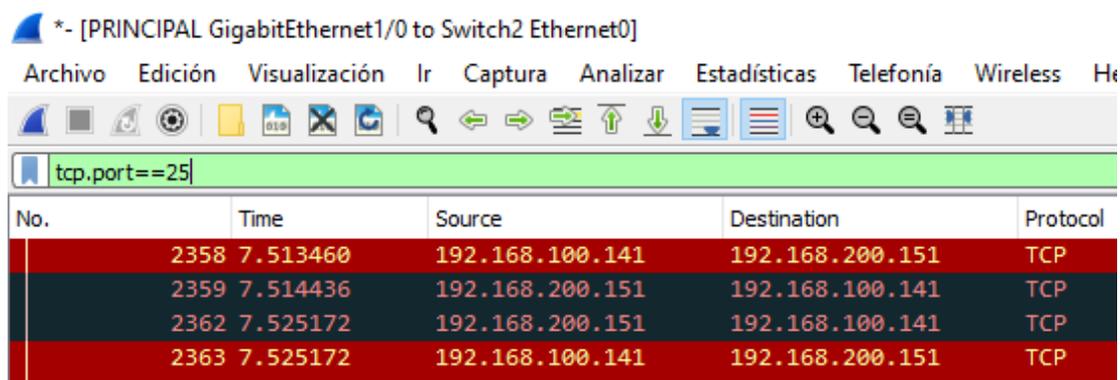
ROUTER R1	CONFIGURACION DE ENRUTAMIENTO ESTATICO	<pre>#ENABLE #CONFIG TERMINAL #HOSTNAME PRINCIPAL #interface GigabitEthernet0/0 #ip address 10.10.10.2 255.255.255.252 #rate-limit output 128000 24576 49152 conform-action transmit exceed-action drop #interface GigabitEthernet1/0 #ip address 192.168.200.143 255.255.255.0 #rate-limit output 128000 24576 49152 conform-action transmit exceed-act #EXIT</pre>
	CONFIGURACION DE PUERTOS G1/0 Y G0/0	<pre>#ENABLE #CONFIG TERMINAL #ip route 192.168.200.0 255.255.255.0 192.168.200.143 #ip route 192.168.200.0 255.255.255.0 10.10.10.2</pre>

Tabla 8. Configuraciones del router PRINCIPAL.

ROUTER PRINCIPAL	CONFIGURACION DE PUERTOS G1/0 Y G0/0	<pre>#ENABLE #CONFIG TERMINAL #HOSTNAME PRINCIPAL #interface GigabitEthernet0/0 #ip address 10.10.10.2 255.255.255.252 #rate-limit output 128000 24576 49152 conform-action transmit exceed-action drop #interface GigabitEthernet1/0 #ip address 192.168.200.143 255.255.255.0 #rate-limit output 128000 24576 49152 conform-action transmit exceed-act #EXIT</pre>
	CONFIGURACION DE ENRUTAMIENTO ESTatico	<pre>#ENABLE #CONFIG TERMINAL #ip route 192.168.100.0 255.255.255.0 192.168.100.140 # ip route 192.168.100.0 255.255.255.0 10.10.10.1</pre>
	CONFIGURACION DE REGLAS DE ACCESO ACL POR PROTOCOLO	<pre># ip access-list extended VIP-rtp-sip-rtcp # permit tcp any any eq 1720 # permit udp any any eq 2427 # permit tcp any any eq 2428 # permit tcp any any range 2000 2002 # permit udp any any eq 1719 # permit udp any any eq 4569 # permit tcp any any range 5060 5061 # permit udp any any range 5060 5061 # permit icmp any any # permit udp any any range 10000 20000 # permit udp any any range 20000 65535 # ip access-list extended email # permit tcp any any eq smtp # ip access-list extended ftp-sftp # permit tcp any any eq ftp-data # permit tcp any any eq ftp</pre>
	CONFIGURACION DE MARCACION DE PAQUETES QoS	<pre>#class-map match-all MAP-VIP-rtp-sip-rtcp #match access-group name VIP-rtp-sip-rtcp #class-map match-all MAP-email #match access-group name email # class-map match-all MAP-ftp-sftp # match access-group name ftp-sftp</pre>
	CONFIGURACION DE ASIGNACION DE PRIORIDAD CON MAPEO DE CLASE QoS	<pre>#class-map match-all MAP-oro #match dscp ef #class-map match-all MAP-plata # match dscp af22 # class-map match-all MAP-bronze # match dscp af31</pre>
	CONFIGURACION DE POLITICA DE MAPEO DE CLASE Y ASIGNACION DE ANCHO DE BANDA PORCENTUAL QoS	<pre>#policy-map POL-CLASSIFY-OUT #class MAP-oro #bandwidth percent 30 #class MAP-plata #bandwidth percent 30 #class MAP-bronze #bandwidth percent 30 #class class-default #fair-queue #policy-map POL-CLASSIFY-IN #class MAP-VIP-rtp-sip-rtcp #set dscp ef #class MAP-ftp-sftp # set dscp af22 # class MAP-email # set dscp af31</pre>
	CONFIGURACION DE ASIGNACION DE POLITICAS DE MAPEO QoS SOBRE LOS PUERTOS G1/0 Y G0/0	<pre>#ENABLE #CONFIG TERMINAL #interface GigabitEthernet0/0 # service-policy output POL-CLASSIFY-OUT #interface GigabitEthernet1/0 # service-policy input POL-CLASSIFY-IN</pre>

3.2.2 Análisis de los resultados Red VoIP con QoS

En la Fig. 8 se comprueba que se a generado los paquetes TCP, por esta razón se filtrar la captura del tráfico mediante Wireshark a través del puerto destino 25, para una mejor visualización de estos paquetes. Además, en la Fig. 9 se observa 3 flujos diferentes de tráfico IP capturados durante las pruebas de simulación. EL flujo del color morado representa el tráfico VoIP, el verde representa el tráfico FTP y el amarillo representa el tráfico de correo. En la misma gráfica se observa que el tráfico VoIP alcanzó picos de ancho de banda de 100 kbps, el tráfico FTP alcanzó picos de ancho de banda de 200 kbps y el tráfico de correo alcanzó picos de ancho de banda de 420 kbps. En total durante la simulación se generó un promedio de 408 kbps de flujo de tráfico. Así, confirmando que en esta red existe tráfico de correo, FTP Y VoIP simultáneamente.



The screenshot shows the Wireshark interface with the following details:

- Window title: *- [PRINCIPAL GigabitEthernet1/0 to Switch2 Ethernet0]
- Menu bar: Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, He
- Filter bar: tcp.port==25
- Packet list table:

No.	Time	Source	Destination	Protocol
2358	7.513460	192.168.100.141	192.168.200.151	TCP
2359	7.514436	192.168.200.151	192.168.100.141	TCP
2362	7.525172	192.168.200.151	192.168.100.141	TCP
2363	7.525172	192.168.100.141	192.168.200.151	TCP

Fig. 8. Paquetes TCP, correo, captados mediante Wireshark de la red VoIP con QoS.



Fig. 9. Se visualiza los 3 tipos de tráfico generados a través de la red VoIP con QoS mediante Wireshark y su promedio de bits/s.

Y en la Fig. 10 se muestra el resultado del comando “show policy-map interface GigaEthernet0/0”, donde muestra la política de servicio llamada “POL-CLASSIFY-OUT”, que consiste en dividir el tráfico en cuatro clases utilizando diferentes criterios de coincidencia (class-map). Las clases se denomina "MAP-oro", "MAP-plata", "MAP-bronce" y "class-default". Estas class-maps se utilizan para clasificar tipos de tráfico en función de las diferencias en el valor DSCP. Cada class-map tiene una correspondencia con un valor DSCP específico. Los paquetes de la clase "MAP-oro" coinciden con el valor DSCP ef (46). Los paquetes de la clase "MAP-plata" coinciden con el valor DSCP af22 (20). Los paquetes de la clase "MAP-bronce" coinciden con el

valor DSCP af31 (26). La clase "class-default" es una clase que captura cualquier paquete que no coincida con las clases anteriores. Se especifica una limitación de cola para cada class-map con un límite de 64 paquetes. La salida muestra la profundidad de la cola, la cantidad total de paquetes descartados y la cantidad de paquetes enviados. Cada class-map tiene una asignación de ancho de banda del 30% en la política de salida. Así, demostrando las configuraciones de QoS en la interfaz GigabitEthernet0/0, la cual está diseñada para clasificar y asignar ancho de banda a diferentes tipos de tráfico en función del valor DSCP de los paquetes. Y que cada class-map tiene su propia asignación de ancho de banda y límite de cola.

```

PRINCIPAL>show policy-map interface g0/0
GigabitEthernet0/0

Service-policy output: POL-CLASSIFY-OUT
Class-map: MAP-oro (match-all)
  2199 packets, 493084 bytes
  5 minute offered rate 12000 bps, drop rate 0000 bps
  Match: dscp ef (46)
  Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 1582/360866
    bandwidth 30% (300000 kbps)
Class-map: MAP-plata (match-all)
  35 packets, 2178 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: dscp af22 (20)
  Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 34/2112
    bandwidth 30% (300000 kbps)
Class-map: MAP-bronze (match-all)
  999 packets, 83916 bytes
  5 minute offered rate 1000 bps, drop rate 0000 bps
  Match: dscp af31 (26)
  Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 427/35868
    bandwidth 30% (300000 kbps)
Class-map: class-default (match-any)
  405 packets, 546537 bytes
  5 minute offered rate 12000 bps, drop rate 0000 bps
  Match: any
  Queueing
    queue limit 64 packets
    (queue depth/total drops/no-buffer drops/flowdrops) 0/0/0/0
    (pkts output/bytes output) 271/343661
  Fair-queue: per-flow queue limit 16 packets

```

Fig. 10. Configuraciones del router principal de la red VoIP con QoS

Capítulo 4

4. Conclusiones y recomendaciones

4.1 Conclusiones

- Se implementó un generador de tráfico adecuado para la ejecución del proyecto, utilizando la plataforma GNS3 como emulador. En este entorno, se integraron máquinas virtuales mediante VirtualBox para sistemas operativos Windows y Linux. Para la simulación de tráfico de correo electrónico, se empleó Scapy. El servidor de llamadas VoIP se implementó a través de Asterisk, mientras que Zoiper se utilizó para simular teléfonos VoIP. Además, para generar tráfico FTP, se recurrió a WinSCP.
- Se implementó un esquema de QoS con el propósito de clasificar diversos paquetes y otorgar prioridad al tráfico IP. Esto se logró mediante la asignación de categorías de ancho de banda, en las cuales se designó "Premium" a los paquetes de VoIP con la máxima prioridad, "Silver" a los paquetes de correo electrónico con prioridad media y "Bronce" a los demás paquetes, que abarcan el tráfico de envío por FTP con la prioridad más baja.
- Se obtuvo y se analizó estadísticas sobre el flujo de paquetes durante llamadas VoIP utilizando Wireshark, que proporcionó una visualización detallada del tráfico VoIP en la red. Esto permitió simular efectivamente el desempeño de un servicio de telefonía VoIP en un entorno realista. Además, se implementaron métodos de optimización de ancho de banda y políticas de QoS para mejorar la calidad de servicio, mediante configuraciones de política de mapeo de clase y asignación de ancho de banda porcentual.

4.2 Recomendaciones

- Antes de la implementación de un sistema de políticas de QoS en un entorno de producción real, es prudente realizar pruebas en un ambiente de simulación. Mediante la combinación de una configuración específica y una evaluación completa, es posible obtener discernimientos significativos acerca del comportamiento de la calidad de servicio en un entorno simulado de comunicación VoIP.
- Se implementó el protocolo SIP para la transmisión de VoIP; sin embargo, se sugiere emplear métodos de compresión de códecs actuales y disponibles, con el objetivo de disminuir el uso de ancho de banda. Estos métodos deberían ser capaces de lograr una compresión más efectiva en la transmisión de audio sin que se vea comprometida la calidad de voz.
- Se utilizó Wireshark con el propósito de realizar un análisis estadístico del ancho de banda transmitido. No obstante, para lograr una mejor comprensión, se aconseja el uso de herramientas más abarcadoras, como el protocolo simple de manejo de red (SNMP), este protocolo permite llevar a cabo el estudio y supervisión exhaustiva de información, incluyendo el uso de ancho de banda, disponibilidad de memoria RAM, entre otros aspectos relevantes.

Referencias

- [1] V. J. M. Galleno, Optimización en el despliegue de servicios de Voz sobre IP (VoIP) sobre redes WiFi con restricciones de calidad, Tesis doctoral, Sevilla: Escuela Técnica Superior de Ingeniería Universal de Sevilla, 2020.
- [2] E. D. R. R. y. J. I. O. d. B. Domínguez, Sistemas de telefonía fija y móvil, Madrid: Ediciones Paraninfo, 2018.
- [3] C. P. C. Fuentes, Ruta óptima de tráfico de una red virtual basada en análisis de datos y algoritmo de machine learning, Trabajo de titulación previo a la obtención del grado académico de Magíster en Telecomunicaciones, Ambato: Universidad técnica de Ambato, 2021.
- [4] E. d. R. Ruiz, Sistemas de telefonía fija y móvil, Madrid: Ediciones Paraninfo, 2023.
- [5] Quarea, «¿Que es Asterisk?: Centralita telefónica IP,» Quarea Voz Datos IP, [En línea]. Available: quarea. <https://quarea.com/es/que-es-asterisk-centralita-telefonica-ip/>. [Último acceso: 28 mayo 2023].
- [6] R. S. J. Joscowicz, «Medida de la calidad de voz en Redes IP,» de *Memoria de trabajos de difusión científica y técnica*, n.º 5, Montevideo, Univesidad de Montevideo, 2007, pp. 12-23.
- [7] J. Andreu, Voz IP (Servicios en red), Madrid: Editorial Editex, 2011.
- [8] L. A. U. Armijo, Evaluación De Herramientas De Generación De Tráfico Malicioso Aplicadas A Una Red IP Virtualizada, Tesis para el grado de Maestría, Valencia: Universidad Politécnica de Valencia, 2017.
- [9] F. García., «Arsys Blog,» Debian: características, origen y distribuciones derivadas, 20 julio 2022. [En línea]. Available: arsys. <https://www.arsys.es/blog/distribucion-linux-debian> (accedido el 28 de mayo de 2023).. [Último acceso: 28 mayo 2023].
- [10] M. Blog, «Softphone Zoiper: qué es, para qué sirve y características,» <https://www.masip.es>, [En línea]. Available: /blog/softphone-zoiper/. [Último acceso: 28 mayo 2023].
- [11] vay3t.medium , «Hacking con Python 3: Capitulo 8 — Entendiendo Scapy". Medium,» <https://vay3t.medium.com>, 12 diciembre 2020. [En línea]. Available: <https://vay3t.medium.com/hacking-con-python-3-capitulo-8-entendiendo-scapy8bf619514d04>. [Último acceso: 2 junio 2023].
- [12] L. M. S. Blasco, "CALIDAD DE SERVICIO (QoS) CON ROUTERS CISCO", trabajo fin de grado, Valencia: Universidad Politécnica de València, 2019.
- [13] S. Bisrat, Improving the Quality of Service of Voice over Internet Protocol in Ethio Telecom Service Level Agreement Customers, Tesis para el grado de Maestría, Addis Ababa: St. Mary's University, 2021.
- [14] Capterra, «Linphone y Zoiper, Capterra,» <https://www.capterra.ec>, [En línea]. Available: <https://www.capterra.ec/compare/158709/158719/linphone-vs/zoiper> . [Último acceso: 25 agosto 2023].

- [15] Capterra, «3CX y Linphone. Capterra.,» <https://www.capterra.ec>, [En línea]. Available: <https://www.capterra.ec/compare/158704/158709/3cx/vs/linphone> . [Último acceso: 25 agosto 2023].
- [16] Capterra, «Aircall y Asterisk,» <https://www.capterra.ec>, [En línea]. Available: <https://www.capterra.ec/compare/144486/60249/aircall/vs/asterisk>. [Último acceso: 25 agosto 2023].
- [17] liveagent, «Software de ^centro de llamadas^ entrantes. LiveAgent,» <https://www.liveagent.es>, [En línea]. Available: <https://www.liveagent.es/software-de-centro-de-llamadas-para-llamadas-entrantes/>. [Último acceso: 25 agosto 2023].
- [18] X. d. C. P. Armijos, Análisis de herramientas de software para la simulación y emulación de redes de computadores para aprendizaje en entornos de laboratorio, Trabajo titulación para propuestas tecnológicas, Machala: Universidad técnica de Machala, 2022.
- [19] FREEDSD BLOG, «Comparación con Linux, Solaris y FreeBSD,» <http://frebsd-sistemas-operativos.blogspot.com>, [En línea]. Available: <http://frebsd-sistemas-operativos.blogspot.com/p/comparacion-con-linux-y-solaris.html> . [Último acceso: 25 AGOSTO 2023].
- [20] Geekflare, «12 analizadores de paquetes de red para administradores de sistemas y analistas de seguridad,» <https://geekflare.com>, [En línea]. Available: <https://geekflare.com/es/network-packet-analyzers/>. [Último acceso: 25 agosto 2023].
- [21] vay3t, «Hacking con Python3: Capítulo 8 - entendiendo scrapy,» <https://www.vay3t.medium.com>, 12 diciembre 2020. [En línea]. [Último acceso: 28 mayo 2023].
- [22] L. M. S. Blasco, CALIDAD DE SERVICIO (QoS) CON ROUTERS CISCO", trabajo fin de grado, 2019.

Anexos

Anexo 1. Guía 1-Red VoIP

GUÍA N°2 Red VoIP

Objetivos:

- Instalar el software para emular máquinas virtuales - Virtual Box.
- Familiarizarse con la máquina virtual y el simular de red instalado.
- Implementar una central VoIP.
- Realizar el análisis estadístico del flujo de paquetes durante una llamada de VOIP.

Marco teórico:

Asterisk

Es una plataforma de telefonía de código abierto que permite crear sistemas de telefonía IP con características avanzada. Es altamente flexible, escalable y se utiliza para realizar llamadas a través de redes IP. Es ampliamente utilizado para desarrollar soluciones personalizadas de comunicación de voz y video.

Ventajas de la telefonía IP

La telefonía convencional tiene un costo considerablemente superior en comparación con la telefonía IP. Las ventajas de la telefonía IP:

- No hay costos de comunicación entre los usuarios que se encuentran en los mismos centros de trabajo, edificios o incluso en la misma red de proveedores de VoIP P2P.
- Si se utiliza en conjunto con redes inalámbricas en centros que tienen una línea de visión directa, no se aplican tarifas o cuotas.
- Ofrece la posibilidad de roaming (itinerancia, movilidad), permitiendo la transmisión simultánea de voz y datos, e incluso facilitando el envío de fax, vídeo y televisión por IP.
- No depende del tipo de conexión a Internet. No está ligado al hardware, puede ser virtualizado y tiene capacidad de escalabilidad.
- Posibilita que las personas que nos llaman puedan realizar llamadas locales a bajo costo. La implementación de softphones tiene un costo muy reducido.

Equipos requeridos:

- Laptop o PC
- Conexión a Internet

Instrucciones

Instalación de Virtual Box

1. Entrar en la página oficial de VirtualBox
2. <https://www.virtualbox.org/wiki/Downloads>
3. Dar click en Windows Hosts

Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

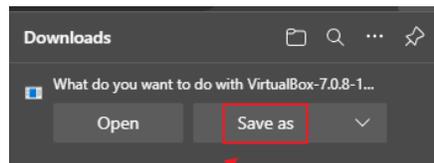
If you're looking for the latest VirtualBox 6.1 packages, see [VirtualBox 6.1 builds](#). Versi

VirtualBox 7.0.8 platform packages

- [Windows hosts](#)
- [macOS / Intel hosts](#)
- [Developer preview for macOS / Arm64 \(M1/M2\) hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)
- [Solaris 11 IPS hosts](#)

Captura 1: Captura de pantalla de la página de descarga de VirtualBox.

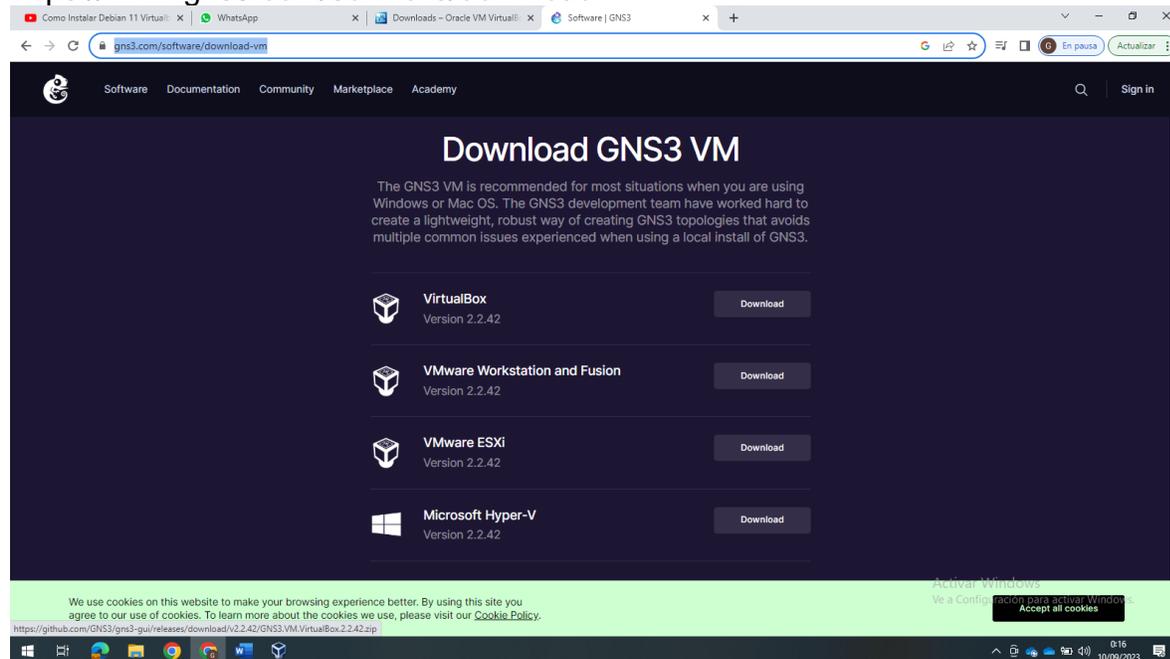
- Se abrirá un mensaje de descarga, dar click en Guardar o Save y esperar que termine la descarga.



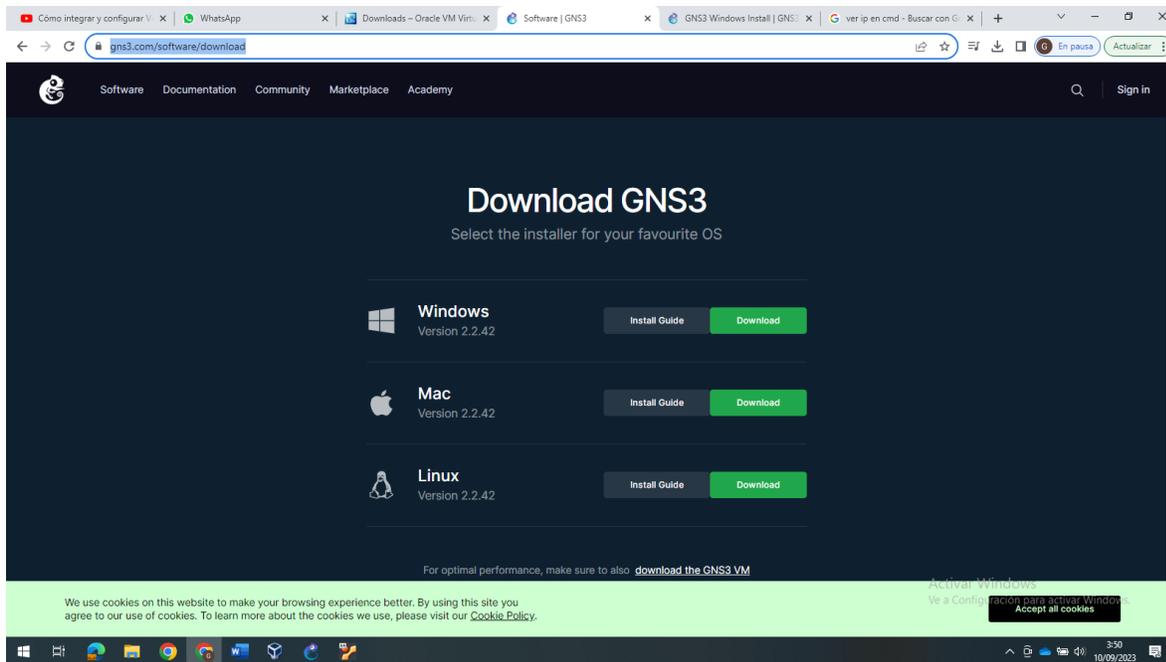
Captura 2: Captura para guardar la descarga de VirtualBox.

Instalación de GNS3

<https://www.gns3.com/software/download-vm>

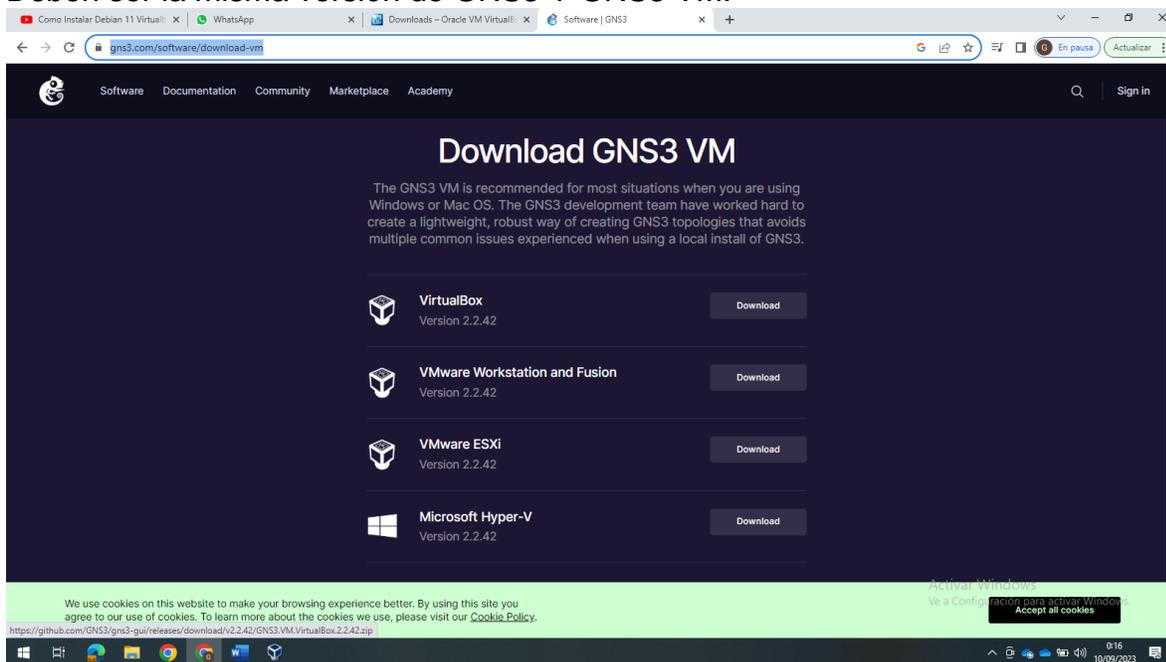


Los pasos a seguir se encuentran detallados en la página oficial de GNS3 donde se debe seleccionar para cual sistema operativo se desea: <https://www.gns3.com/software/download>



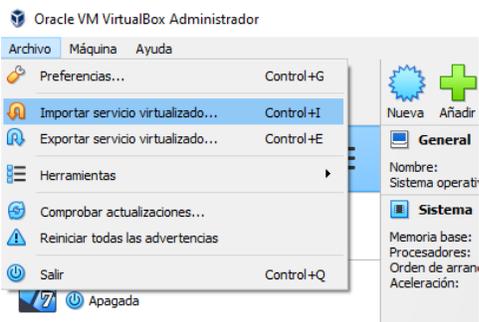
Instalación de máquinas virtuales para GNS3

Descargar el VM de GNS3 desde el siguiente link:
<https://www.gns3.com/software/download-vm>
 Deben ser la misma versión de GNS3 Y GNS3 VM.

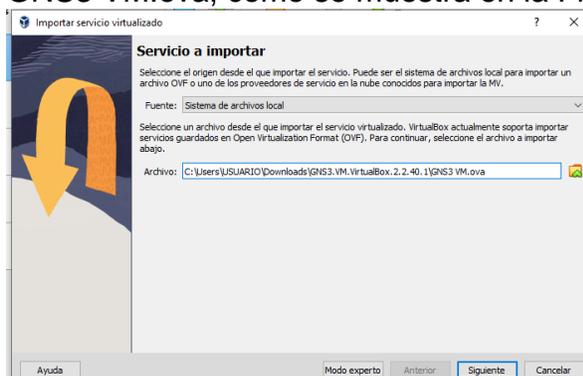


Crear las siguientes máquinas virtuales

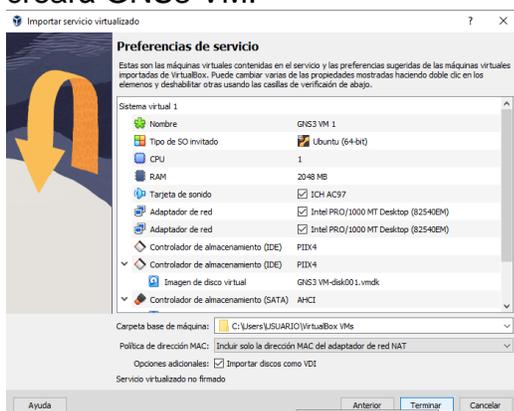
Seleccionar Importar servicios virtualizado..., que se encuentra en Archivos como se muestra en la Fig.

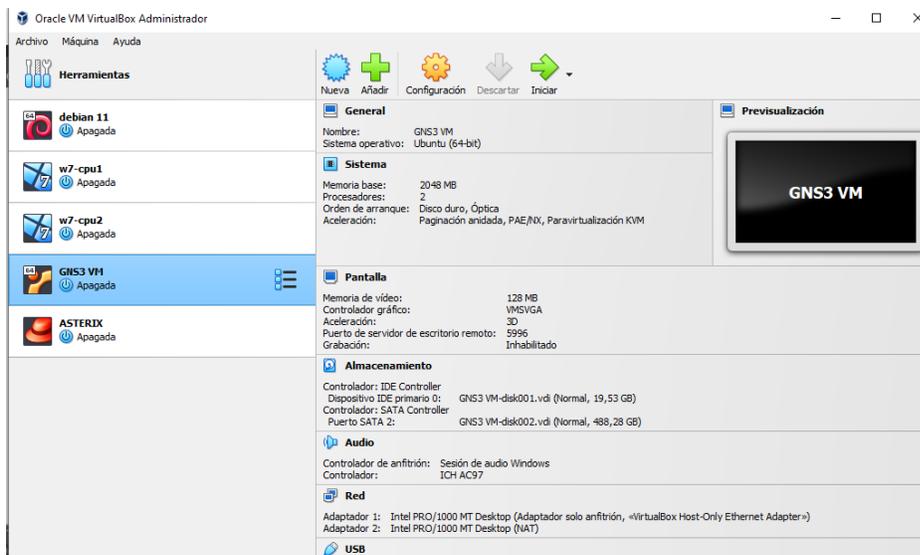


Se abre la siguiente imagen donde se debe importar el archivo de servicio virtualizado, GNS3 VM.ova, como se muestra en la Fig.



Adecuar la CPU y RAM en base a la capacidad de la computadora donde se encuentran trabajando. Por ejemplo, si su computadora es de 4 núcleos ajustar a un núcleo la máquina virtual. Dejar habilitado los dos adaptadores. Siguiendo dar clic en terminal y se creará GNS3 VM.





Para las creacion de las maquinas virtuales, debemos descargar primero las imágenes ISO de los sistemas operativos que se van a utilizar, en este caso haremos uso de 3 sistemas operativos, el primero es Windows 7 basado en Microsoft, pero puede ser cualquier version de Windows, el segundo es Debian 11 basado en linux y el tercero es Elastix 2.5.0 basado en linux.

Descarga de Windows 7: <https://www.microsoft.com/es-es/software-download/windows7>

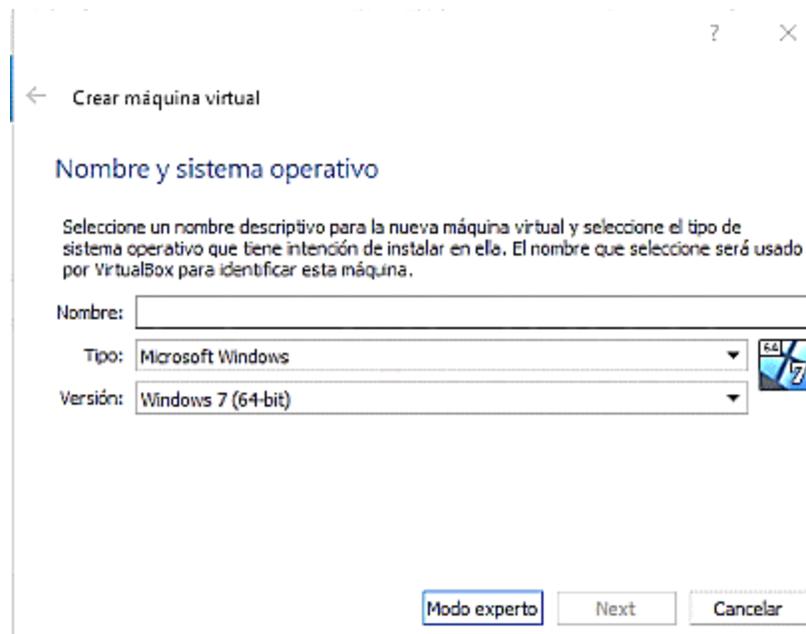
Descarga de Debian 11: <https://www.debian.org/download>

Descarga de Elastix 2.5.0: <https://archive.org/details/Elastix2.5.0Stable1386Bin21oct2014>

Una vez descargados las imágenes abriremos VirtualBox y haremos clic en el boton Nueva

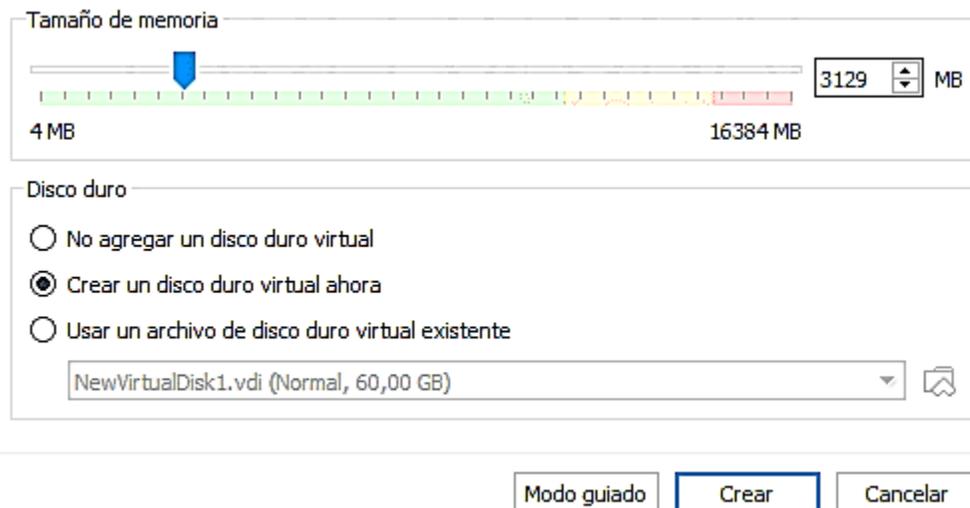


Luego nos Aparecera una ventana para crear la Maquina Virtual Y le damos un nombre:



En nombre le ponemos el nombre que deseamos, en la opción Tipo elegimos el sistema operativo adecuado, si es basado en Microsoft elegimos Microsoft Windows, si es basado en Linux elegiremos Linux.

Presionamos Next y elegimos el tamaño de memoria ram, esto dependerá de las características del equipo que hospeda estas máquinas virtuales pero por lo general en Windows se puede asignar 2 GB (2048 MB) de ram y en Linux 1 GB (1024 MB), luego elegimos crear un disco duro nuevo para la creación de la máquina virtual



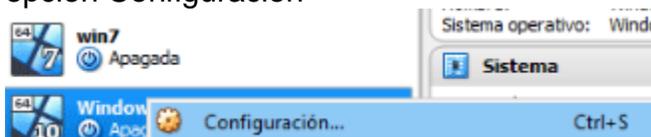
En ubicación del disco duro elegimos haciendo clic en el icono  y elegimos la ubicación a nuestro gusto

En tipo de disco duro elegimos por defecto VDI y en Almacenamiento dejamos elegido Reservado dinámicamente

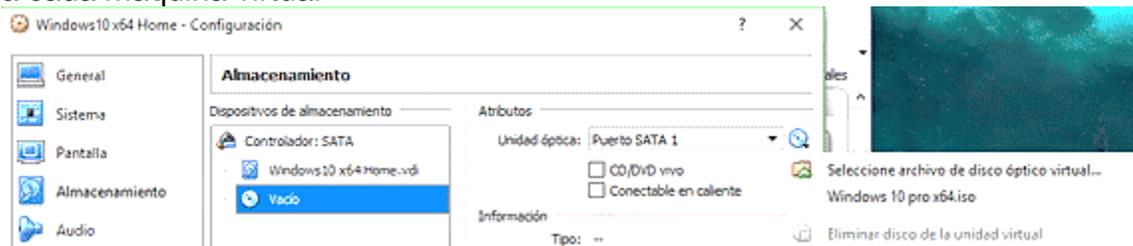
Tipo de archivo de disco duro	Almacenamiento en unidad de disco duro física
<input checked="" type="radio"/> VDI (VirtualBox Disk Image)	<input checked="" type="radio"/> Reservado dinámicamente
<input type="radio"/> VHD (Virtual Hard Disk)	<input type="radio"/> Tamaño fijo
<input type="radio"/> VMDK (Virtual Machine Disk)	Dividir en archivos de menos de 2 GB
<input type="radio"/> HDD (Parallels Hard Disk)	
<input type="radio"/> QCOW (QEMU Copy-On-Write)	
<input type="radio"/> QED (QEMU enhanced disk)	
<input type="button" value="Modo guiado"/> <input checked="" type="button" value="Crear"/> <input type="button" value="Cancelar"/>	

Luego hacemos clic en el Boton Crear, y asi lo hacemos con el resto de Maquinas virtuales

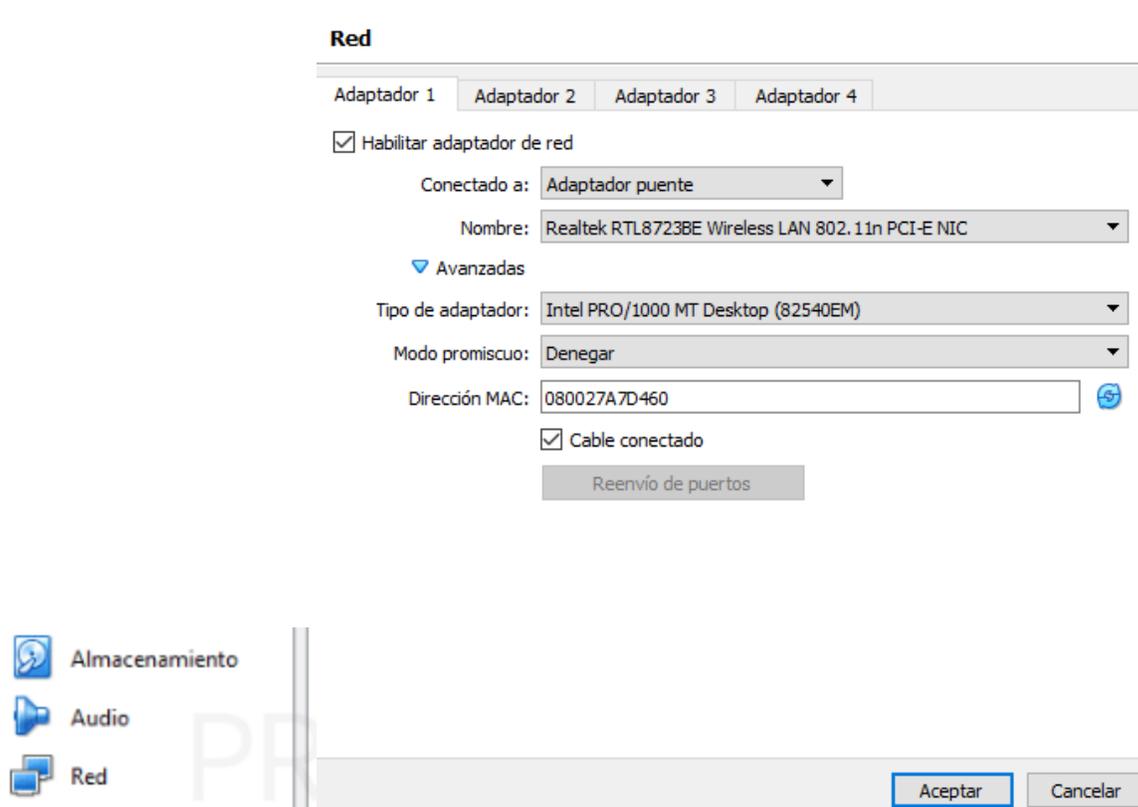
Una vez creadas las Maquinas Virtuales hacemos clic en una de ellas y elegimos la opcion Configuracion



Nos dirigimos a la seccion Almacenamiento y elegimos la imagen ISO correspondiente a cada maquina virtual

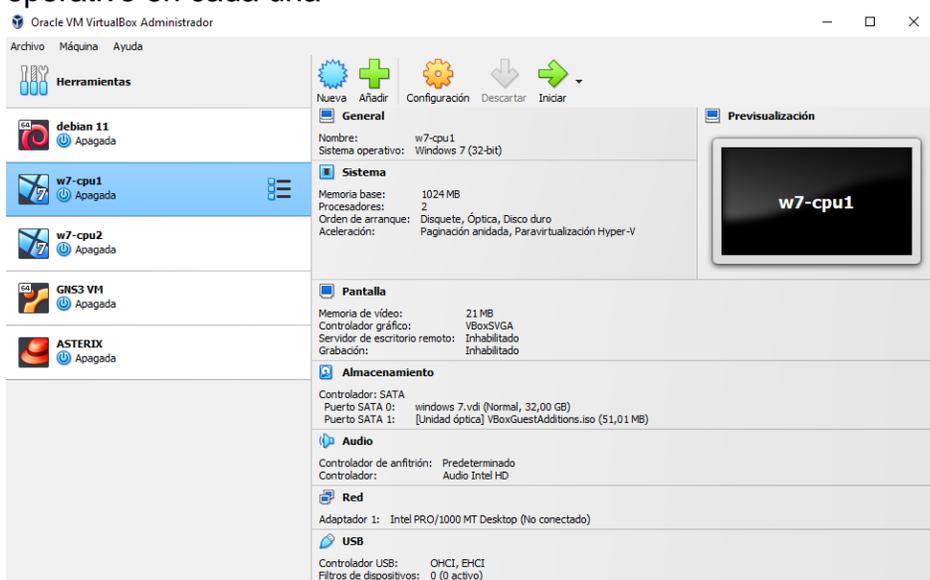


Luego nos dirigimos a la sesión Red y elegimos el modo Adaptador Puente en cada maquina virtual para que las maquinas virtuales pueda conectarse a la red local del equipo Anfitrión mediante la misma tarjeta de red



Luego presionamos el boton Aceptar y hacemos los mismos pasos para el resto de maquinas virtuales

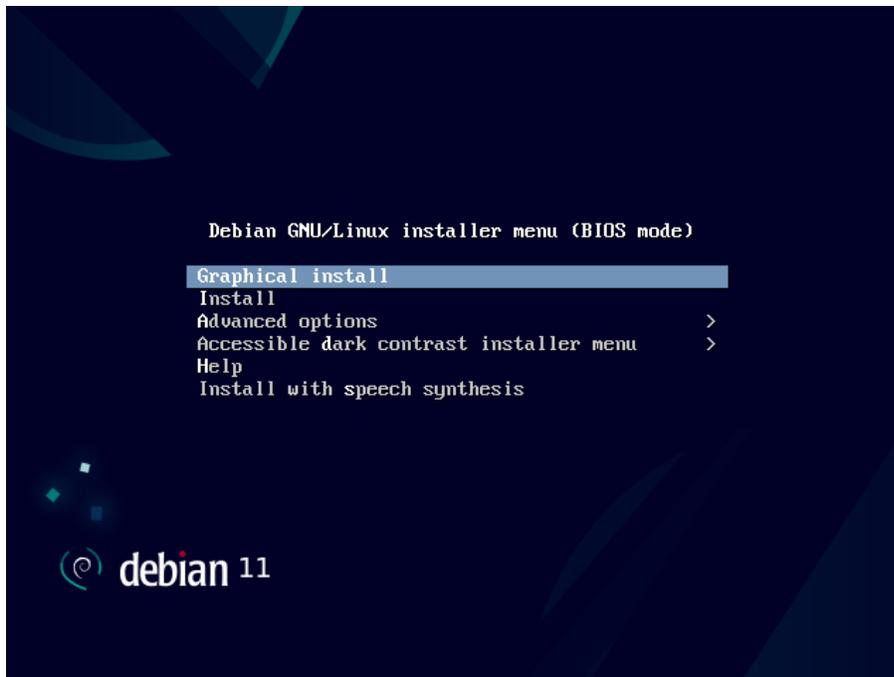
Una vez hecho esto en todas las maquinas procedemos a la instalacion del sistema operativo en cada una



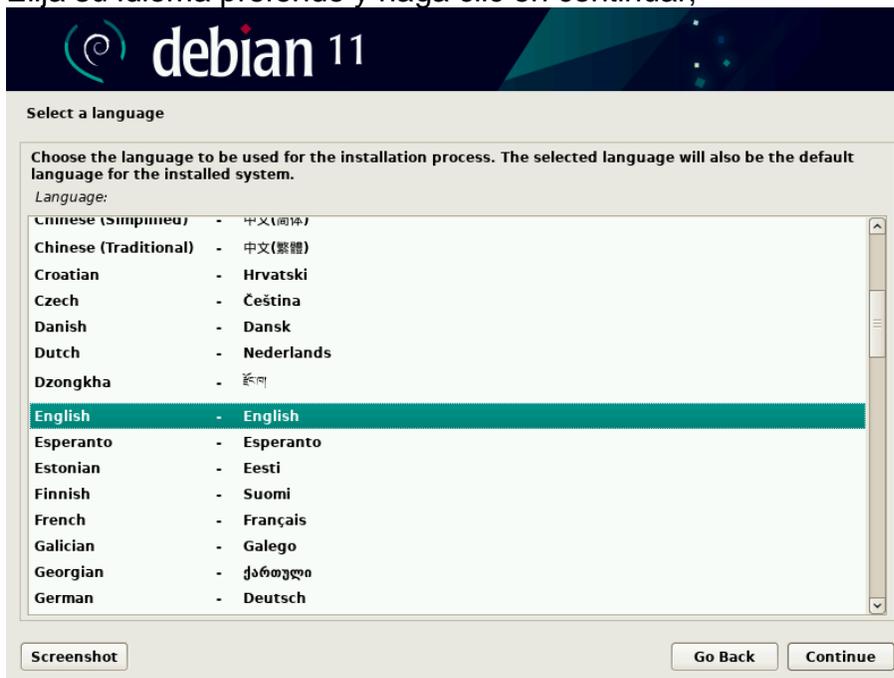
INSTALACION DE DEBIAN 11

Iniciamos la maquina virtual Debian creada previamente.

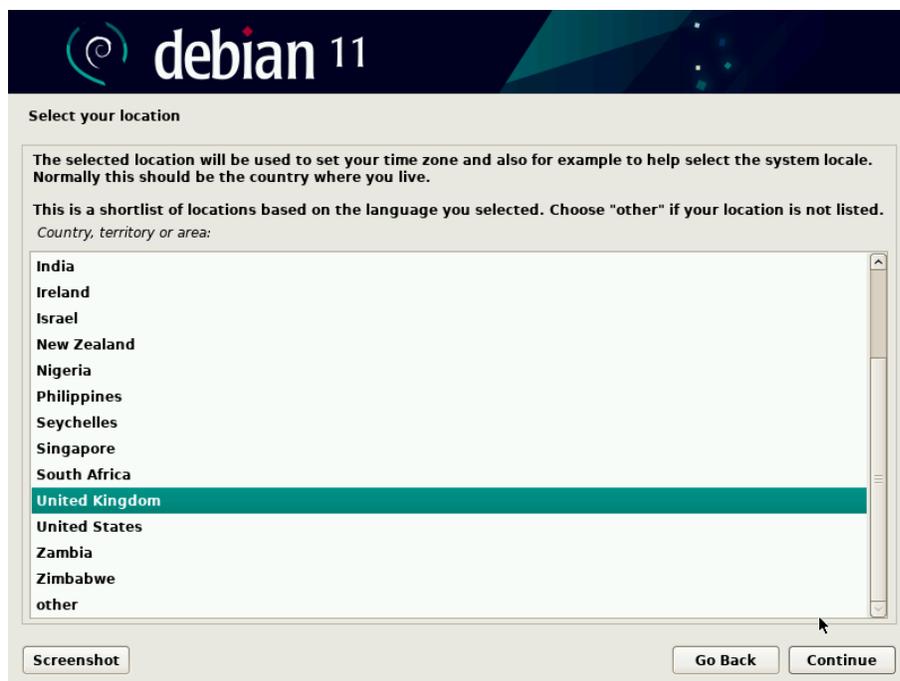
Una vez que el sistema arranque con un medio de arranque, obtendremos la siguiente pantalla.



Elija la opción 'Instalación gráfica' y presione enter.
Elija su idioma preferido y haga clic en continuar,

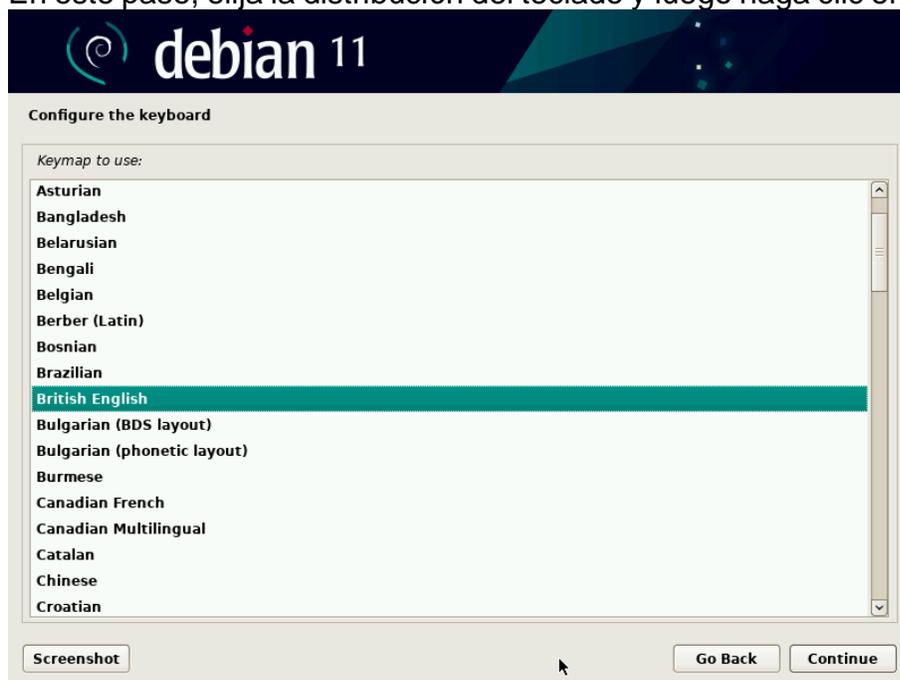


Elija su ubicación preferida que se usará para configurar la zona horaria de su sistema.



Haga clic en Continuar

En este paso, elija la distribución del teclado y luego haga clic en continuar para proceder



En este paso, el instalador le pedirá que configure el nombre de host, así que especifique el nombre de host que desea configurar y luego haga clic en continuar.



Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

Screenshot Go Back Continue

En la siguiente pantalla, especifique el nombre de dominio.



Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

Screenshot Go Back Continue

Especifique la contraseña del usuario raíz y presione continuar para continuar



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

●●●●●●

Show Password in Clear

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●●●

Show Password in Clear

Screenshot

Especifique el nombre completo de su usuario local,



Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Pradeep Kumar

Screenshot

Especifique el nombre de usuario, en mi caso estoy usando 'pkumar' como nombre de usuario.



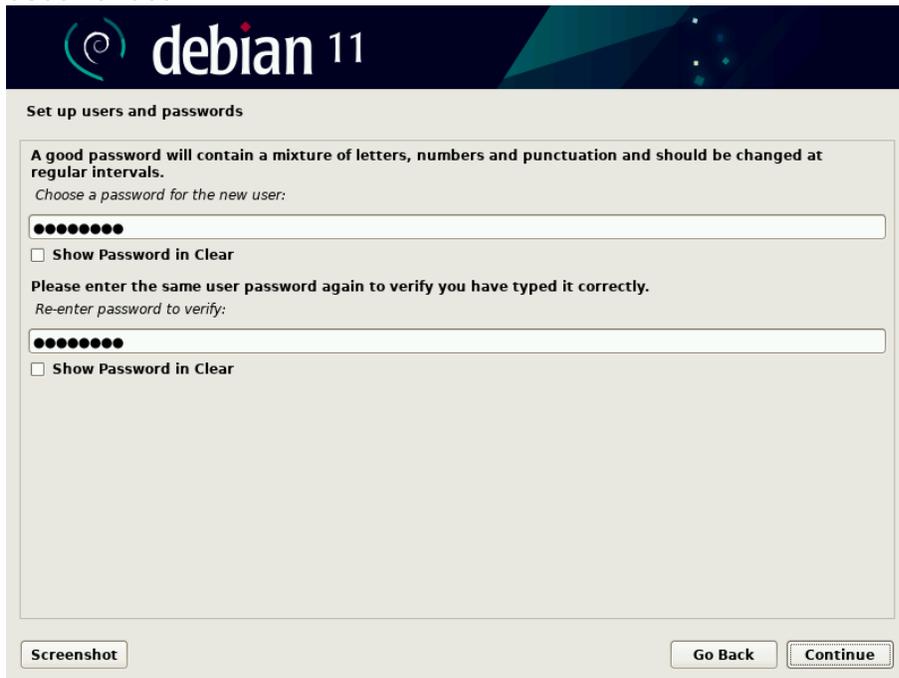
Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.
Username for your account:

pkumar

Screenshot Go Back Continue

Haga clic en continuar y luego en la siguiente pantalla, especifique la contraseña del usuario local.



Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
Choose a password for the new user:

●●●●●●●●

Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:

●●●●●●●●

Show Password in Clear

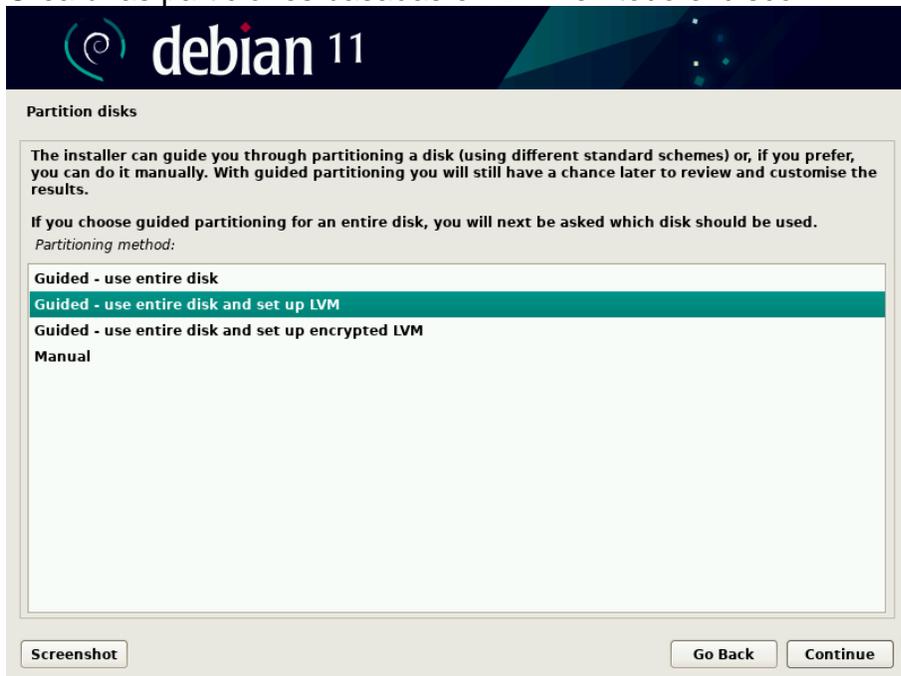
Screenshot Go Back Continue

En este paso, el instalador le pedirá que elija el método de partición.

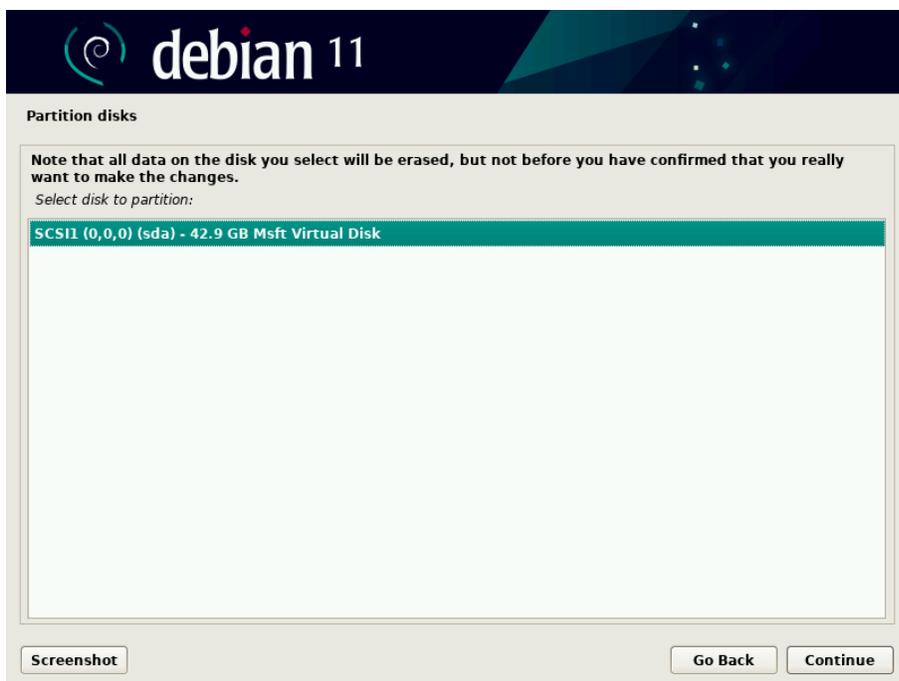
- Guiado: use todo el disco (se creará una partición automáticamente en todo el disco)

- Guiado: use todo el disco y configure LVM (se creará una partición basada en LVM automáticamente en todo el disco)
- Guiado: use todo el disco y configure LVM encriptado (creará particiones basadas en LVM y encriptará el disco)
- Manual: permitirá crear sus propias particiones personalizadas.

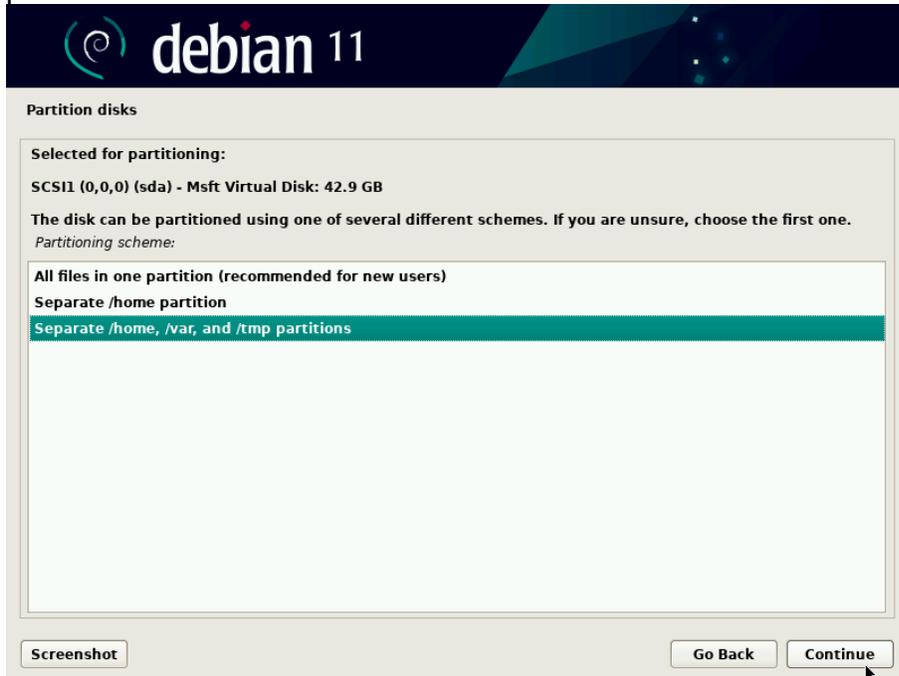
Elija la opción que se adapte a su instalación, en esta publicación voy con la 2da opción. Creará las particiones basadas en LVM en todo el disco.



Haga clic en Continuar para continuar,
En la siguiente pantalla, elija el disco en el que se crearán las particiones para Debian 11.



En la siguiente pantalla siguiente, debemos elegir el esquema de partición. Según el tamaño del disco y los requisitos, elija el esquema de particiones en consecuencia. Para el propósito de demostración, voy con la última opción 'Separar /home, /var y /tmp partición'.



Elija 'Continuar' para continuar.

Elija 'Sí' para escribir los cambios en el disco y luego haga clic en Continuar



Partition disks

Before the Logical Volume Manager can be configured, the current partitioning scheme has to be written to disk. These changes cannot be undone.

After the Logical Volume Manager is configured, no additional changes to the partitioning scheme of disks containing physical volumes are allowed during the installation. Please decide if you are satisfied with the current partitioning scheme before continuing.

The partition tables of the following devices are changed:
SCSI1 (0,0,0) (sda)

Write the changes to disks and configure LVM?

No

Yes

Screenshot Continue

En la siguiente pantalla, especifique el tamaño del disco que desea usar para las particiones de Debian 11, por defecto toma el tamaño completo del disco. En mi caso, voy con el tamaño de disco predeterminado.



Partition disks

You may use the whole volume group for guided partitioning, or part of it. If you use only part of it, or if you add more disks later, then you will be able to grow logical volumes later using the LVM tools, so using a smaller part of the volume group at installation time may offer more flexibility.

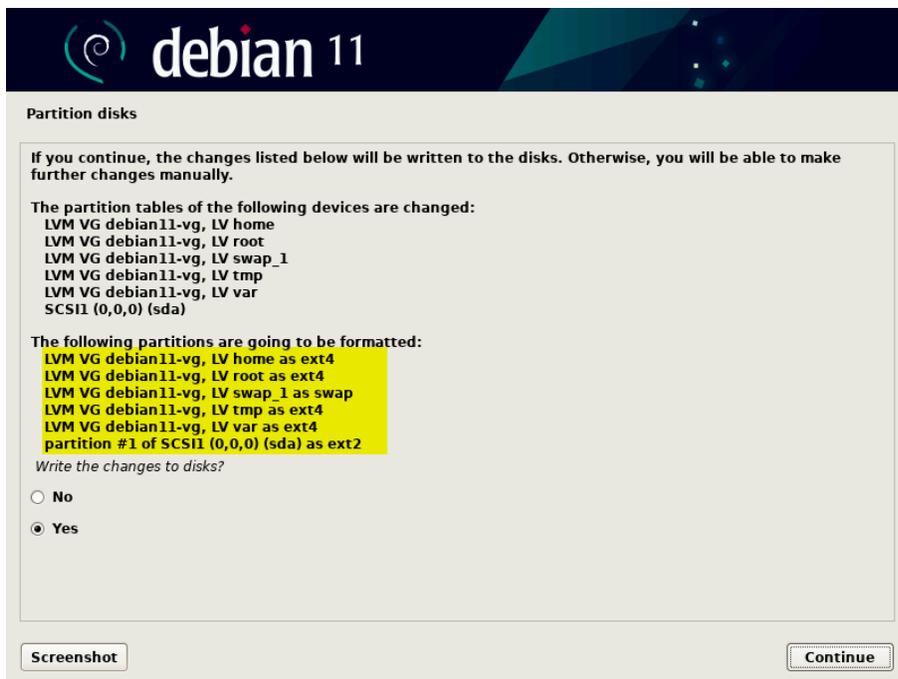
The minimum size of the selected partitioning recipe is 8.3 GB (or 19%); please note that the packages you choose to install may require more space than this. The maximum available size is 42.4 GB.

Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage (e.g. "20%") to use that percentage of the maximum size.

Amount of volume group to use for guided partitioning:

Screenshot Go Back Continue

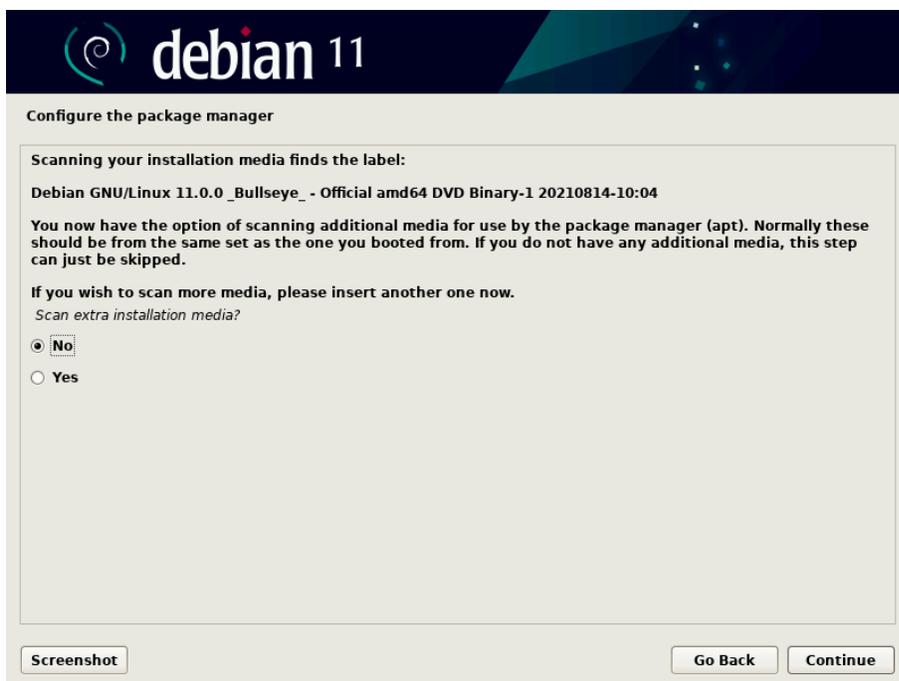
En la siguiente pantalla, obtendremos el resumen de las particiones, lo verificaremos y elegiremos 'Sí' para escribir los cambios en el disco.



Haga clic en Continuar para iniciar la instalación.
En este paso, se inicia la instalación real de Debian 11,



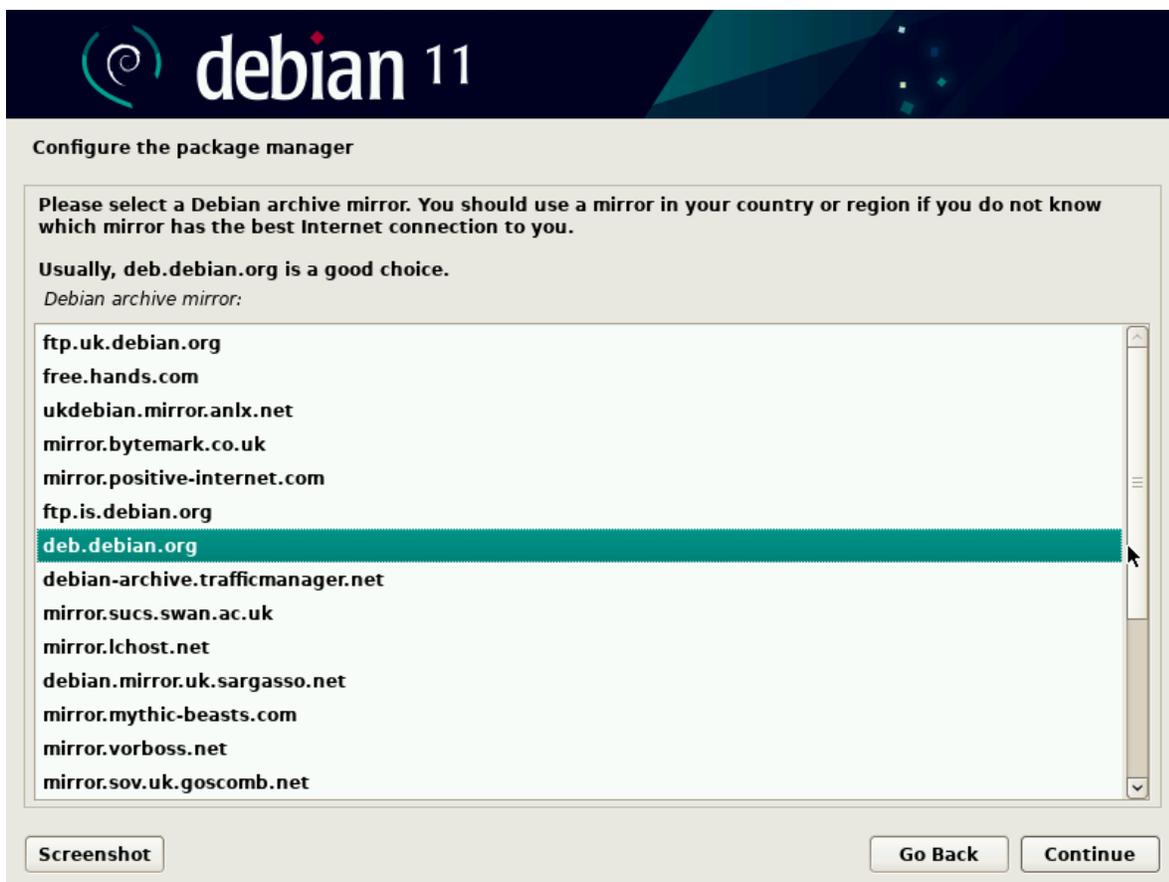
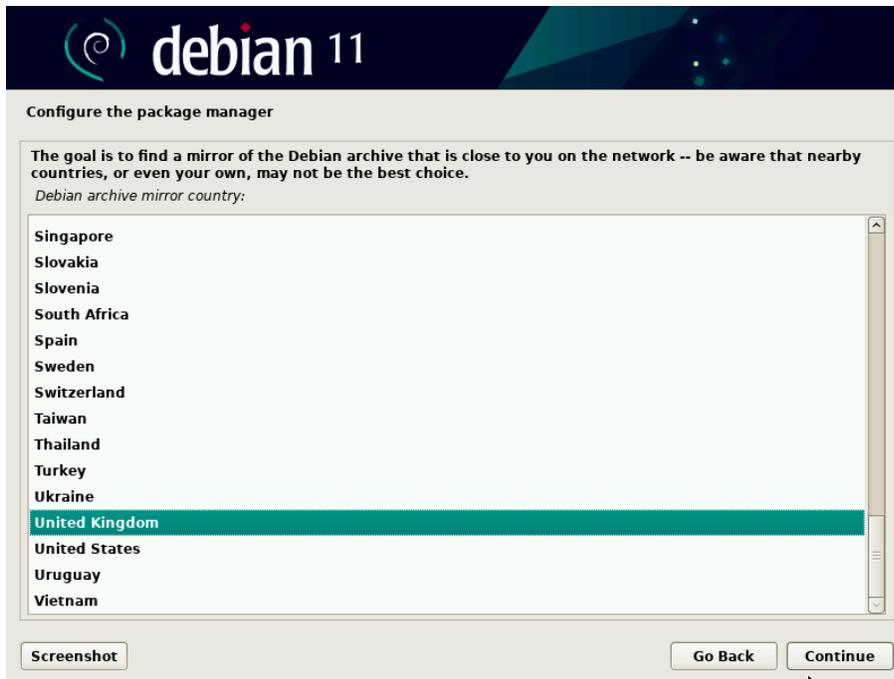
Después de un par de minutos, se le pedirá que escanee los medios de instalación, elija 'No' y haga clic en continuar para continuar con la instalación.



En la pantalla Siguiete, elija 'Sí' para configurar el espejo de red.



Elija 'País espejo del archivo Debian' y haga clic en continuar

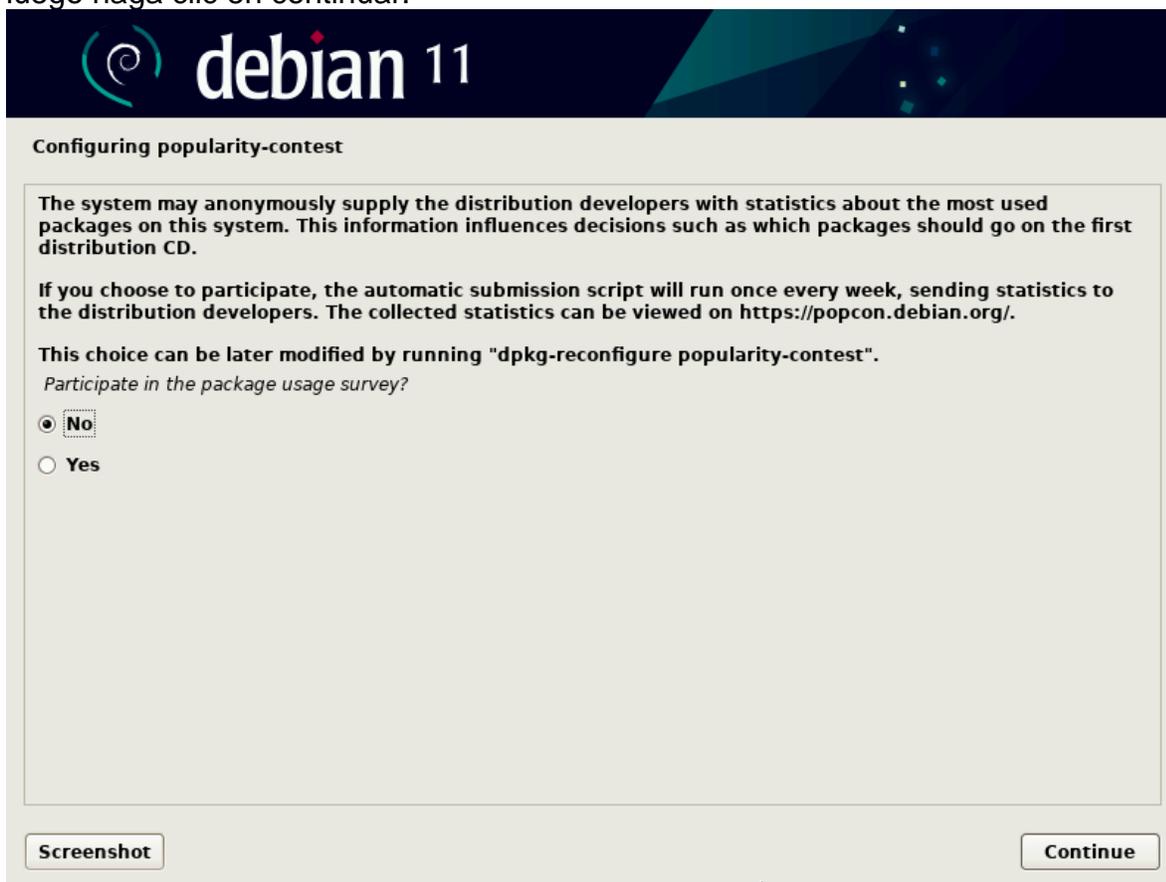


En la siguiente pantalla, haga clic en Continuar si su sistema no utiliza ningún servidor proxy. En caso de que lo esté utilizando, especifique los detalles y luego continúe.

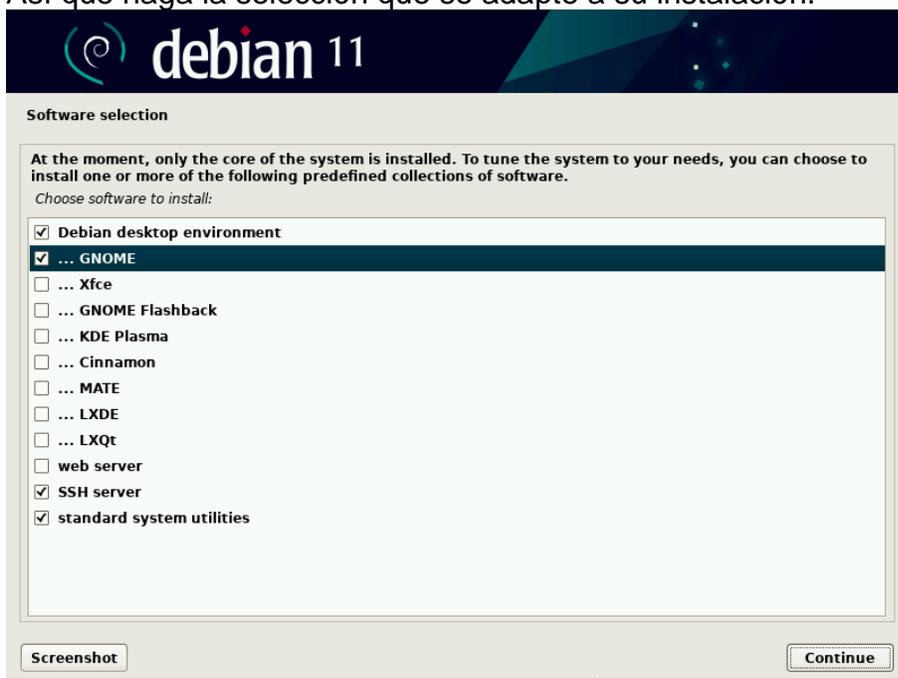


Haga clic en Continuar para continuar con la instalación.

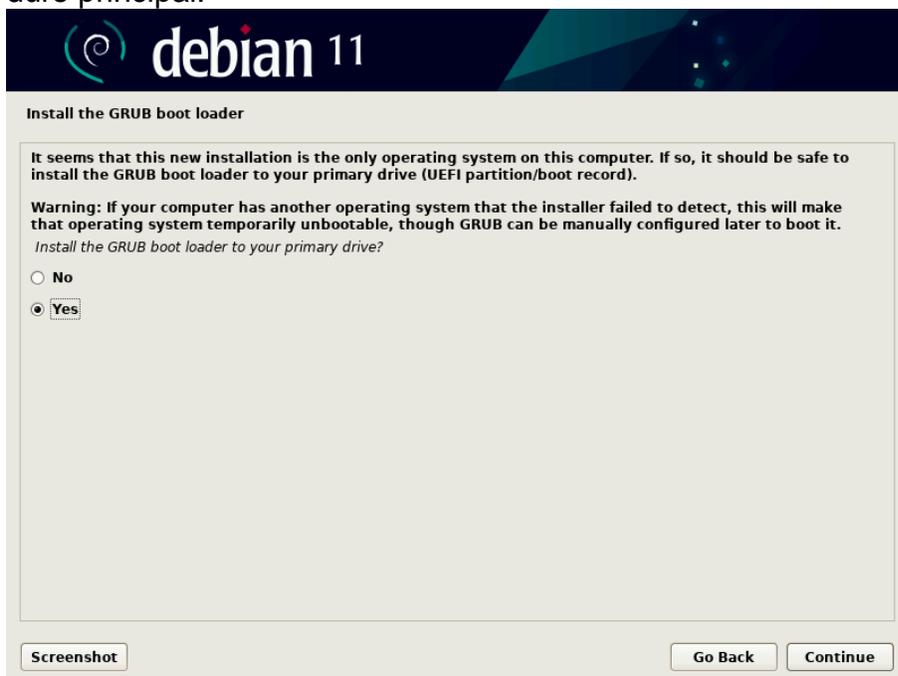
En la siguiente pantalla se le pedirá que participe en la encuesta del paquete, elija 'No' y luego haga clic en continuar.



Ahora elija el software que desea instalar, como entorno de escritorio y servidores, etc. Así que haga la selección que se adapte a su instalación.



Haga clic en Continuar para continuar con la instalación.
En la siguiente pantalla, elija 'Sí' para instalar el cargador de arranque Grub en el disco duro principal.



Haga clic en Continuar.
En la siguiente ventana, elija el disco en el que se instalará grub loader,

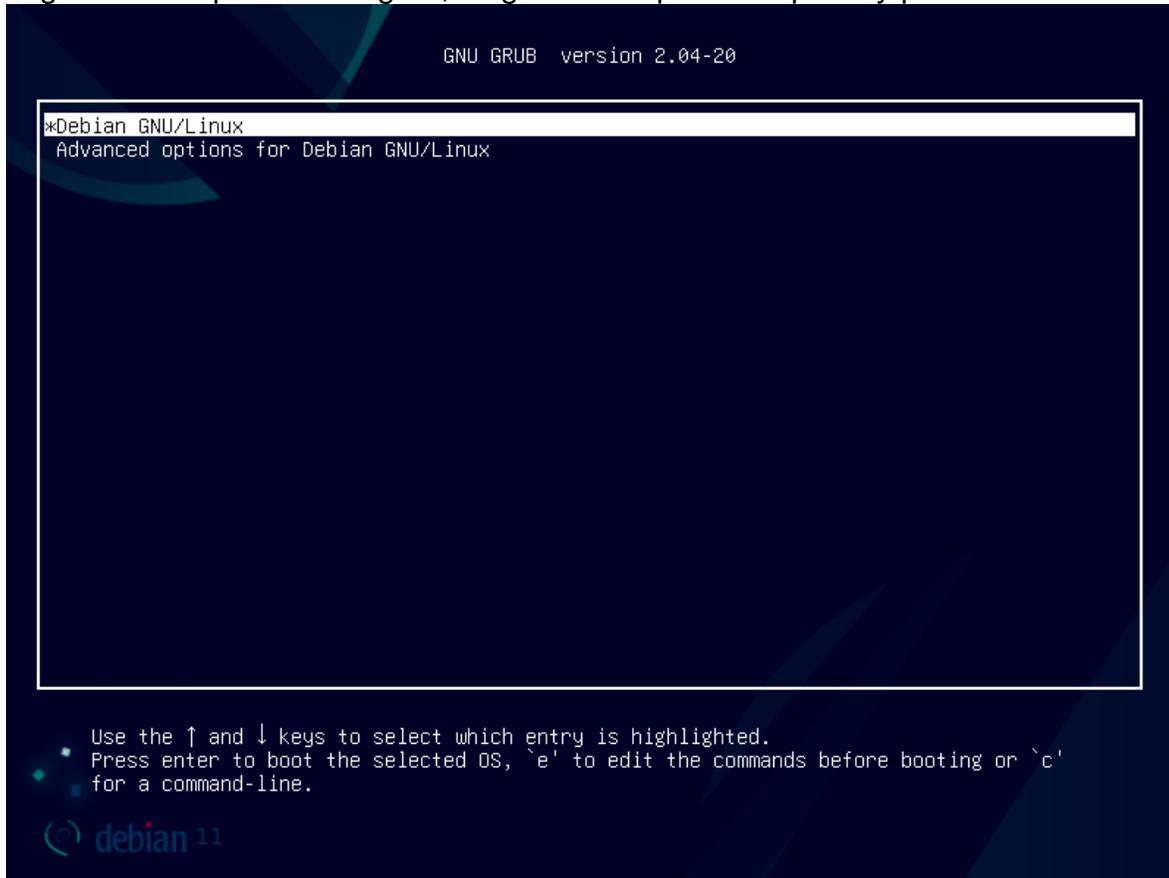


Elija Continuar y presione enter para finalizar la instalación.
Una vez que se complete la instalación, el instalador le pedirá que reinicie el sistema una vez.

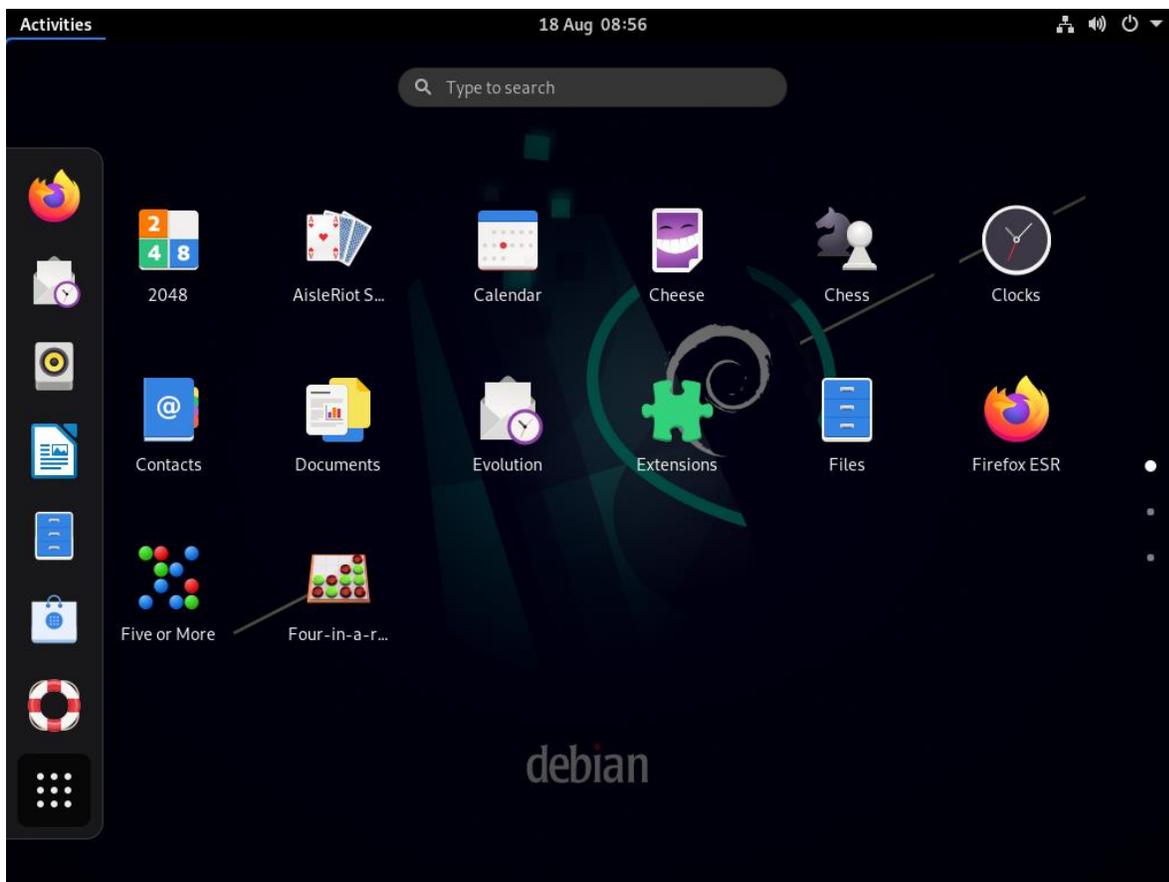
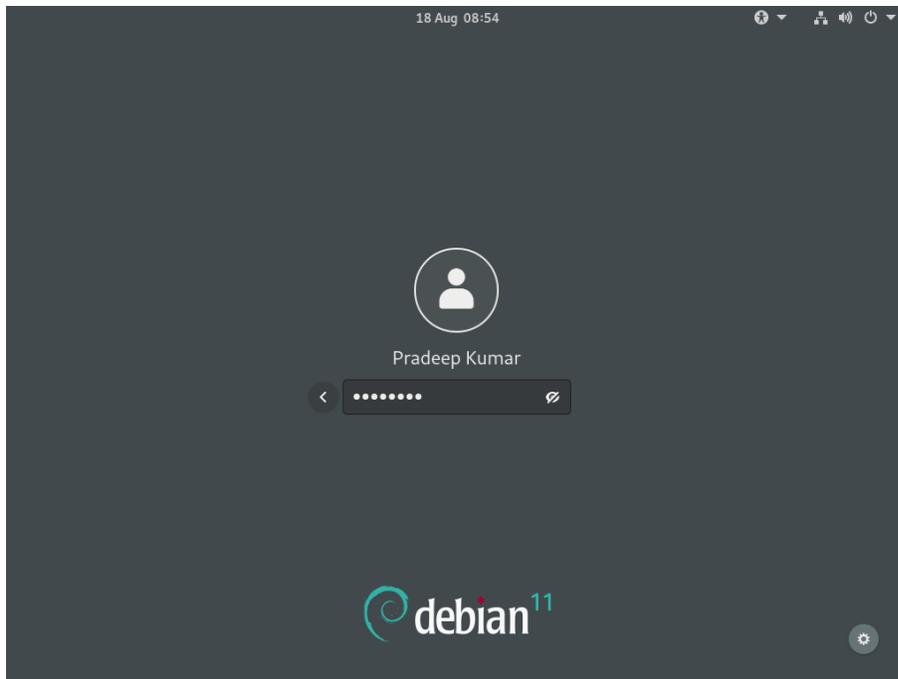


Haga clic en 'Continuar' para reiniciar el sistema y no olvide cambiar el medio de arranque del medio de instalación al disco duro.

Una vez que el sistema se reinicie después de la instalación exitosa de Debian 11, seguiremos la pantalla de grub, elegiremos la primera opción y presionaremos enter.



Cuando el sistema se inicie, obtendremos la siguiente pantalla de inicio de sesión, use el mismo usuario local y sus credenciales que hemos creado durante la instalación.



La instalación esta lista una vez ingresado al sistema operativo
INSTALACION DE ELASTIX

Ejecutamos la maquina virtual Aterix
Nos aparece la siguiente pantalla

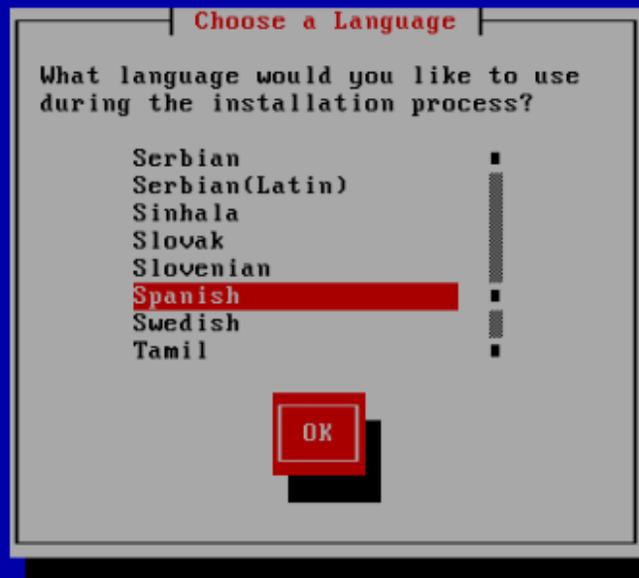


- To install or upgrade in graphical mode, press the <ENTER> key.
- To install or upgrade in text mode, type: linux text <ENTER>.
- Use the function keys listed below for more information.

[F1=Main] [F2=Options] [F3=General] [F4=Kernel] [F5=Rescue]

Presionamos la tecla Enter para arrancar la instalación

Welcome to Elastix

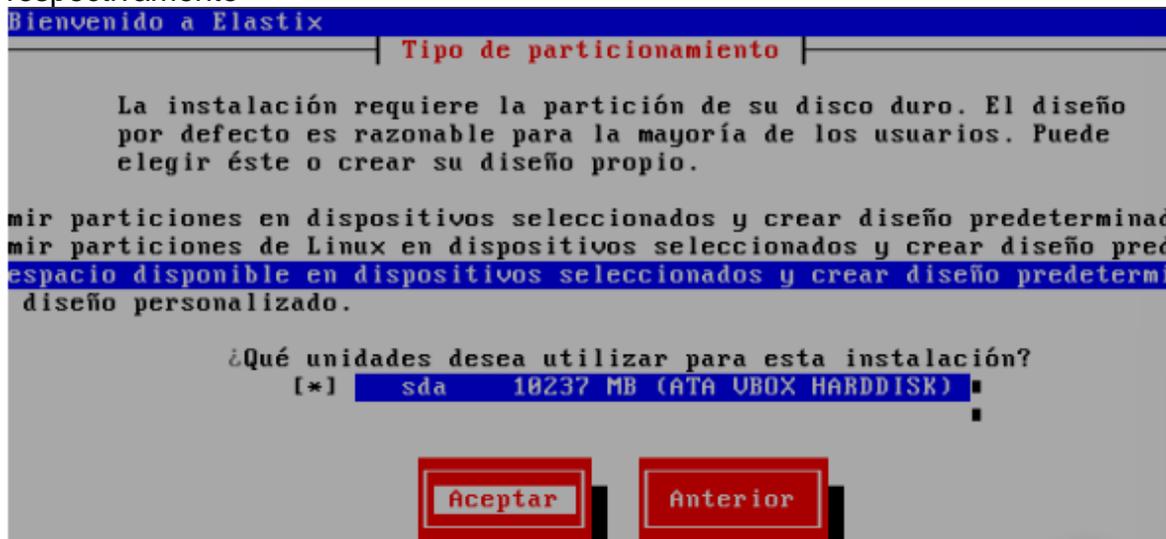


<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

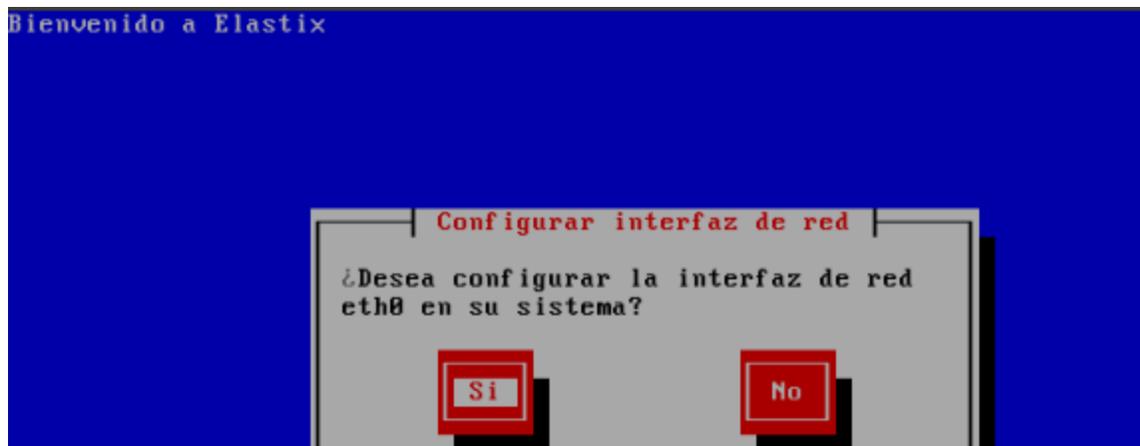
Elegimos con las flechas direccionales el idioma Spanish



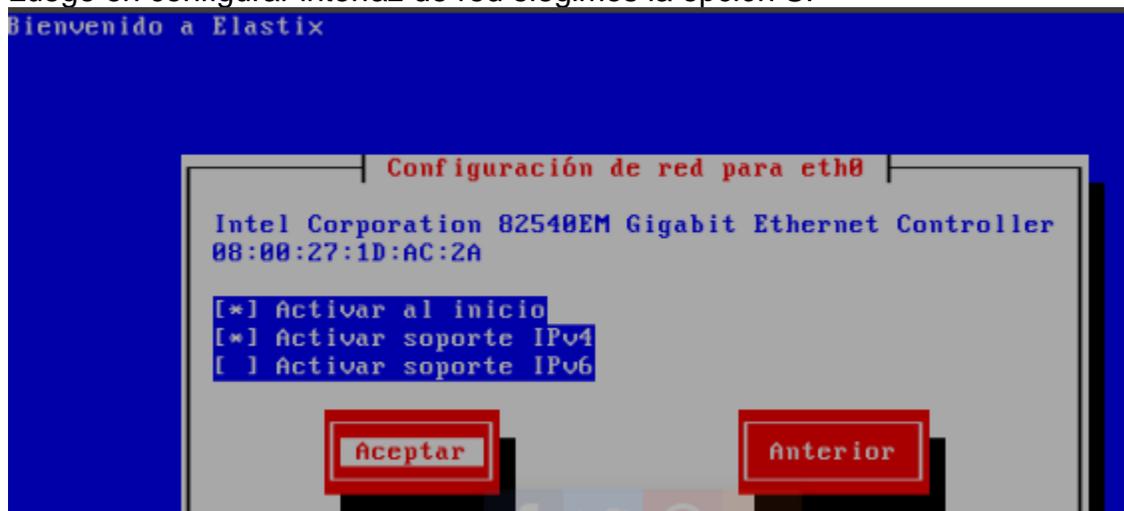
Luego escogemos el tipo de teclado y seleccionamos aceptar con la tecla TAB y Enter respectivamente



En tipo de Particionamiento elegimos la única partición que es SDA con la tecla de espacio, luego con TAB elegimos el botón Aceptar y hacemos clic en Enter



Luego en configurar interfaz de red elegimos la opción SI



Escogemos la tarjeta de nuestra red y ponemos activar soporte IPv4 para colocar la dirección IP

Ingresamos la dir ip y la mascara que le vamos a asignar al equipo



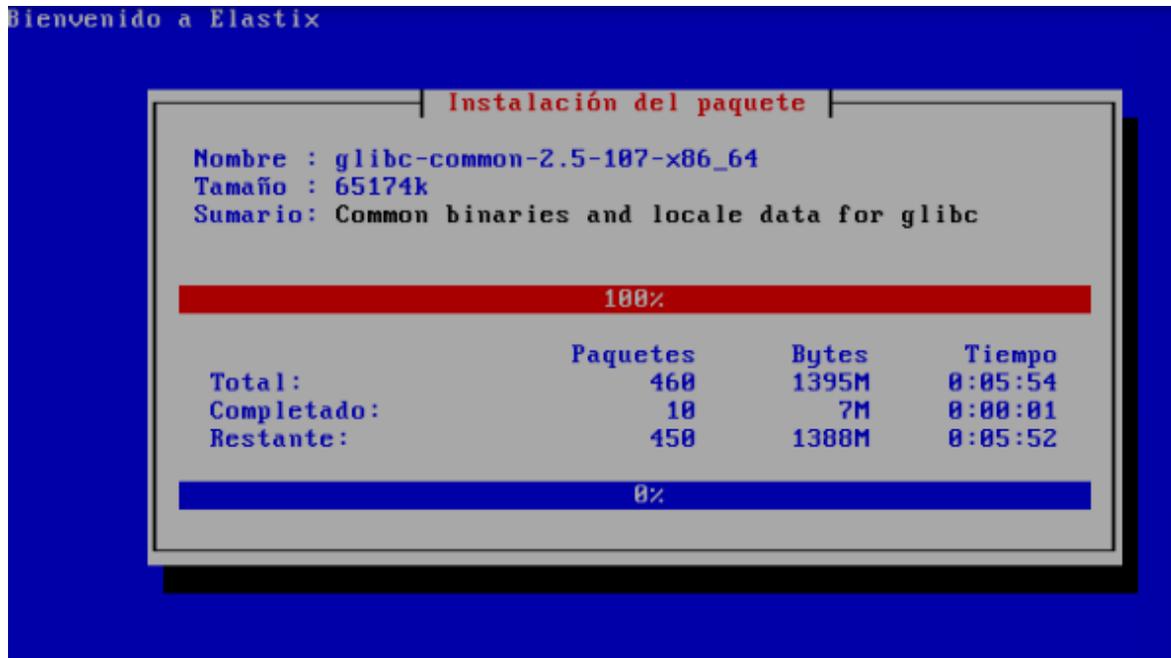
Presionamos aceptar



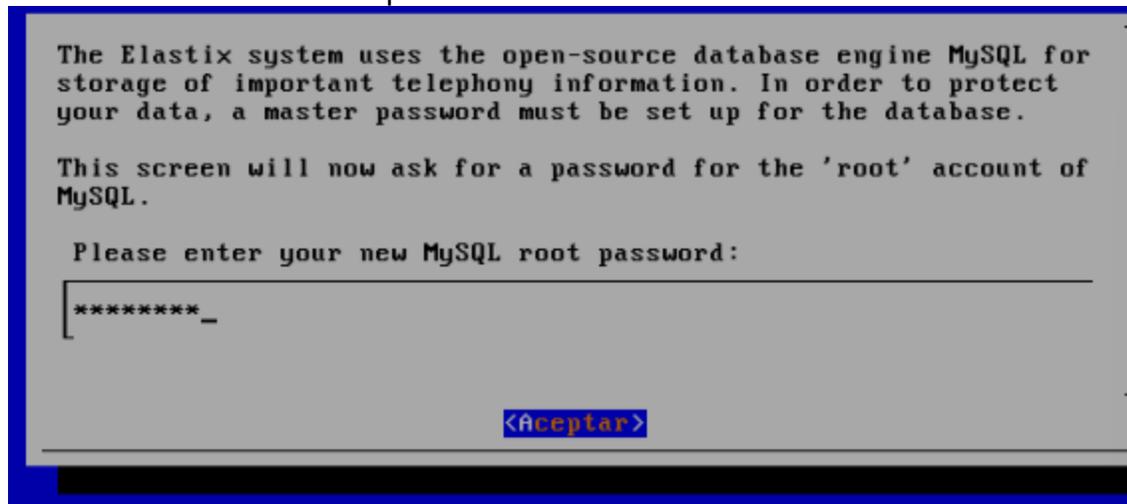
En reloj elegimos la opción America/Guayaquil



En contraseña de root elegimos una contraseña y la mantenemos guardada para poder ingresar
Esperamos la instalación de los paquetes



Añadimos una contraseña para la base de datos de Elastix



Una vez instalado ya nos aparece la siguiente pantalla con la IP para conectarnos a Elastix

```
CentOS release 5.9 (Final)
Kernel 2.6.18-348.1.1.el5 on an x86_64

vepbx login: root
Password:

Welcome to Elastix
-----

Elastix is a product meant to be configured through a web browser.
Any changes made from within the command line may corrupt the system
configuration and produce unexpected behavior; in addition, changes
made to system files through here may be lost when doing an update.

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://192.168.1.104
```

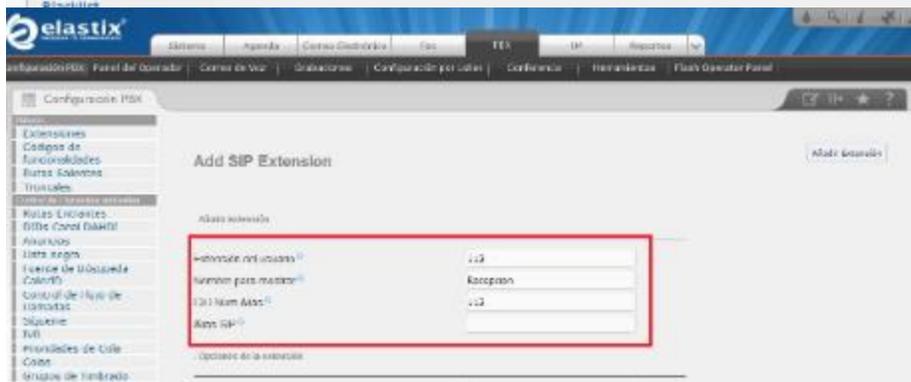
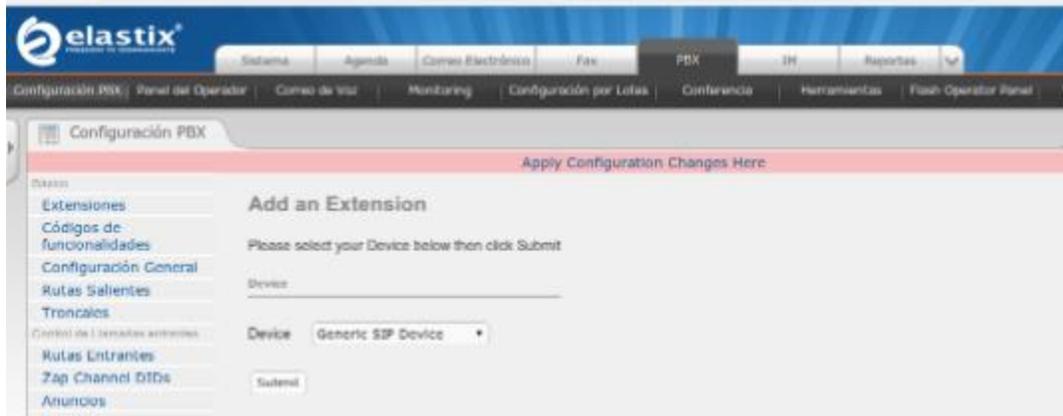
Con un navegador en la red ingresamos al portal web con nuestras credenciales



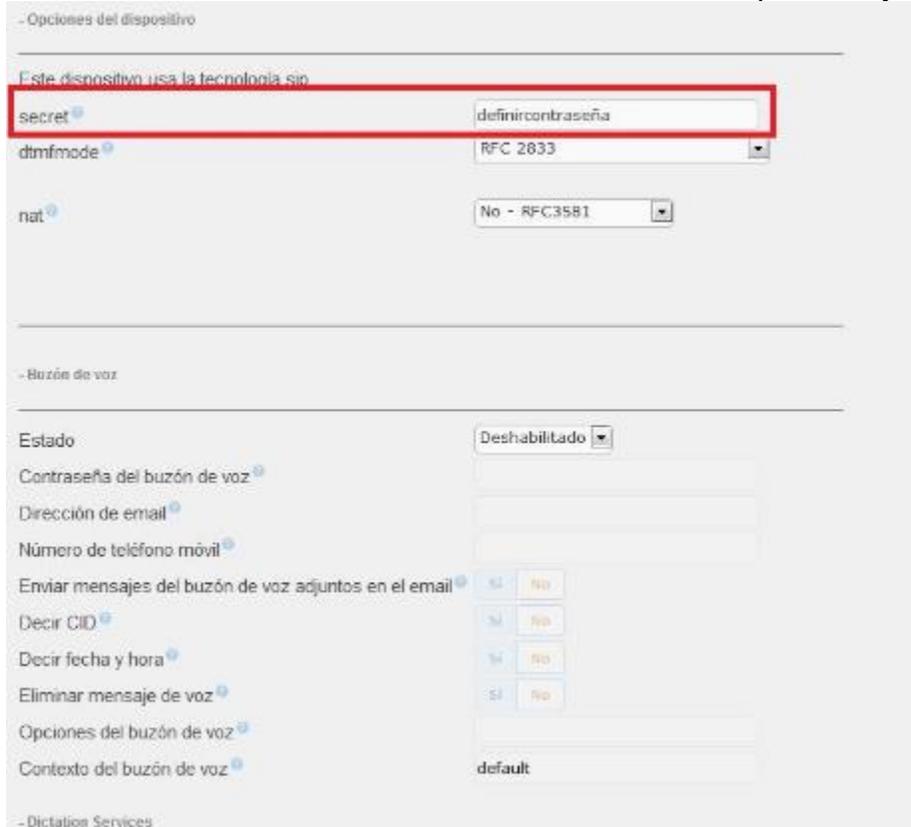
Luego en el interior podremos ver todo el dashboard de Elastix



En la sección PBX podremos crear todas las extensiones que deseemos para los softphone



Añadimos el numero de la extensión el nombre de la persona y un alias



Luego definimos una contraseña para esa extensión y finalmente hacemos clic en el botón Enviar

Localizador VmX™ Deshabilitado ▾

Usar cuando: No disponible Ocupado

Instrucciones del buzón de voz: Standard Voicemail prompts

Al pulsar 0: Ir al operador

Al pulsar 1:

Al pulsar 2:

Optional Destinations

No Answer: Unavail Voicemail if Enabled ▾

CID Prefix:

Ocupado: Busy Voicemail if Enabled ▾

CID Prefix:

Not Reachable: Unavail Voicemail if Enabled ▾

CID Prefix:

Enviar

INSTALACION DE EXTENSION EN SOFTPHONE ZOIPER

Lo primero que vamos a realizar será descargarnos el ZOIPER desde el sitio web oficial

zoiper.com/en/voip-softphone/download/current

Sitios sugeridos Favoritos Cerrar

Zoiper BRANDING SDK DOWNLOAD PRODUCTS

Latest versions

Zoiper 5

free VoIP softphone for non-commercial use

Desktop

Windows	Download
Mac	Download
Linux	Download

Mobile

Android	Download
iOS iOS	Download

Nos descargamos la versión Free:

The screenshot shows the Zoiper website's pricing page. It features three columns representing different service tiers:

- Free (€0):** Represented by a rotary phone icon. It includes a 'Download' button and is described as 'Basic functionality for occasional use' with a note that it is 'non-commercial use only'. The only feature listed is 'Basic functionality'.
- Premium (€49.95):** Represented by a smartphone icon. It includes a 'Purchase' button and is described as 'Business functionality for the power user'. Features listed include:
 - Auto Provisioning
 - Contacts integration (Outlook, LDAP, Thunderbird, Mac OS X, Windows)
 - Browser integration (click to dial, open url)
 - Better quality/Lower bandwidth (G.729/H.264 codecs)
 - Business Features (transfer, conferencing)
- Custom On demand:** Represented by a smartphone icon with a person and a satellite dish. It includes a 'Contact us' button and is described as 'Fully customized solutions according to your specs'. Features listed include:
 - Your design
 - Your feature set
 - Locked to your service
 - Branded with your name and logo
 - Balance display

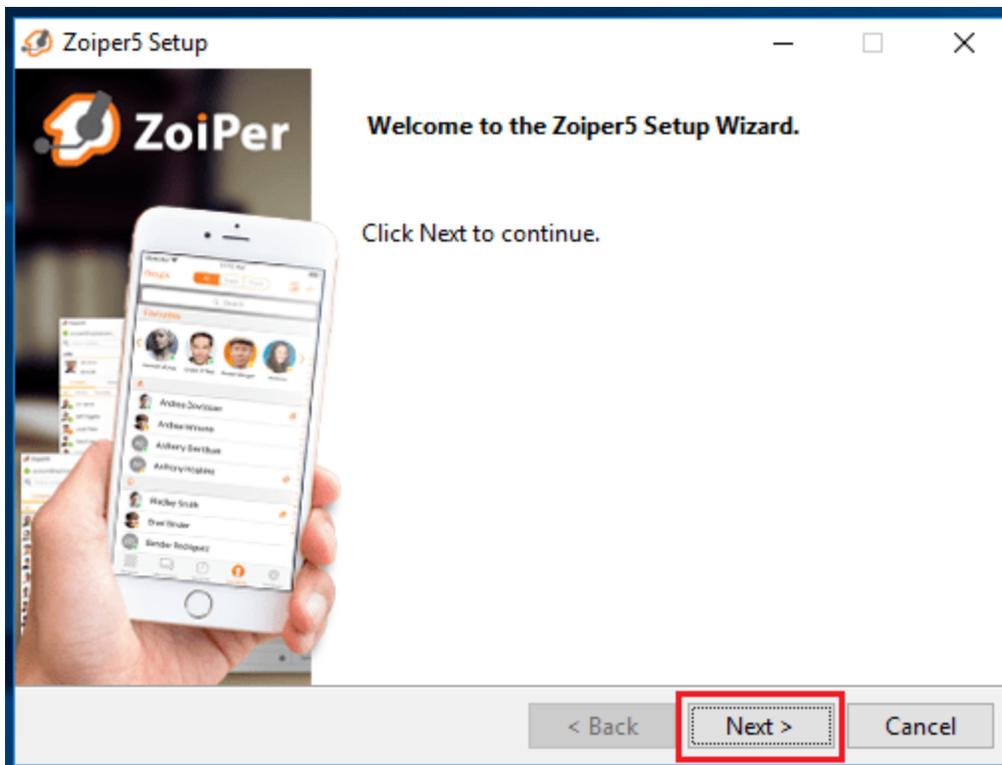
Como podemos ver aquí lo tenemos descargado:

The screenshot shows a Windows File Explorer window with the following details:

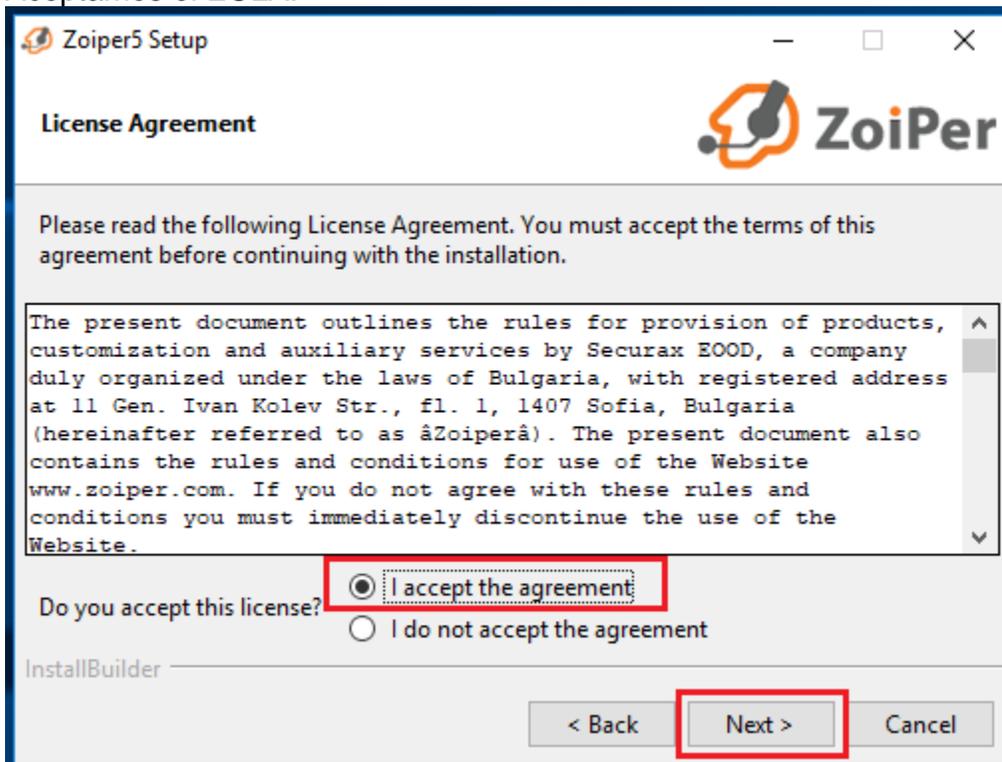
- Path:** Este equipo > DATOS (E:) > PROGRAMAS Y UTILIDADES > VOIP > Softphone > Zoiper > Ultimo
- File List:**

Nombre	Fecha de modifica...	Tipo	Tamaño
Zoiper5_Installer_v5.4.8	29/09/2020 20:16	Aplicación	171.619 KB

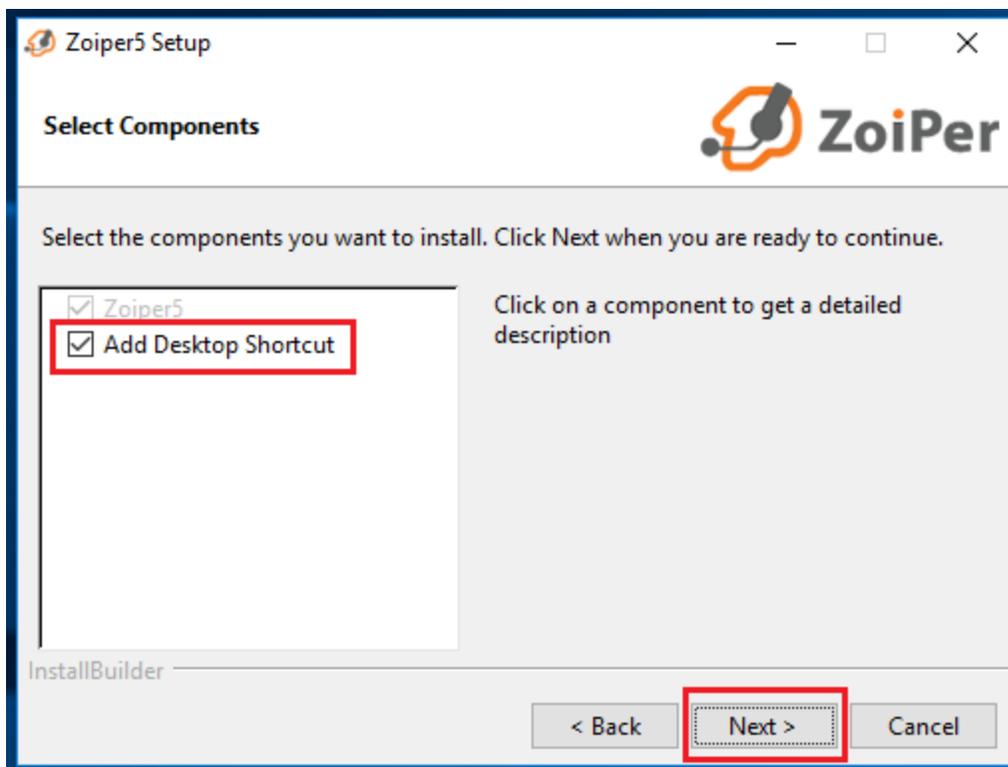
Procedemos con la instalación, clic en siguiente para continuar:



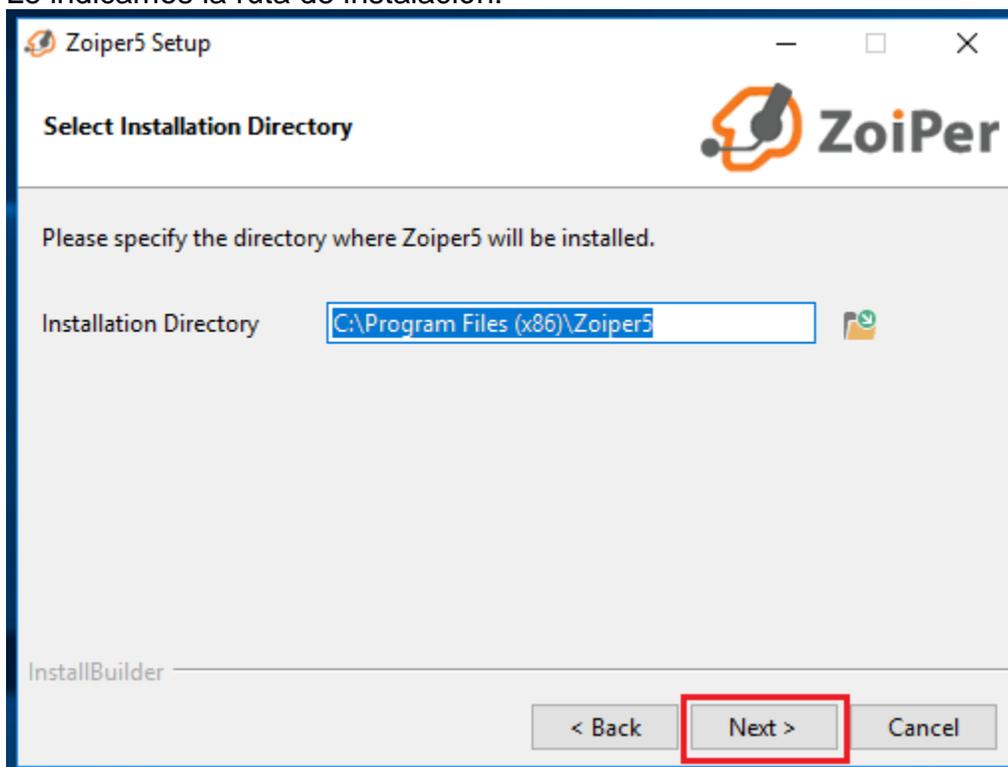
Aceptamos el EULA:



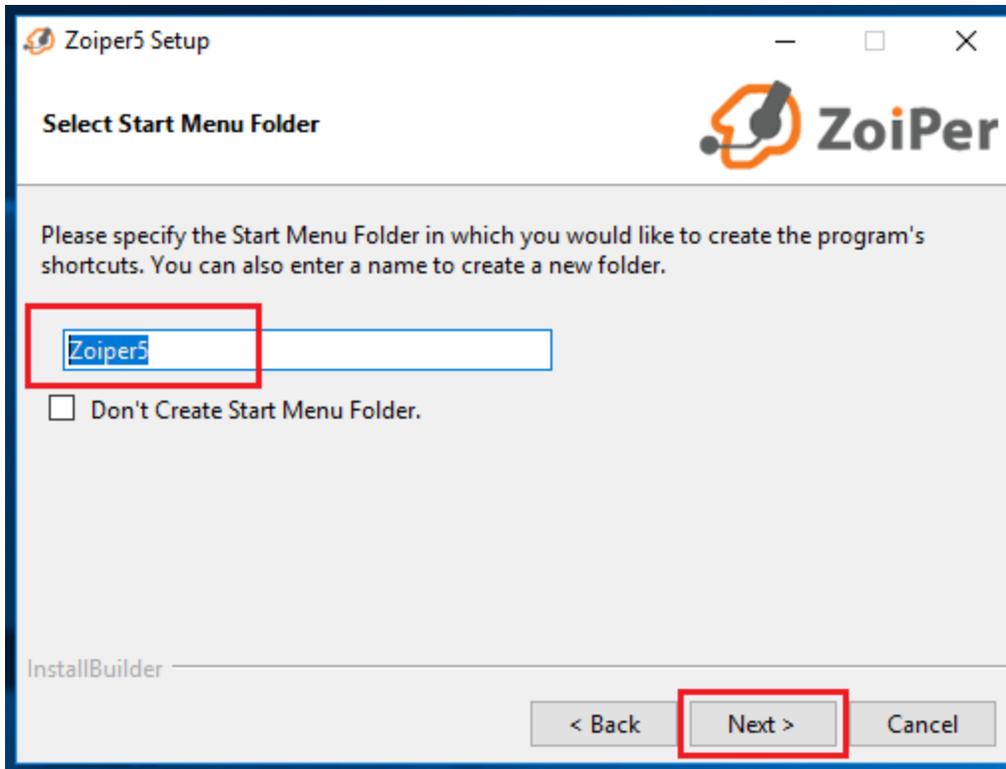
Añadimos un acceso directo al escritorio:



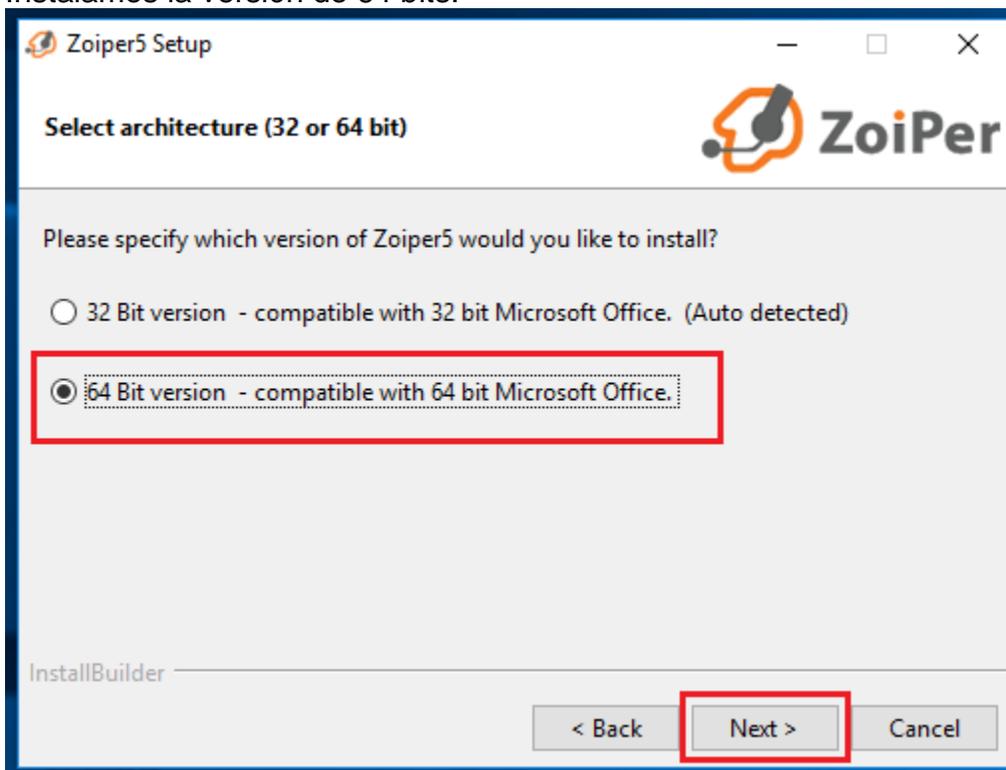
Le indicamos la ruta de instalación:



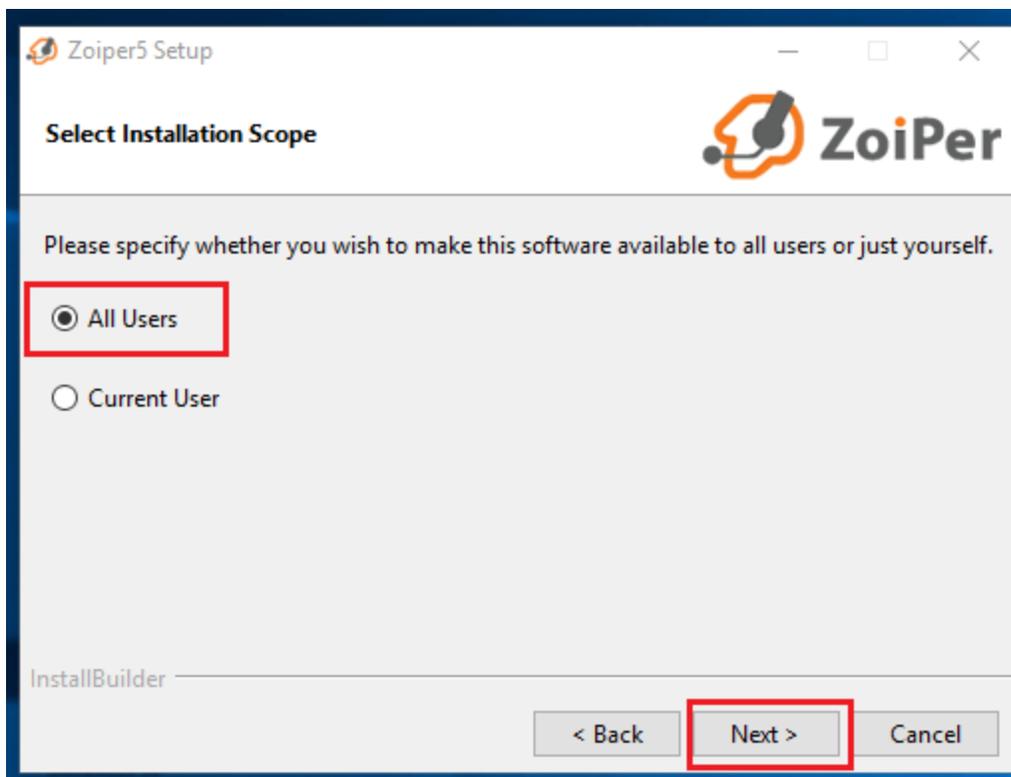
Le indicamos el nombre de la carpeta en el menú de inicio:



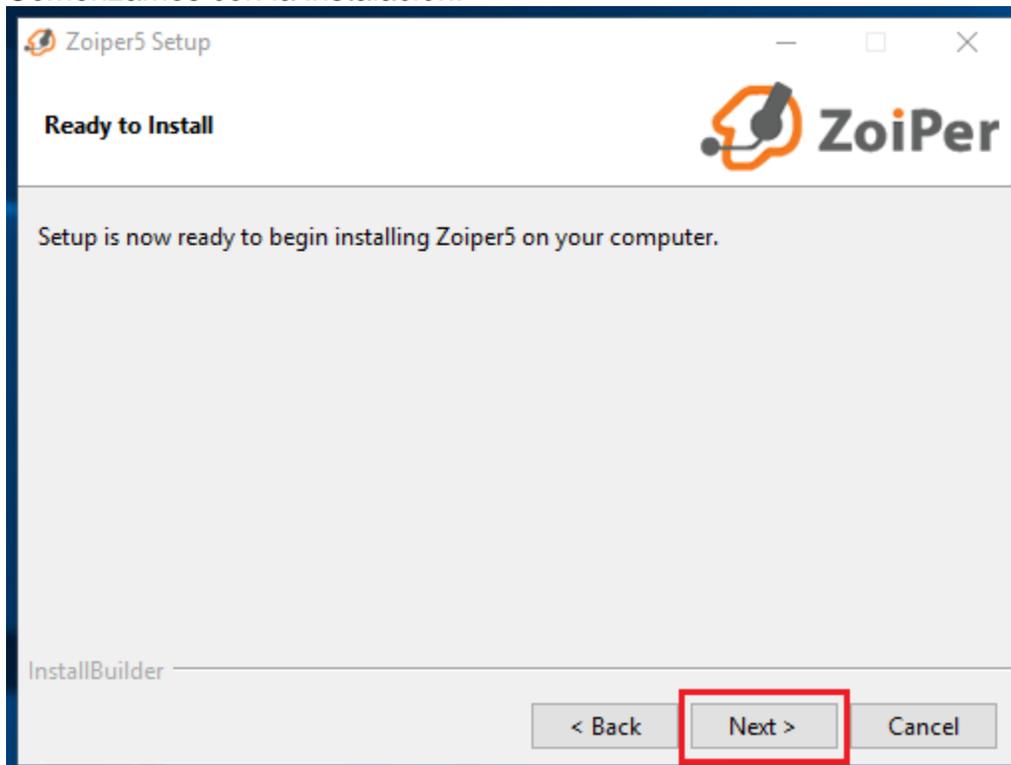
Instalamos la versión de 64 bits:

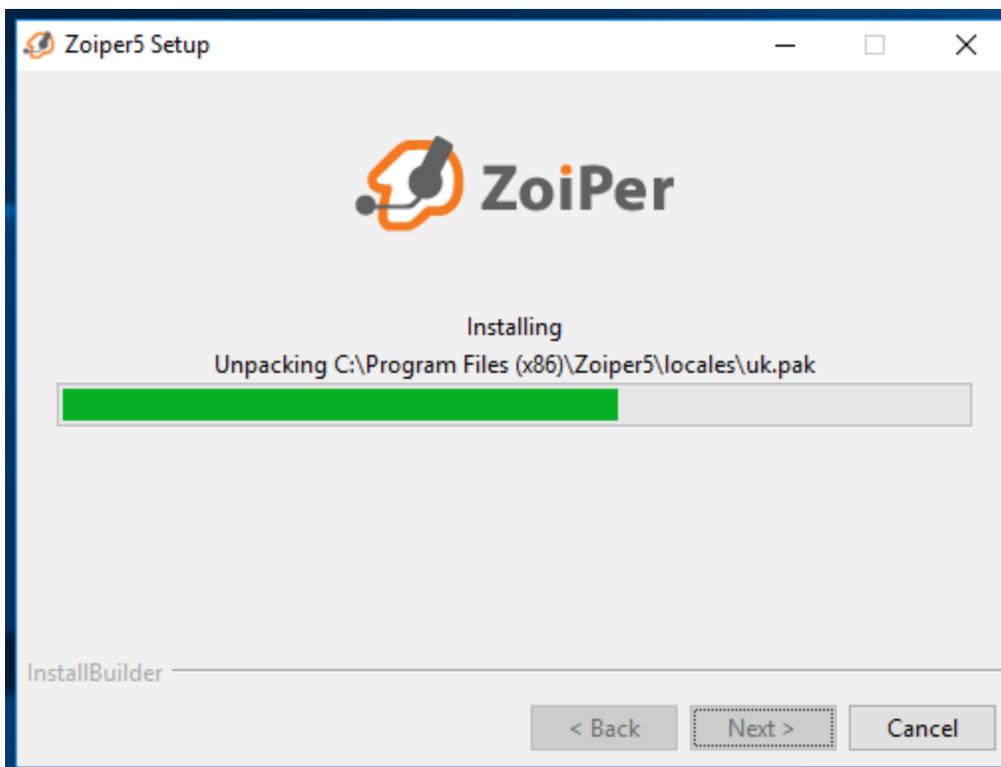


Instalamos la aplicación en todos los perfiles de usuarios:

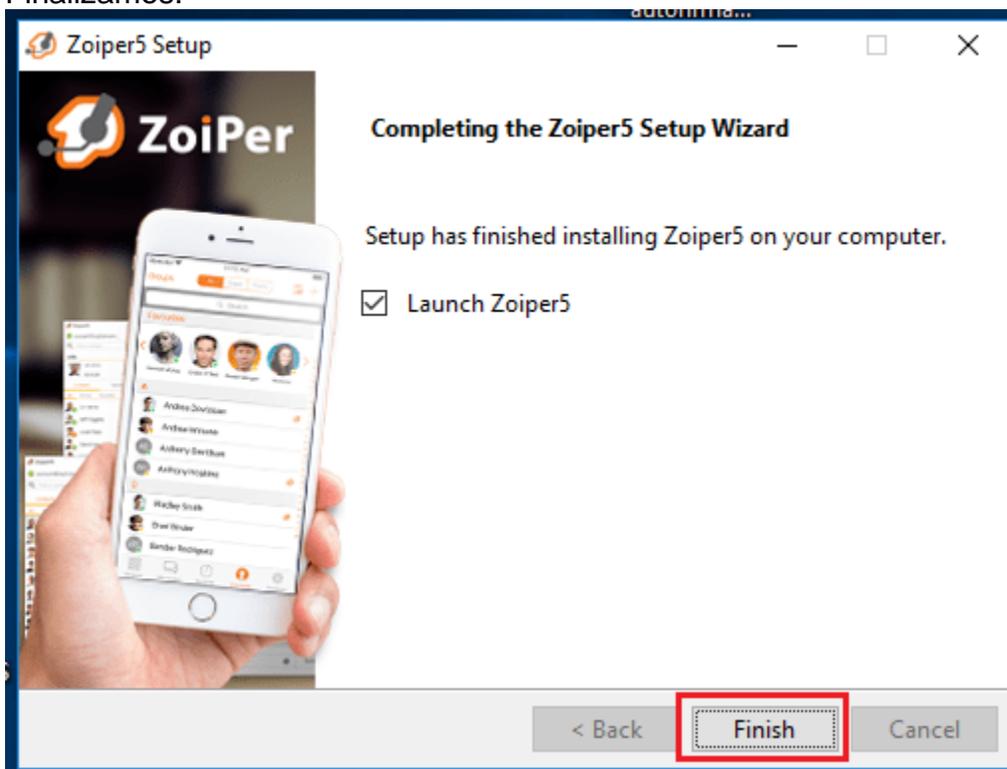


Comenzamos con la instalación:

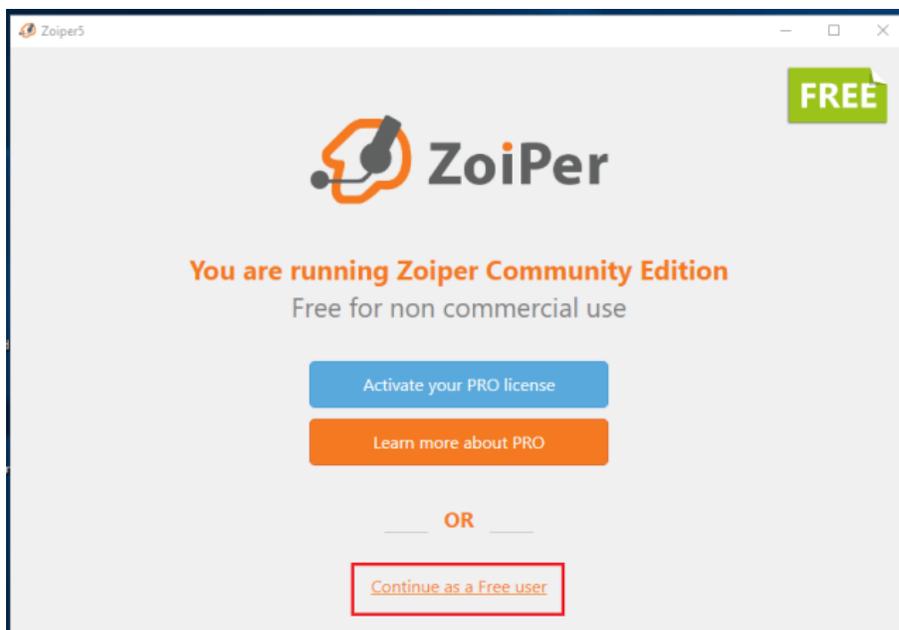




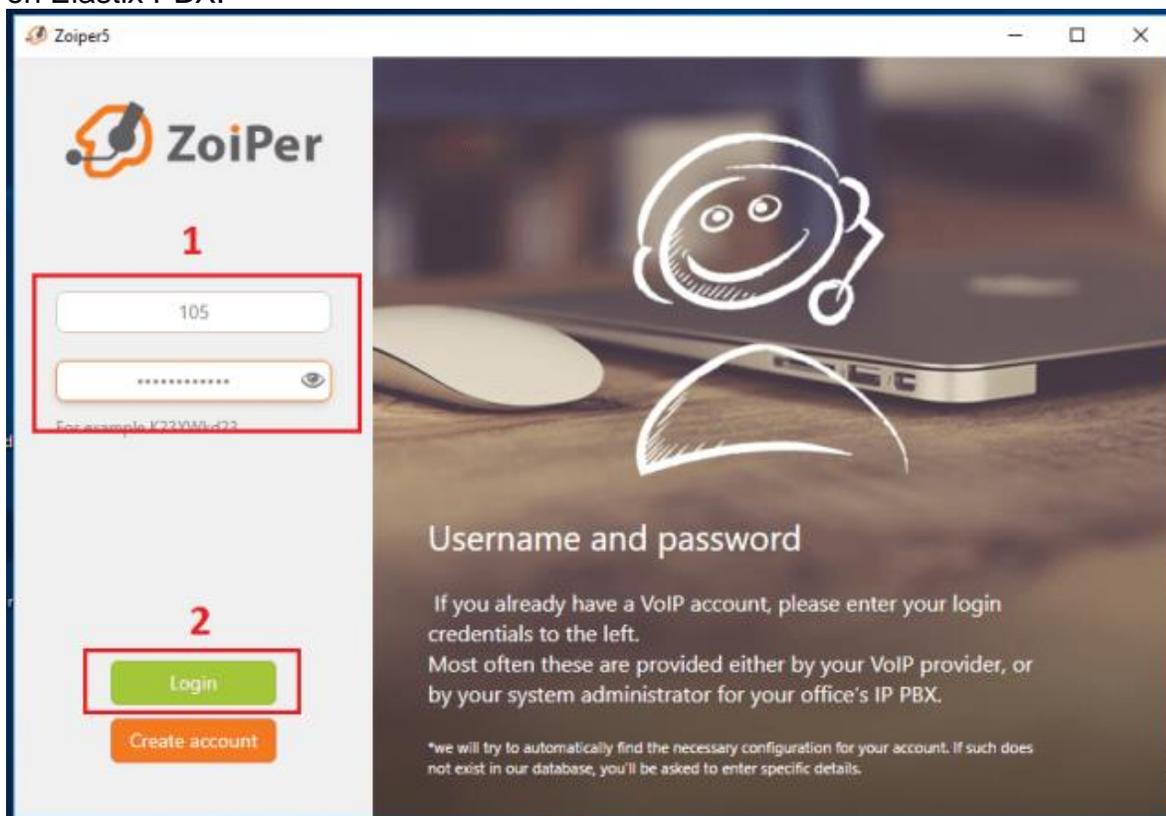
Finalizamos:



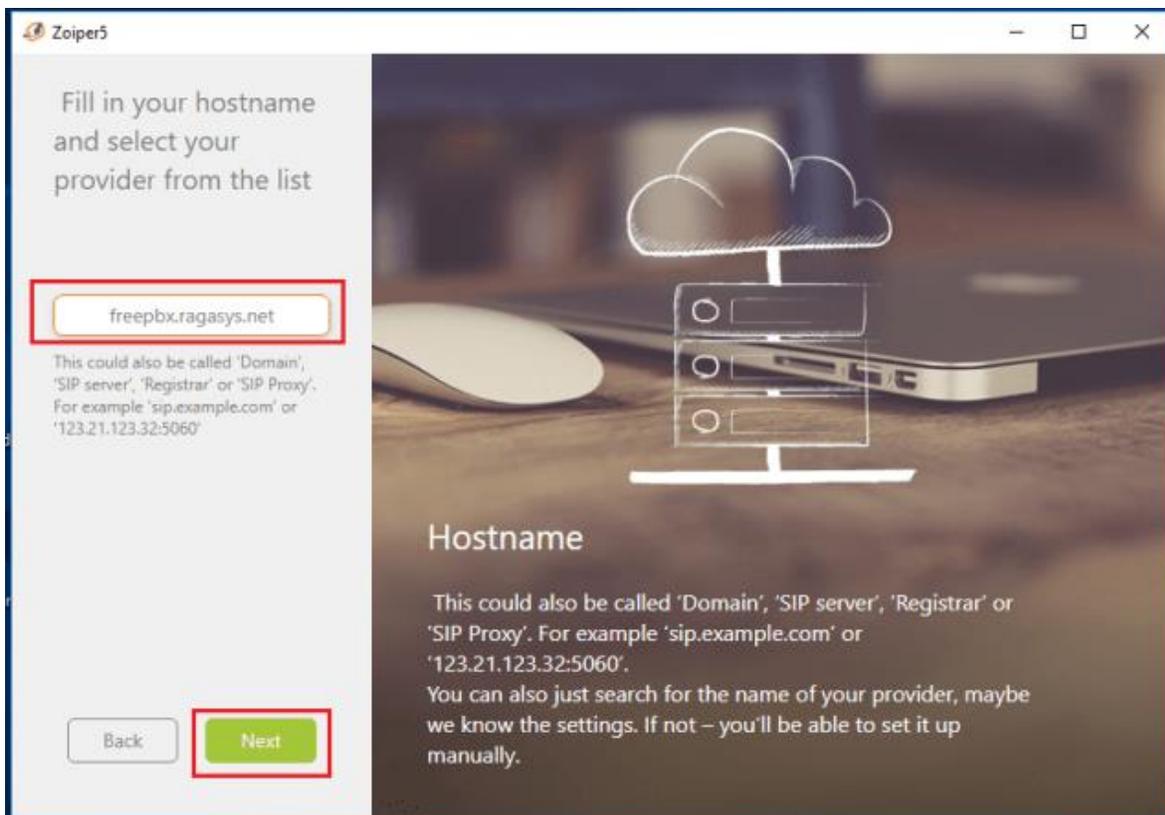
Ahora vamos a proceder a configurar nuestro Zoiper 5 con una de las extensiones que hemos configurado en nuestra FreePBX, accedemos como usuario free:



Inicio el Login introduciendo el número de extensión con la contraseña que configuramos en Elastix PBX.



Introducimos el nombre DNS o la dirección IP de la centralita Asterik FreePBX:



Zoiper5

Fill in your hostname and select your provider from the list

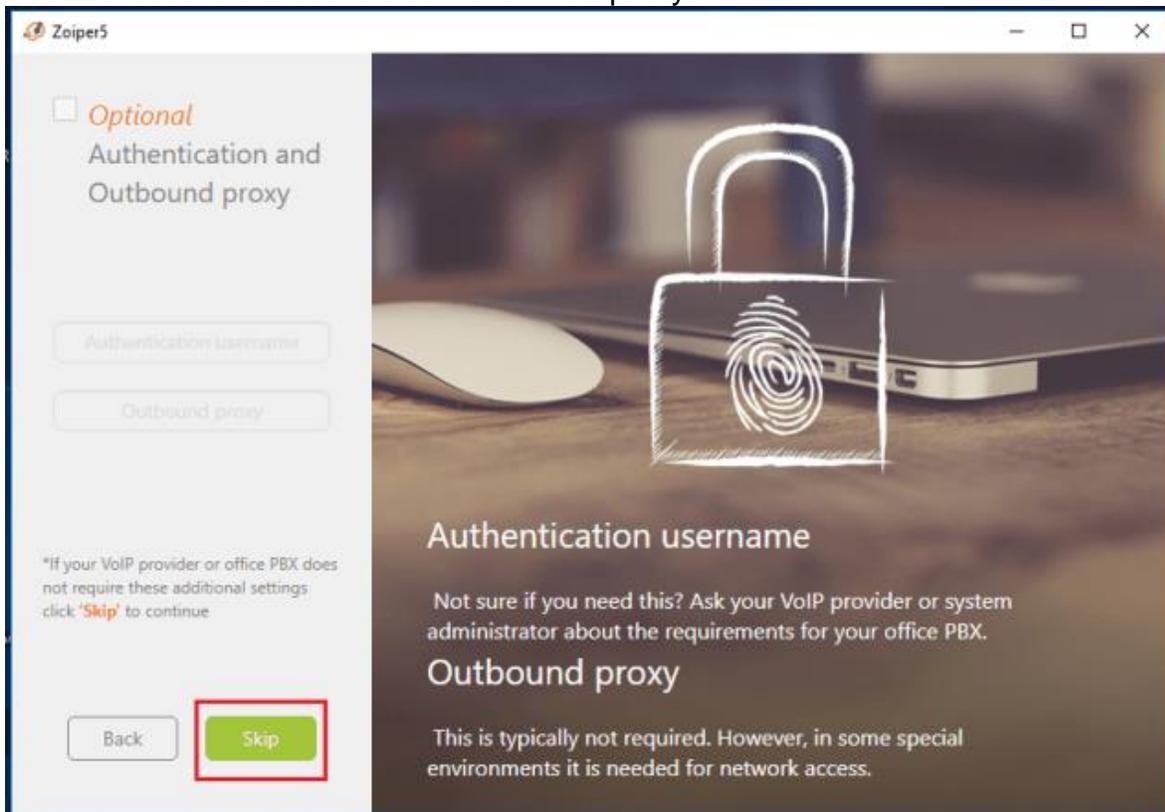
This could also be called 'Domain', 'SIP server', 'Registrar' or 'SIP Proxy'. For example 'sip.example.com' or '123.21.123.32:5060'

Back Next

Hostname

This could also be called 'Domain', 'SIP server', 'Registrar' or 'SIP Proxy'. For example 'sip.example.com' or '123.21.123.32:5060'. You can also just search for the name of your provider, maybe we know the settings. If not – you'll be able to set it up manually.

Nos saltamos la autenticación a través del proxy:



Zoiper5

Optional
Authentication and Outbound proxy

*If your VoIP provider or office PBX does not require these additional settings click **'Skip'** to continue

Back Skip

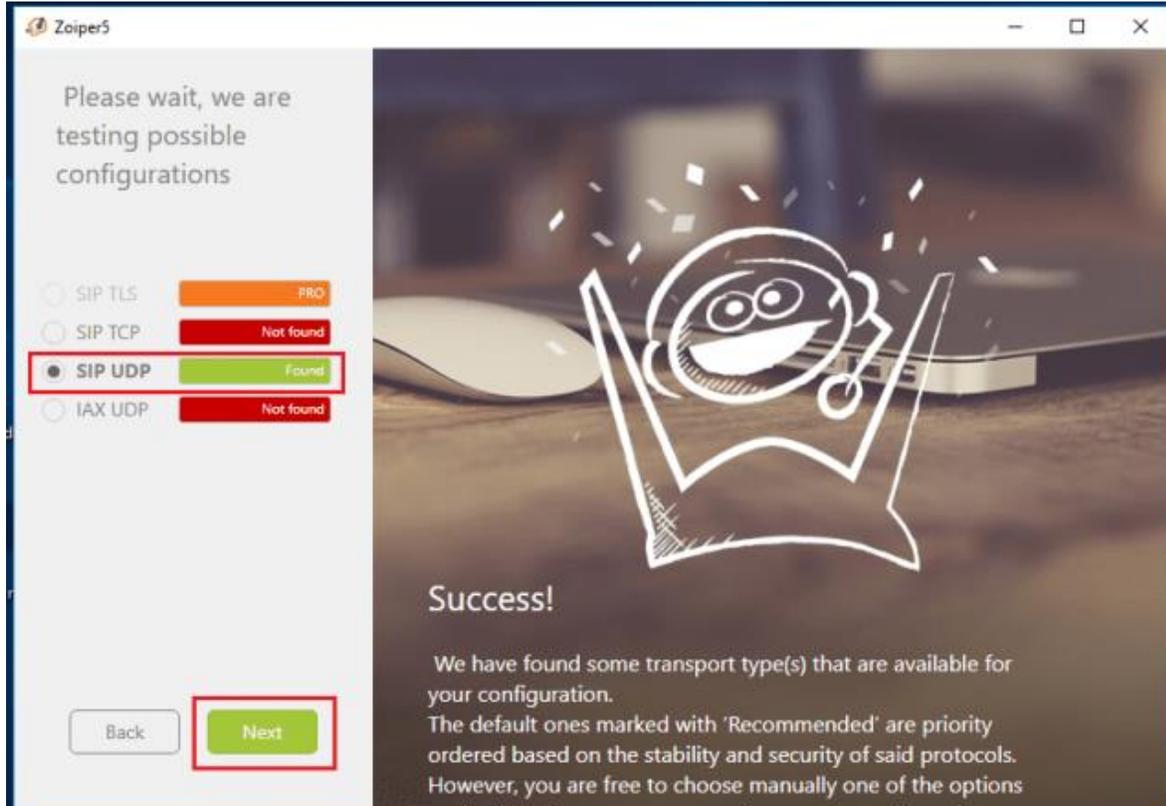
Authentication username

Not sure if you need this? Ask your VoIP provider or system administrator about the requirements for your office PBX.

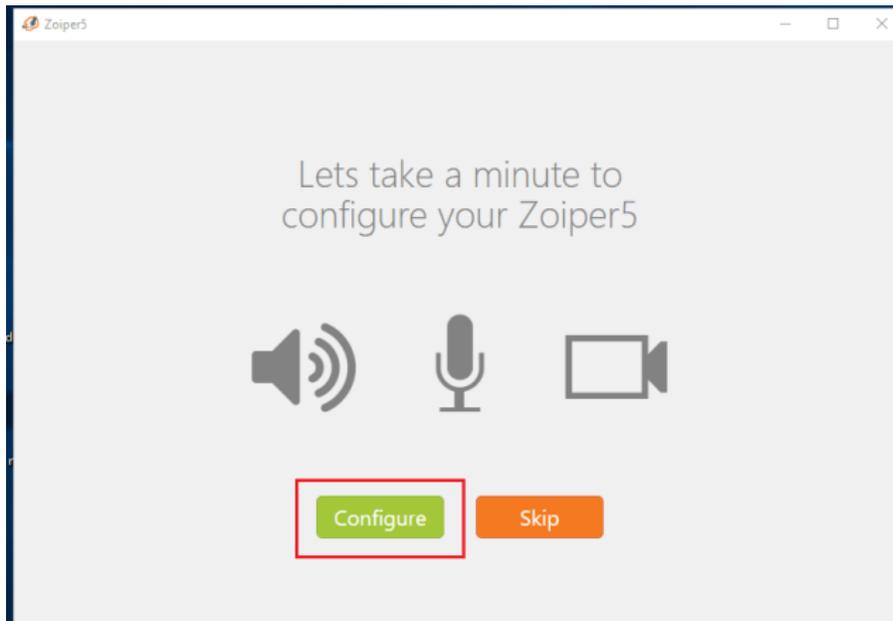
Outbound proxy

This is typically not required. However, in some special environments it is needed for network access.

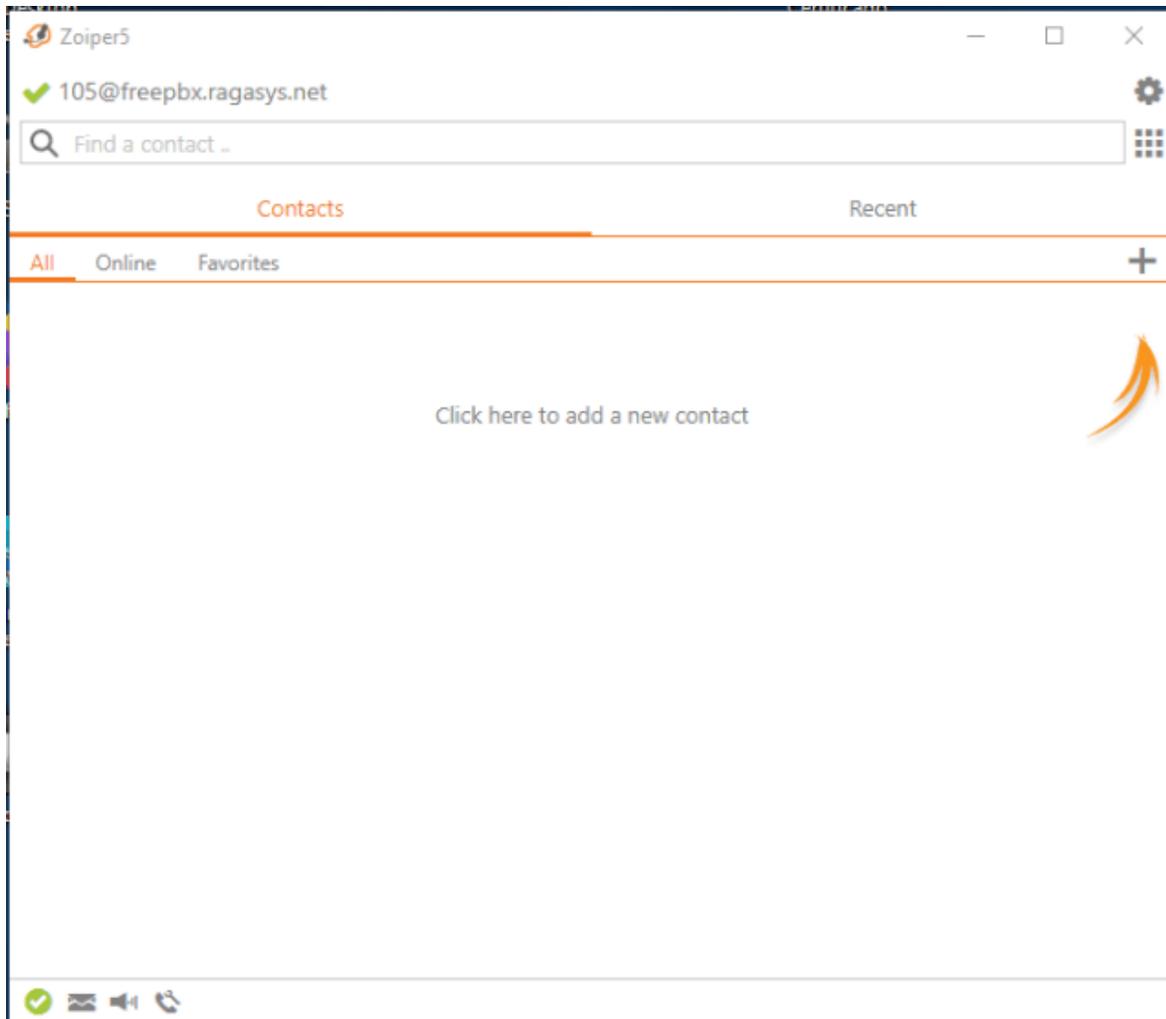
Como podemos ver a encontrado el servicio SIP UDP que hemos configurado en nuestras extensiones:



Damos clic a configurar y nos saldrán los testeos para los altavoces, micrófono y webcam:

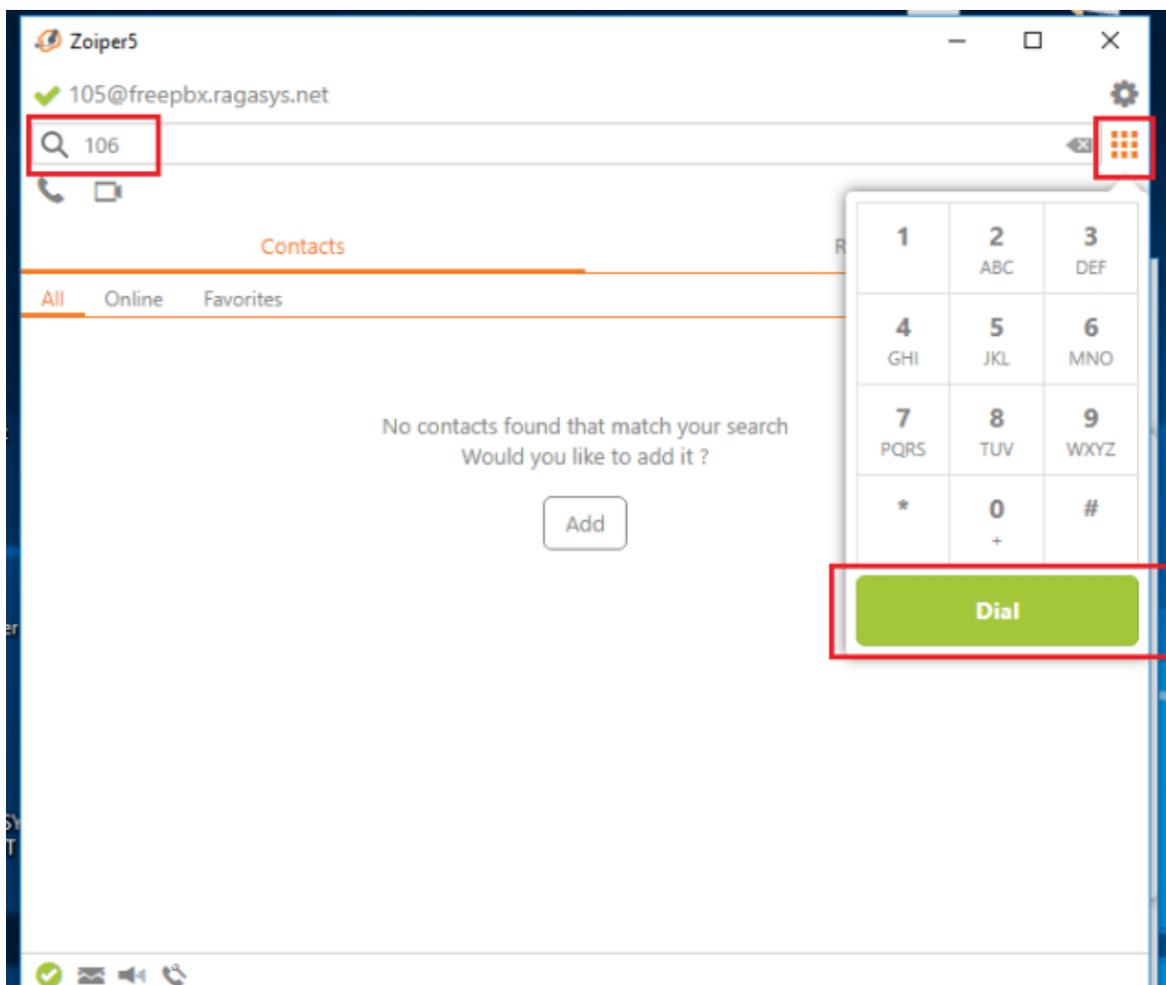


Una vez pasados los test, ya tenemos listo nuestro Zoiper para enviar y recibir llamadas:

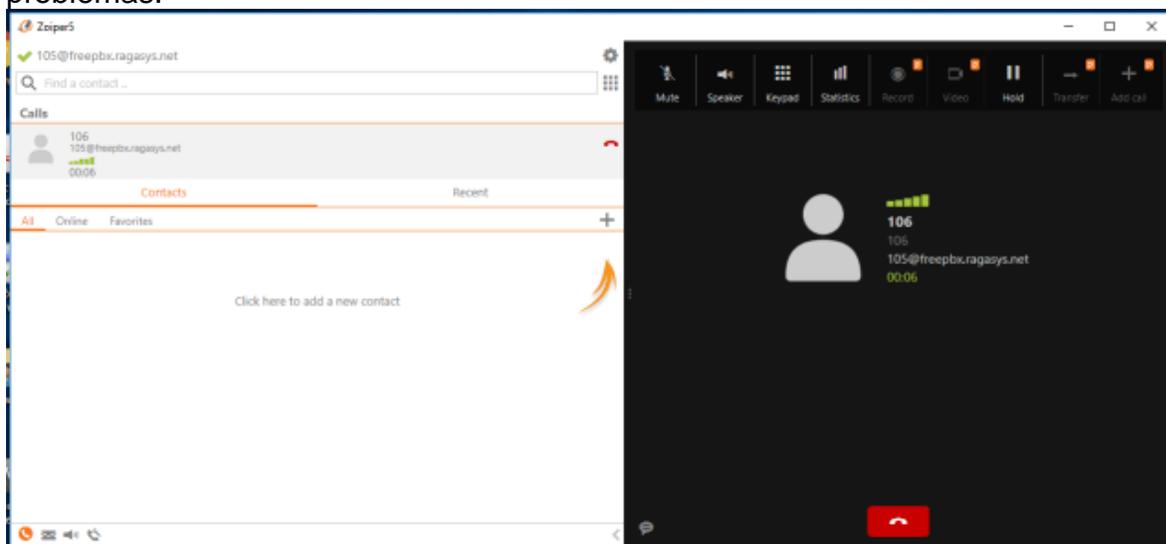


Para las demás extensiones, instalamos y configuramos el Zoiper 5 de igual manera en sus respectivos equipos.

Ahora vamos a probar una llamada entre extensiones, para ello, nos abrimos el teclado numérico y marcamos la extensión a la que queremos llamar, en este caso la 106, pulsamos sobre **Dial**:

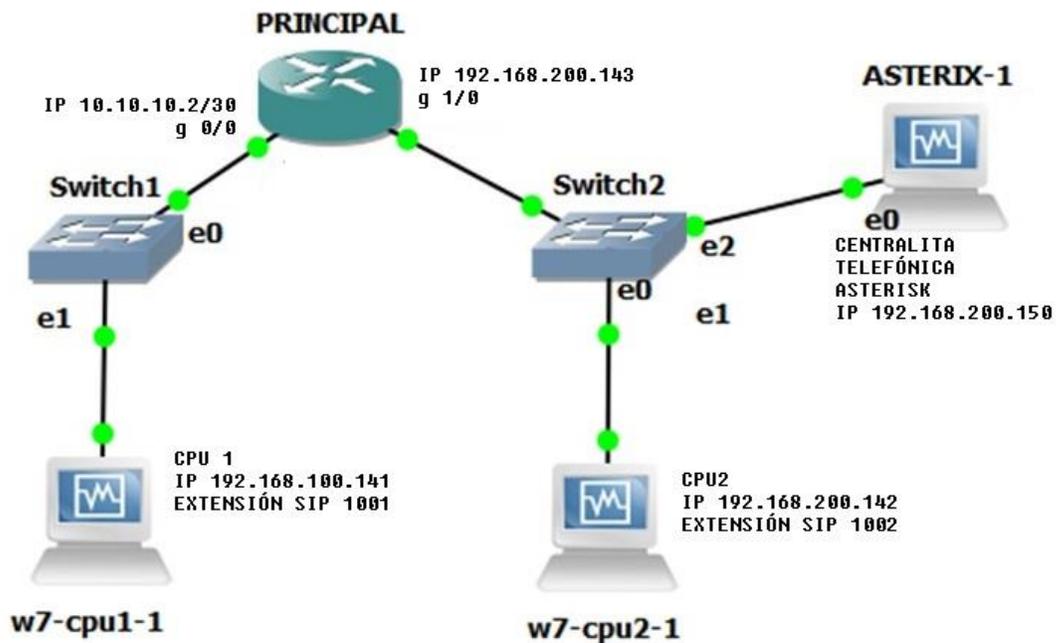


Como podemos ver ya tenemos la llamada establecida y podemos comunicarnos sin problemas:



Construcción de la red

Armar la red como indica la Fig.



Actividades por desarrollar:

1.- Realizar ping y tracert desde pcu1 a todos. Los resultados deben parecer a las siguientes capturas

```

C:\Windows\system32\cmd.exe

C:\Users\cpu-1>ping 192.168.200.142

Haciendo ping a 192.168.200.142 con 32 bytes de datos:
Respuesta desde 192.168.200.142: bytes=32 tiempo=46ms TTL=127
Respuesta desde 192.168.200.142: bytes=32 tiempo=17ms TTL=127
Respuesta desde 192.168.200.142: bytes=32 tiempo=16ms TTL=127
Respuesta desde 192.168.200.142: bytes=32 tiempo=14ms TTL=127

Estadísticas de ping para 192.168.200.142:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 14ms, Máximo = 46ms, Media = 23ms

C:\Users\cpu-1>ping 192.168.200.150

Haciendo ping a 192.168.200.150 con 32 bytes de datos:
Respuesta desde 192.168.200.150: bytes=32 tiempo=18ms TTL=63
Respuesta desde 192.168.200.150: bytes=32 tiempo=13ms TTL=63
Respuesta desde 192.168.200.150: bytes=32 tiempo=21ms TTL=63
Respuesta desde 192.168.200.150: bytes=32 tiempo=20ms TTL=63

Estadísticas de ping para 192.168.200.150:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 13ms, Máximo = 21ms, Media = 18ms

C:\Users\cpu-1>ping 192.168.200.143

Haciendo ping a 192.168.200.143 con 32 bytes de datos:
Respuesta desde 192.168.200.143: bytes=32 tiempo=13ms TTL=255
Respuesta desde 192.168.200.143: bytes=32 tiempo=9ms TTL=255
Respuesta desde 192.168.200.143: bytes=32 tiempo=7ms TTL=255
Respuesta desde 192.168.200.143: bytes=32 tiempo=5ms TTL=255

Estadísticas de ping para 192.168.200.143:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 5ms, Máximo = 13ms, Media = 8ms

C:\Users\cpu-1>

C:\Windows\system32\cmd.exe

C:\Users\cpu-1>tracert 192.168.200.142

Traza a la dirección CPU-2-PC [192.168.200.142]
sobre un máximo de 30 saltos:

  1    8 ms    10 ms    10 ms    192.168.100.140
  2   22 ms    20 ms    19 ms    CPU-2-PC [192.168.200.142]

Traza completa.

C:\Users\cpu-1>tracert 192.168.200.150

Traza a 192.168.200.150 sobre caminos de 30 saltos como máximo.

  1     5 ms    10 ms    10 ms    192.168.100.140
  2    14 ms    20 ms    20 ms    192.168.200.150

Traza completa.

C:\Users\cpu-1>tracert 192.168.200.143

Traza a 192.168.200.143 sobre caminos de 30 saltos como máximo.

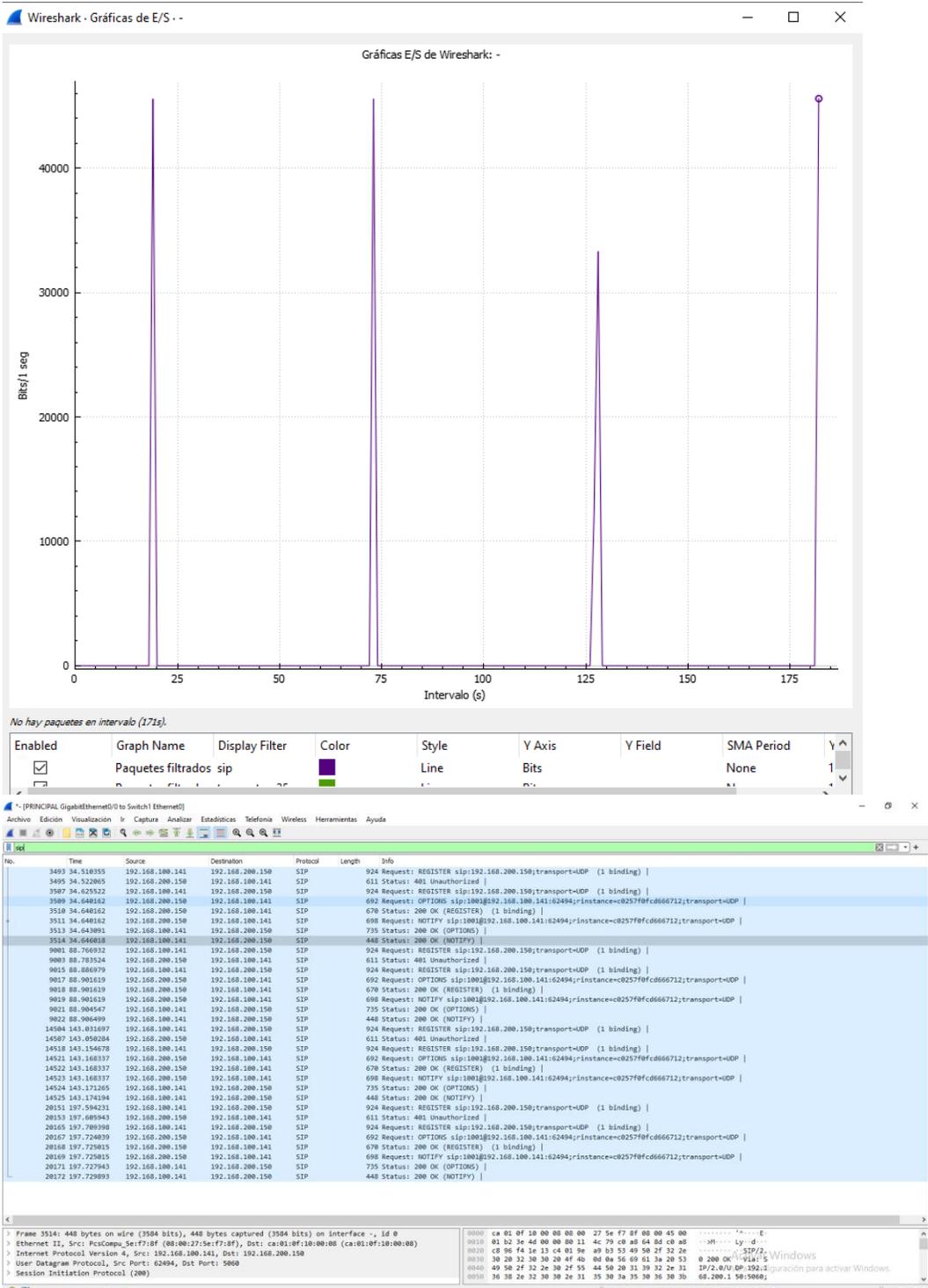
  1    12 ms    10 ms    10 ms    192.168.200.143

Traza completa.

C:\Users\cpu-1>

```

2.- Captar tráfico mediante Wireshark. Su resultado debe parecerse a las siguientes capturas.



Anexo 2. Guía 2-Red VoIP con QoS.

GUÍA Nº2 Red VoIP con QoS

Objetivos:

- Implementar un generador de tráfico en una red de prueba con su marcación de paquetes IP y monitoreo de tráfico VoIP.
- Aplicar políticas de gestión de QoS para la clasificación y priorización del tráfico IP.
- Realizar el análisis estadístico del flujo de paquetes durante una llamada de VOIP.

Marco teórico:

Asterisk

Es una plataforma de telefonía de código abierto que permite crear sistemas de telefonía IP con características avanzada. Es altamente flexible, escalable y se utiliza para realizar llamadas a través de redes IP. Es ampliamente utilizado para desarrollar soluciones personalizadas de comunicación de voz y video.

Zoiper

Es una aplicación de software VoIP que permite realizar llamadas de voz y video a través de internet, es compatible con diferentes plataformas y proveedores de servicios VoIP, con una interfaz fácil de usar y funciones avanzadas utilizadas por usuarios individuales o empresas.

Scapy

Es una herramienta de código abierto en Python que permite crear, enviar, capturar y analizar paquetes de red. Permite personalizar y manipular el tráfico de la red, realizar escaneos y pruebas de seguridad, de gran utilidad para administradores de redes y profesionales de seguridad informática.

Debian

Es un sistema operativo basado en Linux de código abierto, es muy utilizada por su estabilidad, seguridad y amplia selección de software libre. Utiliza el gestor de herramienta de paquetes avanzado (ATP) y admite diversas arquitecturas de hardware.

Equipos requeridos:

- Laptop o PC
- Conexión a Internet

Instrucciones

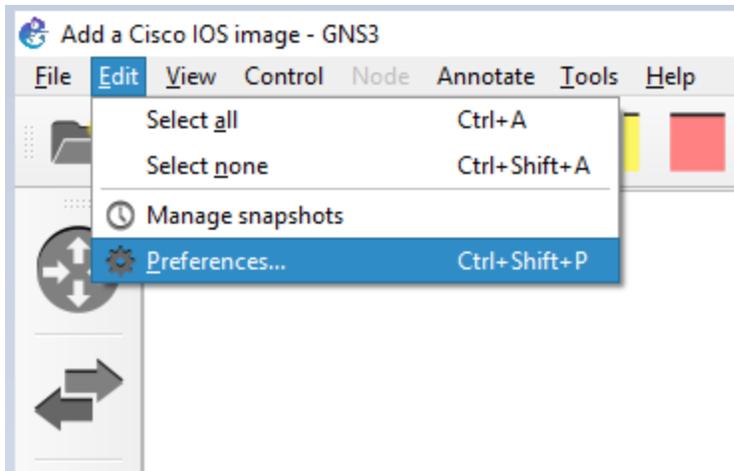
Instalación de Componentes en GNS3

ROUTER CISCO:

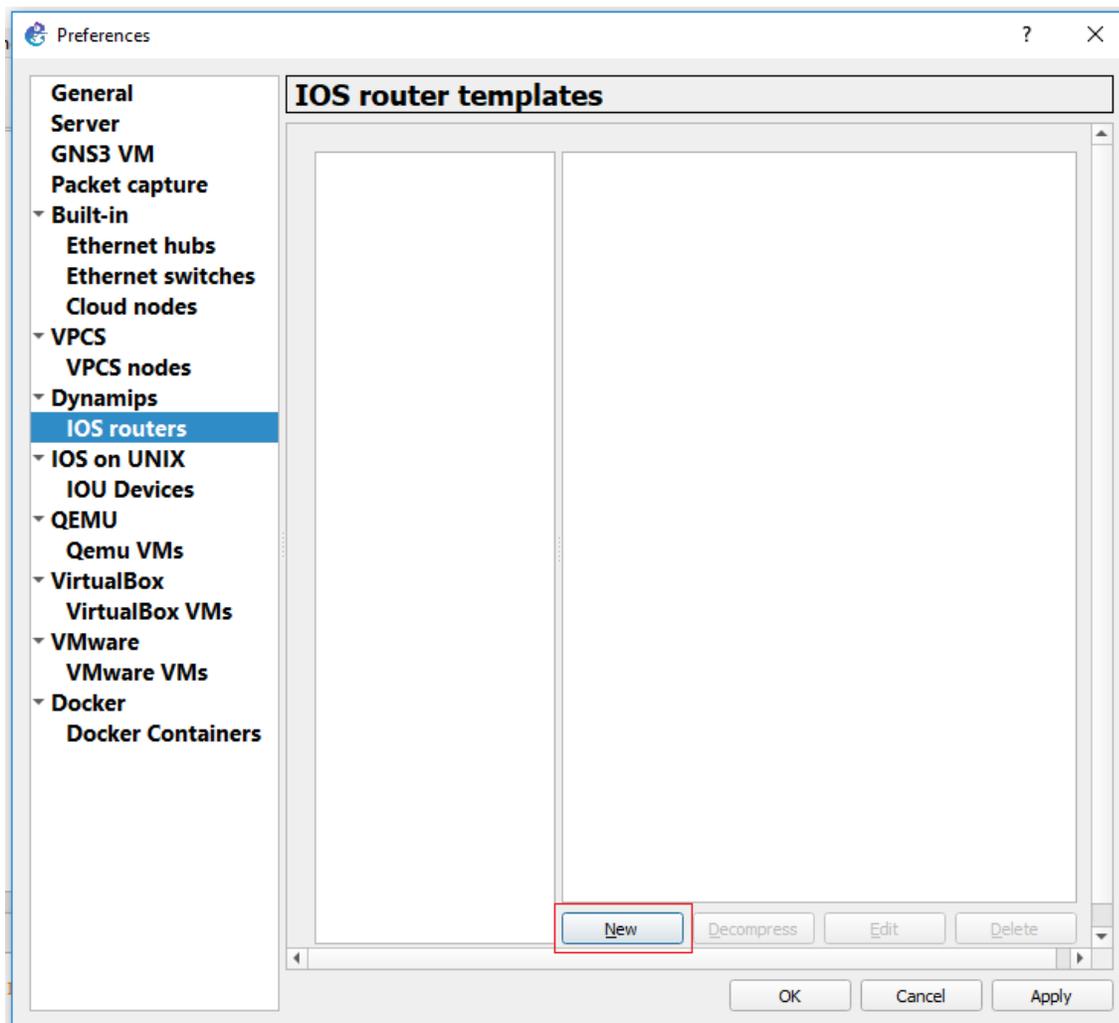
Descarga las imágenes de cisco del siguiente enlace:

<https://www.telectronika.com/descargas/cisco-imagenes-ios-para-gns3-dynamips-y-vm/>

Una vez descargado abre el GNS3 y ve a **Edit > Preferences...**



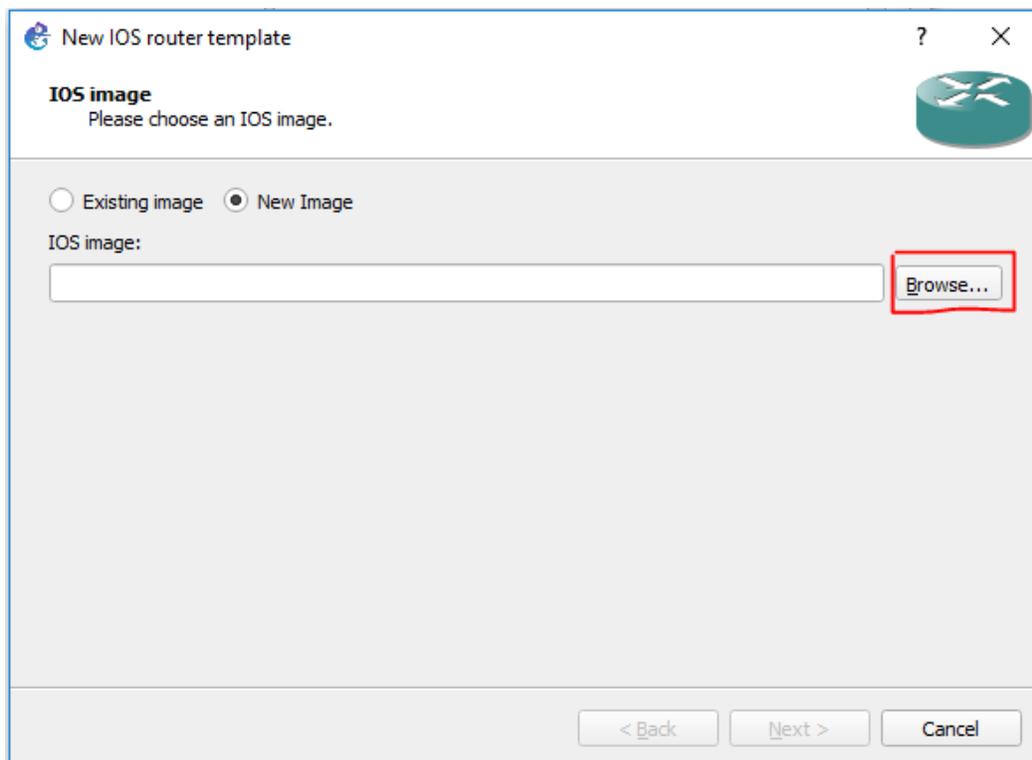
Una vez que aparezca la nueva ventana, ve a **Dynamips > IOS routers** y da click en **New**.



Otra ventana va a aparecer, ésta es un tipo de “setup Wizard”, sólo sigue los pasos, muy intuitivo.

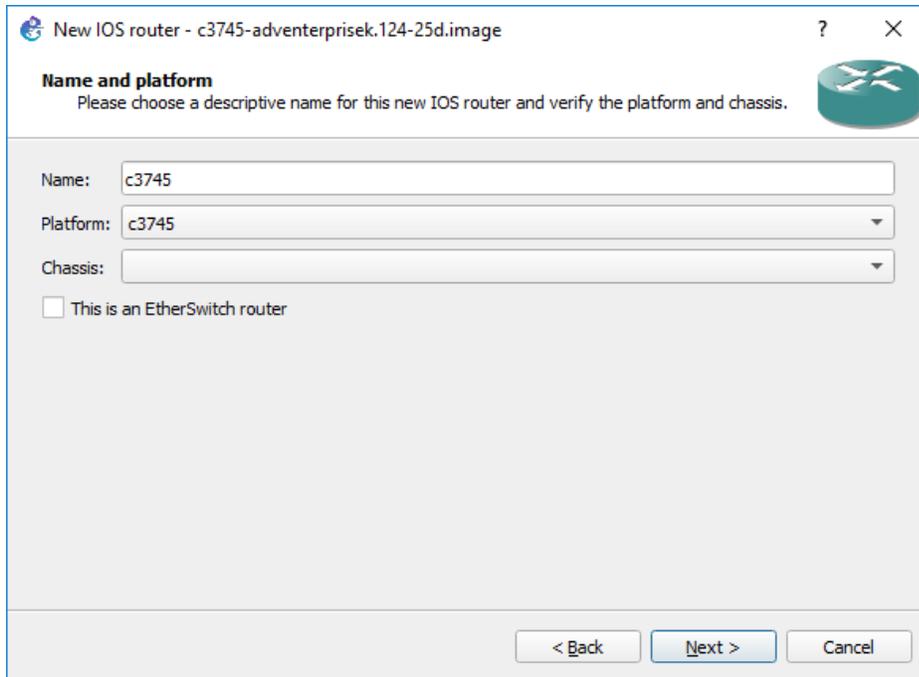
De cualquier forma, aquí los muestro.

Selecciona la opción **New Image** y después da click en **Browse** y busca la carpeta donde tengas la imagen del router a agregar.



Una vez seleccionado el IOS del router, da click en **Next** y a continuación verás la siguiente ventana.

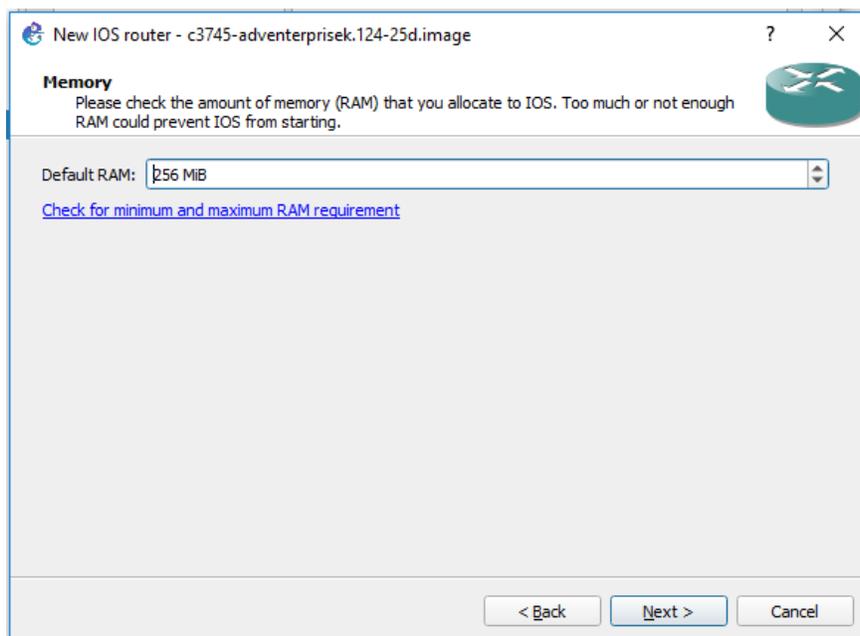
Elige un nombre y da click en **Next**.



The screenshot shows a configuration window titled "New IOS router - c3745-adventerprisek.124-25d.image". The window has a help icon and a close icon in the top right corner. Below the title bar, there is a router icon. The main heading is "Name and platform" with a sub-instruction: "Please choose a descriptive name for this new IOS router and verify the platform and chassis." The form contains three input fields: "Name:" with the value "c3745", "Platform:" with a dropdown menu showing "c3745", and "Chassis:" with a dropdown menu. Below these fields is a checkbox labeled "This is an EtherSwitch router" which is currently unchecked. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

En la siguiente ventana tendrás que especificar la cantidad de memoria RAM que quieres asignar a dicho router.

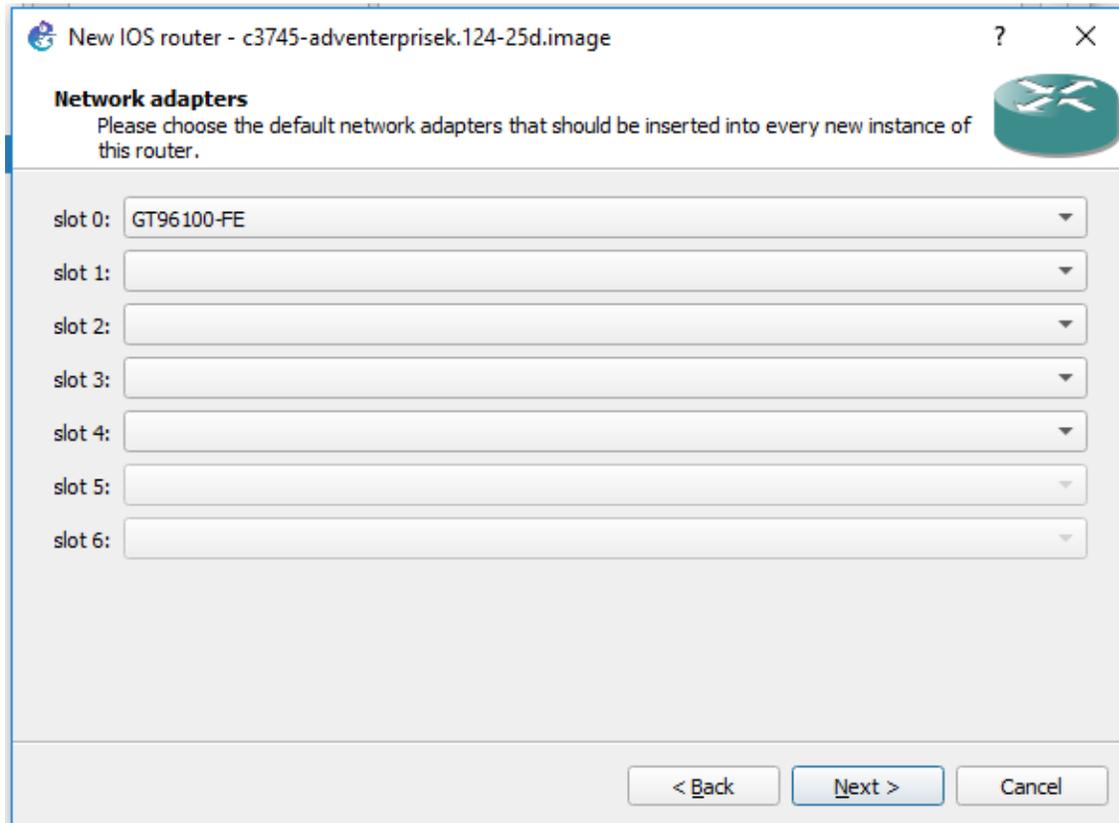
El valor mínimo recomendado de RAM será automáticamente asignado, tú puedes aumentarlo o disminuirlo.



The screenshot shows a configuration window titled "New IOS router - c3745-adventerprisek.124-25d.image". The window has a help icon and a close icon in the top right corner. Below the title bar, there is a router icon. The main heading is "Memory" with a sub-instruction: "Please check the amount of memory (RAM) that you allocate to IOS. Too much or not enough RAM could prevent IOS from starting." The form contains a "Default RAM:" field with a dropdown menu showing "256 MIB". Below this field is a blue hyperlink: "Check for minimum and maximum RAM requirement". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

Una vez hayas terminado aquí, da click en **Next**.

En la siguiente ventana puedes agregar interfaces por cada “slot”, según el modelo del equipo es la cantidad y tipo de interfaces que te permite agregar.



Tipos de interfaces:

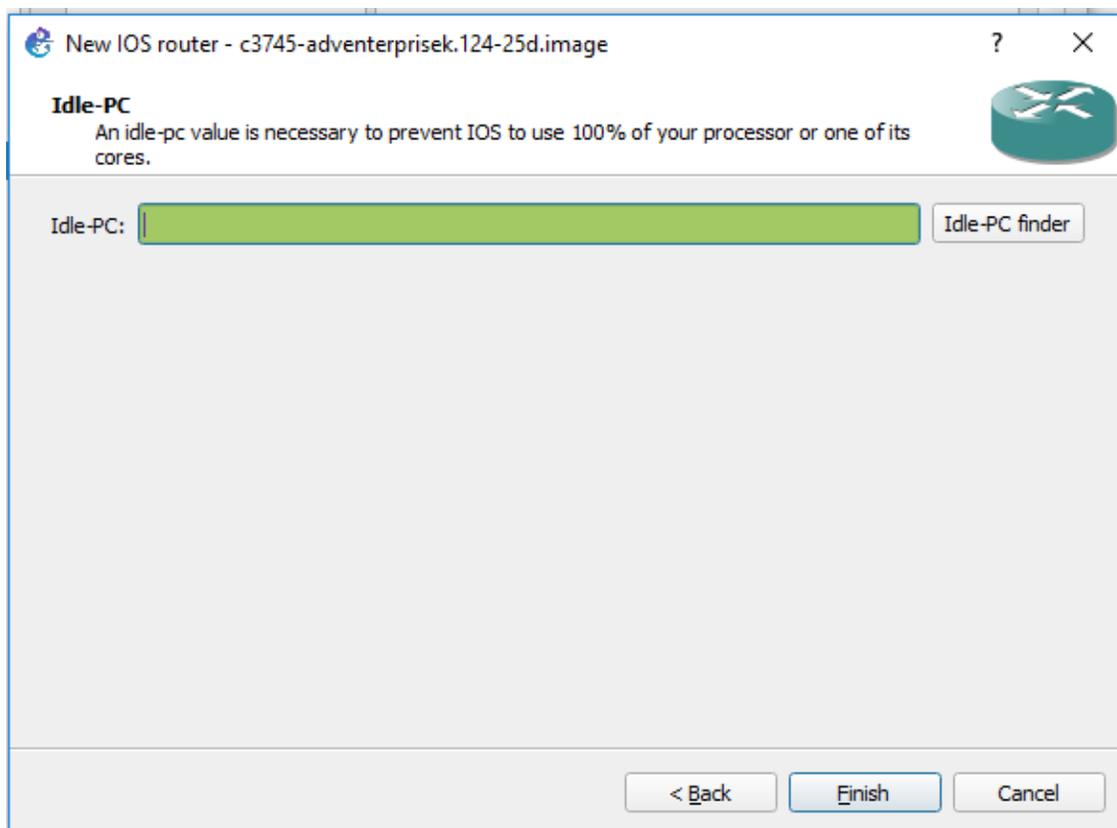
- **NM-1E**, tiene 1 puerto Ethernet.
- **NM-1FE-TX**, tiene 1 puerto FastEthernet.
- **NM-16ESW**, es un modulo de Switch con 16 puertos FastEthernet y tiene funciones básicas de switching (capa2).
- **NM-4T**, tiene 4 puertos Serial para conexiones WAN.

La siguiente ventana (WIC modules) te permite agregar todavía más puertos Serial.

Da click en **Next** una vez hayas terminado.

En la siguiente ventana te pedirá ingresar un “idle-pc value”, éste es muy importante para que el CPU de tu PC no se eleve al límite.

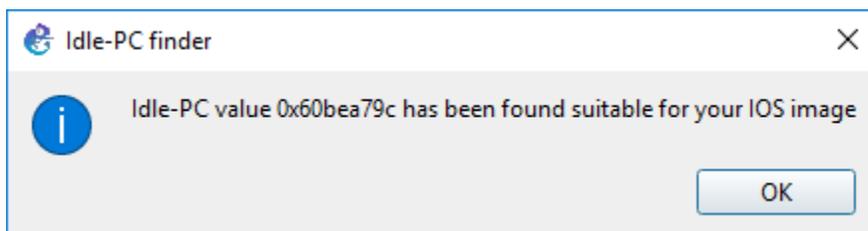
Da click en **Idle-PC finder** para que GNS3 encuentre de manera automática el valor recomendado para el equipo que vas a agregar.



NOTA:

Este paso **NO** debe omitirse.

Te aparecerá algo como esto.

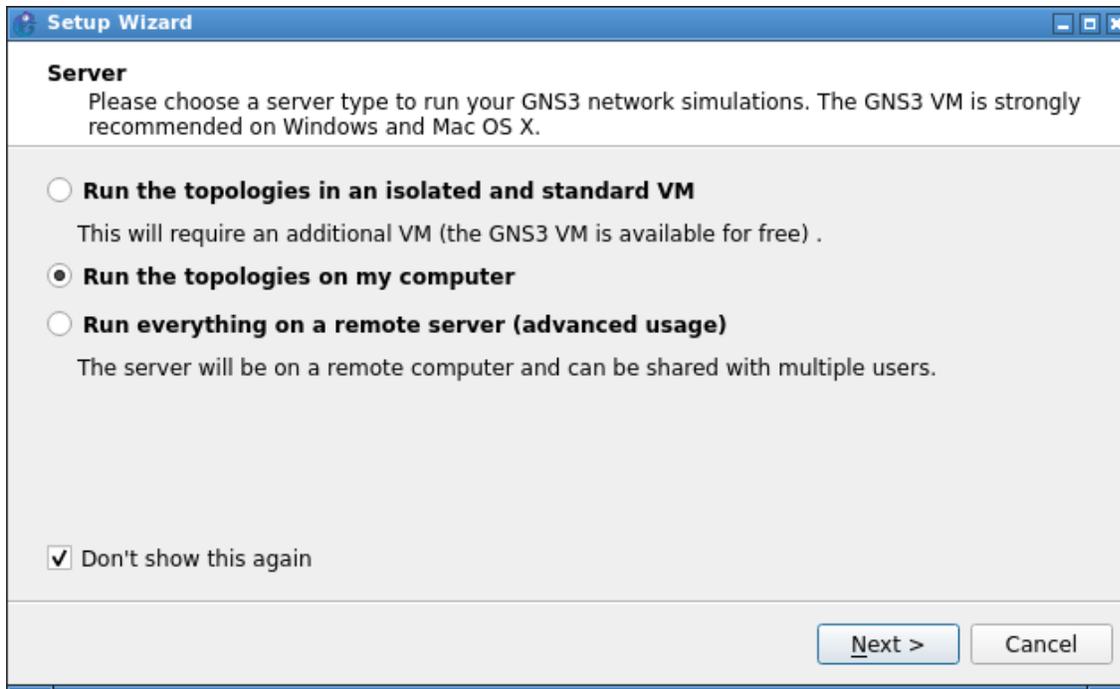


Has terminado, da click en Finish, después en Apply y repite el proceso para agregar tantos equipos como necesites

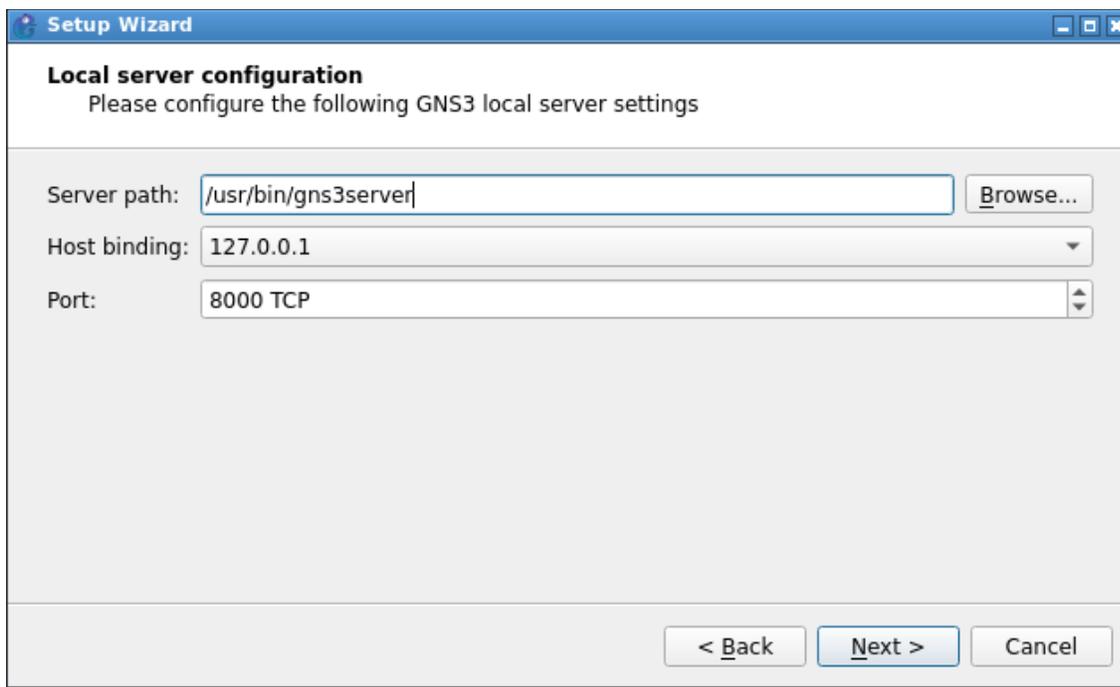
AÑADIR MAQUINAS VIRTUALES DE VIRTUALBOX:

Vamos a hacer uso del asistente de configuración que provee la herramienta. El asistente suele lanzarse inmediatamente cuando ejecutamos el GUI, si no en el menú **Help/Ayuda** lo veremos también:

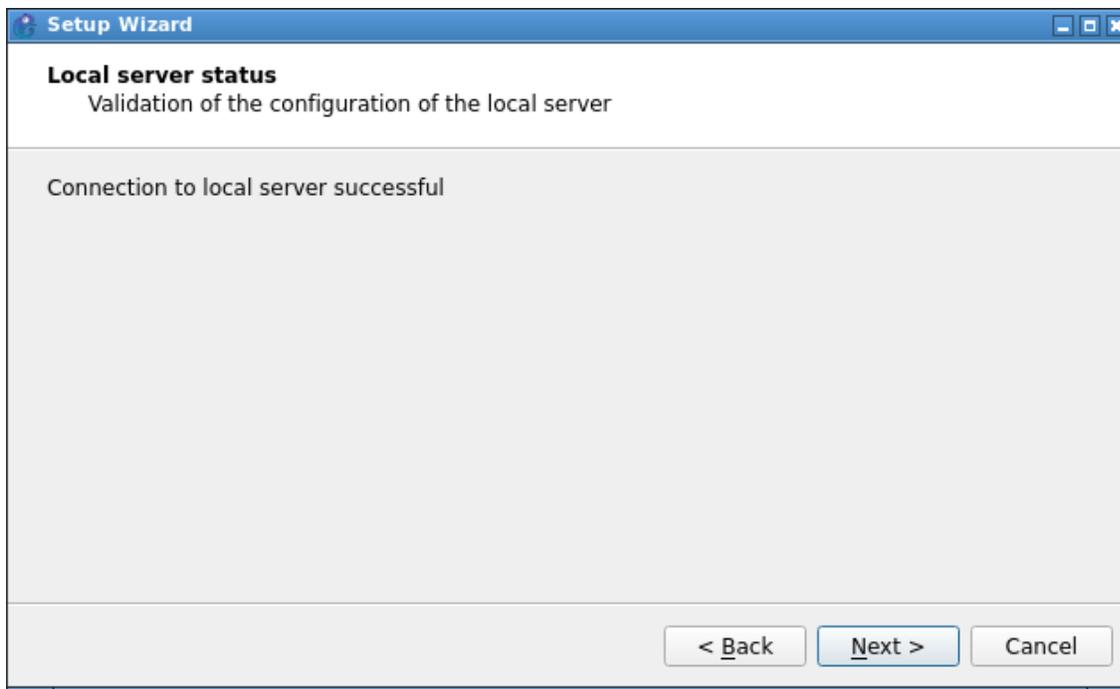
Primer paso: Seleccionamos correr las topologías en nuestra computadora:



Luego dejamos los datos por defecto en general. Tenemos la ubicación del binario del servidor, la dirección IP en la que atiende, y el puerto.

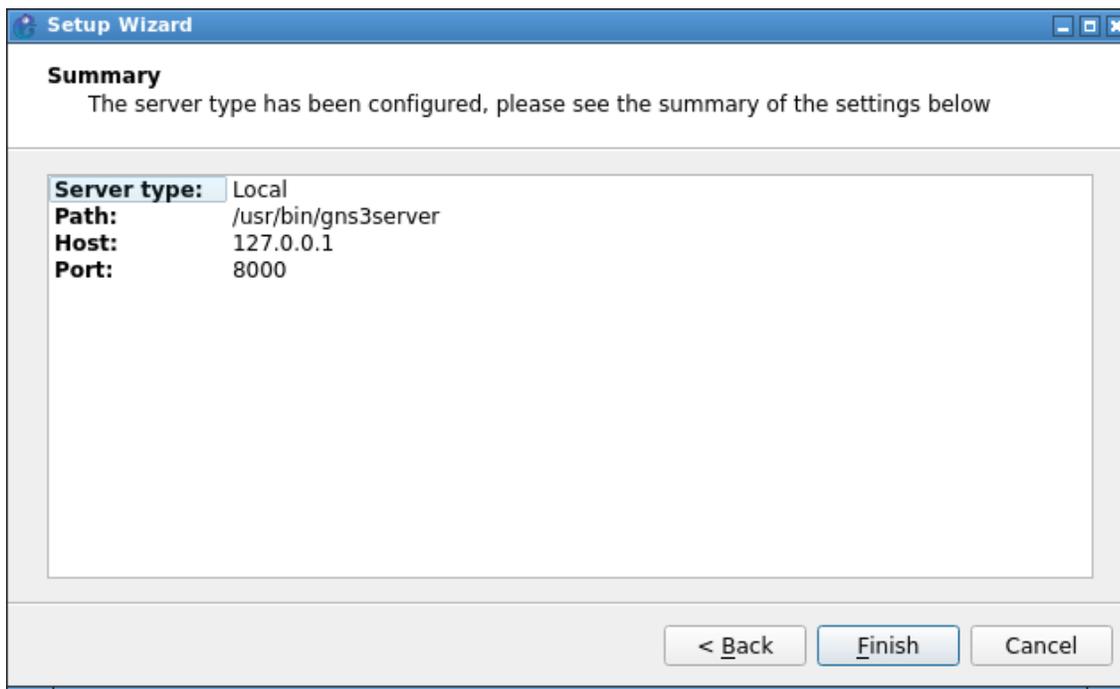


Paso siguiente, la GUI intentará conectar con el servidor. Si el servidor se ejecutó correctamente, la GUI podrá linkear, y veremos una ventana como esta:

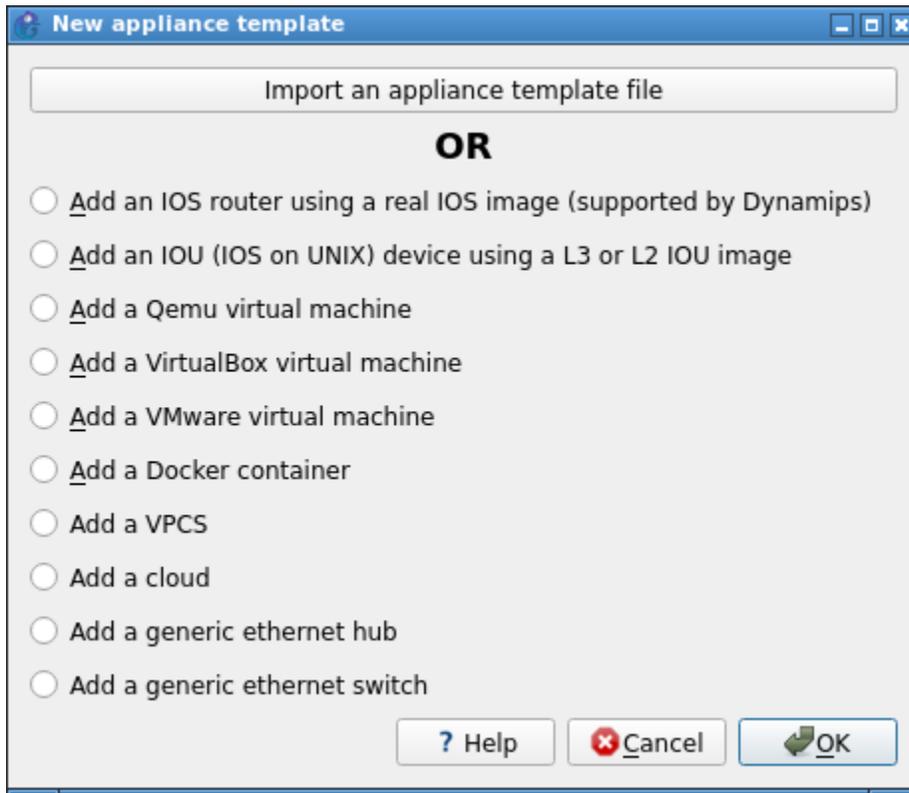


En el caso de que no pueda conectar, será porque el servidor no está corriendo... deberemos analizarlo y depurarlo. Un consejo interesante en este punto: si no corre el servidor, tomar la línea del binario de la captura anterior (Server Path) y ejecutarlo por terminal... en general suelen faltar algunas dependencias de Python.

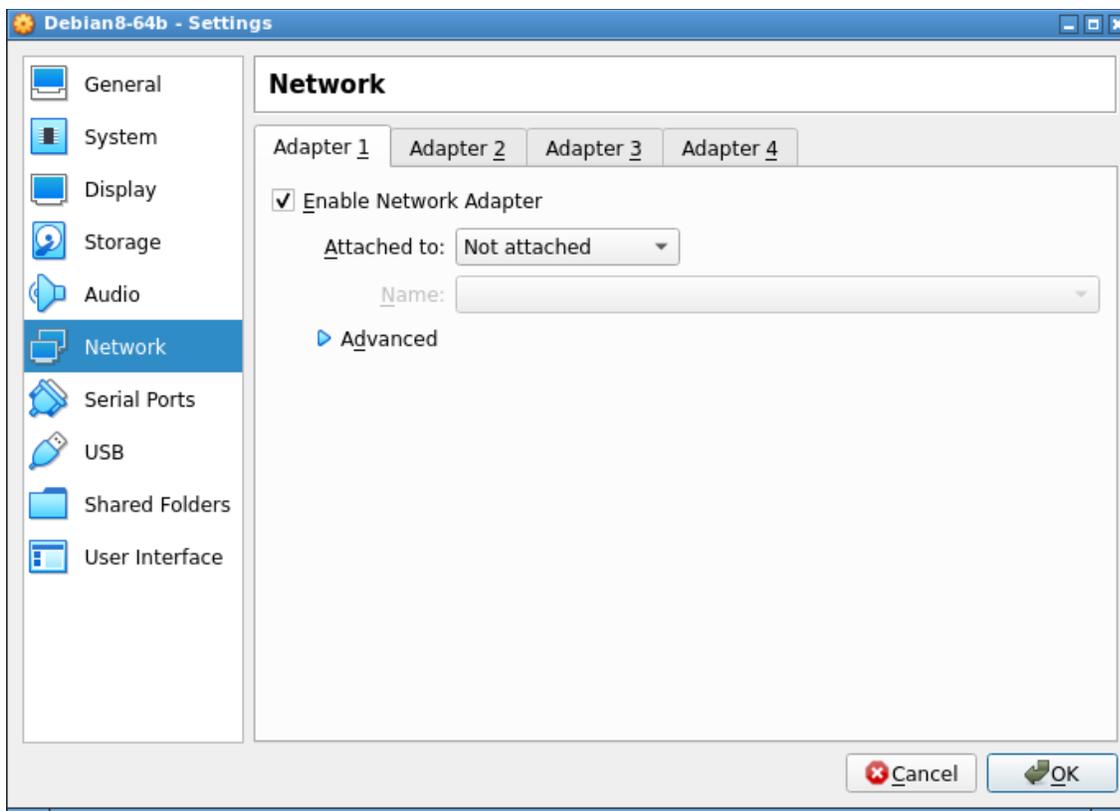
Si todo salió bien, en la siguiente pantalla veremos un resumen de la configuración:



Finalmente, al terminar el asistente nos preguntará si queremos cargar algún archivo template al sistema, que luego podremos utilizar en nuestros proyectos:

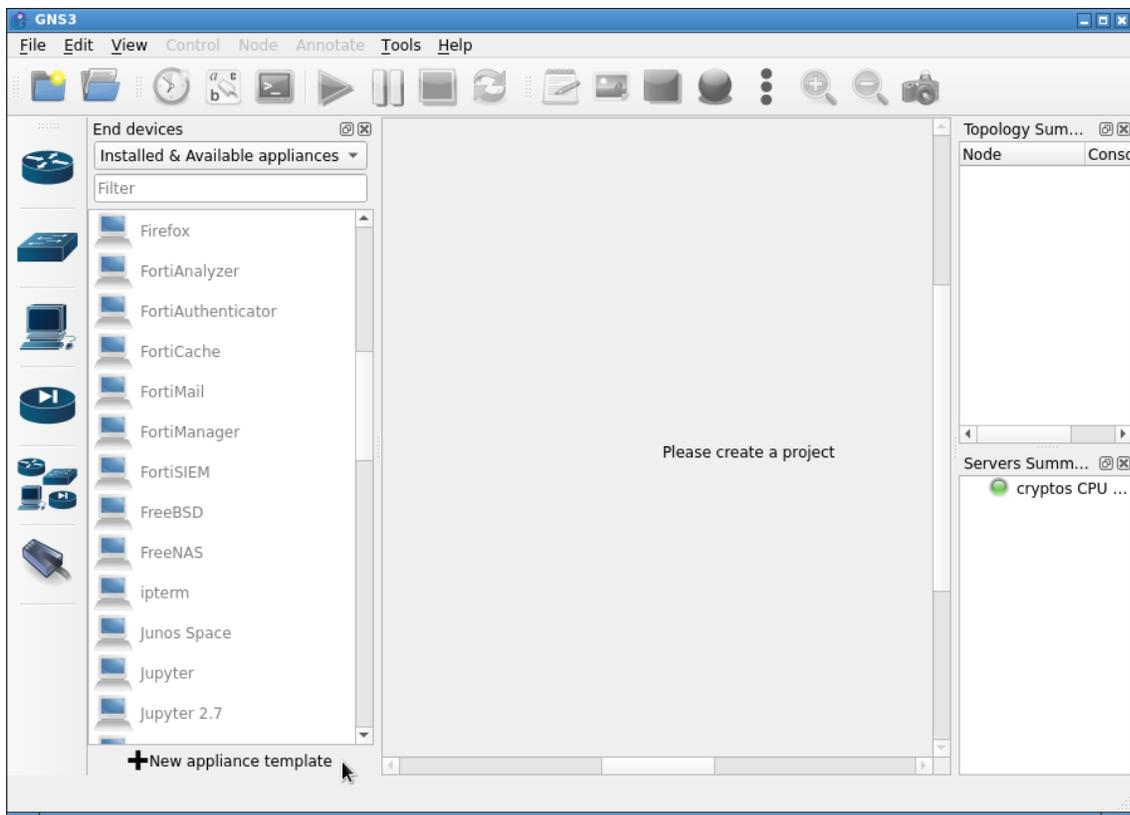


Para agregar los componentes de vinculación de VirtualBox a GNS3 debemos hacer lo siguiente: Por un lado, entrar a la configuración de las interfaces de red del equipo virtual, y en la sección de red/network, configurar la interfaz de red como "no attached"

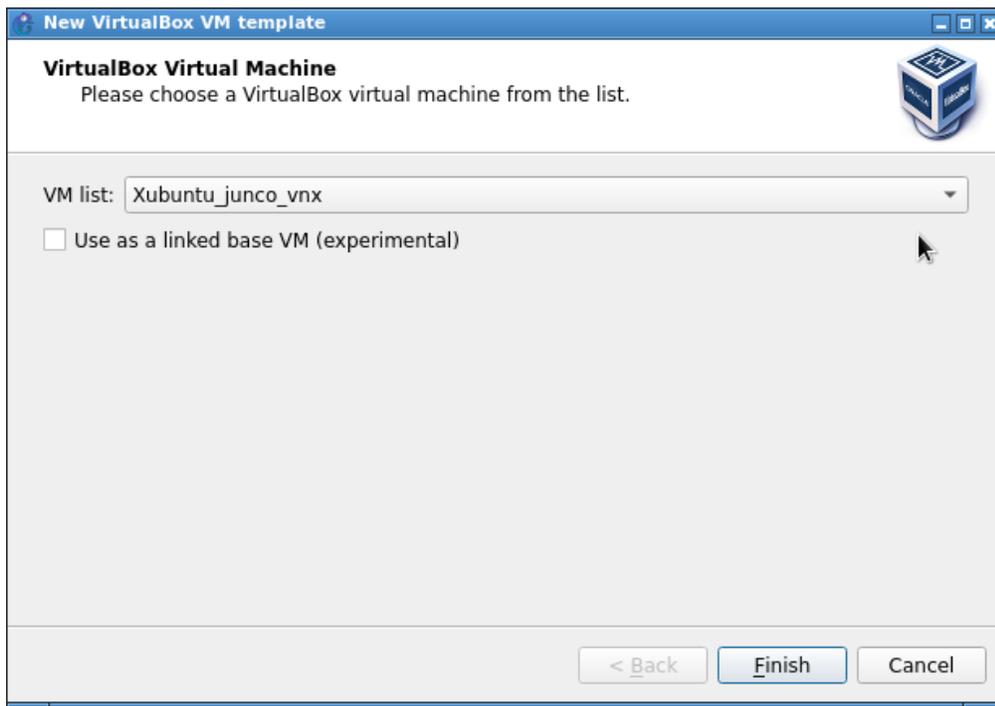


Esto es porque de esa forma GNS3 puede tomar el control de la interfaz de red, y luego que corramos la topología podremos configurar el direccionamiento en el equipo virtual, o configurar un router virtual que le de IP dinámica a las computadoras.

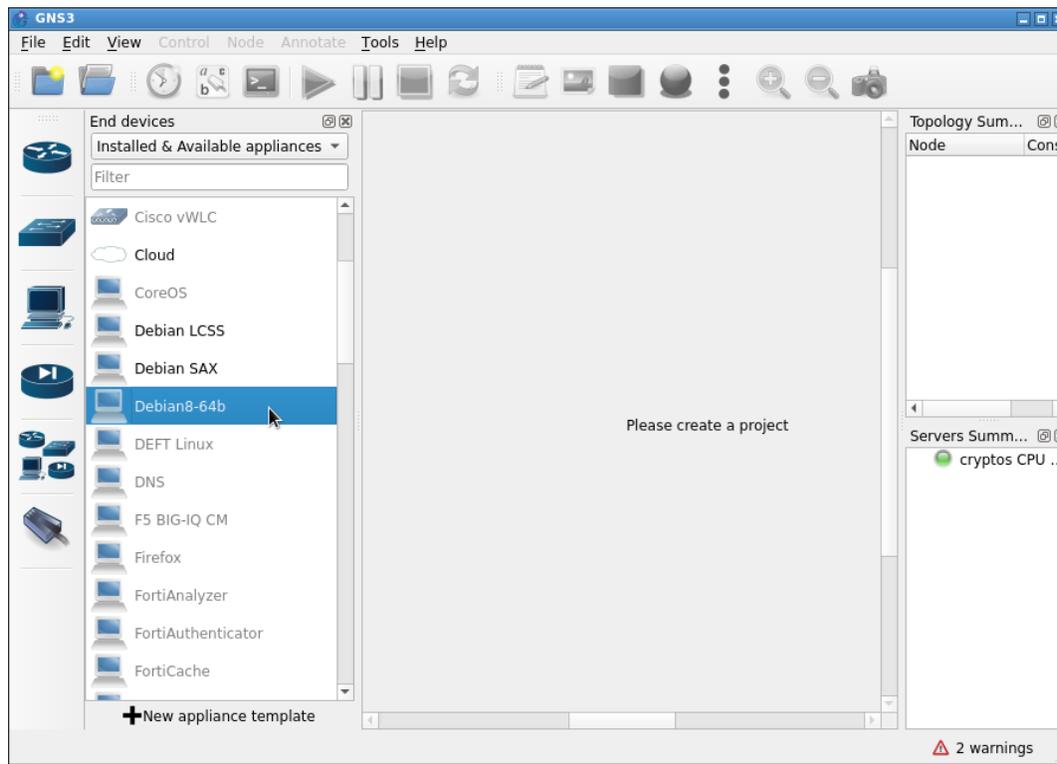
Acto seguido, en la columna de la izquierda de GNS3 vamos a seleccionar los end-devices (el iconito de la computadora), y en la parte inferior veremos un botón que nos permitirá agregar nuevos equipos a la configuración:



Si damos clic vamos a ver la misma ventana de carga de templates que mostré arriba, en la que vamos a seleccionar «Máquina virtual Virtual Box», y damos «OK», con lo que veremos lo siguiente:

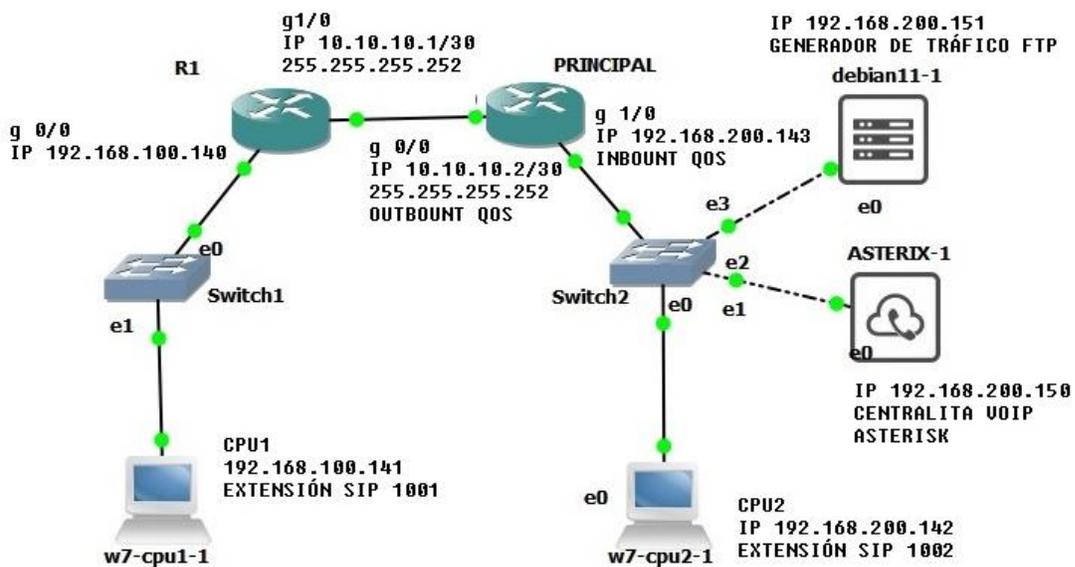


En el desplegable veremos todos los equipos virtuales que tenemos en VirtualBox... no tenemos más que seleccionar el que configuramos recién, y terminar con "Finish"



Y podremos añadir las máquinas virtuales a nuestra topología

Construcción de la red



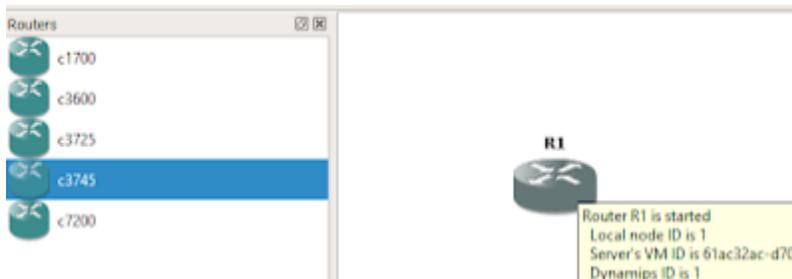
Para la construcción de esta red se utilizo los siguientes Componentes

- 2 Router Cisco C7200
- 2 VirtuaBox con Windows 7
- 1 VirtualBox con Debian 11
- 1 VirtualBox con Elastix (Asterisk)
- 2 Switch no configurables

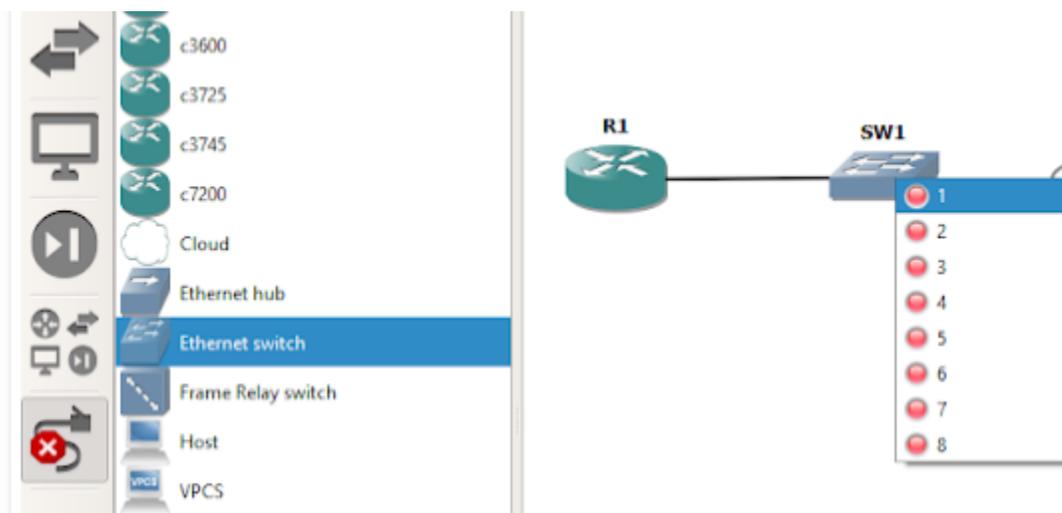
Luego para ir añadiendo cada componente hacemos clic en el botón “All Devices”



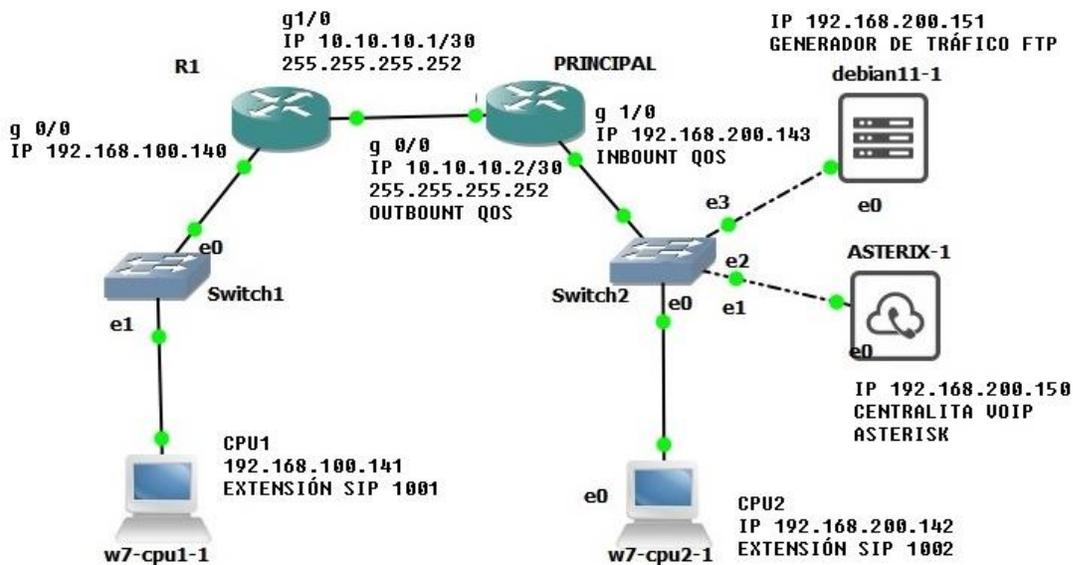
y añadimos los componentes necesarios haciendo un clic sobre este y colocándolo en el espacio en blanco de GNS3



Hacemos lo mismo con el resto de componentes, luego con el icono Link cableamos cada componente para que este interconectado



Finalmente armamos nuestra topología de red y colocamos etiquetas de texto para tener mas claro el diseño y direcciones que tendrá cada componente



CONFIGURACION DE ROUTERS Y POLITICAS DE MAPEO DE CALIDAD DE SERVICIO

PRINCIPAL

---CONFIGURACION DE PUERTOS G1/0 Y G0/0

```
#ENABLE
```

```
#CONFIG TERMINAL
```

```
#HOSTNAME PRINCIPAL
```

```
#interface GigabitEthernet0/0
```

```
#ip address 10.10.10.2 255.255.255.252
```

```
#rate-limit output 128000 24576 49152 conform-action transmit exceed-action drop
```

```
#interface GigabitEthernet1/0
```

```
#ip address 192.168.200.143 255.255.255.0
```

```
#rate-limit output 128000 24576 49152 conform-action transmit exceed-act
```

```
#EXIT
```

CONFIGURACION DE ENRUTAMIENTO ESTATICO

```
#ENABLE
```

```
#CONFIG TERMINAL
```

```
#ip route 192.168.100.0 255.255.255.0 192.168.100.140
```

```
# ip route 192.168.100.0 255.255.255.0 10.10.10.1
```

CONFIGURACION DE REGLAS DE ACCESO ACL POR PROTOCOLO

```
# ip access-list extended VIP-rtp-sip-rtcp
```

```
    # permit tcp any any eq 1720
```

```
    # permit udp any any eq 2427
```

```
    # permit tcp any any eq 2428
```

```
    # permit tcp any any range 2000 2002
```

```
    # permit udp any any eq 1719
```

```
    # permit udp any any eq 4569
```

```
    # permit tcp any any range 5060 5061
```

```
    # permit udp any any range 5060 5061
```

```
    # permit icmp any any
```

```
    # permit udp any any range 10000 20000
```

```
    # permit udp any any range 20000 65535
```

```
# ip access-list extended email
```

```
    # permit tcp any any eq smtp
```

```
# ip access-list extended ftp-sftp
```

```
    # permit tcp any any eq ftp-data
```

```
    # permit tcp any any eq ftp
```

CONFIGURACION DE MARCACION DE PAQUETES QoS

```
#class-map match-all MAP-VIP-rtsp-sip-rtcp  
  
#match access-group name VIP-rtsp-sip-rtcp  
  
#class-map match-all MAP-email  
  
#match access-group name email  
  
# class-map match-all MAP-ftp-sftp  
  
# match access-group name ftp-sftp
```

CONFIGURACION DE ASIGNACION DE PRIORIDAD CON MAPEO DE CLASE QoS

```
#class-map match-all MAP-oro  
  
#match dscp ef  
  
#class-map match-all MAP-plata  
  
# match dscp af22  
  
# class-map match-all MAP-bronze  
  
# match dscp af31
```

CONFIGURACION DE POLITICA DE MAPEO DE CLASE Y ASIGNACION DE ANCHO DE BANDA PORCENTUAL QoS

```
#policy-map POL-CLASSIFY-OUT  
  
#class MAP-oro  
  
#bandwidth percent 30  
  
#class MAP-plata  
  
#bandwidth percent 30  
  
#class MAP-bronze  
  
#bandwidth percent 30  
  
#class class-default
```

```
#fair-queue  
  
#policy-map POL-CLASSIFY-IN  
  
#class MAP-VIP-rtp-sip-rtcp  
  
#set dscp ef  
  
#class MAP-ftp-sftp  
  
# set dscp af22  
  
# class MAP-email  
  
# set dscp af31
```

CONFIGURACION DE ASIGNACION DE POLITICAS DE MAPEO QoS SOBRE LOS PUERTOS G1/0 Y G0/0

```
#ENABLE  
  
#CONFIG TERMINAL  
  
#interface GigabitEthernet0/0  
  
# service-policy output POL-CLASSIFY-OUT  
  
#interface GigabitEthernet1/0  
  
# service-policy input POL-CLASSIFY-IN
```

ROUTER R1

---CONFIGURACION DE PUERTOS G1/0 Y G0/0

```
#ENABLE  
  
#CONFIG TERMINAL  
  
#HOSTNAME PRINCIPAL  
  
#interface GigabitEthernet0/0  
  
#ip address 10.10.10.2 255.255.255.252  
  
#rate-limit output 128000 24576 49152 conform-action transmit exceed-action drop
```

```
#interface GigabitEthernet1/0

#ip address 192.168.200.143 255.255.255.0

#rate-limit output 128000 24576 49152 conform-action transmit exceed-act

#EXIT
```

CONFIGURACION DE ENRUTAMIENTO ESTATICO

```
#ENABLE

#CONFIG TERMINAL

#ip route 192.168.200.0 255.255.255.0 192.168.200.143

#ip route 192.168.200.0 255.255.255.0 10.10.10.2
```

CONSTRUCCIÓN DE SIMULADOR DE PAQUETES DE CORREO A TRAVÉS DE SCAPY EN DEBIAN

Abrir el terminal en Debian 11

[Escribir los siguientes comandos](#)

```
Su
1234
Sudo scapy -H
from scapy.all import *

# Configuración de parámetros
src_ip = "192.168.100.150" # Dirección IP de origen
dst_ip = "192.168.200.142" # Dirección IP de destino
src_port = 12345 # Puerto de origen
dst_port = 25 # Puerto de destino (SMTP)

# Crear paquete de correo electrónico
packet = IP(src=src_ip, dst=dst_ip) / TCP(sport=src_port, dport=dst_port) /
Raw("Mensaje de correo electrónico")

# Enviar paquete
send(packet, count=1000)
```

Actividades por desarrollar:

1.- Realizar ping y tracert desde pcu1 a todos. Los resultados deben parecer a las siguientes capturas

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\cpu-1>ping 192.168.200.142

Haciendo ping a 192.168.200.142 con 32 bytes de datos:
Respuesta desde 192.168.200.142: bytes=32 tiempo=44ms TTL=126
Respuesta desde 192.168.200.142: bytes=32 tiempo=27ms TTL=126
Respuesta desde 192.168.200.142: bytes=32 tiempo=32ms TTL=126
Respuesta desde 192.168.200.142: bytes=32 tiempo=30ms TTL=126

Estadísticas de ping para 192.168.200.142:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 27ms, Máximo = 44ms, Media = 33ms

C:\Users\cpu-1>ping 192.168.200.151

Haciendo ping a 192.168.200.151 con 32 bytes de datos:
Respuesta desde 192.168.200.151: bytes=32 tiempo=33ms TTL=62
Respuesta desde 192.168.200.151: bytes=32 tiempo=28ms TTL=62
Respuesta desde 192.168.200.151: bytes=32 tiempo=33ms TTL=62
Respuesta desde 192.168.200.151: bytes=32 tiempo=32ms TTL=62

Estadísticas de ping para 192.168.200.151:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 28ms, Máximo = 33ms, Media = 31ms

C:\Users\cpu-1>ping 192.168.200.150

Haciendo ping a 192.168.200.150 con 32 bytes de datos:
Respuesta desde 192.168.200.150: bytes=32 tiempo=33ms TTL=62
Respuesta desde 192.168.200.150: bytes=32 tiempo=31ms TTL=62
Respuesta desde 192.168.200.150: bytes=32 tiempo=24ms TTL=62
Respuesta desde 192.168.200.150: bytes=32 tiempo=23ms TTL=62

Estadísticas de ping para 192.168.200.150:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 23ms, Máximo = 33ms, Media = 27ms

C:\Users\cpu-1>

```

```

C:\Windows\system32\cmd.exe
C:\Users\cpu-1>
C:\Users\cpu-1>
C:\Users\cpu-1>tracert 192.168.200.142

Traza a la dirección CPU-2-PC [192.168.200.142]
sobre un máximo de 30 saltos:

  1    6 ms    9 ms    9 ms    192.168.100.140
  2   16 ms   20 ms   20 ms   10.10.10.2
  3   25 ms   30 ms   31 ms   CPU-2-PC [192.168.200.142]

Traza completa.

C:\Users\cpu-1>tracert 192.168.200.151

Traza a 192.168.200.151 sobre caminos de 30 saltos como máximo.

  1   12 ms    9 ms    9 ms    192.168.100.140
  2   25 ms   30 ms   31 ms   10.10.10.2
  3   35 ms   41 ms   41 ms   192.168.200.151

Traza completa.

C:\Users\cpu-1>tracert 192.168.200.150

Traza a 192.168.200.150 sobre caminos de 30 saltos como máximo.

  1    4 ms    9 ms    9 ms    192.168.100.140
  2   25 ms   30 ms   30 ms   10.10.10.2
  3   35 ms   41 ms   42 ms   192.168.200.150

Traza completa.

C:\Users\cpu-1>tracert 10.10.10.1

Traza a 10.10.10.1 sobre caminos de 30 saltos como máximo.

  1   13 ms    9 ms    9 ms   10.10.10.1

Traza completa.

C:\Users\cpu-1>tracert 192.168.200.143

Traza a 192.168.200.143 sobre caminos de 30 saltos como máximo.

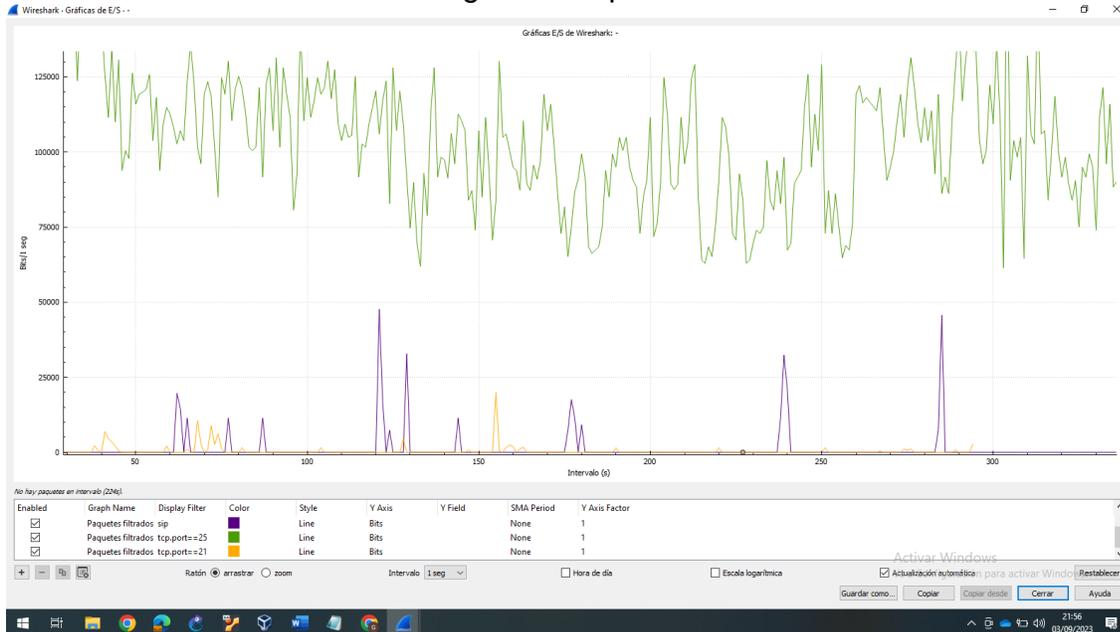
  1    6 ms    9 ms    9 ms    192.168.100.140
  2   19 ms   20 ms   20 ms   192.168.200.143

Traza completa.

C:\Users\cpu-1>

```

Luego de realizar la llamada entre cpu1 cpu2. Realizar la transferencia de archivos entre cpu2 y cpu1. Y generar tráfico de correo. Captar el tráfico mediante Wireshark en la interfaz g0/0 del router principal para analizar los distintos tipos de flujo de paquetes. Su resultado debe ser similar a la siguiente captura.



Filtrar paquetes de correo mediante el comando `tcp.port==25` en Wireshark. Así, confirmando el generador de correo. Su respuesta debe ser similar a la siguiente captura

* - [PRINCIPAL GigabitEthernet1/0 to Switch2 Ethernet0]

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port==25

No.	Time	Source	Destination	Protocol	Length	Info
2358	7.513460	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2359	7.514436	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2362	7.525172	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2363	7.525172	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2364	7.526149	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2365	7.531028	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2365	7.534831	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2366	7.536885	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2370	7.540859	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2371	7.545741	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2372	7.546715	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2373	7.554597	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2374	7.556549	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2377	7.563388	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2378	7.567284	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2379	7.567284	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2380	7.569237	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2381	7.578821	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2382	7.578821	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2383	7.579972	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2385	7.587781	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2386	7.589840	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2387	7.590787	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2390	7.592738	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2391	7.596643	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2393	7.599570	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2394	7.602499	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2395	7.610307	192.168.100.141	192.168.200.151	TCP	54	25 → 12345 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2396	7.613235	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30
2397	7.618114	192.168.200.151	192.168.100.141	TCP	84	[TCP Retransmission] 12345 → 25 [SYN] Seq=0 Win=8192 Len=30

Anexo 3. Configuraciones del dispositivo de red-Router Principal

```
PRINCIPAL#show run
Building configuration...
```

```
Current configuration : 3166 bytes
```

```
!  
upgrade fpd auto  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname PRINCIPAL  
!  
boot-start-marker  
boot-end-marker  
!  
!  
!  
no aaa new-model  
!  
!  
!  
!  
no ip domain lookup  
ip cef  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
redundancy  
!  
!  
!  
class-map match-all MAP-oro  
  match dscp ef  
class-map match-all MAP-plata  
  match dscp af22  
class-map match-all MAP-VIP-rtp-sip-rtcp  
  match access-group name VIP-rtp-sip-rtcp  
class-map match-all MAP-email  
  match access-group name email  
class-map match-all MAP-ftp-sftp  
  match access-group name ftp-sftp  
class-map match-all MAP-bronce  
  match dscp af31  
!  
policy-map POL-CLASSIFY-OUT  
  class MAP-oro  
    bandwidth percent 30
```

```
class MAP-plata
  bandwidth percent 30
class MAP-bronze
  bandwidth percent 30
class class-default
  fair-queue
policy-map POL-CLASSIFY-IN
  class MAP-VIP-rtp-sip-rtcp
    set dscp ef
  class MAP-ftp-sftp
    set dscp af22
  class MAP-email
    set dscp af31
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
  no ip address
  shutdown
  duplex auto
!
interface GigabitEthernet0/0
  ip address 10.10.10.2 255.255.255.252
  rate-limit output 128000 24576 49152 conform-action transmit exceed-action drop
  duplex full
  speed 1000
  media-type gbic
  negotiation auto
  service-policy output POL-CLASSIFY-OUT
!
interface GigabitEthernet1/0
  ip address 192.168.200.143 255.255.255.0
  rate-limit output 128000 24576 49152 conform-action transmit exceed-action drop
  negotiation auto
  service-policy input POL-CLASSIFY-IN
!
interface FastEthernet2/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface FastEthernet2/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
```

```
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet4/0
no ip address
shutdown
negotiation auto
!
interface Serial5/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
interface POS6/0
no ip address
shutdown
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 192.168.100.0 255.255.255.0 192.168.100.140
ip route 192.168.100.0 255.255.255.0 10.10.10.1
!
ip access-list extended VIP-rtp-sip-rtcp
permit tcp any any eq 1720
permit udp any any eq 2427
permit tcp any any eq 2428
permit tcp any any range 2000 2002
permit udp any any eq 1719
permit udp any any eq 4569
```

```

permit tcp any any range 5060 5061
permit udp any any range 5060 5061
permit icmp any any
permit udp any any range 10000 20000
permit udp any any range 20000 65535
ip access-list extended email
permit tcp any any eq smtp
ip access-list extended ftp-sftp
permit tcp any any eq ftp-data
permit tcp any any eq ftp
!
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
transport input all
!
!
End

```

Anexo 4. Configuraciones del dispositivo de red-Router 1

```

MONITOREO#show run
Building configuration...

Current configuration : 1889 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MONITOREO
!
boot-start-marker
boot-end-marker
!
!
!

```



```
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet3/1
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet4/0
no ip address
shutdown
negotiation auto
!
interface Serial5/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial5/3
no ip address
shutdown
serial restart-delay 0
!
interface POS6/0
no ip address
shutdown
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 192.168.200.0 255.255.255.0 192.168.200.143
ip route 192.168.200.0 255.255.255.0 10.10.10.2
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
```

```
gatekeeper
shutdown
!
!
line con 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  login
  transport input all
!
!
end
```