



**Escuela Superior
de Ingeniería y Tecnología**
Universidad de La Laguna

Trabajo de Fin de Grado

**Diseño de infraestructura de red para
una empresa multisede**

Design of network infrastructure for a multi-site company

Cheuk Kelly Ng Pante

La Laguna, 10 de julio de 2025

D. **Jonás Philipp Lüke**, profesor contratado Doctor de Universidad adscrito al Departamento de Ingeniería Industrial de la Universidad de La Laguna, como tutor.

C E R T I F I C A

Que la presente memoria titulada:

"Diseño de infraestructura de red para una empresa multisede"

ha sido realizada bajo su dirección por D. **Cheuk Kelly Ng Pante**.

Y para que así conste, en cumplimiento de la legislación vigente y a los efectos oportunos firman la presente en La Laguna a 10 de julio de 2025

Agradecimientos

En primer lugar, quiero agradecer profundamente a mi tutor Jonás Philipp Lüke, por aceptar la realización de este proyecto y por su apoyo constante durante todo el proceso.

Su orientación, conocimientos y experiencia han sido fundamentales para el desarrollo de este trabajo.

También quiero agradecer a todas las amistades que he ido haciendo a lo largo de mi carrera, que me han brindado su apoyo y amistad. Su compañía y apoyo han sido una fuente de inspiración y motivación constante.

Por último, quiero agradecer a mi familia, que siempre ha estado ahí para mí, brindándome su amor y apoyo incondicional. Su confianza en mí y su aliento constante me han dado la fuerza necesaria para completar este proyecto y alcanzar mis metas académicas.

Licencia



© Esta obra está bajo una licencia de Creative Commons
Reconocimiento-CompartirIgual 4.0 Internacional.

Resumen

Este proyecto presenta el diseño y simulación de una infraestructura red, orientada a la mejora de la conectividad y la gestión centralizada de una organización con varias sedes. Este estudio propone una arquitectura de red moderna, escalable y segura; diseñada conforme a las necesidades actuales de comunicación y gestión tecnológica en entornos distribuidos.

Para ello, se han empleado herramientas de simulación para validar el funcionamiento del diseño, incluyendo la implementación de protocolos de enrutamiento o servicios de red internos. El resultado ha sido una solución escalable y adaptable, alineada con los requisitos técnicos y operativos de una red corporativa moderna.

Palabras clave: GNS3, Infraestructura, Interconexión, IPv6, Redes corporativas, SD-WAN, VPN, VoIP

Abstract

This project presents the design and simulation of a network infrastructure, aimed at improving connectivity and centralised management of a multi-site organisation. This study proposes a modern, scalable and secure network architecture; designed according to the current needs of communication and technological management in distributed environments.

Simulation tools have been used to validate the performance of the design, including the implementation of routing protocols or internal network services. The result has been a scalable and adaptable solution, aligned with the technical and operational requirements of a modern corporate network.

Keywords: GNS3, Infrastructure, Interconnection, IPv6, Corporate Networks, SD-WAN, VPN, VoIP

Índice general

1. Introducción	1
1.1. Objetivos	2
1.2. Antecedentes	3
1.2.1. SD-WAN (Software-Defined Wide Area Network)	4
1.2.2. MPLS (Multiprotocol Label Switching)	4
1.2.3. VPN (Virtual Private Network)	5
1.2.4. VoIP (Voice over IP)	6
1.2.5. MP-BGP (Multiprotocol Border Gateway Protocol)	6
1.3. Herramientas	7
1.3.1. GNS3	7
1.3.2. Wireshark	7
1.3.3. Docker	7
1.3.4. VirtualBox	7
1.3.5. MicroSIP	7
1.3.6. Telefonos Grandstream GRP2601	8
1.3.7. Router Mikrotik RB2011UiAS-RM	8
1.3.8. Switches TP-Link T2500G-10TS	8
2. Análisis de requisitos y requerimientos	9
2.1. Comunicaciones de datos e internet	9
2.2. Servicio de electrónica de red gestionada	9
2.3. Servicio de seguridad gestionado	10
2.3.1. Especificaciones técnicas del equipamiento	11
2.4. Comunicaciones fijas de voz	11
3. Diseño	13
3.1. Diseño de red	13
3.1.1. Diseño estructural	15
3.1.2. Dispositivos de red	16
3.1.2.1. Dispositivos de interconexión	16
3.1.2.2. Switches	18
3.1.2.3. Firewall	19
3.1.2.4. Telefonía IP	19
3.1.2.5. Resumen de los dispositivos de red	20
3.1.3. Servicios de red necesarios	20
3.2. Esquema de direccionamiento	21
3.3. Seguridad y firewall	21

3.3.1. Plataforma de seguridad	22
3.3.2. Reglas firewall	22
3.4. FreePBX como centralita de telefonía IP	22
3.4.1. Arquitectura de implementación	23
3.4.2. Plan de numeración y configuración de extensiones	23
3.4.3. Sistema IVR y operadora automática	24
3.4.3.1. Nivel 1 - Menú principal	24
3.4.3.2. Nivel 2 - IVR por sede	24
3.4.3.3. Nivel 2 - IVR de incidencias	24
3.4.4. Grupos de salto y grupos de captura	25
3.4.5. Servicios adicionales	25
3.5. Elección de herramientas de monitorización	25
4. Simulación	27
4.1. Simulación de la red de ISP	27
4.1.1. Configuración de interfaces loopback y asignar IPs a interfaces físicas .	29
4.1.2. OSPF como protocolo de enrutamiento	30
4.1.3. Configuración de la distribución de etiquetas (LDP)	31
4.1.4. Multi-Protocolo BGP (MP-BGP)	31
4.1.5. Configuración de VRF y VPN	32
4.1.6. Comunicación entre routers PE y CE	33
4.1.7. Acceso a Internet	34
4.1.8. Comprobación de la configuración	35
4.2. Simulación de la Oficina Central	36
4.2.1. Configuración de los routers	36
4.2.2. Configuración de los switches	38
4.2.3. Configuración del servidor DHCP	39
4.2.4. Configuración de los servidores DNS	40
4.2.5. Configuración de los hosts	41
4.3. Simulación entre sedes remotas y red ISP	42
4.4. Laboratorio	45
5. Conclusiones y líneas futuras	49
6. Summary and Conclusions	51
7. Presupuesto	53
7.1. Costes del proyecto	53
A. Instalación de programas necesarios	55
A.1. Instalación y configuración de GNS3	55
A.2. Instalación de VirtualBox	56
A.2.1. Instalación FreePBX	57
A.2.2. Instalacion Softphone	61
A.3. Instalación de Docker	63
A.3.1. Añadir el repositorio Docker	63
A.3.2. Instalar Docker y Docker Compose	64

B. Configuración de los servicios y dispositivos	65
B.1. Configuración de los routers de la red de ISP	65
B.1.1. Configuración de los routers PE	65
B.1.2. Configuración de los routers P	67
B.1.3. Configuración de los routers CE	69
B.2. Configuración de la Oficina Central	70
B.2.1. Configuración router CE1	70
B.2.2. Configuración del router CE1_backup ARREGLAR	71
B.2.3. Docker Compose para los servicios de red	73
B.2.4. Servidor DHCP	74
B.2.4.1. Dockerfile para el servidor DHCP	75
B.2.4.2. Archivo dhcpcd6.conf	76
B.2.5. Servidor DNS Primario	76
B.2.5.1. Dockerfile para el servidor DNS primario	76
B.2.5.2. Archivo /etc/bind/named.conf.options	77
B.2.5.3. Archivo /etc/bind/named.conf.local	78
B.2.5.4. Archivo /etc/bind/zones/db.cazg.es	78
B.2.5.5. Archivo /etc/bind/zones/db.2001.db8.1234.0102	79
B.2.6. Servidor DNS Secundario	79
B.2.6.1. Dockerfile para el servidor DNS secundario	79
B.2.6.2. Archivo /etc/bind/named.conf.options	80
B.2.6.3. Archivo /etc/bind/named.conf.local	81
B.2.7. Configuración del contenedor Docker para pruebas de red	81
B.2.7.1. Dockerfile para el contenedor de pruebas de red	81
B.2.7.2. Script de entrada para el contenedor de pruebas de red	82
B.2.7.3. Docker Compose para el contenedor de pruebas de red	82
B.3. Configuración de sedes remotas e ISP	82
B.3.1. Configuración del router CE1 (Oficina Central)	82
B.3.2. Servidor DHCP	84
B.3.2.1. Dockerfile para el servidor DHCP	84
B.3.2.2. Archivo dhcpcd.conf	85
B.3.3. Servidores DNS	85
B.3.3.1. Configuración del servidor DNS primario	85
B.3.3.2. Configuración del servidor DNS secundario	88
B.3.4. Configuración del router CE2 (San Cristóbal)	90
B.4. Configuración de los switches	91
B.4.1. Configuración del switch de distribución	91
B.4.2. Configuración del switch de acceso LAN	93
B.4.3. Configuración del switch de acceso DMZ	94
B.5. Docker Compose para la FreePBX	95
c. Otros apéndices	96
C.1. Script para la generación del mapa con las diferentes sedes	96

Índice de Figuras

1.1. Ubicación de las instalaciones	3
1.2. Arquitectura MPLS	5
3.1. Esquema de interconexión de sedes	14
3.2. Diseño vertical de la red	15
3.3. Diseño representativo de la red de la empresa	16
4.1. Red MPLS configurada en GNS3	28
4.2. Tabla de enrutamiento de P1	30
4.3. Traceroute desde PE1 a PE2	31
4.4. Sesiones BGP establecidas en PE1 y PE2	32
4.5. Sesiones BGP establecidas en los routers CE	34
4.6. Comprobación de la configuración	35
4.7. Esquema de la oficina central	36
4.8. Estado de los VRRP en el router CE1	37
4.9. Estado de los VRRP en el router CE1_Backup	37
4.10. Asignación y conectividad IPv6	38
4.11. Obtención de una dirección IPv6	38
4.12. Estado del protocolo Spanning Tree	39
4.13. Simulación de la red completa	42
4.14. Resultado de un traceroute desde un PC San Cristóbal a Internet	43
4.15. Configuración de los switches de la sede de San Cristóbal	44
4.16. Comprobación de la VoIP sobre IPv4	45
4.17. Servicios de red utilizados en el laboratorio	45
4.18. Interconexión de red y dispositivos físicos utilizados en el laboratorio	46
4.19. Extensiones configuradas en la centralita FreePBX	46
4.20. Configuración del buzón de voz para la extensión 1001	47
A.1. Descarga de VirtualBox	56
A.2. Descarga de VirtualBox	57
A.3. Descarga de FreePBX	58
A.4. Configuración de la máquina virtual para FreePBX	58
A.5. Configuración de la red en VirtualBox	59
A.6. Configuración de la máquina virtual para FreePBX	60
A.7. Instalación de FreePBX	60
A.8. Panel de configuración de FreePBX	61
A.9. Configuración de FreePBX	61
A.10. Configuración de la máquina virtual para Softphone	62
A.11. Configuración de la máquina virtual para Softphone	62

A.12. Configuración de la máquina virtual para Softphone 63

Índice de Tablas

1.1. Sedes del Consorcio de Aguas de la Zona Gaditana	3
3.1. Comparativa de proveedores de servicios de telecomunicaciones	14
3.2. Justificación técnica de los dispositivos Cisco Meraki MX por sede	17
3.3. Número de puertos de acceso a la red	18
3.4. Comparativa de switches por fabricante y sedes según necesidades.	18
3.5. Comparativa de Teléfonos IP	19
3.6. Resumen de dispositivos de red seleccionados	20
3.7. Resumen de servicios de red necesarios	20
3.8. Esquema de direccionamiento IPv6 para todas las sedes	21
3.9. Reglas del firewall	22
3.10. Plan de numeración por sede	23
3.11. Comparativa de herramientas de monitorización de red	26
4.1. Esquema de direccionamiento para la red ISP	29
4.2. Rango de etiquetas para cada router	31
4.3. Esquema de direccionamiento para la red MPLS	43
7.1. Costes de personal	53
7.2. Presupuesto.	53

Capítulo 1

Introducción

En la actualidad, la conectividad y la seguridad de las redes corporativas son pilares fundamentales para garantizar su correcto funcionamiento, es por ello, que la mayoría de las empresas están en un proceso de transformación digital. Por supuesto, aquellas organizaciones con varias sedes requieren de una infraestructura de red eficiente, robusta, escalable y que cuente con una comunicación segura entre ellas.

A medida que la tecnología sigue avanzando y los servicios en línea se vuelven parte esencial del día a día (como ocurre con la telefonía basada en IP, las plataformas en la nube o el acceso remoto a sistemas), se hace cada vez más necesario contar con redes que integren herramientas actuales, por lo que la elección de las tecnologías core adquieren un papel crucial. El objetivo es facilitar la interacción entre ubicaciones en diferentes áreas geográficas, lo cual permite que los datos se transmitan de manera eficiente entre redes y dispositivos. También es importante garantizar un tránsito de información ágil y confiable en toda la estructura de red.

La elección de la tecnología de interconexión adecuada depende de varios factores, como el tamaño de la red, el tipo de tráfico que se espera, la latencia o el ancho de banda requerido. Cada una de estas presenta sus propias ventajas y desventajas, y la selección de la más apropiada debe basarse en las necesidades específicas de la organización. Existen diversas tecnologías [1], como por ejemplo:

- **ATM (Asynchronous Transfer Mode):** es la conjunción de las redes de conmutación de circuitos y de conmutación de paquetes, también conocida como “cell relay”. Está basada principalmente en el concepto de conmutación de paquetes, pero con un tamaño fijo, y es capaz de prestar servicios que requieren una velocidad constante o prestaciones de la conmutación de circuitos, todo ello utilizando señalización por canal común.
- **Frame Relay:** es un protocolo WAN de alto rendimiento que funciona en las capas físicas y de enlace de datos del modelo de referencia OSI. Frame Relay reduce los costos de redes a través del uso de menos equipos, menos complejidad y una implementación más fácil. Proporciona un mayor ancho de banda, mejor fiabilidad y resistencia a fallas que las líneas privadas o arrendadas.
- **X.25:** es un estándar de protocolo de la Unión Internacional de Telecomunicaciones, Sector de Estandarización de Telecomunicaciones (ITU-T) para la comunicación WAN que define cómo los dispositivos de usuario y los dispositivos de red establecen y mantienen conexiones.

- **MPLS (Multiprotocol Label Switching):** es una técnica de alto rendimiento para transportar datos en redes de telecomunicaciones, donde ha ido reemplazando a Frame Relay y ATM. MPLS se encarga de dirigir los datos de un nodo de red al siguiente utilizando etiquetas de ruta en lugar de direcciones de red. De esta forma conseguimos agilizar la red, pues los nodos no tienen que desencapsular direcciones de red muy largas y cotejarlas en una tabla de enrutamiento [2].
- **SD-WAN (Software-Defined Wide Area Network):** es una red de área extensa (WAN) que utiliza tecnología de redes definidas por software, como la comunicación a través de Internet mediante túneles superpuestos que se cifran cuando se destinan a ubicaciones internas de la organización [3].
- **VPN (Virtual Private Network):** es una tecnología de red que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que dispositivos en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada [4].

Por lo tanto, el diseño de red es importante a la hora de crear una infraestructura de comunicaciones eficiente, ya que esta se encarga de definir la estructura física y lógica, como elegir los componentes que se van a utilizar, las tecnologías de interconexión, etc. La creación de una red bien diseñada no solo garantiza conectividad, sino que también optimiza el rendimiento, la escalabilidad y la seguridad mediante el diseño de una red jerárquica.

1.1. Objetivos

El objetivo fundamental de este Trabajo de Fin de Grado es implantar un sistema de comunicaciones unificado que facilite la gestión e integración de servicios, mejorando así la eficiencia y seguridad de las comunicaciones entre las distintas sedes de una empresa. Para ello, se ha tomado como referencia el pliego técnico del expediente [5] del Consorcio de Aguas de la Zona Gaditana, el cual plantea una propuesta integral de modernización, equipamiento y mejora de la conectividad del consorcio. No obstante, este trabajo no aborda la totalidad del contenido del pliego, sino que se centra únicamente en el diseño y simulación de determinados aspectos clave de la infraestructura de red. Para alcanzar estos fines, se plantean también una serie de objetivos específicos, entre los cuales se encuentran los siguientes:

- Diseñar una red de interconexión entre las sedes del consorcio utilizando tecnologías de interconexión modernas y eficientes.
- Utilizar herramientas de simulación como GNS3 para validar el diseño y la configuración de la red.
- Elección de dispositivos de red adecuados para la infraestructura, incluyendo routers, switches y firewalls.
- Crear un esquema de direccionamiento IPv6 para garantizar la escalabilidad y la compatibilidad con las tecnologías actuales.

1.2. Antecedentes

El Consorcio de Aguas de la Zona Gaditana (CAZG) es una entidad pública, con sede principal en Jerez de la Frontera, que se encarga de gestionar el ciclo integral del agua en la provincia de Cádiz. Su función principal es asegurar el abastecimiento de agua potable y el saneamiento de aguas residuales para la población de la zona. Actualmente, el consorcio cuenta con una infraestructura de telefonía fija bastante obsoleta y con líneas duplicadas en terminales móviles de sobremesa y móviles usuales. Además, algunas sedes de menor tamaño carecen de una infraestructura de comunicaciones modernas así como de un acceso a Internet adecuado ya que se conectan a la red mediante ADSL/FTTH o redes WiMAX. Por último, no dispone de una plataforma de Firewall de Nueva Generación (NGFW), por lo que actualmente no satisface los requerimientos y necesidades de seguridad de la organización.

La empresa dispone de varias sedes distribuidas geográficamente, tal como se recoge en la Tabla 1.1, que incluye la Oficina Central, diferentes estaciones de tratamiento de agua potable (ETAP) y depósitos, junto con sus respectivas ubicaciones. Además, en la Figura 1.1 se muestra la localización de estas instalaciones sobre un mapa.

Sede	Dirección/Zona
Oficina central	Calle Ancha, Jerez de la Frontera
San Cristóbal	Ctra. A2003 - Cuartillos
ETAP de Cuartillos	Ctra. Puerto Real - Paterna
ETAP de Montañés	Ctra. de acceso a Algar
ETAP de Paterna	Paterna de Rivera
ETAP de Algar	Antigua ctra. Jerez - El Puerto
Depósito de Cádiz	Zona Franca - Cádiz

Tabla 1.1: Sedes del Consorcio de Aguas de la Zona Gaditana

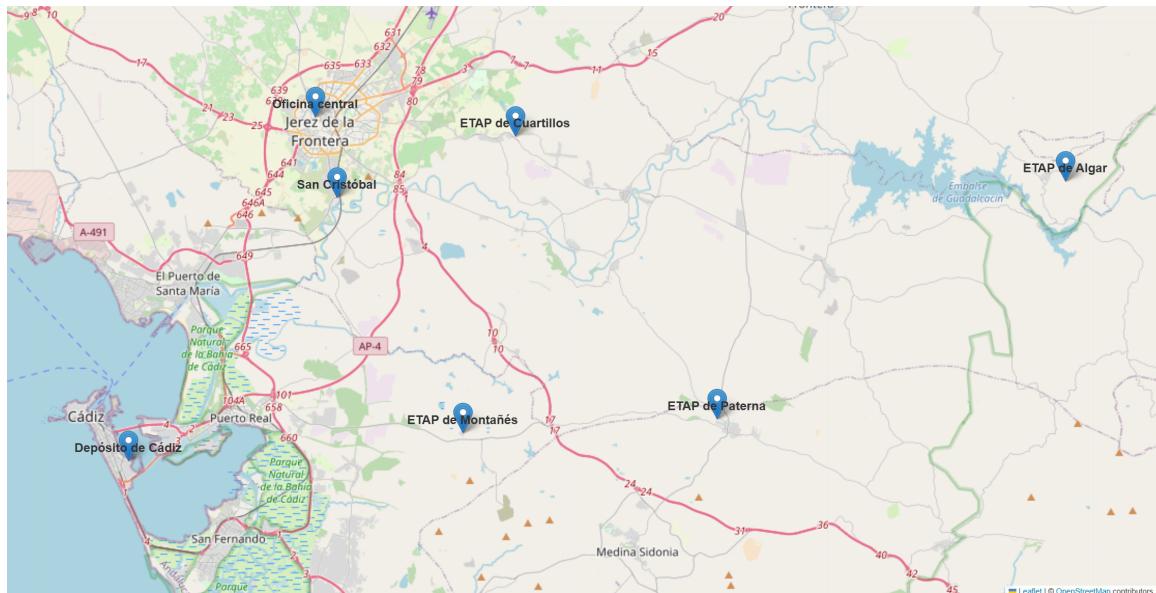


Figura 1.1: Ubicación de las instalaciones

1.2.1. SD-WAN (Software-Defined Wide Area Network)

SD-WAN [6] es una red de área extensa (WAN) que utiliza tecnología de redes definidas por software, ofreciendo servicios de red confiables y escalables. Esta tecnología permite simplificar el control y la administración de la infraestructura de red al proporcionar una arquitectura WAN virtual que conecta de manera segura a los usuarios con las aplicaciones y servicios que necesitan. Asimismo, SD-WAN utiliza una combinación de tecnologías, como por ejemplo, MPLS, Internet de banda ancha y LTE, para ofrecer una conectividad flexible y de alto rendimiento.

El funcionamiento de SD-WAN se basa en crear una superposición para virtualizar la red de área extensa, lo que permite un control centralizado, la simplificación de la administración y la implementación de los servicios de red.

En cuanto a la arquitectura de este tecnología [7], esta se compone de varios componentes clave, como:

- **Dispositivos en el extremo:** son los dispositivos físicos o virtuales instalados en ubicaciones remotas, centro de datos y ubicaciones en la nube. Las cuales, tienen un rol importante como distribuir el tráfico según las políticas definidas y de medir en tiempo real el estado de la red.
- **Organizador de SD-WAN:** sirve para controlar las decisiones de política, como la gestión del tráfico y las rutas a utilizar.
- **Capa de transporte:** SD-WAN funciona con cualquier tecnología de transporte basado en IP, como MPLS, LTE, o 5G. Esta capa forma la red subyacente mientras que SD-WAN crea una red superpuesta inteligente con selección dinámica de rutas y comutación de fallos.

1.2.2. MPLS (Multiprotocol Label Switching)

MPLS (Multiprotocol Label Switching) [8] es un mecanismo de transporte de datos que opera entre la capa de enlace de datos y la capa de red del modelo OSI. Este fue diseñado para unificar el servicio de circulación de datos para las redes basadas en circuitos y en paquetes. Asimismo, puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo el de voz y el de paquetes IP.

En una red MPLS existen diferentes elementos [2] que desempeñan distintas funciones en la red. En la Figura 1.2 se puede observar una arquitectura de red MPLS típica.

1. Routers según ubicación y función en la red:

- **Router del cliente (CE - Customer Edge):** es el router que se encuentra en el extremo del cliente. Puede ser cualquier router que se use para comunicarse con el proveedor de servicios.
- **Router de proveedor (PE - Provider Edge) o LER (Label Edge Router):** es el router frontera entre la red del cliente y la red MPLS del proveedor de servicios. Estos routers son los puntos de entrada y salida de la red MPLS.
- **Router troncal (P - Provider) o LSR (Label Switching Router):** es el router que se encarga de comutar las etiquetas en el core de la red MPLS. Estos routers son responsables de dirigir el tráfico a través de la red utilizando las etiquetas

asignadas. Además, intercambian estas etiquetas para dirigir el tráfico rápidamente a través de la red sin necesidad de analizar la dirección de destino de cada paquete. Su unión es puramente interno para el enrutamiento basado en etiquetas, por lo que no interactúan con los clientes.

2. Otros elementos:

- **LSP (Label Switched Path):** es el nombre genérico de un camino MPLS, es decir, es un túnel MPLS unidireccional establecido entre los extremos formado por un conjunto de LSRs.
- **LDP (Label Distribution Protocol):** es un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- **FEC (Forwarding Equivalence Class):** es un grupo de paquetes tratados del mismo modo por el comutador. Es decir, un conjunto de paquetes que se encaminan a través de la misma ruta en la red MPLS.

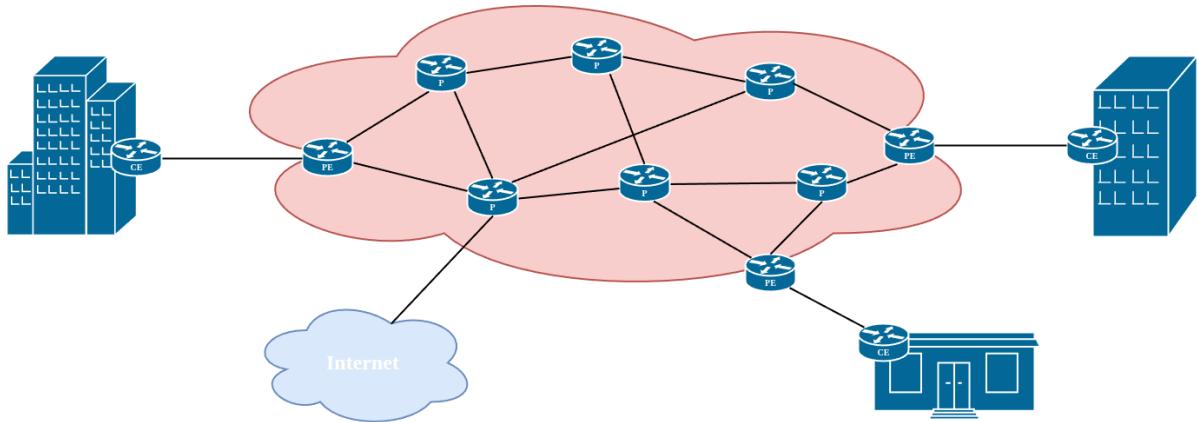


Figura 1.2: Arquitectura MPLS

1.2.3. VPN (Virtual Private Network)

Una VPN (Virtual Private Network) [4] es una tecnología que garantiza una extensión segura de la red de área local (LAN) sobre Internet. Lo que permite establecer un enlace punto a punto con el uso de conexiones dedicadas, cifradas o la combinación de ambas. Existen diferentes arquitecturas VPN, cada una con sus propias características y casos de uso. A continuación, se describen las más comunes:

- **VPN de acceso remoto:** permite a los usuarios conectarse a la red de la empresa desde ubicaciones remotas utilizando una conexión segura a través de Internet. Una vez conectados, tienen un nivel de acceso parecido al que tendrían en la red local de la empresa.
- **VPN punto a punto:** este esquema permite conectar dos redes remotas a través de Internet de forma segura, como si estuvieran en la misma red local.
- **VPN de sitio a sitio:** permite conectar múltiples redes remotas entre sí a través de Internet, creando una red privada virtual que conecta todas las sedes de la empresa.
- **VPN de extranet:** permite a socios comerciales o proveedores acceder de forma segura a recursos específicos de la red de la empresa.

1.2.4. VoIP (Voice over IP)

La tecnología VoIP [9] (Voice over IP) se refiere a la capacidad de realizar llamadas de voz a través de Internet en lugar de utilizar las líneas telefónicas tradicionales. Esencialmente, VoIP convierte las señales de voz en paquetes de datos que se transmiten a través de la red de Internet hasta llegar al destinatario, donde se convierten de nuevo en señales de voz.

VoIP ofrece varias ventajas sobre la telefonía tradicional, como costes más bajos en comparación con las tarifas de las líneas telefónicas convencionales, especialmente en llamadas de larga distancia e internacionales, e incluso suelen ser gratuitas o a un coste muy bajo. También, ofrece una mayor flexibilidad y escalabilidad, ya que permite añadir fácilmente líneas adicionales y funcionalidades avanzadas sin necesidad de instalar hardware adicional. Asimismo, permite la movilidad de los usuarios, ya que las llamadas pueden realizarse desde cualquier dispositivo con conexión a Internet.

1.2.5. MP-BGP (Multiprotocol Border Gateway Protocol)

MP-BGP (Multiprotocol Border Gateway Protocol) [10] es una extensión del protocolo BGP (Border Gateway Protocol) que permite distribuir en paralelo diferentes tipos de direcciones IP, como IPv4 e IPv6, además de, otros protocolos de red. Asimismo, utiliza una arquitectura básica con sistemas autónomos (AS) que se comunican a través de sesiones BGP e intercambian información de accesibilidad de red en forma de actualizaciones BGP [11]. Estas se pueden clasificar en dos formas según el sistema autónomo (AS) al que pertenecen los routers que intercambian información de enrutamiento:

- **iBGP (Internal BGP):** es la comunicación de routers del mismo sistema autónomo (AS) que intercambian información de enrutamiento.
- **eBGP (External BGP):** es la comunicación de routers de diferentes sistemas autónomos (AS) que intercambian información de enrutamiento.

Por otro lado, existen cuatro tipos de mensajes BGP [12] que se utilizan para establecer y mantener las sesiones BGP:

- **OPEN:** se utiliza para establecer una sesión BGP una vez haya sido establecido la conexión TCP.
- **UPDATE:** es un mensaje de actualización que contiene los anuncios de nuevos prefijos.
- **KEEPALIVE:** una vez la sesión BGP está activa, envía periódicamente un mensaje para mantener activa la conexión.
- **NOTIFICATION:** envía al cerrar una sesión BGP. Esto sucede cuando ocurre algún error.

1.3. Herramientas

Las herramientas que se han utilizado para la realización de este proyecto son las siguientes:

1.3.1. GNS3

GNS3 (Graphic Network Simulator-3) [13], un simulador gráfico de red libre y de código abierto que permite crear topologías de red complejas y poner en funcionamiento simulaciones sobre ellas, permitiendo así la combinación de dispositivos reales como virtuales.

Entre las principales características de GNS3 [14], podemos destacar, que es un software gratuito y de código abierto, siendo disponible para Windows, Linux y macOS. De igual forma, no tiene límite en la cantidad de dispositivos que se pueden simular, a excepción de la limitación hardware: CPU y memoria. Además, permite la captura de paquetes de red con Wireshark, la conexión de redes simuladas con redes reales y está constantemente actualizado ya que cuenta con una comunidad de usuarios grande y activa (+800.000 usuarios).

Pero la ventaja principal es que los equipos de red simulados disponen de todas las funcionalidades de un equipo real, ya que ejecuta el mismo firmware que el equipo real. Permitiendo diseñar una topología de red simulada lo más parecida posible a una red real sin necesidad de tener los equipos físicos.

1.3.2. Wireshark

Wireshark [15] es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para análisis de datos y protocolos, y como una herramienta didáctica.

1.3.3. Docker

Docker es [16] una aplicación que simplifica el proceso de administración de procesos de software en contenedores. Estos permiten ejecutar aplicaciones en procesos con aislamiento de recursos. Son similares a las máquinas virtuales, pero son más portátiles, más flexibles con los recursos y más dependientes del sistema operativo host.

1.3.4. VirtualBox

Oracle VirtualBox [17] es una herramienta de virtualización multiplataforma que permite ejecutar múltiples sistemas operativos simultáneamente en un mismo equipo físico, mediante la creación de máquinas virtuales (VM). Esta aplicación amplía las capacidades del sistema anfitrión, haciendo posible, por ejemplo, ejecutar distribuciones de Linux en un sistema Windows, o viceversa, así como combinar diferentes entornos como Windows y macOS o servidores Linux.

1.3.5. MicroSIP

MicroSIP [18] es un softphone de código abierto y portable, diseñado para sistemas operativos Windows y basado en la pila PJSIP. Esta herramienta permite realizar llamadas VoIP de alta calidad, tanto entre usuarios como hacia teléfonos convencionales, mediante el protocolo SIP (Session Initiation Protocol).

1.3.6. Telefonos Grandstream GRP2601

El teléfono Grandstream GRP2601 [19] es un modelo esencial de 2 líneas diseñado con aprovisionamiento zero-touch para implementación masiva y fácil gestión. Se caracteriza por tener un diseño elegante y un conjunto de funciones de última generación incluyendo conferencia de voz de 5 participantes para maximizar la productividad, soporte EHS para auriculares Plantronics, Jabra y Sennheiser y soporte en múltiples idiomas.

1.3.7. Router Mikrotik RB2011UiAS-RM

El router RB2011UiAS-RM [20] de Mikrotik funciona con RouterOS, un sistema operativo de enrutamiento avanzado que ofrece funcionalidades como enrutamiento dinámico, hotspot, cortafuegos, MPLS, VPN, calidad de servicio, equilibrio de carga, supervisión en tiempo real y más. Este modelo destaca por sus cinco puertos LAN Gigabit, cinco puertos LAN Fast Ethernet, puerto serie RJ45, puerto USB, 128MB de RAM, licencia RouterOS L5 y pantalla LCD táctil para facilitar la configuración y gestión.

1.3.8. Switches TP-Link T2500G-10TS

El T2500G-10TS [21] es un switch gestionable con puertos Gigabit en todas sus interfaces, ideal para redes de alto rendimiento. Ofrece seguridad avanzada (IP-MAC-puerto, ACL, 802.1X, Radius, DoS, DHCP Snooping), QoS en L2/L3/L4 e ICMP Snooping para optimizar voz y video, y múltiples opciones de gestión (Web, CLI, Telnet, SSH, SNMP). Además, soporta funciones L2 como VLAN 802.1Q, QinQ, port mirroring y STP/RSTP/MSTP para una red estable y segura.

Capítulo 2

Análisis de requisitos y requerimientos

Como se indicó anteriormente no es objetivo implementar en la totalidad de las condiciones del pliego [5]. Aquí se detallan los aspectos más importantes que se van a considerar.

2.1. Comunicaciones de datos e internet

El proyecto contempla la provisión de servicios de transmisión de datos entre las distintas sedes del Consorcio y el acceso a Internet, estableciendo una red IP privada y asegurando su alineación con los principios de calidad, flexibilidad, fiabilidad, capacidad y tecnología avanzada. Los servicios de comunicación entre las sedes serán:

- **Implementación de red IP privada:** se creará una red de datos utilizando circuitos dedicados para interconectar todas las sedes de manera segura, extendiendo y unificando las redes LAN existentes.
- **Acceso a Internet:** todas las sedes accederán a Internet a través del circuito ubicado en la Oficina Central. La totalidad de las sedes se conectarán a la red mediante la Intranet, utilizando un acceso único corporativo que estará soportado por fibra óptica, garantizando así una conexión eficiente y centralizada.
- **Escalabilidad y priorización de tráfico:** la red se diseñará para permitir un crecimiento futuro, garantizando el soporte para nuevos servicios y priorizando el tráfico, asegurando la calidad de la telefonía IP.
- **Tecnología de conexión:** se preferirá utilizar enlaces terrestres de fibra óptica, evitando tecnologías satelitales, con una obligación de mantener un alto nivel de disponibilidad en la configuración de la red.
- **Monitoreo y gestión:** elección de sistemas de monitorización en tiempo real que permitan la consulta del uso del caudal y alertas rápidas en caso de fallos.
- **Capacidades técnicas:** las conexiones deberán soportar una serie de requisitos de calidad del servicio (QoS), garantizando la baja latencia, alta capacidad de gestión de tráfico y compatibilidad con los estándares de direccionamiento de ITU-T.

2.2. Servicio de electrónica de red gestionada

La infraestructura de red electrónica gestionada del Consorcio se diseñará para proporcionar una base sólida, flexible y escalable que permita el crecimiento y la adaptación a las necesidades cambiantes de la organización. Cada sede tendrá una red de área local (LAN) que garantice la conectividad eficiente de todos los dispositivos, asegurando la integración con la red IP privada y el resto de servicios corporativos.

Para ello, se instalarán switches gestionables que proporcionen la densidad de puertos Ethernet necesaria para conectar todos los equipos requeridos en cada sede, evitando el uso de hubs y asegurando una infraestructura moderna y eficiente. Estos switches soportarán velocidades mínimas de 100 Mbps por puerto y contarán con capacidades Power over Ethernet (PoE), lo que permitirá alimentar terminales VoIP y otros dispositivos de red directamente a través del cableado de datos, simplificando la instalación y el mantenimiento.

La solución de electrónica de red incluirá funcionalidades avanzadas como la configuración de VLANs para segmentar el tráfico, así como herramientas de Calidad de Servicio (QoS) que permitan clasificar y priorizar el tráfico, garantizando la calidad en servicios críticos como la telefonía IP. Además, se implementará la norma IEEE 802.3az para mejorar la eficiencia energética de la infraestructura.

En cuanto a la conectividad entre sedes, se proveerán routers de alto rendimiento que permitan la integración con tecnologías SD-WAN, facilitando la gestión centralizada y flexible de la red, así como el acceso seguro a través de conexiones VPN. Todo el equipamiento será seleccionado para asegurar la alta disponibilidad, la seguridad y la capacidad de adaptación a futuras ampliaciones o cambios en la red del consorcio.

2.3. Servicio de seguridad gestionado

El servicio de seguridad gestionado se diseñará para proteger la infraestructura de red del consorcio, garantizando la confidencialidad, integridad y disponibilidad de los datos y servicios. Este servicio incluirá la elección de un cortafuegos de nueva generación (NGFW) que proporcionará una defensa robusta contra amenazas externas e internas, así como la gestión centralizada de la seguridad a través de un sistema de monitorización y gestión.

El consorcio dispondrá de un sistema de consulta estadística online para monitorizar y gestionar el uso del caudal mediante una aplicación web segura con autenticación de usuario. Además, dispondrá de un sistema de alertas en caso de que se produzca un fallo en los enlaces o en las líneas de acceso principales o de respaldo. También, el sistema de seguridad gestionado deberá incluir las siguientes características:

- **Recepción de información:** el sistema permitirá la recepción de datos a través de SYSLOG para facilitar la monitorización continua y la identificación temprana de vulnerabilidades.
- **Actualizaciones y modificaciones:** se realizarán recomendaciones y actualizaciones remotas del software en caso de detectar vulnerabilidades, así como modificaciones en políticas de seguridad como respuesta a incidentes.
- **Centro de gestión:** habrá un centro de gestión en las instalaciones del licitador, que operará de manera coordinada y homogénea con el Consorcio.

Por otro lado, se elegirá una plataforma de seguridad avanzada para la gestión de amenazas que limite el tráfico entre Internet y la red interna del Consorcio, proporcionando funcionalidades como filtrado antivirus, detección de aplicaciones, control de navegación y respuesta ante incidentes. Además, se combinará con un sistema de respuesta ante incidentes que automatice procedimientos predefinidos y gestione accesos mediante VPN, garantizando una solución rápida y efectiva ante eventos de seguridad.

2.3.1. Especificaciones técnicas del equipamiento

El cortafuegos debe cumplir con las siguientes especificaciones:

- **Certificaciones:** ICSA, NSS Labs y Common Criteria.
- **Rendimiento:** hasta 20/20/9 Gbps de firewall, 2 millones de sesiones concurrentes, 135.000 nuevas sesiones por segundo, y 1.2 Gbps de Threat Protection.
- **Funcionalidades:** IPS (hasta 6 Gbps), proxy explícito, visualización de tráfico, escaneo de vulnerabilidades, antivirus, antispam y filtrado de contenidos.
- **Licenciamiento:** por equipo, no por usuario.
- **Interfaces:** 14 puertos 1GE RJ45 internos, 2 puertos WAN, 2 slots SFP, 2 puertos Management/DMZ, 2 para HA, 1 consola y 1 USB.
- **Virtualización:** soporte de 10 dominios virtuales con monitorización de recursos.
- **Control de aplicaciones:** identificación de 2900+ aplicaciones, clasificación granular y detección bajo túneles HTTPS.
- **Visibilidad:** consolidación de logs, visualización en tiempo real y gestión de sesiones.
- **Filtrado de contenidos:** control granular de URLs, cuotas de tiempo, listas blancas/-negras, filtrado DNS y sinkhole.
- **Seguridad:** políticas por interfaz, prevención de amenazas, DLP, actualizaciones automáticas, doble factor de autenticación, bloqueo de botnets, inspección SSL y motor WAF.
- **VPN:** hasta 9 Gbps IPsec, 300 usuarios VPN SSL simultáneos, soporte para múltiples protocolos VPN.

2.4. Comunicaciones fijas de voz

En este apartado se detallan alguno de los requisitos que debe cumplir el servicio de comunicaciones fijas de voz, aunque no se contempla su implementación en el alcance de este proyecto. Estos requisitos servirán como referencia para futuras fase.

Las especificaciones requeridas incluyen:

- **Integración y escalabilidad:** se contempla al menos 38 extensiones, renovando los terminales actuales por modelos de VoIP.
- **Requisitos técnicos:** la centralita estará alojada preferentemente en la nube, con los terminales IP instalados localmente en cada sede. Se utilizarán conexiones IP estándar para la gestión de llamadas, permitiendo una numeración integrada y acceso a diferentes tipos de terminales, incluidos modelos de sobremesa.
- **Funcionalidades avanzadas:** se requerirán características como buzones de voz, grabación de llamadas y operadora automática personalizada. Se definirán grupos de salto y captura para optimizar el manejo de las llamadas.
- **Cableado y accesibilidad:** se deberá contemplar el cableado de datos de categoría CAT6, asegurando la conectividad necesaria para la telefonía IP y los servicios de datos, así como la posibilidad de adaptación a futuras necesidades en infraestructura.
- **Gestión y mantenimiento:** se exigirá la operación y mantenimiento integral de la red durante el contrato, garantizando la gestión continua y la evolución de los servicios conforme avance la tecnología.

Asimismo, los teléfonos IP que se utilicen deberán cumplir, como mínimo, los siguientes requisitos:

- Dos puertos Ethernet de 100Mbps o de 1Gbps: uno para la alimentación y conexión a la red del terminal y otro para la conexión del PC al terminal, permitiendo la alimentación tanto por red eléctrica como a través del puerto Ethernet (PoE, Power over Ethernet).
- Disponer de manos libres full dúplex con altavoz y micrófono ambiente. Los terminales deberán ser completamente nuevos.
- Permitir la asignación de dirección IP mediante DHCP.

Capítulo 3

Diseño

En este capítulo se describirá el diseño de la red de la empresa, incluyendo la topología, la infraestructura de red, los dispositivos de red que se van a utilizar y las tecnologías implementadas.

3.1. Diseño de red

Para interconectar las sedes de la empresa se ha optado por una topología en estrella porque se centraliza la gestión en un nodo central (oficina central). Además, el pliego de proyectos ¹ especifica que “accederán a internet através del circuito ubicado al efecto en la Sede Principal”, por lo que el acceso a Internet será únicamente en este punto, simplificando así la administración y el mantenimiento de la red. Además, permite que sea escalable, ya que se pueden agregar más edificios sin tener que reconfigurar toda la red. Esta estructura facilita redundancia en el núcleo y reduce costos al evitar conexiones complejas. En la Figura 3.1 se puede observar una representación gráfica de la topología en estrella de las instalaciones de la empresa.

Como tecnología principal de interconexión entre las sedes se ha optado por SD-WAN (Software Defined Wide Area Network) ya que permite una gestión centralizada, mayor flexibilidad, seguridad avanzada y facilita la integración de múltiples sedes e integración en tiempo real sin interrupciones. Esta tecnología es ideal para empresas que necesitan conectar varias ubicaciones de manera eficiente, segura y con capacidad de adaptación a diferentes proveedores y tipos de acceso. Además, permite priorizar el tráfico crítico, aplicar políticas de seguridad de forma centralizada y simplificar la administración de la red.

Para la interconexión de las sedes se han estudiado varios proveedores de servicios de telecomunicaciones, como Vodafone, Orange y Telefónica. Para este proyecto se ha optado por Vodafone como principal operador por su mejor oferta de servicios, precios y por ajustarse a las necesidades de la red. Vodafone ofrece un servicio de SD-WAN de Cisco Meraki que permite la creación de redes privadas virtuales (VPN), proporciona una mayor seguridad y control sobre el tráfico de datos, y facilita la gestión centralizada de la red. En la Tabla 3.1 se puede observar los proveedores de servicios de telecomunicaciones estudiados y las características principales de cada uno.

¹Pliego de prescripciones técnicas para la contratación de servicios de telecomunicaciones de voz, fijas y móviles, red de acceso de datos, intranet e internet para el Consorcio de Aguas de la Zona Gaditana

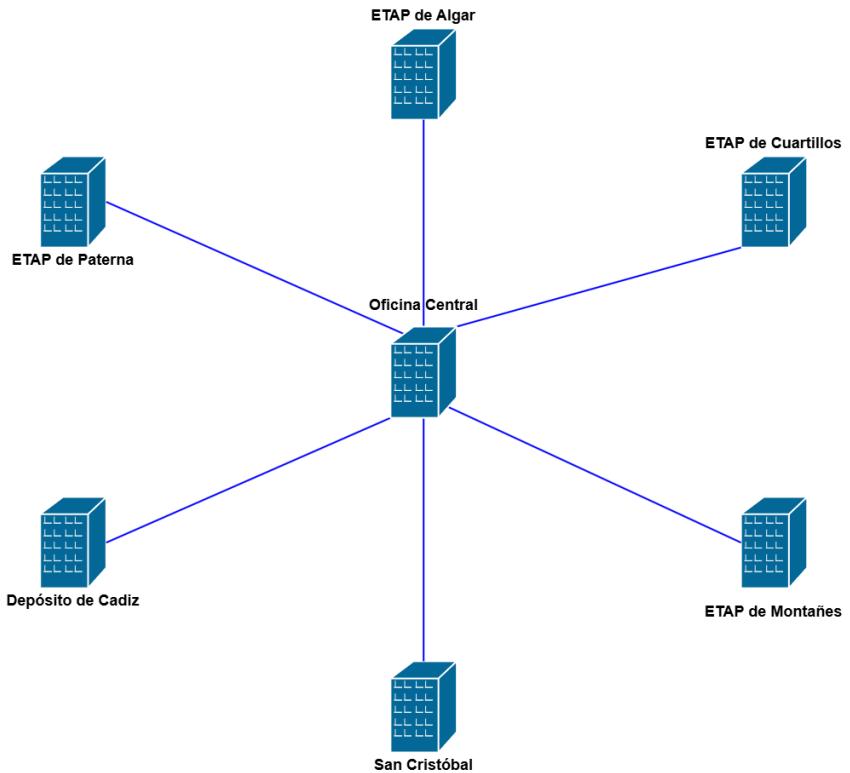


Figura 3.1: Esquema de interconexión de sedes

Proveedor	Tecnología principal	Seguridad y gestión	Ventajas destacadas	Precio/mes/sede (IVA no incluido)
Orange	VPN, FTTH	Soluciones de seguridad integrales en la nube.	Red privada y unificada, acceso sencillo a recursos compartidos.	50 €
Telefónica	SD-WAN (Cisco Meraki), MPLS	Firewall avanzado y control de accesos, detección de amenazas.	Integración con Cisco Meraki y gestión centralizada sin inversión inicial.	75 €
Vodafone	SD-WAN (Cisco Meraki), VPN	Firewall de última generación y gestión centralizada.	Visualización avanzada del tráfico y conectividad mejorada entre sedes.	64 €

Tabla 3.1: Comparativa de proveedores de servicios de telecomunicaciones

Por otro lado, se pide para algunas sedes (no se especifica cuáles), un caudal de respaldo obligatorio que tiene que ir montado sobre distinta infraestructura o aplicando tecnologías diferentes o distinto operador. Para ello, se va a optar por Telefónica utilizando también su servicio SD-WAN de Cisco Meraki. Además, se pide que se tenga un dispositivo independiente y distinto al principal para el enlace de respaldo, para esto, contará con un dispositivo diferente configurado en modo *Warm Spare (HA)* [22], lo que garantiza la continuidad del servicio mediante un segundo equipo en espera, preparado para asumir el control en caso de que el principal falle. También, la funcionalidad de SD-WAN inteligente de Meraki permitirá balancear el tráfico entre el enlace principal y el enlace de respaldo (en este caso, la solución flexWAN de Telefónica), seleccionando dinámicamente el mejor camino según la calidad del enlace y las políticas definidas, asegurando así la redundancia de red y alta disponibilidad

3.1.1. Diseño estructural

La arquitectura de red se ha diseñado siguiendo un modelo jerárquico de tres capas: núcleo, distribución y acceso. Esta jerarquía permite una mejor gestión del tráfico, escalabilidad y redundancia en la red.

- **Capa de núcleo:** se encarga de la interconexión entre las diferentes sedes y la oficina central. Se utilizan dispositivos de alto rendimiento para garantizar una alta disponibilidad y baja latencia en la comunicación entre sedes.
- **Capa de distribución:** se encuentran los dispositivos que conectan los diferentes segmentos de la red, como switches y routers. Se encargan de la gestión del tráfico y la seguridad de la red.
- **Capa de acceso:** se conectan los hosts finales, como ordenadores, impresoras y teléfonos IP. Se utilizan switches de acceso para conectarlos a la red.

En la Figura 3.2 se puede observar el cableado vertical de alguna de las sedes de la empresa. Esta se encarga de conectar las diferentes plantas de un edificio, permitiendo la interconexión entre los armarios de comunicaciones de cada piso y asegurando la continuidad de la red a lo largo de toda la estructura vertical del edificio. ETAP Cuartillos y ETAP Montañés tienen una organización similar entre ellas y, por otro lado, ETAP Paterna, ETAP Algar y el Depósito de Cádiz comparten una configuración parecida entre sí. La oficina central presenta una estructura diferente al resto, ya que alberga los diferentes servidores de la empresa y la DMZ (zona desmilitarizada) donde se alojan los servidores de la empresa.

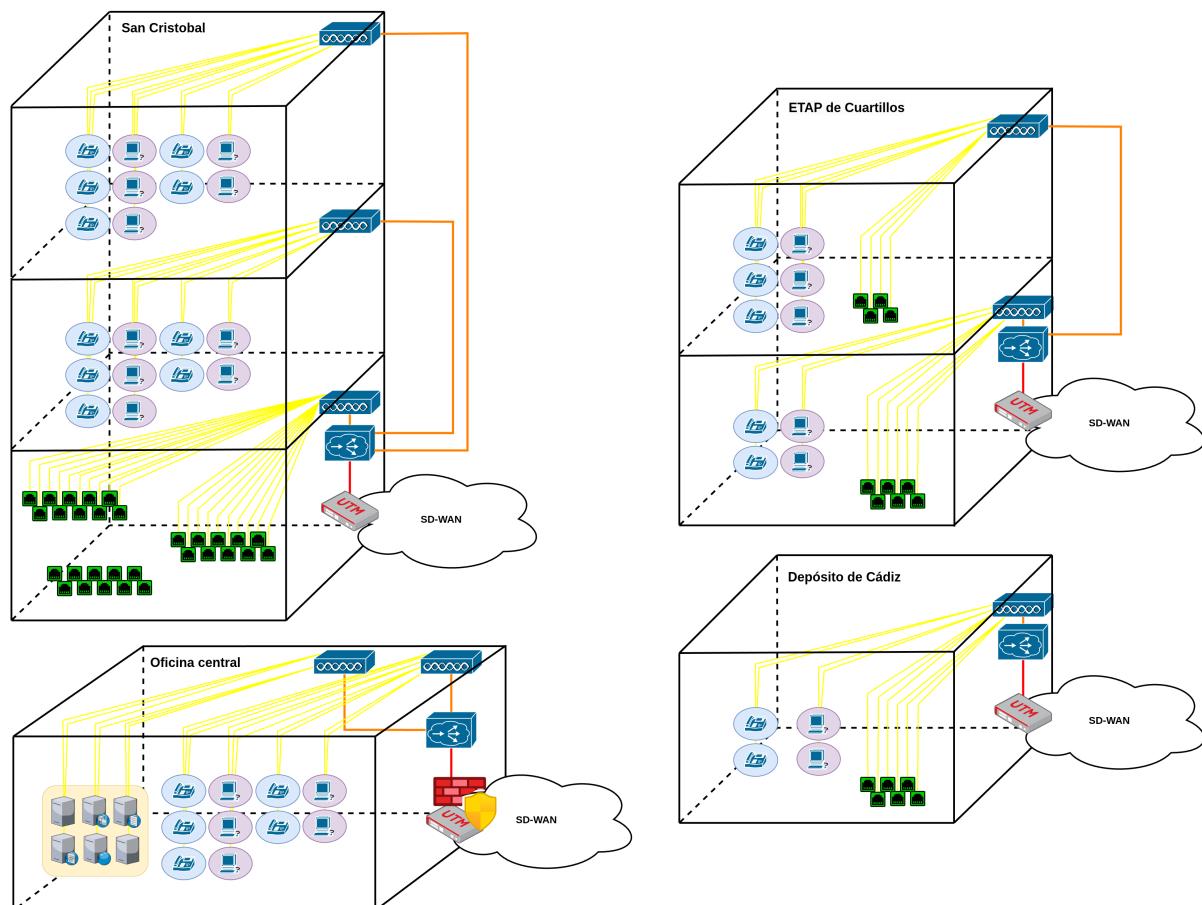


Figura 3.2: Diseño vertical de la red

En el esquema de red de la Figura 3.2, las líneas rojas indican el núcleo de la infraestructura, donde se ubican los dispositivos core y de distribución que manejan el tráfico principal entre sedes. Las líneas naranjas corresponden a la zona de distribución, conectando los equipos de distribución con los de acceso. Por su parte, las líneas amarillas representan la capa de acceso, donde se integran los dispositivos finales. Los círculos en tonos celeste pastel y lila identifican las VLAN de datos y voz, respectivamente, mientras que en la oficina central, el área marcada con un recuadro amarillo indica la DMZ, donde se alojan los servidores corporativos. Para el cableado, se empleará fibra óptica monomodo en los enlaces principales entre los equipos de core y distribución, así como en los tramos verticales entre plantas, garantizando así alta velocidad y baja latencia. En la capa de acceso y para la conexión de los equipos finales, se utilizará cableado estructurado de cobre categoría 6A (Cat 6A), adecuado para velocidades de hasta 10 Gbps dentro de edificios.

En la Figura 3.3 se puede observar el diseño general de la red de la empresa, donde se muestra la interconexión entre las diferentes sedes y la oficina central. Este diseño general permite visualizar cómo se conectan todas las instalaciones de la empresa, formando una red corporativa unificada que facilita la gestión centralizada y la comunicación entre todas las sedes.

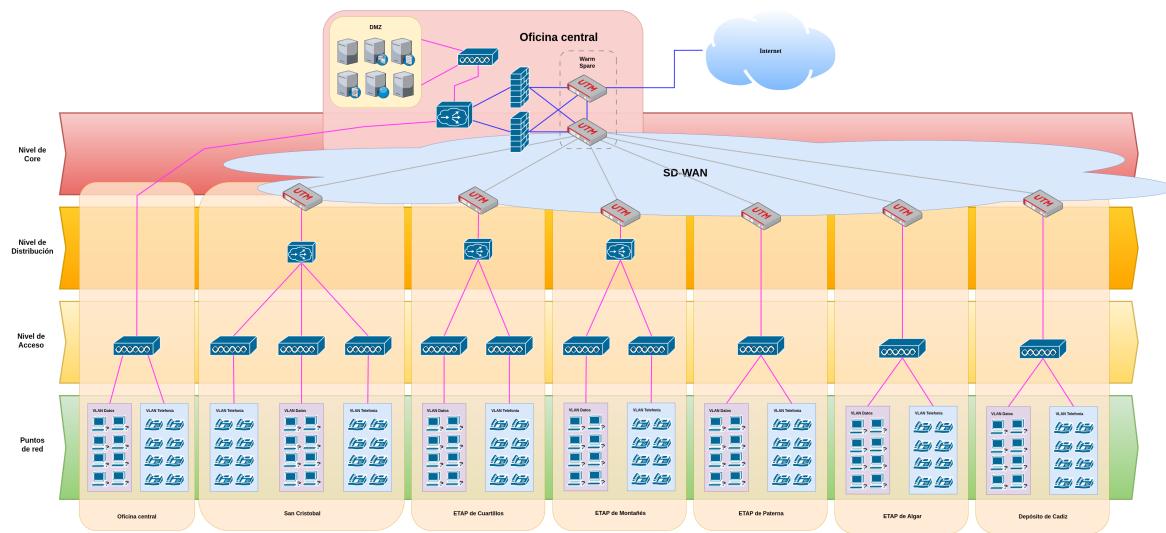


Figura 3.3: Diseño representativo de la red de la empresa

3.1.2. Dispositivos de red

En esta sección se detallan los equipos de red elegidos para poner en marcha la infraestructura de comunicaciones de la empresa. Aunque Vodafone no especifica detalladamente los modelos que se entrega a sus clientes, sí se especifica que su solución SD-WAN está basada en la tecnología Cisco Meraki.

3.1.2.1. Dispositivos de interconexión

Dado que el proveedor de servicios elegido es Vodafone, el cual ofrece soluciones de conectividad basadas en la tecnología SD-WAN de Cisco Meraki, se ha optado por realizar una estimación técnica realista de los dispositivos que podrían instalarse en cada sede.

En este proyecto se propone el uso de dispositivos de la gama Cisco Meraki MX, los cuales son *appliances* de red de tipo UTM (Unified Threat Management). Estos dispositivos combinan en un solo equipo funciones avanzadas de enrutamiento, cortafuegos de nueva generación, conectividad VPN automática (AutoVPN), detección y prevención de intrusiones (IDS/IPS), así como filtrado de contenido.

En la Tabla 3.2 se presenta una justificación técnica de los dispositivos Cisco Meraki MX ² propuestos para cada sede del Consorcio de Aguas de la Zona Gaditana. Se ha seleccionando un modelo específico para cada sede, teniendo en cuenta el tamaño y las necesidades de conectividad de cada una.

Sede	Modelo propuesto	Justificación	Precio estimado (€)
Oficina Central	MX95	Nodo central de la red SD-WAN. Actúa como concentrador VPN y punto de salida único a Internet. Requiere alto rendimiento y escalabilidad.	3.700
	MX85	Será el dispositivo secundario (redundancia) que estará preparado (Warm Spare) en caso de que el principal falle.	2.130
San Cristóbal	MX68	Sede mediana. El modelo permite hasta 50 usuarios y ofrece margen de crecimiento. Adecuado para cargas medias y conexiones VPN estables.	650
ETAP de Cuartillos ETAP de Montañés ETAP de Paterna ETAP de Algar Depósito de Cádiz	MX67	Sedes pequeñas con necesidades similares de conectividad y escalabilidad. El modelo MX67 es compacto, económico y soporta hasta 50 usuarios, ofreciendo suficientes puertos LAN y funcionalidades para entornos de bajo o moderado tráfico, manteniendo un buen balance entre coste y prestaciones.	420

Tabla 3.2: Justificación técnica de los dispositivos Cisco Meraki MX por sede

Los modelos seleccionados de la serie Meraki MX ofrecen las siguientes características:

- **Rendimiento y escalabilidad:** estos modelos están diseñados para manejar cargas de trabajo medianas a altas, con capacidades de procesamiento y memoria adecuadas para soportar múltiples conexiones VPN y tráfico de red.
- **Seguridad avanzada:** todos los modelos incluyen funcionalidades de seguridad integradas, como firewall de nueva generación, detección y prevención de intrusiones (IDS/IPS), filtrado de contenido y protección contra malware, lo que garantiza una defensa robusta contra amenazas cibernéticas.
- **Conectividad VPN:** establecen automáticamente túneles VPN sitio a sitio con conectividad con IPsec
- **Gestión centralizada:** todos los dispositivos se gestionan a través del Meraki Dashboard, que es una plataforma en la nube de Meraki que permite la administración centralizada de la red, la monitorización del rendimiento y la aplicación de políticas de seguridad y calidad de servicio de forma unificada.
- **Facilidad de implementación:** los dispositivos Meraki son conocidos por su facilidad de instalación y configuración, lo que reduce el tiempo y los recursos necesarios para poner en marcha la red.

²Ficha técnica de los Meraki MX

3.1.2.2. Switches

El Consorcio de Aguas de la Zona Gaditana cuenta con siete sedes distribuidas por la provincia de Cádiz. En la Tabla 3.3 se detalla el número mínimo de puntos de acceso requeridos para cada sede. Considerando que cada trabajador necesita un ordenador y un teléfono IP, se ha duplicado el número de puertos solicitados. Además, se ha implementado un margen de crecimiento del 20% para permitir futuras ampliaciones de la infraestructura de red.

Denominación de la sede	Nº de puertos mínimo	Nº de puertos con escalabilidad
Oficina central	30	72
San Cristóbal	15 + 5 + 5	36 + 12 + 12
ETAP de Cuartillos	5 + 5	12 + 12
ETAP de Montañés	5 + 5	12 + 12
ETAP de Paterna	5	12
ETAP de Algar	5	12
Depósito de Cádiz	5	12

Tabla 3.3: Número de puertos de acceso a la red

Se han comparado diferentes modelos de switches por fabricante según las necesidades de cada sede (ver Tabla 3.4). Finalmente, se seleccionan dispositivos Cisco por su relación calidad-precio: el Catalyst 9300-24P [23, 24] para la Oficina Central y San Cristóbal, el Catalyst 3560-CX-12PD-S [25, 26] para el resto de sedes, y el WS-C2960L-16TS-LL [27] como switch de acceso en todos los edificios.

Fabricante	Rol	Modelo	Sedes que lo necesitan	Precio/unidad
Cisco	Distribución	Catalyst 9300-24P	Oficina Central, San Cristóbal	1.160€
		Catalyst 3560-CX-12PD-S	ETAP Cuartillos, ETAP Montañés, ETAP Paterna, ETAP Algar, Depósito Cádiz	1.120€
	Acceso	WS-C2960L-16TS-LL	Oficina Central (5), San Cristóbal (4) ETAP Cuartillos (2), ETAP Montañés (2) ETAP Paterna, ETAP Algar, Depósito Cádiz	410€
Juniper	Distribución	EX4300-24P	Oficina Central, San Cristóbal	2.900€
		EX2300-C-12P	ETAP Cuartillos, ETAP Montañés, ETAP Paterna, ETAP Algar, Depósito Cádiz	700€
	Acceso	EX2300-C-12P	Oficina Central (6), San Cristóbal (5) ETAP Cuartillos (2), ETAP Montañés (2), ETAP Paterna, ETAP Algar, Depósito Cádiz	700€
Huawei	Distribución	S5720-28X-PWR-SI-AC	Oficina Central, San Cristóbal	1.030€
		S5720-14X-PWH-SI-AC	ETAP Cuartillos, ETAP Montañés, ETAP Paterna, ETAP Algar, Depósito Cádiz	700€
	Acceso	S5720-28X-PWR-LI-AC	Oficina Central (3), San Cristóbal (4) ETAP Cuartillos (2), ETAP Montañés (2), ETAP Paterna, ETAP Algar, Depósito Cádiz	360€

Tabla 3.4: Comparativa de switches por fabricante y sedes según necesidades.

NOTA:

El número reflejado en cada paréntesis indica la cantidad de dispositivos de ese tipo en las sedes mencionadas

3.1.2.3. Firewall

Siguiendo las especificaciones técnicas descritas en la sección 2.3.1, y teniendo en cuenta que Vodafone trabaja con dispositivos de la marca Fortinet, se ha seleccionado el modelo Fortinet FortiGate FG-100F-HA como solución de seguridad perimetral para la sede central.

Este firewall de próxima generación proporciona un conjunto completo de funcionalidades de protección, incluyendo prevención de intrusiones, inspección profunda de paquetes (DPI), control de aplicaciones, filtrado web y antivirus. Su integración permite reforzar la seguridad del perímetro WAN y complementar las funciones básicas de firewall ya incluidas en los dispositivos Cisco Meraki MX utilizados en la red SD-WAN.

El modelo FG-100F-HA permite configuraciones en alta disponibilidad (HA), soporta múltiples interfaces de red de alta velocidad y está diseñado para entornos empresariales de tráfico medio-alto, como es el caso de la oficina central que actúa como nodo concentrador del tráfico de todas las sedes.

Esta solución permite reforzar la seguridad global de la red, especialmente en el punto crítico donde se concentra todo el tráfico proveniente de las sedes remotas. El FortiGate actúa como firewall perimetral, mientras que el *appliance* Cisco Meraki MX250 se encarga de la conectividad SD-WAN, aunque tiene firewall integrado pero no suficiente para esta red de la empresa, estos se complementan entre sí para proporcionar una solución de seguridad robusta y escalable.

3.1.2.4. Telefonía IP

En cuanto a la telefonía IP, se ha optado por teléfonos que cumplen con los requisitos que se comentan en la sección 2.4. En la Tabla 3.5 se muestran algunos modelos que cumplen con los requisitos necesarios que pide el pliego de proyectos.

Fabricante	Modelo	Precio aprox.	Características principales
Grandstream	GRP2602G	37€	2 líneas y 4 cuentas SIP, puertos Gigabit con PoE integrado, pantalla LCD, manos libres Full-Duplex, audio HD, EHS
Grandstream	GRP2612G	45€	4 líneas multiuso y 4 cuentas SIP, dobles puertos GE a 10/100/1000 Mbps con PoE integrada, audio HD (Noise Shield), Wi-Fi de doble banda integrado
Yealink	SIP-T31G	55€	2 cuentas VoIP, pantalla LCD, doble puerto Gigabit Ethernet, manos libre Full-Duplex, soporte IPv6, EHS
Fanvil	X3SP Pro	65€	4 líneas SIP, Auriculares inalámbricos EHS, Puertos rápidos duales, PoE integrado, Full-Duplex (AEC)

Tabla 3.5: Comparativa de Teléfonos IP

Se va a optar por el modelo Grandstream GRP2612G [28] para toda la empresa, ya que es un modelo que cumple con los requisitos técnicos necesarios y es compatible con la solución de telefonía en la nube.

3.1.2.5. Resumen de los dispositivos de red

En la Tabla 3.6 se presenta un resumen de los dispositivos de red seleccionados para el Consorcio de Aguas de la Zona Gaditana.

Dispositivo	Modelo	Cantidad	Precio/unidad	Precio total
Dispositivo SD-WAN	Cisco Meraki MX95	1	3.700€	3.700€
Dispositivo SD-WAN	Cisco Meraki MX85	1	2.130€	2.130€
Dispositivo SD-WAN	Cisco Meraki MX68	1	650€	650€
Dispositivo SD-WAN	Cisco Meraki MX67	5	420€	2.100€
Switch de distribución	Catalyst 9300-24P	2	1.160€	2.320€
Switch de distribución	Catalyst 3560-CX-12PD-S	5	1.120€	5.600€
Switch de acceso	WS-C2960L-16TS-LL	16	410€	6.560€
Firewall	FortiGate FG-100F-HA	1	1800€	1.800€
Teléfono IP	Grandstream GRP2612G	38	45€	1.710€
Total estimado				26.570€

Tabla 3.6: Resumen de dispositivos de red seleccionados

3.1.3. Servicios de red necesarios

En este proyecto no se implementarán directamente todos los servicios de red, ya que el objetivo es realizar un diseño de red adaptado a las necesidades tomadas de referencia del pliego del Consorcio de Aguas de la Zona Gaditana. A continuación, se describen los servicios de red que se consideran necesarios para el correcto funcionamiento de la infraestructura de comunicaciones de la empresa, tal y como se recoge en la Tabla 3.7. Estos servicios son fundamentales para garantizar la conectividad, la seguridad y la gestión eficiente de la red.

Servicio	Descripción	Observaciones
Red Privada Virtual (VPN)	Conectividad segura entre todas las sedes	Nodo central (Oficina Central) como HUB + VPN Site-to-Site para cada sede.
Active Directory (AD)	Gestión centralizada de usuarios, políticas y accesos.	Servidor virtualizado en Oficina Central.
DNS interno	Resolución de nombres para servicios internos.	Integrado con el AD en la Oficina Central.
DHCP	Asignación dinámica de IP por sede.	Centralizado en Oficina Central + DHCP Relay en cada sede.
Centralita VoIP en la nube	Telefonía fija integrada	Con terminales IP en cada sede.
Correo electrónico corporativo	Gestión de cuentas de correo, buzones compartidos y seguridad.	Solución cloud (Microsoft 365).
Web corporativa	Sitio web institucional accesible públicamente.	Alojamiento en la nube.
Cortafuegos de nueva generación (NGFW)	Seguridad perimetral, visibilidad del tráfico, control de acceso.	Instalado en la Oficina Central como único punto de acceso a Internet.
Backup en la nube	Copias de seguridad de sistemas físicos y virtuales.	Almacenamiento en la nube.
Acceso a Internet	Salida a Internet centralizada desde la Oficina Central	A través del firewall central en la Oficina Central.

Tabla 3.7: Resumen de servicios de red necesarios

3.2. Esquema de direccionamiento

Para abordar el problema del agotamiento de direcciones, se ha diseñado un esquema en IPv6. Cada sede dispone de dos VLANs principales, una para datos con ID 10 y otra para voz con ID 20, lo que permite segmentar el tráfico y mejorar la seguridad y el rendimiento de la red. Además, la Oficina Central incluye una VLAN DMZ con ID 30 para los servidores que deben ser accesibles desde Internet. Cada sede tendrá asignado un bloque de direcciones IPv6 /56, lo que permite crear hasta 256 subredes /64 dentro de cada sede, una para cada VLAN. Esto proporciona una gran flexibilidad y escalabilidad para futuras expansiones de la red, ya que cada VLAN puede crecer independientemente sin necesidad de reconfigurar la red completa.

Se asume que el ISP asigna el bloque 2001:db8:1234::/48. A partir de este bloque, se han reservado subredes /64 para cada VLAN de cada localización. Además, todas las direcciones IP se asignarán mediante un servidor DHCP (Dynamic Host Configuration Protocol), que proporcionará las direcciones dentro de los rangos definidos en la Tabla 3.8, evitando conflictos de direcciones en la red. El servidor DHCP estará centralizado en la Oficina Central, y cada router de delegación actuará como relay DHCP para reenviar las solicitudes de los dispositivos de su ubicación al servidor central. De este modo, se garantiza que cada oficina reciba direcciones IP dentro de su rango específico, sin solapamientos entre instalaciones ni VLANs. En la DMZ, las IPs serán asignadas de forma estática.

Sede	Prefijo de sede	VLAN	Dir. de Red	Máscara
Oficina central	2001:db8:1234:0100::/56	Datos	2001:db8:1234:0100::	/64
		Voz	2001:db8:1234:0101::	/64
		DMZ	2001:db8:1234:0102::	/64
San Cristóbal	2001:db8:1234:0200::/56	Datos	2001:db8:1234:0200::	/64
		Voz	2001:db8:1234:0201::	/64
ETAP Cuartillos	2001:db8:1234:0300::/56	Datos	2001:db8:1234:0300::	/64
		Voz	2001:db8:1234:0301::	/64
ETAP Montañés	2001:db8:1234:0400::/56	Datos	2001:db8:1234:0400::	/64
		Voz	2001:db8:1234:0401::	/64
ETAP Paterna	2001:db8:1234:0500::/56	Datos	2001:db8:1234:0500::	/64
		Voz	2001:db8:1234:0501::	/64
ETAP Algar	2001:db8:1234:0600::/56	Datos	2001:db8:1234:0600::	/64
		Voz	2001:db8:1234:0601::	/64
Depósito de Cádiz	2001:db8:1234:0700::/56	Datos	2001:db8:1234:0700::	/64
		Voz	2001:db8:1234:0701::	/64

Tabla 3.8: Esquema de direccionamiento IPv6 para todas las sedes

3.3. Seguridad y firewall

En esta sección se abordarán los aspectos de seguridad de la red, incluyendo la plataforma de seguridad a utilizar y las reglas del firewall. Cabe recalcar que no se implementarán los servicios de seguridad por el poco tiempo que se tiene para realizar el proyecto.

3.3.1. Plataforma de seguridad

Como plataforma de firewall de nueva generación se ha seleccionado el FortiGate Next-Generation Firewall (NGFW) [29], que están diseñados para ofrecer seguridad avanzada en cualquier entorno (on-premise, nube, remoto). Además, FortiGate es el firewall que utiliza Vodafone en sus redes, lo que garantiza una integración fluida con los servicios de telecomunicaciones de la empresa. También, es el cortafuegos más implementado, con más del 50 % de la participación en el mercado global.

Por otro lado, la plataforma de respuesta ante incidentes se basará en Microsoft Sentinel [30], que es un servicio de SIEM (*Security Information and Event Management*) y SOAR (*Security Orchestration, Automation, and Response*) en la nube. Microsoft Sentinel permite la recopilación, análisis y correlación de datos de seguridad de toda la infraestructura, facilitando la detección y respuesta ante amenazas.

3.3.2. Reglas firewall

La Oficina Central de la empresa contará con un esquema de seguridad perimetral para proteger la red, incluyendo una zona desmilitarizada (DMZ). Todas las sedes remotas accederán a Internet a través de la Oficina Central, por lo que el firewall de esta sede será el punto de control de acceso a Internet para toda la organización. A continuación se describen algunas reglas básicas de seguridad que tendrá el firewall de la Oficina Central:

Regla	Acción	IP Origen	IP Destino	Protocolo	Puerto Origen	Puerto Destino
Entrada	Permitir	Internet	DMZ	TCP	Cualquiera	80, 443
Entrada	Permitir	Internet	Router	TCP	Cualquiera	22
Entrada	Permitir	PBX Nube	Red Interna	UDP	Cualquiera	5060, 10000-20000
Entrada	Permitir	VPN	Red Interna	TCP/UDP	Cualquiera	443, 21
Entrada	Denegar	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Tránsito	Permitir	Red Interna	DMZ	TCP/UDP	Cualquiera	80, 443, 25, 53
Tránsito	Permitir	Red Interna	PBX Nube	UDP	Cualquiera	5060, 10000-20000
Tránsito	Permitir	DMZ	Internet	TCP/UDP	Cualquiera	Servicios necesarios
Tránsito	Denegar	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Salida	Permitir	Red Interna	Internet	TCP	Cualquiera	80, 443
Salida	Permitir	Red Interna	DMZ	TCP/UDP	Cualquiera	Servicios necesarios
Salida	Permitir	Red Interna	PBX Nube	UDP	Cualquiera	5060, 10000-20000
Salida	Denegar	Red Interna	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Salida	Permitir	DMZ	Internet	TCP/UDP	Cualquiera	Servicios necesarios
Salida	Permitir	DMZ	Red Interna	TCP/UDP	Cualquiera	Servicios necesarios

Tabla 3.9: Reglas del firewall

Por otro lado, también se aplicarán reglas NAT para permitir la traducción de direcciones IP privadas a públicas y viceversa. Estas reglas se aplicarán en el router de la Oficina Central.

3.4. FreePBX como centralita de telefonía IP

Para la gestión de la telefonía IP del Consorcio de Aguas de la Zona Gaditana se ha elegido FreePBX [31], una solución de código abierto ampliamente reconocida en el ámbito empresarial. FreePBX destaca por su flexibilidad y capacidad de integración con protocolos y servicios VoIP, así como por su compatibilidad con una amplia gama de teléfonos SIP

y dispositivos gateway. Además, ofrece funcionalidades avanzadas como planes de marcado, sistemas IVR (Respuesta de Voz Interactiva), grabación de llamadas, buzones de voz y conferencias, entre otras. Al ser una centralita basada en web y *open-source*, permite una personalización completa y una gestión sencilla a través de su interfaz gráfica. Además, al ser una solución basada en Asterisk, FreePBX proporciona una plataforma robusta y escalable para la implementación de servicios de telefonía IP.

Cabe destacar que, en el contexto de este proyecto, no se va a implementar la centralita FreePBX ni sus servicios asociados, sino que se presenta únicamente como propuesta técnica para cubrir los requisitos de telefonía IP del Consorcio.

3.4.1. Arquitectura de implementación

El sistema se desplegará en una arquitectura distribuida y alojada en la nube de Microsoft Azure [32], asegurando alta disponibilidad y escalabilidad. La solución se compone de los siguientes elementos:

- **Servidor FreePBX principal:** máquina virtual (Azure VM) donde se gestiona la configuración de la centralita.
- **Base de datos MySQL:** alojada en Azure Database for MySQL, para la gestión de configuraciones y registros.
- **Almacenamiento Blob:** almacenamiento de grabaciones de llamadas y mensajes de voz en Azure Blob Storage.
- **Interfaz web:** basada en Apache y PHP.
- **Azure Load Balancer:** gestión de tráfico web y SIP.

3.4.2. Plan de numeración y configuración de extensiones

Se ha diseñado un plan de numeración estructurado por sede, utilizando extensiones de cuatro dígitos con prefijos únicos para cada ubicación como se muestra en la Tabla 3.10. El plan de numeración se ha estructurado para facilitar la identificación de las extensiones según la sede. Cada ubicación cuenta con un prefijo único y un rango de extensiones de cuatro dígitos, lo que simplifica la gestión y el crecimiento futuro.

Sede	Prefijo	Rango
Oficina Central	1XXX	1000-1059
San Cristóbal	2XXX	2000-2024
ETAP de Cuartillos	3XXX	3000-3009
ETAP de Montañés	4XXX	4000-4009
ETAP de Paterna	5XXX	5000-5004
ETAP de Algar	6XXX	6000-6004
Depósito de Cádiz	7XXX	7000-7004

Tabla 3.10: Plan de numeración por sede

Cada extensión se configurará con una contraseña SIP robusta, buzón de voz con notificación por correo electrónico, grabación automática de llamadas y opciones de desvío según el estado del usuario. Se prioriza el uso del códec G.711 u-law para garantizar la calidad de audio y se emplea el método DTMF RFC2833 para la señalización de tonos.

3.4.3. Sistema IVR y operadora automática

El IVR (Interactive Voice Response) [33] es un sistema automatizado que permite a las personas que llaman interactuar con un sistema telefónico a través de menús pregrabados y entradas de teclado o voz, sin necesidad de hablar directamente con un agente. Para el Consorcio de Aguas de la Zona Gaditana, se ha diseñado un sistema IVR de dos niveles que permite a los usuarios navegar por las diferentes opciones de contacto y gestionar incidencias de manera eficiente.

El sistema está diseñado para ser intuitivo, permitiendo la entrada directa de extensiones en cualquier momento y la selección de idioma. Se han definido parámetros técnicos como el formato de las locuciones (WAV, 8kHz, mono), tiempos de espera y reintentos, así como la gestión diferenciada de llamadas fuera del horario laboral.

3.4.3.1. Nivel 1 - Menú principal

“Gracias por llamar al Consorcio de Aguas de la Zona Gaditana. Si conoce el número de la extensión con la que desea comunicarse, puede marcarlo en cualquier momento. Para ser atendido por una de nuestras sedes, por favor seleccione una opción:”

- Pulse 1 para contactar con la Oficina Central.
- Pulse 2 para la sede de San Cristóbal.
- Pulse 3 para la planta ETAP de Cuartillos.
- Pulse 4 para la planta ETAP de Montañés.
- Pulse 5 para la planta ETAP de Paterna.
- Pulse 6 para la planta ETAP de Algar.
- Pulse 7 para el Depósito de Cádiz.
- Pulse 9 para comunicar una incidencia.

3.4.3.2. Nivel 2 - IVR por sede

Este es un ejemplo de cómo se estructurará el IVR para la Oficina Central. Cada sede tendrá un IVR similar adaptado a sus necesidades.

“Ha contactado con la Oficina Central. Por favor, seleccione una opción:”

- Pulse 1 para Atención al Cliente.
- Pulse 2 para Facturación.
- Pulse 3 para Mantenimiento.
- Pulse 4 para Recursos Humanos.
- Pulse 5 para Informática.
- Pulse 6 para Calidad.
- Pulse 7 para Administración.
- Pulse 9 para comunicar una incidencia.

3.4.3.3. Nivel 2 - IVR de incidencias

“Ha contactado con el sistema de notificación de incidencias. Por favor, seleccione una opción:”

- Pulse 1 para averías en el suministro de agua.
- Pulse 2 para reportar fugas o incidencias técnicas.
- Pulse 3 para reclamaciones o sugerencias.
- O espere para ser atendido por un agente.

3.4.4. Grupos de salto y grupos de captura

Una estructura de grupos de salto y grupos de captura permite una gestión eficiente y ordenada de las llamadas entrantes, facilitando la operatividad en un entorno distribuido como el que caracteriza a esta organización, con múltiples sedes interconectadas a través de una Red Privada Virtual.

Los **grupos de salto** permiten asignar a cada sede o área funcional un número principal para recibir llamadas, las cuales se distribuyen automáticamente entre varias extensiones según lógicas configurables (circular, simultánea, por orden, etc.). Cada grupo puede definir tiempos de espera, tonos máximos y destinos de desbordamiento, como buzones de voz o una operadora automática, lo que asegura que ninguna llamada quede sin respuesta.

El grupo de salto de la Oficina Central (1000) distribuye las llamadas entrantes entre las extensiones 1001, 1002 y 1003 siguiendo una estrategia de salto secuencial. Si la primera extensión no responde en 15 segundos, la llamada pasa a la siguiente, y así sucesivamente. Si ninguna responde, la llamada se transfiere al buzón de voz del grupo.

Los **grupos de captura**, por su parte, permiten que cualquier usuario pueda atender una llamada dirigida a otro compañero de su grupo marcando un código específico. Esta función es útil en entornos colaborativos como oficinas administrativas y mejora la disponibilidad del servicio.

El grupo de captura de la sede de San Cristóbal (2000) permite que cualquier usuario del grupo (por ejemplo, extensiones 2001, 2002, 2003) pueda atender una llamada destinada a otro miembro marcando el código de captura (por ejemplo, *8). Si suena el teléfono de un compañero y está ausente, otro usuario puede responder la llamada desde su propio terminal.

3.4.5. Servicios adicionales

Entre los servicios adicionales que ofrece la solución destacan el buzón de voz, accesible tanto desde el teléfono como desde una interfaz web, con notificaciones automáticas por correo electrónico. La grabación de llamadas estará activada por defecto, permitiendo su consulta y descarga desde la plataforma o su envío por correo. Todo ello contribuye a una gestión eficiente y segura de las comunicaciones internas y externas del Consorcio.

3.5. Elección de herramientas de monitorización

En esta sección se compararán diferentes herramientas de monitorización de red, teniendo en cuenta los requisitos definidos en la Sección 2.3. Se evaluarán aspectos como el coste, facilidad de uso, gestión remota, escalabilidad, alertas automáticas e integración con redes distribuidas.

En el contexto de este proyecto, la red principal estará formada por dispositivos Cisco Meraki gestionados por Vodafone, lo que implica que se utilizará el *Meraki Dashboard* como herramienta de monitorización y gestión nativa para la infraestructura SD-WAN. No obstante, se ha realizado un análisis comparativo de otras herramientas de monitorización, que podrían emplearse como complemento o para supervisar otros elementos de red como servidores, impresoras o switches no gestionados por Meraki.

Herramienta	Características Clave	Ventajas
Cisco Meraki Dashboard	Monitorización en tiempo real de dispositivos Meraki, alertas automáticas, visualización de red, gestión desde la nube	Integración total con la infraestructura SD-WAN, configuración sencilla, sin instalación local
Zabbix	Monitorización en tiempo real, alertas, interfaz web segura, soporte SNMP y SYSLOG	Open source, altamente personalizable, escalable
ManageEngine OpManager	Interfaz web intuitiva, monitoreo de enlaces WAN y dispositivos, gestión remota	Completa y con buena experiencia de usuario
Nagios XI	Monitoreo avanzado, alertas configurables, gestión SYSLOG, acceso web	Ampliamente compatible, muy personalizable
PRTG Network Monitor	Monitorización todo-en-uno, dashboards web, alertas inteligentes, integración con protocolos de red	Fácil de usar, visual, buena para entornos medianos
SolarWinds NPM	Visualización avanzada, integración con múltiples protocolos, alertas automáticas	Potente para grandes entornos, soporte empresarial

Tabla 3.11: Comparativa de herramientas de monitorización de red

No obstante, se propone como herramienta complementaria la utilización de **Zabbix**, especialmente para monitorizar otros dispositivos de red, servidores o servicios que no están bajo el ámbito de gestión Meraki. Zabbix ofrece monitorización en tiempo real, alertas automáticas, interfaz web segura, soporte para protocolos estándar (SNMP, ICMP, SYSLOG), y es una solución de código abierto, lo que permite reducir costes de licencias y personalizar su despliegue según las necesidades del Consorcio.

Capítulo 4

Simulación

En este capítulo se presenta las simulaciones realizadas para verificar el correcto funcionamiento de la red diseñada. Se ha llevado varias simulaciones de la red utilizando GNS3, en las cuales se ha dividido en cuatro partes:

- Simulación de la red ISP.
- Simulación de la Oficina Central.
- Simulación entre sedes remotas y red ISP.
- Laboratorio de pruebas.

Se han hecho diferentes simulaciones debido a las limitaciones del hardware del ordenador de realización de este proyecto, por lo que impide simular la red completa en una sola simulación.

4.1. Simulación de la red de ISP

Para la simulación de la red ISP se va basar en MPLS VPN L3, aunque en el diseño de la red final se ha optado SD-WAN con Cisco Meraki para la interconexión de las distintas sedes, esta decisión se ha tomado por las limitaciones técnicas de GNS3 el cual no permite emular estos dispositivos, ya que ésta solución depende de una infraestructura en la nube gestionada directamente por ellos. Además, muchas de las funcionalidades clave que definen a una solución SD-WAN, como la gestión centralizada, la aplicación de políticas dinámicas por el tipo de tráfico y el monitoreo inteligente de enlaces, están fuera del alcance de GNS3. Replicar este entorno de forma precisa en este simulador de redes es complejo, poco escalable y alejadas al funcionamiento real de Meraki, perdiendo así la esencia de esta tecnología que es la simplicidad operativa, la visibilidad completa de la red y el control centralizado del tráfico.

Por otro lado, si bien existen imágenes de soluciones SD-WAN que pueden encontrarse en entornos de pruebas, estas requieren licencias oficiales para poder ser utilizadas, lo que representa una limitación importante.

Es por ello que se ha optado por simular una red MPLS VPN L3, que es una tecnología ampliamente utilizada para la interconexión de sedes a través de un *backbone* común y la gestión de tráfico entre ellas. Esta tecnología permite crear redes privadas virtuales (RPV) que proporciona conectividad segura y eficiente entre las distintas sedes, permitiendo el transporte de datos a través de un único canal troncal compartido.

De esta forma, se han usado los routers MikroTik CHR 7.16 [34] que son dispositivos virtuales que permiten simular el comportamiento de un router físico. Estos dispositivos son ideales para la simulación de la red MPLS, ya que ofrecen una amplia gama de funcionalidades y son compatibles con los protocolos utilizados en la red. El único inconveniente es que RouterOS, el sistema operativo de MikroTik, no es compatible con IPv6 para MPLS, por lo que se ha optado por utilizar IPv4 para la simulación.

Se ha utilizado el rango de direcciones privadas 10.0.0.0/30 y 172.16.0.0/30 para los enlaces punto a punto entre routers empleando subredes /30. Además, se han asignado direcciones /32 del rango 1.1.1.0/32 a las interfaces loopback de cada router. Esta estructura permite una separación lógica y ordenada entre los distintos tipos de tráfico en la red MPLS, diferenciando claramente el tráfico interno de cada sede del tráfico troncal entre sedes.

La asignación de direcciones /32 a las interfaces loopback permite identificar de forma única a cada router dentro del dominio MPLS, facilitando la operación de protocolos como LDP y BGP. Incluso en el caso de ciertos routers que no pertenecen directamente a la red MPLS, como los CE, se utilizan estas direcciones para mantener una identificación coherente dentro del diseño general. Por otro lado, las subredes /30 se emplean en los enlaces punto a punto para asegurar una utilización eficiente del espacio de direcciones IP, reduciendo el desperdicio.

En la Figura 4.1 se muestra la red MPLS configurada en GNS3, que incluye los routers PE (Provider Edge) que son los encargados de conectar las sedes a la red MPLS, P (Provider) que son responsables de enrutar el tráfico entre las distintas sedes y los CE (Customer Edge) que son los encargados de conectar la red local a la red MPLS.

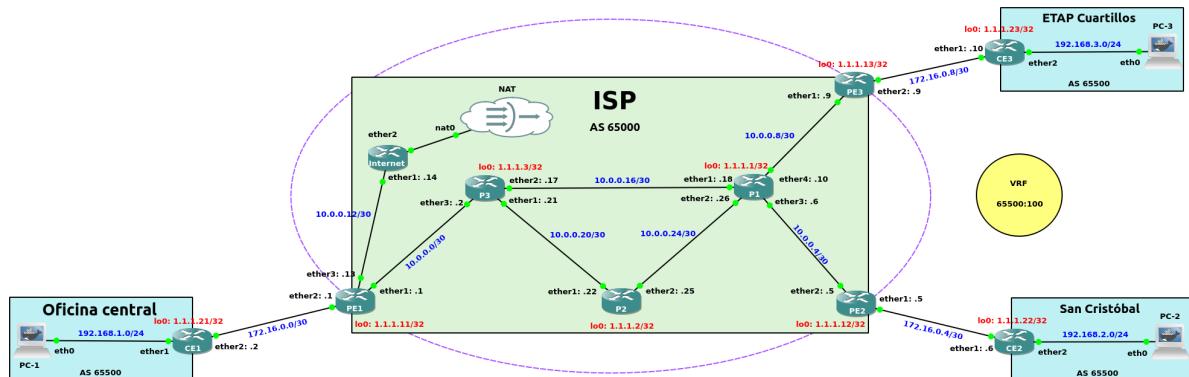


Figura 4.1: Red MPLS configurada en GNS3

A continuación, en la Tabla 4.1 se muestra el esquema de direccionamiento implementado en la red MPLS:

Router	Interfaz	Dirección IP
PE1	Lo0	1.1.1.11/32
	ether1	10.0.0.1/30
	ether2	172.16.0.1/30
	ether3	10.0.0.14/30
PE2	Lo0	1.1.1.12/32
	ether1	172.16.0.5/30
	ether2	10.0.0.5/30
PE3	Lo0	1.1.1.13/32
	ether1	10.0.0.9/30
	ether2	172.16.0.9/30
P1	Lo0	1.1.1.1/32
	ether1	10.0.0.18/30
	ether2	10.0.0.26/30
	ether3	10.0.0.6/30
	ether4	10.0.0.10/30
P2	Lo0	1.1.1.2/32
	ether1	10.0.0.22/30
	ether2	10.0.0.25/30
P3	Lo0	1.1.1.3/32
	ether1	10.0.0.21/30
	ether2	10.0.0.17/30
	ether3	10.0.0.2/30
CE1	Lo0	1.1.1.21/32
	ether1	192.168.1.1/24
	ether2	172.16.0.2/30
CE2	Lo0	1.1.1.22/32
	ether1	192.168.2.1/24
	ether2	172.16.0.6/30
CE3	Lo0	1.1.1.23/32
	ether1	192.168.3.1/24
	ether2	172.16.0.10/30
Internet	Lo0	1.1.1.14/32
	ether1	10.0.0.14/30
	ether2	DHCP

Tabla 4.1: Esquema de direccionamiento para la red ISP

Este esquema permite una gestión eficiente del tráfico entre las sedes, garantizando la conectividad y la seguridad de los datos que circulan por la red MPLS. Las direcciones IP asignadas a cada dispositivo son únicas dentro de la red MPLS, lo que facilita la identificación y el enrutamiento de los paquetes de datos.

4.1.1. Configuración de interfaces loopback y asignar IPs a interfaces físicas

En el contexto de una red MPLS, es imprescindible establecer una única sesión LDP (Label Distribution Protocol) entre cada par de routers con el fin de permitir el correcto intercambio de etiquetas. Para garantizar que este proceso no se vea afectado por el estado operativo o el direccionamiento de las interfaces físicas utilizadas para el reenvío de tráfico, se recurre habitualmente al uso de interfaces loopback. Estas proporcionan una dirección IP estable y siempre activa, independientemente de las condiciones de los enlaces físicos.

En consecuencia, es necesario configurar una interfaz loopback en cada uno de los routers que integran la infraestructura MPLS. Para ello, se implementará una interfaz de tipo *bridge* sin asociación a puertos físicos, a la cual se asignará una dirección IP o subred previamente reservada para las sesiones LDP dentro de la red. Esta configuración contribuye a una mayor estabilidad y resiliencia en el establecimiento de las rutas MPLS.

A continuación, se presenta un ejemplo de configuración de una interfaz loopback en un router MikroTik:

```
1 [admin@MikroTik] > /system identity set name=PE1
2 [admin@PE2] > /interface bridge add name=lo0
3 [admin@PE2] > /ip address add address=1.1.1.12/32 interface=lo0
```

En cuanto a la configuración de las interfaces físicas, se han asignado direcciones IP a las interfaces de los routers que se conectan entre sí. Por ejemplo, en el router PE2 se ha configurado de la siguiente manera:

```
1 [admin@PE2] > /ip address add address=172.16.0.5/30 interface=ether1
2 [admin@PE2] > /ip address add address=10.0.0.5/30 interface=ether2
```

4.1.2. OSPF como protocolo de enrutamiento

Empezaremos aplicando el protocolo OSPF para aprender de forma dinámica las direcciones de los routers que pertenecen a MPLS, es decir, los routers PE y P. Por tanto, las interfaces que no pertenecen a la red MPLS no se incluirán en el proceso de aprendizaje.

Para ello, se ha creado una instancia OSPF y se han añadido las redes correspondientes a la misma. A continuación, se muestra un ejemplo de configuración de OSPF en el router P1:

```
1 [admin@P1] > /routing ospf instance set redistribute-connected=as-type-1 numbers=0
2 [admin@P1] > /routing ospf network add area=backbone network=10.0.0.16/30
3 [admin@P1] > /routing ospf network add area=backbone network=10.0.0.24/30
4 [admin@P1] > /routing ospf network add area=backbone network=10.0.0.4/30
5 [admin@P1] > /routing ospf network add area=backbone network=10.0.0.8/30
```

En la Figura 4.2 se muestra la tabla de enrutamiento del router P1, que refleja las rutas aprendidas a través del protocolo OSPF.

```
[admin@P1] > ip route print
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, o - OSPF; + - ECMP
Columns: DST-ADDRESS, GATEWAY, DISTANCE
      DST-ADDRESS      GATEWAY      DISTANCE
DAc  1.1.1.1/32    lo0          0
DAo  1.1.1.2/32   10.0.0.25%ether2  110
DAo  1.1.1.3/32   10.0.0.17%ether1  110
DAo  1.1.1.11/32  10.0.0.17%ether1  110
DAo  1.1.1.12/32  10.0.0.0.5%ether3 110
DAo  1.1.1.13/32  10.0.0.0.9%ether4 110
DAo  10.0.0.0/30   10.0.0.17%ether1 110
DAc  10.0.0.4/30   ether3          0
DAc  10.0.0.8/30   ether4          0
DAo  10.0.0.12/30  10.0.0.17%ether1 110
DAc  10.0.0.16/30  ether1          0
DAo+ 10.0.0.20/30  10.0.0.25%ether2 110
DAo+ 10.0.0.20/30  10.0.0.17%ether1 110
DAc  10.0.0.24/30  ether2          0
```

Figura 4.2: Tabla de enrutamiento de P1

4.1.3. Configuración de la distribución de etiquetas (LDP)

Para asegurar la correcta distribución de las etiquetas MPLS asociadas a cada una de las rutas activas en la red, es fundamental habilitar el Protocolo de Distribución de Etiquetas (LDP) en todos los enrutadores que forman parte de la red MPLS. A continuación, aplicaremos LDP sobre estos mismos routers, excluyendo las interfaces que se comunican con routers externos a la backbone, ya que no requieren esta configuración. Esta configuración se ha aplicado a todos los routers de la red MPLS, por ejemplo, en P1 se ha configurado de la siguiente manera:

```
1 [admin@P1] > /mpls ldp add afi=ip lsr-id=1.1.1.1 transport-addresses=1.1.1.1
2 [admin@P1] > /mpls ldp interface add interface=ether1
3 [admin@P1] > /mpls ldp interface add interface=ether2
4 [admin@P1] > /mpls ldp interface add interface=ether3
5 [admin@P1] > /mpls ldp interface add interface=ether4
```

Además, se ha configurado el rango de etiquetas dinámicas para el tráfico MPLS según la Tabla 4.2.

Router	Loopback	Rango de etiquetas
PE1	1.1.1.11	10000-11999
PE2	1.1.1.12	12000-13999
PE3	1.1.1.13	14000-15999
P1	1.1.1.1	20000-21999
P2	1.1.1.2	22000-23999
P3	1.1.1.3	24000-25999

Tabla 4.2: Rango de etiquetas para cada router

Para configurar el rango de etiquetas dinámicas, se ha utilizado el siguiente comando:

```
1 [admin@P1] > /mpls settings set dynamic-label-range=20000-21999
```

Para comprobar que la configuración es correcta, se ha realizado un traceroute desde el router PE1 a PE2 y se tendrá que ver la asignación de una etiqueta.

```
[admin@PE1] > tool traceroute 10.0.0.5
Columns: ADDRESS, LOSS, SENT, LAST, AVG, BEST, WORST, STD-DEV, STATUS
# ADDRESS      LO  SENT   LAST    AVG   BES   WORS   STD   STATUS
# 10.0.0.2     0%  265  2.7ms  2.9   1.4  15.4  1.3  <MPLS:L=24005,E=>
# 2 10.0.0.18   0%  265  1.9ms  2.2   1     7     0.7
# 3 10.0.0.5    0%  265  3ms   3.2   1.7  15.3  1.1
```

Figura 4.3: Traceroute desde PE1 a PE2

4.1.4. Multi-Protocolo BGP (MP-BGP)

El Multi-Protocolo BGP (MP-BGP) es una extensión del protocolo BGP (Border Gateway Protocol) que permite propagar direcciones y los atributos que la acompañan a través de múltiples protocolos de red. En este contexto, los Sistemas Autónomos (AS) representan agrupaciones de redes bajo una misma política de enrutamiento, lo que facilita la gestión y el intercambio de rutas entre diferentes dominios administrativos. Por tanto, para establecer la conectividad entre los routers PE de la red MPLS, se creará una sesión BGP entre ellos. Para ello, primero se actualizará la plantilla default de BGP en los routers, acorde al

sistema autónomo (65000 en este caso) y al conjunto de direcciones que enrutará cada router PE.

A continuación, se muestra un ejemplo de configuración de BGP en el router PE2:

```
1 [admin@PE2] > /routing bgp template set default address-families=ip,vpnv4 as=65000
    router-id=1.1.1.12
```

Ahora, se crearán las conexiones BGP entre los otros routers PE de la red MPLS. Unicamente hay que configurar la dirección local, la dirección remota, el AS remoto, el role local de BGP (ibgp en este caso al ser routers de la misma AS) y habilitar la escucha como la conexión.

```
1 [admin@PE2] > /routing bgp connection add name=toPE1 template=default local.address=1.1.1.12
    local.role=ibgp remote.address=1.1.1.11 remote.as=65000 connect=yes listen=yes
2 [admin@PE2] > /routing bgp connection add name=toPE3 template=default local.address=1.1.1.12
    local.role=ibgp remote.address=1.1.1.13 remote.as=65000 connect=yes listen=yes
3 [admin@PE2] > /routing bgp connection add name=toPE4 template=default local.address=1.1.1.12
    local.role=ibgp remote.address=1.1.1.14 remote.as=65000 connect=yes listen=yes
```

Una vez hecho, se podrá comprobar que se ha establecido la sesión BGP ejecutando el comando `/routing bgp session print` en los routers PE:

```
[admin@PE1] > /routing bgp session print
Flags: E - established
1 E name="toPE2-1"
  remote.address=1.1.1.12 .as=65000 .id=1.1.1.12
  .capabilities=mp,rr,gr,as4 .afi=ip,vpnv4 .messages=15
  .bytes=426 .eor=""
  local.role=ibgp .address=1.1.1.11 .as=65000 .id=1.1.1.11
  .cluster-id=1.1.1.11 .capabilities=mp,rr,gr,as4 .afi=ip,vpnv4
  .messages=15 .bytes=426 .eor=""
  output.procId=21 ibgp
  multihop=yes hold-time=3m keepalive-time=1m uptime=12m7s570ms
  last-started=2025-06-22 16:36:31 prefix-count=2

2 E name="toPE3-1"
  remote.address=1.1.1.13 .as=65000 .id=1.1.1.13
  .capabilities=mp,rr,gr,as4 .afi=ip,vpnv4 .messages=6
  .bytes=255 .eor=""
  local.role=ibgp .address=1.1.1.11 .as=65000 .id=1.1.1.11
  .cluster-id=1.1.1.11 .capabilities=mp,rr,gr,as4 .afi=ip,vpnv4
  .messages=6 .bytes=255 .eor=""
  output.procId=22 ibgp
  multihop=yes hold-time=3m keepalive-time=1m uptime=3m7s440ms
  last-started=2025-06-22 16:45:31
  last-stopped=2025-06-22 16:45:31 prefix-count=2
```

(a) Sesiones BGP establecidas en PE1

```
[admin@PE2] > /routing bgp session print
Flags: E - established
0 E name="toPE1-1"
  remote.address=1.1.1.11 .as=65000 .id=1.1.1.11
  .capabilities=mp,rr,gr,as4 .afi=ip,vpnv4 .messages=14
  .bytes=407 .eor=""
  local.role=ibgp .address=1.1.1.12 .as=65000 .id=1.1.1.12
  .cluster-id=1.1.1.12 .capabilities=mp,rr,gr,as4 .afi=ip,vpnv4
  .messages=14 .bytes=407 .eor=""
  output.procId=21 ibgp
  multihop=yes hold-time=3m keepalive-time=1m uptime=11m40s440ms
  last-started=2025-06-22 16:36:31 prefix-count=2

1 E name="toPE3-1"
  remote.address=1.1.1.13 .as=65000 .id=1.1.1.13
  .capabilities=mp,rr,gr,as4 .afi=ip,vpnv4 .messages=5
  .bytes=236 .eor=""
  local.role=ibgp .address=1.1.1.12 .as=65000 .id=1.1.1.12
  .cluster-id=1.1.1.12 .capabilities=mp,rr,gr,as4 .afi=ip,vpnv4
  .messages=5 .bytes=236 .eor=""
  output.procId=22 ibgp
  multihop=yes hold-time=3m keepalive-time=1m uptime=2m40s310ms
  last-started=2025-06-22 16:45:31
  last-stopped=2025-06-22 16:45:31 prefix-count=2
```

(b) Sesiones BGP establecidas en PE2

Figura 4.4: Sesiones BGP establecidas en PE1 y PE2

4.1.5. Configuración de VRF y VPN

Virtual Routing and Forwarding (VRF) es una tecnología que permite que múltiples instancias de una tabla de enrutamiento coexistan en el mismo router. Las sedes se situarán en una tabla VRF configurada con un RD (Route Distinguisher) y un RT (Route Target) de importación y exportación. El RD es un identificador de rutas VPN que se antepone a la dirección de red para formar un prefijo único (ASN:número de ruta). El RT es el valor numérico definido por cada PE que está asociado a las rutas que exporta a los puertos BGP. Existen dos tipos de RT:

- **RT de exportación:** Identifican los sitios remotos a los que se exportan las rutas.
- **RT de importación:** Utilizados por los routers PE para importar las rutas en sus tablas VRF.

Para la configuración, antes se crearán las VRFs únicamente en los routers PE que servirán para consultar el direccionamiento de las sedes que están conectadas a la red MPLS. Se creará una tabla VRF por router PE de la siguiente manera:

```
1 [admin@PE2] > /ip vrf add name=CE2 interfaces=ether1
```

Ahora, se configurará la VPN a través de BGP en los routers PE. Se definirá el Router Distinguishers (RD), el cual identifica la ruta VPN y es representado como ASN:número de ruta.

También se definirán los Route Target (RT) de exportación y de importación, que indicarán qué rutas se distribuirán al peer PE según la VPN que identifique. En este caso, se ha definido el mismo valor para RD y RT.

Finalmente, se especificará la política de asignación de etiquetas, la tabla VRF que se empleará y el tipo de rutas que se compartirán desde la VRF hacia VPNV4. Además de las rutas estáticas (static) y conectadas (connected), se activará BGP, dado que este será el protocolo utilizado entre los routers PE y CE en su variante External BGP (eBGP).

```
1 [admin@PE2] > /routing bgp vpn add route-distinguisher=65000:100 import.route-targets=65000:100  
vrf=CE2 label-allocation-policy=per-vrf export.route-targets=65000:100  
.redistribute=connected,static,bgp
```

4.1.6. Comunicación entre routers PE y CE

Para garantizar la conectividad entre los routers PE y CE, implementaremos el protocolo eBGP, asignando un número de sistema autónomo (AS) distinto al de la red troncal MPLS, específicamente el AS 65500.

Configuración de los routers PE

En los routers PE, se van a crear nuevas conexiones BGP con los routers CE. Se va a indicar la dirección local, el AS local, el role local, el AS remoto, la dirección remota, y a habilitar la conexión y la escucha. Además, hay que indicar el ID del router que será la interfaz loopback, el VRF que se usará y la tabla de routing asociada al VRF. Por último, para asegurar que todas las rutas puedan ser anunciadas por la red MPLS, es necesario configurar output.default-originate=always. Esta acción genera una ruta por defecto en el router CE, la cual se aprende mediante eBGP y es crucial para la comunicación de direcciones privadas a través de MPLS.

```
1 [admin@PE2] > /routing bgp connection add name=toCE2 router-id=1.1.1.12 as=65000  
local.address=172.16.0.5 .role=ebgp remote.address=172.16.0.6 .as=65500 routing-table=CE2  
vrf=CE2 connect=yes listen=yes output.default-originate=always
```

Configuración de los routers CE

Para los routers CE, hay una lista de direcciones que se van a exportar a través de BGP. En esta lista de direcciones se asignarán a la conexión BGP para permitir que los paquetes recibidos en el CE puedan ser enviados a través de la red MPLS.

```
1 [admin@CE2] > /ip firewall address-list add address=192.168.2.0/24 list=BGP_OUT
```

Ahora con la lista direcciones creada, se puede configurar la conexión BGP entre el router CE y el router PE. Se indicará el ID del router, AS, dirección local, role local, dirección remota, AS remoto y la lista de direcciones que se van a exportar. También se activará la conexión y la escucha.

```
[1] [admin@CE2] > /routing bgp connection add name=toPE2 as=65500 router-id=1.1.1.22
    local.address=172.16.0.6 .role=ebgp remote.address=172.16.0.5 remote.as=65000
    output.network=BGP_OUT connect=yes listen=yes
```

Con las conexiones BGP configuradas, se puede comprobar que se ha establecido la sesión BGP ejecutando el comando `/routing bgp session print` en los routers CE:

```
[admin@CE1] > /routing bgp session print
Flags: E - established
0 E name="toPE1-1"
  remote.address=172.16.0.1 .as=65000 .id=1.1.1.11
  .capabilities=mp,rr,gr,as4 .afi=ip .messages=4 .bytes=102
  .eor=""
  local.address=172.16.0.2 .as=65500 .id=1.1.1.21
  .cluster-id=1.1.1.21 .capabilities=mp,rr,gr,as4 .afi=ip
  .messages=4 .bytes=105 .eor=""
  output.proc-id=20 .network=BGP_OUT
  input.proc-id=20 ebgp
  hold-time=3m keepalive-time=1m uptime=2m13s900ms
  last-started=2025-06-22 22:26:03 prefix-count=0
```

(a) Sesiones BGP establecidas en CE1

```
[admin@CE3] > /routing bgp session print
Flags: E - established
0 E name="toPE3-1"
  remote.address=172.16.0.9 .as=65000 .id=1.1.1.13
  .capabilities=mp,rr,gr,as4 .afi=ip .messages=5 .bytes=121
  .eor=""
  local.address=172.16.0.10 .as=65500 .id=1.1.1.23
  .cluster-id=1.1.1.23 .capabilities=mp,rr,gr,as4 .afi=ip
  .messages=5 .bytes=124 .eor=""
  output.proc-id=20 .network=BGP_OUT
  input.proc-id=20 ebgp
  hold-time=3m keepalive-time=1m uptime=3m12s740ms
  last-started=2025-06-22 22:30:49 prefix-count=0
```

(b) Sesiones BGP establecidas en CE3

Figura 4.5: Sesiones BGP establecidas en los routers CE

NOTA:

Todas las configuraciones mostradas en los ejemplos anteriores se aplicarán de forma análoga en el resto de los routers, adaptando únicamente las direcciones IP, nombres de interfaces y parámetros específicos según corresponda a cada dispositivo.

4.1.7. Acceso a Internet

Para proporcionar acceso a Internet se ha centralizado en el router CE1 que este actuará como gateway, es decir todo el tráfico que quiera salir a Internet pasará por este router y luego volverá al router PE1 y de ahí a otro router que se conecta a Internet. Para ello, se ha configurado el router CE1 para que realice NAT (Network Address Translation) y permita que los dispositivos una red local accedan a Internet. Además, se ha quitado la conexión BGP entre el router PE1 y CE1, añadiendo una ruta estática en el router PE1 hacia CE1 dentro de la VRF CE1. La configuración de la conexión BGP entre el router PE1 y CE1 se ha realizado de la siguiente manera:

```
[1] [admin@PE1] > /routing bgp connection
[2] add as=65000 connect=yes disabled=yes listen=yes local.address=172.16.0.1 .role=ebgp name=toCE1
    output.default-originate=always remote.address=172.16.0.2 .as=65500 router-id=1.1.1.11
    routing-table=CE1 vrf=CE1
```

Para que el router CE1 pueda realizar NAT, se ha configurado una regla de NAT que permite que el tráfico que sale por la interfaz ether2 (que es la interfaz conectada a Internet) sea traducido. La configuración de la regla de NAT se ha realizado de la siguiente manera:

```
[1] [admin@CE1] > /ip firewall nat add action=masquerade chain=srcnat dst-address=!192.168.0.0/16
    out-interface=ether2
```

Además, se ha configurado una ruta estática en el router CE1 para que el tráfico que sale a Internet pase por la interfaz ether2. La configuración de la ruta estática se ha realizado de la siguiente manera:

```
1 [admin@CE1] > /ip route add gateway=172.16.0.1
```

Para que el router CE1 pueda enviar tráfico a la red local, se ha configurado una ruta estática en el router PE1 hacia CE1 dentro de la VRF CE1. La configuración de la ruta estática se ha realizado de la siguiente manera:

```
1 [admin@PE1] > /ip route add dst-address=172.16.0.0/30 gateway=CE1@CE1 routing-table=main  
2 [admin@PE1] > /ip route add gateway=172.16.0.2@CE1 routing-table=CE1
```

Por otro lado, para que el tráfico que sale por la interfaz ether2 del router PE1 se enrute correctamente, se ha configurado una regla de mangle que marca el tráfico que no es de la red local (192.168.0.0/16) y lo enruta a través de la tabla de enrutamiento principal. La configuración de la regla de mangle se ha realizado de la siguiente manera:

```
1 [admin@PE1] > /ip firewall mangle add action=mark-routing chain=prerouting  
dst-address=!192.168.0.0/16 in-interface=ether2 new-routing-mark=main passthrough=yes
```

4.1.8. Comprobación de la configuración

Para comprobar que la configuración es correcta se hará un ping entre los PCs, por ejemplo, desde el PC1 a la IP 192.168.2.100. Pero antes hay que configurar la IP estática. Para ello, se edita el archivo /etc/network/interfaces y añadiendo la siguiente configuración:

```
1 auto eth0  
2 iface eth0 inet static  
3   address 192.168.X.100  
4   netmask 255.255.255.0  
5   gateway 192.168.X.1
```

NOTA:

La X será según en que sede esté el PC. Por ejemplo, si el PC está en la Oficina Central, la X será 1.

Una vez configurada la IP estática, se puede comprobar que la configuración es correcta como se ve en la Figura 4.6.

```
root@Debian:~# ping 192.168.2.100 -c 4  
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.  
64 bytes from 192.168.2.100: icmp_seq=1 ttl=60 time=6.89 ms  
64 bytes from 192.168.2.100: icmp_seq=2 ttl=60 time=7.65 ms  
64 bytes from 192.168.2.100: icmp_seq=3 ttl=60 time=7.68 ms  
64 bytes from 192.168.2.100: icmp_seq=4 ttl=60 time=7.24 ms  
  
--- 192.168.2.100 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 6.896/7.370/7.686/0.329 ms  
root@Debian:~#
```

Figura 4.6: Comprobación de la configuración

4.2. Simulación de la Oficina Central

La oficina central se ha configurado con un prefijo global de 2001:db8:1234:0100::/56 y se han creado tres VLANs para segmentar el tráfico de datos, voz y DMZ. La VLAN 10 se ha asignado para el tráfico de datos, la VLAN 20 para el tráfico de voz y la VLAN 30 para la DMZ. Por otro lado, esta sede contará con dos routers CE (Customer Edge) configurados en alta disponibilidad mediante el protocolo VRRP (Virtual Router Redundancy Protocol) [35]. Además, se ha configurado un servidor DHCP para asignar direcciones IP dinámicamente a los dispositivos de la red local y dos servidores DNS para resolver nombres de dominio y direcciones IP. La topología de switching implementa el protocolo RSTP (Rapid Spanning Tree Protocol) [36] para garantizar redundancia en los enlaces y prevenir bucles de red, asegurando una convergencia rápida ante fallos.

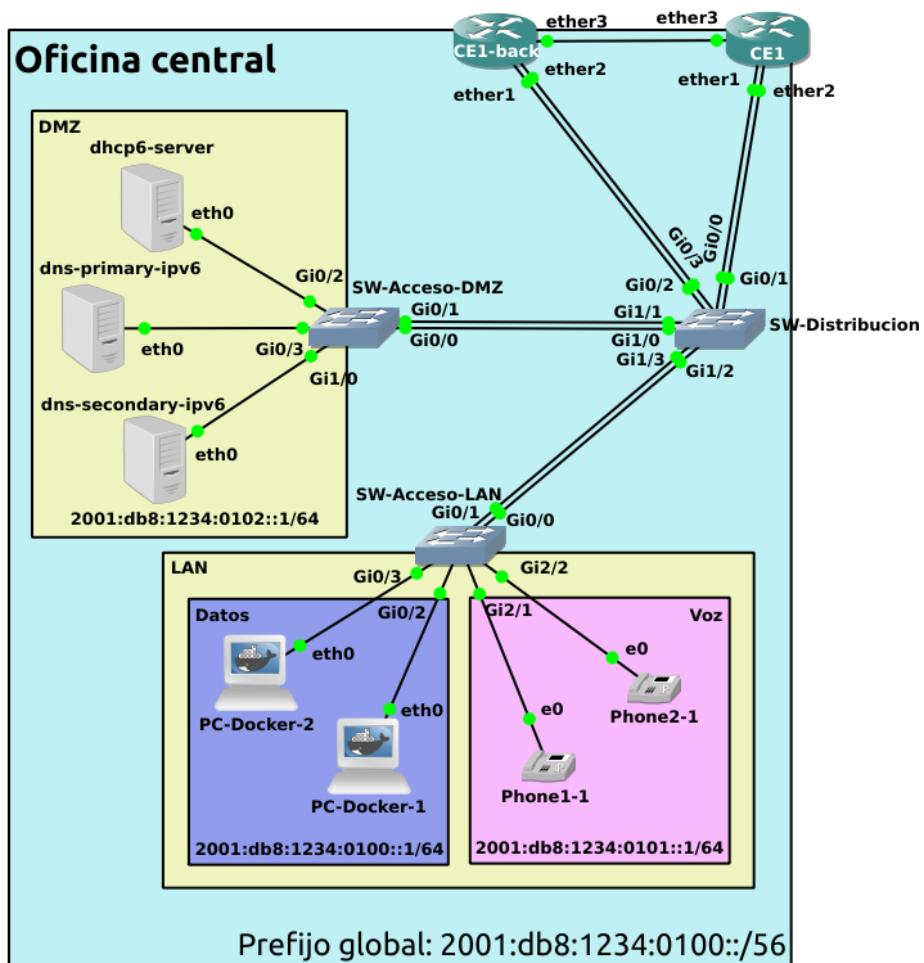


Figura 4.7: Esquema de la oficina central

4.2.1. Configuración de los routers

Para la red local se han utilizado dos routers MikroTik CE1 B.2.1 y CE1_backup B.2.2 configurados con alta disponibilidad mediante VRRP y conectados a través de un enlace de sincronización dedicado. Ambos dispositivos emplean un bonding LACP (802.3ad) sobre dos interfaces físicas para mejorar la redundancia y el ancho de banda. Sobre este bonding se han definido tres VLANs: datos, voz y DMZ, a cada una de las cuales se le asigna

una dirección IPv6. En cada VLAN se implementa VRRP, configurando CE1 como maestro (prioridad 150) y CE1_backup como respaldo (prioridad 100), y se asignan direcciones virtuales que actúan como gateway para los dispositivos de la red. Además, se configura un relay DHCPv6 en las VLANs de datos y voz, se anuncian los servidores DNS mediante Neighbor Discovery [37] y se aplica un firewall básico para IPv6.

Para comprobar el funcionamiento de la configuración VRRP, se ha ejecutado en el router CE1 el comando `/interface vrrp print` y se ha obtenido lo que se muestra en la Figura 4.8.

```
[admin@CE1] > /interface vrrp print
Flags: R - RUNNING; M - MASTER
Columns: NAME, INTERFACE, MAC-ADDRESS, VRID, PRIORITY, INTERVAL, VERSION, V3-PROTOCOL, SYNC-CONNECTION-TRACKING
# NAME INTERFACE MAC-ADDRESS VRID PRIORITY INTERVAL VERSION V3-PROTOCOL SYNC-CONNECTION-TRACKING
0 RM vrrp-datos vlan10-datos 00:00:5E:00:02:0A 10 150 1s 3 ipv6 no
1 RM vrrp-dmz vlan30-dmz 00:00:5E:00:02:1E 30 150 1s 3 ipv6 no
2 RM vrrp-voz vlan20-voz 00:00:5E:00:02:14 20 150 1s 3 ipv6 no
[admin@CE1] > |
```

```
[admin@CE1-Backup] > /interface vrrp print
Flags: B - BACKUP
Columns: NAME, INTERFACE, MAC-ADDRESS, VRID, PRIORITY, INTERVAL, VERSION, V3-PROTOCOL, SYNC-CONNECTION-TRACKING
# NAME INTERFACE MAC-ADDRESS VRID PRIORITY INTERVAL VERSION V3-PROTOCOL SYNC-CONNECTION-TRACKING
0 B vrrp-datos vlan10-datos 00:00:5E:00:02:0A 10 100 1s 3 ipv6 no
1 B vrrp-dmz vlan30-dmz 00:00:5E:00:02:1E 30 100 1s 3 ipv6 no
2 B vrrp-voz vlan20-voz 00:00:5E:00:02:14 20 100 1s 3 ipv6 no
```

Figura 4.8: Estado de los VRRP en el router CE1

Al ejecutar el comando, en el CE1, se puede observar que están las letras R y M que significan que están en *RUNNING* y *MASTER* respectivamente, confirmando que es el router maestro de VRRP. Además, se puede ver que el Priority es 150, es decir, que tiene más prioridad que el router CE1_Backup que tiene el Priority en 100. Otra prueba que se hizo es apagar temporalmente la interfaz VLAN 10 del router CE1 y se puede ver que el router CE1_Backup se convierte en maestro en esta interfaz, siendo anterior el maestro. En la Figura 4.9 se puede ver el estado de los VRRP en el router CE1_Backup.

```
[admin@CE1-Backup] > /interface vrrp print
Flags: B - BACKUP
Columns: NAME, INTERFACE, MAC-ADDRESS, VRID, PRIORITY, INTERVAL, VERSION, V3-PROTOCOL, SYNC-CONNECTION-TRACKING
# NAME INTERFACE MAC-ADDRESS VRID PRIORITY INTERVAL VERSION V3-PROTOCOL SYNC-CONNECTION-TRACKING
0 B vrrp-datos vlan10-datos 00:00:5E:00:02:0A 10 100 1s 3 ipv6 no
1 B vrrp-dmz vlan30-dmz 00:00:5E:00:02:1E 30 100 1s 3 ipv6 no
2 B vrrp-voz vlan20-voz 00:00:5E:00:02:14 20 100 1s 3 ipv6 no
[admin@CE1-Backup] > |
```

```
[admin@CE1-Backup] > /interface vrrp print
Flags: R - RUNNING; M - MASTER, B - BACKUP
Columns: NAME, INTERFACE, MAC-ADDRESS, VRID, PRIORITY, INTERVAL, VERSION, V3-PROTOCOL, SYNC-CONNECTION-TRACKING
# NAME INTERFACE MAC-ADDRESS VRID PRIORITY INTERVAL VERSION V3-PROTOCOL SYNC-CONNECTION-TRACKING
0 RM vrrp-datos vlan10-datos 00:00:5E:00:02:0A 10 100 1s 3 ipv6 no
1 B vrrp-dmz vlan30-dmz 00:00:5E:00:02:1E 30 100 1s 3 ipv6 no
2 B vrrp-voz vlan20-voz 00:00:5E:00:02:14 20 100 1s 3 ipv6 no
```

Figura 4.9: Estado de los VRRP en el router CE1_Backup

Otra comprobación, como se muestra en la Figura 4.10, es la correcta asignación de direcciones IPv6 y conectividad con la interfaz VRRP de cada VLAN. En la izquierda un teléfono en la VLAN 20 y en la derecha un PC en la VLAN 10.

```

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2016, Computer Worms Team Corporation
C:\Users\Ernesto>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : lan9.cs
IPv6 Address . . . . . : 2001:db8:1234:101::809d
  Primary IPv6 Address . . . . . : 2001:db8:1234:101:a991:c6a1:809d:a47:5b9c
  Link-local IPv6 Address . . . . . : fe80::15b3:7c5e:348:4f55%11
  Autoconfiguration IPv4 Address . . . . . : 169.254.79.85
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : fe80::e7e:0ff:fe89:0%11

C:\Users\Ernesto>ping 2001:db8:1234:101::2 -4
Pinging 2001:db8:1234:101::2 with 32 bytes of data:
Reply from 2001:db8:1234:101::2: time=3ms
Reply from 2001:db8:1234:101::2: time=3ms
Reply from 2001:db8:1234:101::2: time=6ms
Reply from 2001:db8:1234:101::2: time=5ms

Ping statistics for 2001:db8:1234:101::2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 5ms

root@PC-Docker-1:/# ip -c addr show dev eth0
31: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
  state UNKNOWN group default qlen 1000
    link/ether 02:42:ec:6a:18:00 brd ff:ff:ff:ff:ff:ff
    inet6 2001:db8:1234:100::93ae/128 scope global dynamic
      valid_lft 597sec preferred_lft 372sec
    inet6 fe80::42:ecff:fe6a:1800/64 scope link
      valid_lft forever preferred_lft forever
root@PC-Docker-1:/# ping6 2001:db8:1234:100::2 -c 4
PING 2001:db8:1234:100::2(2001:db8:1234:100::2) 56 data bytes
64 bytes from 2001:db8:1234:100::2: icmp_seq=1 ttl=64 time=11.8 ms
64 bytes from 2001:db8:1234:100::2: icmp_seq=2 ttl=64 time=4.28 ms
64 bytes from 2001:db8:1234:100::2: icmp_seq=3 ttl=64 time=6.36 ms
64 bytes from 2001:db8:1234:100::2: icmp_seq=4 ttl=64 time=3.69 ms

--- 2001:db8:1234:100::2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 3.691/6.535/11.804/3.199 ms
root@PC-Docker-1:/#

```

Figura 4.10: Asignación y conectividad IPv6

Además, si desde un host se pide otra dirección IPv6, se puede ver que se obtiene una dirección ofrecida por el relay DHCPv6. En la Figura 4.11 se puede ver que un host de la VLAN 10 obtiene la dirección 2001:db8:1234:100::93ae.

```

dhcpv6
No. Time Source Destination Protocol Length Info
28 13.6. fe80::42:ecff:fe6a:1800 ff02::1:2 DHCPv6 146 Confirm XID: 0xc2f17c CID: 000100012ff845c10242ec6a1800 IAA: 2001:db8:1234:100::93ae
29 13.6. fe80::e7e:ffff:fe89:0 fe80::42:ecff:fe6a:1800 DHCPv6 108 Reply XID: 0xc2f17c CID: 000100012ff845c10242ec6a1800
55 24.5. fe80::42:ecff:fe6a:1800 ff02::1:2 DHCPv6 146 Confirm XID: 0xd2edeb CID: 000100012ff845c10242ec6a1800 IAA: 2001:db8:1234:100::93ae
56 24.5. fe80::e7e:ffff:fe89:0 fe80::42:ecff:fe6a:1800 DHCPv6 108 Reply XID: 0xd2edeb CID: 000100012ff845c10242ec6a1800
68 29.9. fe80::42:ecff:fe6a:1800 ff02::1:2 DHCPv6 164 Renew XID: 0xf9eb3e CID: 000100012ff845c10242ec6a1800 IAA: 2001:db8:1234:100::93ae
69 29.9. fe80::e7e:ffff:fe89:0 fe80::42:ecff:fe6a:1800 DHCPv6 195 Reply XID: 0xf9eb3e CID: 000100012ff845c10242ec6a1800 IAA: 2001:db8:1234:100::93ae

root@PC-Docker-1:/# ip -6 addr del 2001:db8:1234:100::93ae/128 dev eth0
root@PC-Docker-1:/# dhclient -6 -v eth0
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on Socket/eth0
Sending on Socket/eth0
PRC: Confirming active lease (INIT-REBOOT).
KMT: Forming Confirm, 0 ms elapsed.
XMT: X-- IA_NA ec6:a:18:00
XMT: | X-- Confirm Address 2001:db8:1234:100::93ae
XMT: V IA_NA appended.
XMT: Confirm on eth0, interval 1040ms.
RCV: Reply message on eth0 from fe80::e7e:ffff:fe89:0.
RCV: X-- Server ID: 00:01:00:01:2f:f8:30:d9:02:42:4b:5f:b3:00
message status code Success.
PRC: Bound to lease 00:01:00:01:2f:f8:30:d9:02:42:4b:5f:b3:00.
root@PC-Docker-1:/#

```

Figura 4.11: Obtención de una dirección IPv6

4.2.2. Configuración de los switches

En la simulación se han utilizado tres switches: uno de distribución B.4.1 y dos de acceso. El switch de distribución se encarga de conectar los switches de acceso, uno a la red local B.4.2 y otro a la DMZ B.4.3. Los switches de acceso conectan los dispositivos finales a la red.

Se han configurado las VLANs en los switches para segmentar el tráfico de datos, voz y DMZ. Además, se ha implementado el protocolo Rapid Spanning Tree Protocol (RSTP), que permite una convergencia más rápida ante fallos de enlace en comparación con el STP tradicional.

Por otra parte, para aprovechar los enlaces redundantes entre los switches y aumentar el rendimiento de la red, se ha implementado EtherChannel utilizando el protocolo LACP (Link Aggregation Control Protocol). Esto permite agrupar múltiples enlaces físicos en un único enlace lógico, lo cual proporciona redundancia y balanceo de carga sin que los puertos se bloqueen por RSTP.

Para verificar el funcionamiento de RSTP, se ha utilizado el comando `show spanning-tree` en los switches, que muestra el estado de las VLANs y sus interfaces asociadas. Como ejemplo, desde el switch de acceso a la LAN, al ejecutar el comando `show spanning-tree vlan 10`, se obtiene lo que se muestra en la Figura 4.12, donde se puede ver que el protocolo RSTP está habilitado y funcionando adecuadamente, y que el Root Bridge de la VLAN 10 es el switch de distribución. También, el enlace hacia el Root Bridge se establece a través de la interfaz Port-channel4, correspondiente a un EtherChannel configurado con LACP, que se encuentra en estado Root Forwarding. Esto indica que el enlace lógico está activo y es utilizado como camino principal hacia el Root Bridge, sin necesidad de bloquear enlaces físicos. Luego, los demás puertos del switch aparecen en estado Designated Forwarding, lo que demuestra que están activos y conectan con los dispositivos finales. El hecho de que no existan puertos en estado de bloqueo confirma que EtherChannel está funcionando, evitando bucles sin que RSTP tenga que bloquear enlaces individuales.

```
SW_Acceso_LAN>show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
              Address     0c8b.67c0.0000
              Cost         3
              Port        65 (Port-channel4)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
              Address     0cd7.b9c7.0000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec

  Interface      Role Sts Cost      Prio.Nbr Type
  -----  -----
  Gi0/2          Desg FWD 4       128.3    P2p
  Gi0/3          Desg FWD 4       128.4    P2p
  Gi1/1          Desg FWD 4       128.6    P2p
  Gi1/2          Desg FWD 4       128.7    P2p
  Gi1/3          Desg FWD 4       128.8    P2p
  Gi2/0          Desg FWD 4       128.9    P2p
  Po4            Root FWD 3       128.65   P2p
```

Figura 4.12: Estado del protocolo Spanning Tree

4.2.3. Configuración del servidor DHCP

Para el servidor DHCP, se ha utilizado `isc-dhcp-server` sobre un contenedor Docker basado en Ubuntu 20.04, con una configuración automatizada mediante un Dockerfile B.2.4.1. El servidor se ha configurado con una IP estática `2001:db8:1234:0102::132/64` y se han definido rangos de direcciones IP para cada segmento de red, asegurando que los dispositivos conectados reciban direcciones válidas según el segmento al que pertenezcan. El archivo de configuración principal se encuentra en `/etc/dhcp/dhcpd6.conf` B.2.4.2, donde se especifican los tiempos de concesión, las opciones de dominio y servidores DNS, así como las subredes correspondientes. Para las VLANs se han definido los siguientes rangos de direcciones IPv6:

- **Red de datos:** rango `2001:db8:1234:0100::2` a `2001:db8:1234:0100::ffff`.
- **Red de voz:** rango `2001:db8:1234:0101::2` a `2001:db8:1234:0101::ffff`.
- **DMZ:** no se ha configurado DHCP, ya que los dispositivos en esta red tienen direcciones estáticas.

Por otro lado, el archivo `isc-dhcp-server` se especifica la interfaz de red que utilizará el servidor DHCP para escuchar las solicitudes de los clientes. En este caso, se ha configurado para que escuche en la interfaz `eth0`, por lo que se ha añadido la siguiente línea al archivo de configuración: `INTERFACESv6="eth0"`

4.2.4. Configuración de los servidores DNS

Para la infraestructura DNS, se han implementado dos servidores DNS utilizando `bind9` en contenedores Docker, uno como servidor primario y otro como secundario, ambos basados en Ubuntu 20.04. La configuración de los servidores DNS se ha realizado de manera que se garantice la alta disponibilidad y la resolución de nombres de dominio para la red local.

Servidor DNS primario

El servidor DNS primario se va a configurar con la IP `2001:db8:1234:0102::133/64`. El archivo de configuración principal de `bind9` se encuentra en `/etc/bind/named.conf.options` B.2.5.2. Aquí se especifica que el servidor escuchará únicamente en IPv6, se define el rango de direcciones IP autorizadas para consultas y transferencias, se configuran los servidores de reenvío para consultas externas, y se habilita la recursión para las redes autorizadas. Además, se habilita la validación DNSSEC para mejorar la seguridad de las respuestas DNS.

Por otro lado, en `/etc/bind/named.conf.local` B.2.5.3 se configuran las zonas DNS. Este archivo define dos zonas: una zona directa para el dominio `cazg.es` y una zona inversa para la red de servicios `2001:db8:1234:0102::/64`. La zona directa permite resolver nombres de dominio a direcciones IP, mientras que la zona inversa permite resolver direcciones IP a nombres de dominio. En ambas zonas, se especifica el servidor de nombres primario (`ns1.cazg.es`) y se permite la transferencia de zona al servidor secundario (`ns2.cazg.es`) para garantizar la sincronización de la información entre ambos servidores.

Por otro lado, el archivo de zona directa `/etc/bind/zones/db.cazg.es` B.2.5.4 contiene la configuración de los registros DNS para el dominio `cazg.es`. Se define el registro SOA (Start of Authority) que indica el servidor de nombres principal para el dominio, así como los registros NS (Name Server) que especifican los servidores de nombres autoritativos para el dominio. También se incluyen registros AAAA para los servidores DNS y el servidor DHCP, que permiten la resolución de nombres a direcciones IPv6.

El archivo de zona inversa `/etc/bind/zones/db.2001.db8.1234.0102` B.2.5.5 se define el registro SOA que indica el servidor de nombres principal para la zona inversa, así como los registros NS que especifican los servidores de nombres autoritativos para la zona. También se incluyen registros PTR (Pointer) que permiten la resolución inversa de direcciones IPv6 a nombres de dominio, facilitando la identificación de los servidores DNS y el servidor DHCP en la red de servicios.

Servidor DNS secundario

El servidor DNS secundario va a tener la IP estática `2001:db8:1234:0102::134/64` y la configuración es similar a la del servidor primario, pero se debe especificar que es un servidor esclavo y se debe indicar la IP del servidor primario para las transferencias de zona.

El archivo de configuración principal /etc/bind/named.conf.options B.2.6.2 se especifica que el servidor escuchará únicamente en IPv6, se define el rango de direcciones IP autorizadas para consultas, se configuran los servidores de reenvío para consultas externas, y se habilita la recursión para las redes autorizadas. Además, se habilita la validación DNSSEC para mejorar la seguridad de las respuestas DNS.

Las zonas DNS se definen en el archivo /etc/bind/named.conf.local B.2.6.3. En este archivo, se configuró como un esclavo para las zonas directas e inversas, y se especifica la IP del servidor primario para las transferencias de zona. El archivo de zona directa db.cazg.es y el archivo de zona inversa db.2001.db8.1234.0102 serán idénticos a los del servidor primario, ya que el servidor secundario replicará la información de las zonas desde el primario.

NOTA:

Para que los servidores DNS y DHCP puedan comunicarse con los dispositivos de la red en GNS3 se ha creado una red personalizada de Docker llamada services_.net que permite la comunicación entre los contenedores y los dispositivos de la red. Esta red se ha configurado con el controlador bridge y se ha habilitado IPv6 para permitir la comunicación con las direcciones IPv6 de la red.

4.2.5. Configuración de los hosts

Para los dispositivos finales de acceso a la red se ha creado un contenedor Docker personalizado basado en Debian Bookworm [38] que actúa como PC de prueba para realizar comprobaciones de conectividad y funcionalidad de red en el entorno de simulación. Esta decisión se tomó debido a las limitaciones de recursos computacionales del equipo de desarrollo, ya que los contenedores Docker consumen significativamente menos recursos hardware comparado con máquinas virtuales completas.

El contenedor se ha configurado con privilegios elevados para permitir la manipulación de interfaces de red y se ha habilitado explícitamente IPv6 mediante la configuración de parámetros del kernel. El Dockerfile B.2.7.1 incluye múltiples herramientas de red esenciales para realizar pruebas exhaustivas de conectividad y diagnóstico.

El script de entrada (entrypoint.sh) B.2.7.2 configura automáticamente los servidores DNS al arranque del contenedor, estableciendo los servidores DNS primario y secundario de la red de servicios.

Esta configuración permite que el contenedor pueda resolver nombres de dominio desde el inicio, facilitando las pruebas de conectividad y la verificación del funcionamiento de los servicios DNS. El contenedor se mantiene activo ejecutando bash, permitiendo realizar pruebas interactivas y comandos de diagnóstico de red. Se puede desplegar fácilmente utilizando Docker Compose B.2.7.3, lo que simplifica su gestión y permite su integración con el entorno de simulación de GNS3, proporcionando una herramienta versátil para realizar pruebas exhaustivas de la funcionalidad de red, incluyendo la verificación de conectividad IPv6, resolución DNS, asignación DHCP y análisis de tráfico de red.

4.3. Simulación entre sedes remotas y red ISP

Para este caso, se ha intentado realizar una simulación completa de la red, sin embargo, debido a las limitaciones de recursos computacionales del equipo de desarrollo, no se ha podido simular completamente la red. Por lo tanto, se ha usado la red de la Oficina Central y se ha conectado a una red ISP simplificada basada en L3 MPLS VPN conectada a otra sede de la empresa, en este caso, la sede de San Cristóbal. En la Figura 4.13 se puede ver la topología de la red de esta simulación.

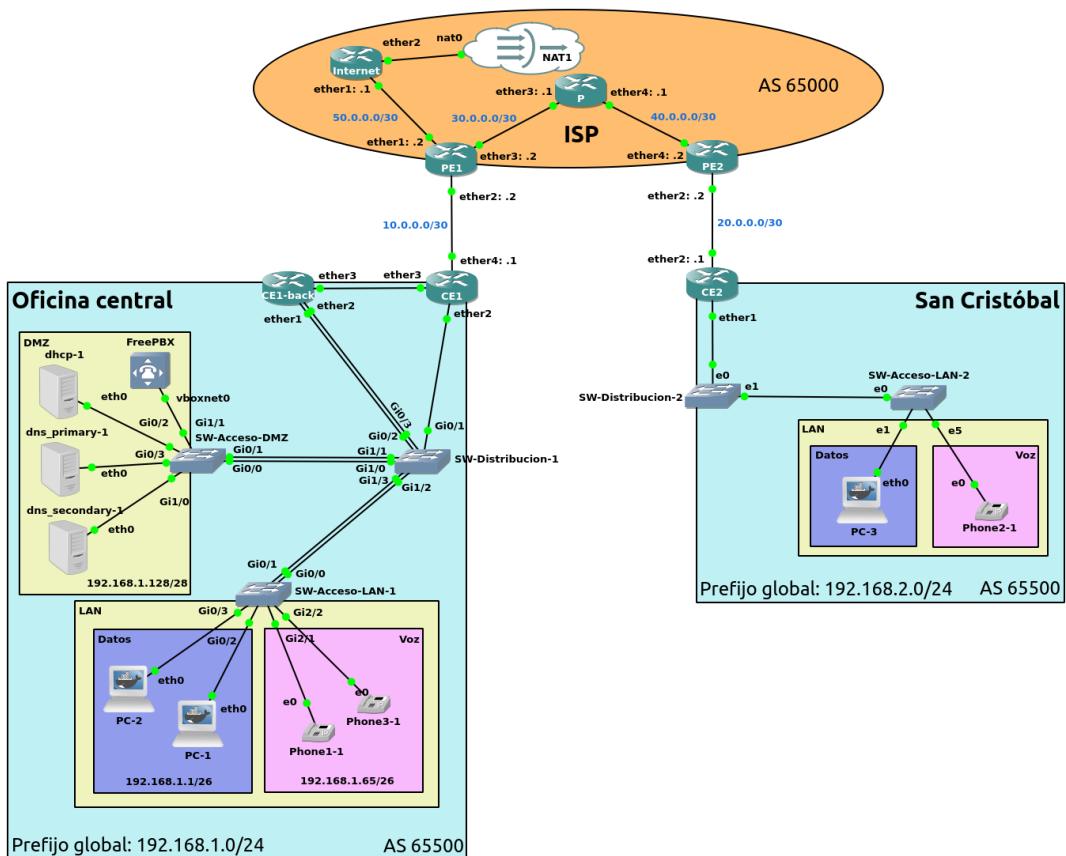


Figura 4.13: Simulación de la red completa

Para la red ISP se ha tomado como referencia la topología L3 MPLS VPN del Trabajo de Fin de Grado de D. Carpio Ortiz [39], adaptándola a los requisitos de la simulación. Se han empleado cuatro routers MikroTik (PE1, PE2, P y un router conectado a una Cloud de GNS3), configurados de forma similar a lo descrito en la sección 4.1. Además, se ha seguido el esquema de direccionamiento de la Tabla 4.3 para asignar la red MPLS.

Para completar la simulación, se ha centralizado el acceso a Internet a través de la Oficina Central. De este modo, todo el tráfico externo generado por los hosts de las sedes remotas (por ejemplo, San Cristóbal) no se dirige directamente fuera de su propia sede, sino que primero es redirigido a la Oficina Central. Allí, el router CE1 actúa como puerta de enlace principal, aplicando NAT al tráfico saliente. La configuración correspondiente en el router CE1 es la siguiente:

```
[admin@CE1] > /ip firewall nat add action=masquerade chain=srcnat dst-address=!192.168.0.0/16
out-interface=ether4
```

Router	Interfaz	Dirección IP
CE1	Lo0	192.170.0.1/32
	ether1	10.0.0.1/30
	ether2	192.168.1.1/30
	ether3	10.0.0.14/30
PE1	Lo0	192.170.0.2/32
	ether1	10.0.0.2/30
	ether2	30.0.0.2/30
	ether3	50.0.0.1/30
P	Lo0	192.170.0.3/32
	ether1	30.0.0.1/30
	ether2	40.0.0.1/30

Router	Interfaz	Dirección IP
PE2	Lo0	192.170.0.4/32
	ether1	40.0.0.2/30
	ether2	20.0.0.2/30
CE2	Lo0	192.170.0.5/32
	ether1	20.0.0.1/30
	ether2	192.168.2.1/30
Internet	Lo0	192.170.0.1/32
	ether1	50.0.0.2/30
	ether2	DHCP

Tabla 4.3: Esquema de direccionamiento para la red MPLS

Esta regla de NAT se aplica a todo el tráfico que sale por la interfaz ether4 (que está conectada a la red ISP) y que no tiene como destino una dirección de la red interna (192.168.0.0/16). Esto asegura que todo el tráfico de salida a Internet desde las sedes remotas sea enmascarado con la dirección IP pública del router CE1, permitiendo que los hosts de las sedes remotas puedan acceder a Internet a través de la Oficina Central. Además, se ha añadido una ruta estática para dirigir el tráfico hacia el router PE1 de la red ISP para que pueda salir a Internet.

```
[1] [admin@CE1] > /ip route add gateway=10.0.0.2
```

En la Figura 4.14 se puede ver el resultado de un traceroute desde un PC en la sede San Cristóbal a un servidor de Google (8.8.8.8) donde se puede observar que el tráfico sale de la LAN de la sede remota, atraviesa el router CE2, luego viaja por la red backbone MPLS (VPN L3) hasta llegar al router CE1 en la Oficina Central, donde se reenvía al router PE1, que es el punto de salida hacia el ISP. Finalmente, el tráfico atraviesa el router de frontera a Internet y accede a la nube (Internet).

```
root@PC-3:/# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.2.1 (192.168.2.1)  6.376 ms  7.005 ms  7.022 ms
 2  20.0.0.2 (20.0.0.2)  15.519 ms  15.537 ms  15.694 ms
 3  * *
 4  10.0.0.1 (10.0.0.1)  27.453 ms  27.525 ms  27.703 ms
 5  10.0.0.2 (10.0.0.2)  37.066 ms  37.105 ms  37.186 ms
 6  50.0.0.2 (50.0.0.2)  44.222 ms  39.523 ms  39.679 ms
 7  192.168.122.1 (192.168.122.1)  45.186 ms  37.602 ms  37.862 ms
 8  192.168.1.1 (192.168.1.1)  38.313 ms  26.762 ms  26.798 ms
 9  192.0.0.1 (192.0.0.1)  66.050 ms  57.616 ms  60.812 ms
10  10.255.116.13 (10.255.116.13)  60.868 ms  53.780 ms  50.605 ms
11  10.34.216.141 (10.34.216.141)  50.394 ms  47.494 ms *
12  193.251.247.13 (193.251.247.13)  47.069 ms  52.545 ms  52.038 ms
13  74.125.48.64 (74.125.48.64)  52.026 ms  72.14.204.60 (72.14.204.60)  69.836 ms  72.14.209.130 (72.14.209.130)  68.733 ms
14  142.251.231.147 (142.251.231.147)  65.673 ms  192.178.110.157 (192.178.110.157)  66.925 ms  192.178.110.155 (192.178.110.155)  69.494 ms
15  74.125.37.87 (74.125.37.87)  67.062 ms  142.251.60.115 (142.251.60.115)  66.878 ms  74.125.253.201 (74.125.253.201)  67.219 ms
16  8.8.8.8 (8.8.8.8)  66.545 ms  61.136 ms  61.272 ms
```

Figura 4.14: Resultado de un traceroute desde un PC San Cristóbal a Internet

Por otro lado, las sedes tienen direccionamiento IPv4 para simplificar la simulación ya que los routers MikroTik tienen algunas limitaciones con IPv6, como la falta de soporte para trabajar con MPLS. Por lo tanto, la Oficina Central tendrá una configuración similar a la que se realizó anteriormente, pero con direccionamiento IPv4 con un prefijo 192.168.1.0/24. Para los servidores de red, se han creado contenedores Docker personalizados para el

servicio DHCP y para el servicio DNS, con una configuración similar a la utilizada en la simulación de la Oficina Central, pero adaptada a direccionamiento IPv4. En los apéndices B.3.2 y B.3.3 se puede consultar la configuración detallada de cada uno de estos servicios. En cuanto a los switches de la Oficina Central, se ha utilizado los de la simulación de la Oficina Central y con la misma configuración.

En cuanto a la sede de San Cristóbal se ha realizado una configuración básica, donde se ha usado un router MikroTik identificado como CE2 B.3.4 con un prefijo 192.168.2.0/24 y se ha usado switches ethernet de GNS3 para hacer una configuración sencilla de VLANs y conectividad. En la figura 4.15 se puede ver la configuración de los switches de la sede de San Cristóbal.

Port	VLAN	Type
0	1	dot1q
1	1	dot1q
2	1	access
3	1	access
4	1	access
5	1	access

Port	VLAN	Type
0	1	dot1q
1	10	access
2	1	access
3	1	access
4	1	access
5	20	access

(a) Switch de distribución de San Cristóbal

(b) Switch de acceso de San Cristóbal

Figura 4.15: Configuración de los switches de la sede de San Cristóbal

En esta sede se ha configurado en el propio router CE2 un servidor DHCP (para simplificar la configuración), que asigna las direcciones IP a los dispositivos de la red. Para ello, se ha creado un pool de direcciones IP para cada VLAN y se ha configurado el servidor para que asigne direcciones IP dentro de estos pools. Además, se ha configurado el gateway para cada VLAN.

```

1 # Pool de direcciones DHCP
2 /ip pool add name=pool_datos ranges=192.168.2.2-192.168.2.30
3 /ip pool add name=pool_voz ranges=192.168.2.34-192.168.2.62
4
5 # Servidor DHCP para VLAN 10 (Datos)
6 /ip dhcp-server add name=dhcp_datos interface=vlan10-datos address-pool=pool_datos disabled=no
7 /ip dhcp-server network add address=192.168.2.0/26 gateway=192.168.2.1
8
9 # Servidor DHCP para VLAN 20 (Voz)
10 /ip dhcp-server add name=dhcp_voz interface=vlan20-voz address-pool=pool_voz disabled=no
11 /ip dhcp-server network add address=192.168.2.32/26 gateway=192.168.2.33

```

Por último, para la conectividad de los dispositivos finales, se han creado contenedores Docker personalizados que actúan como PCs de prueba, parecidos a los utilizados en la Oficina Central pero para funcionar en IPv4. Además, como softphone se ha usado una máquina virtual ligera que viene instalada con algunas aplicaciones VoIP, obtenida de un tutorial de Youtube de C. E. Carrillo Arellano [40]. En esta máquina virtual viene instalado algunos softphones como Zoiper y Microsip y se ha configurado para que se pueda usar en la VLAN de voz. Para la centralita de telefonía IP se ha instalado FreePBX en una máquina

virtual en VirtualBox y se ha configurado con una IP estática 192.168.1.135 y se ha conectado en la DMZ de la Oficina Central. Para simplificar la configuración, esta centralita se ha configurado para que pueda gestionar las llamadas entre los teléfonos IP de la Oficina Central y se han creado dos extensiones para comprobar la comunicación entre los teléfonos IP de esta sede. En la Figura 4.16 se puede ver la comprobación de la VoIP, donde se puede ver que se ha realizado una llamada entre dos teléfonos IP y se ha establecido la comunicación correctamente.

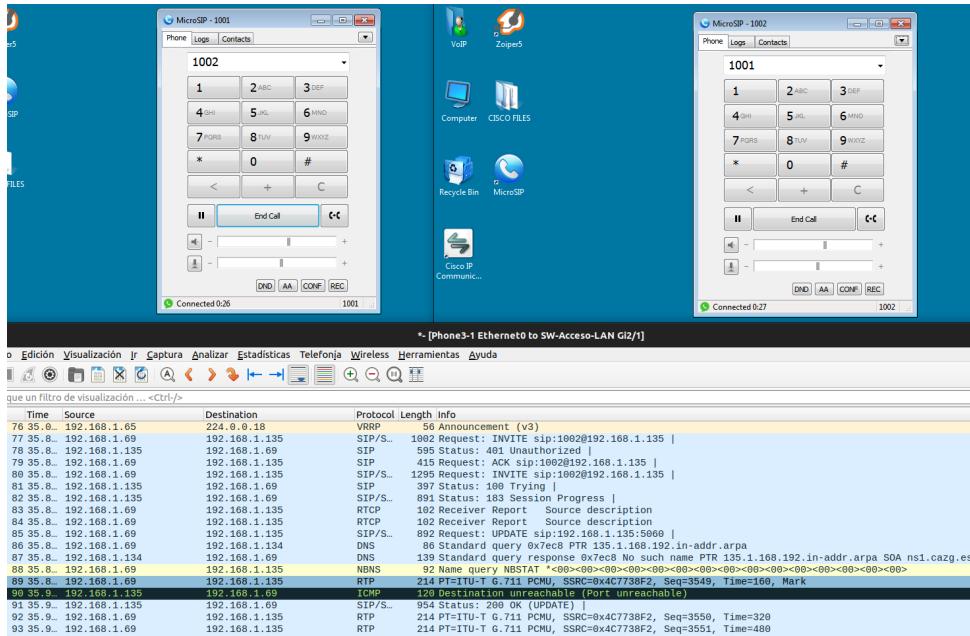


Figura 4.16: Comprobación de la VoIP sobre IPv4

4.4. Laboratorio

En esta sección se describe la prueba que se realizó en el laboratorio efectuada para comprobar la comunicación entre dos teléfonos IP utilizando dispositivos físicos. Para ello, se emplearon un router MikroTik RB2011UiAS-RM, switches TP-Link T2500G-10TS y teléfonos IP Grandstream GRP2601. Los servicios de red DHCP y DNS se implementaron de forma simulada mediante GNS3 y se han usado los mismos contenedores que se han usado para las simulación de la red completa 4.3. Estos contendores se estarán ejecutando en un ordenador físico (PC1) del laboratorio siguiendo el esquema de la Figura 4.17.

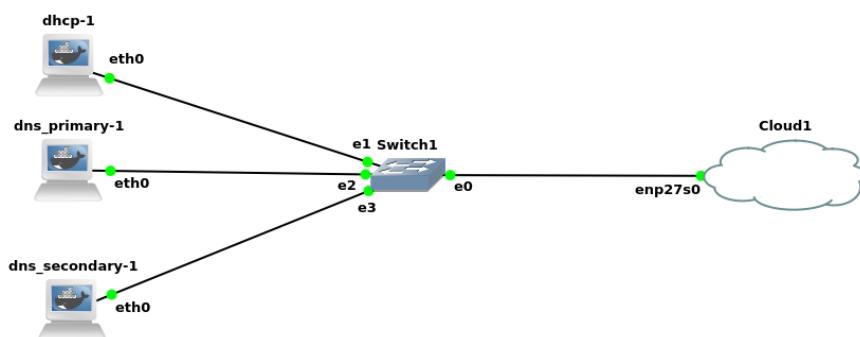


Figura 4.17: Servicios de red utilizados en el laboratorio

Además, se ha usado otro ordenador físico (PC2) para operar como la centralita FreePBX y se ha ejecutado un contenedor Docker con la imagen de FreePBX, y en este PC se ha configurado con una IP estática 192.168.1.135. El docker-compose para la centralita que se ha usado se encuentra en el apéndice B.5. En la Figura 4.18 se muestra la interconexión que se ha realizado en el laboratorio.

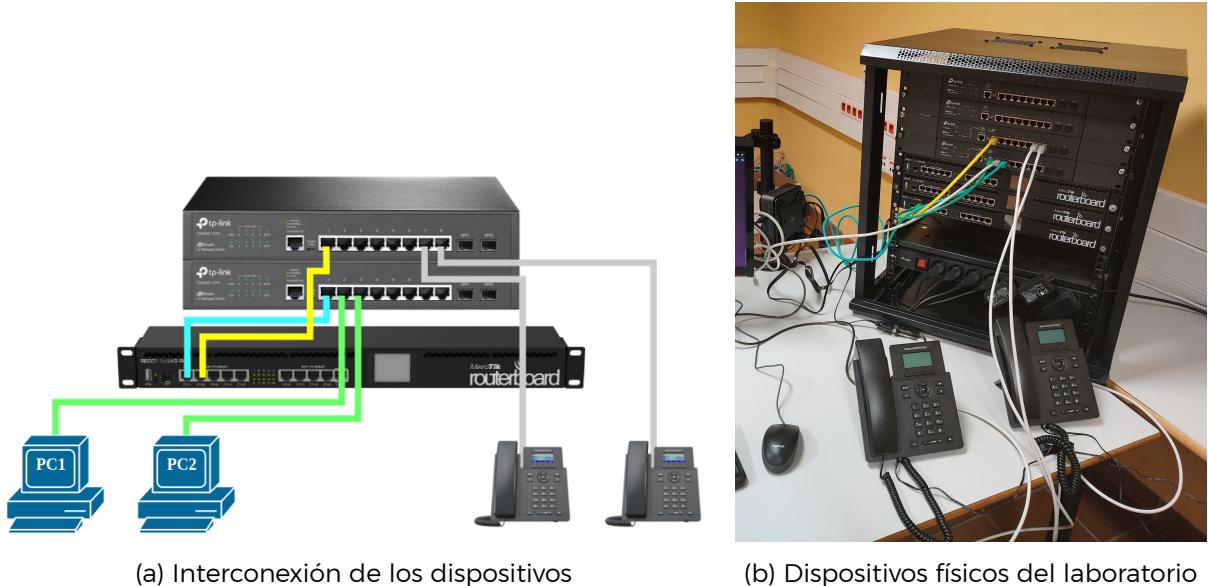


Figura 4.18: Interconexión de red y dispositivos físicos utilizados en el laboratorio

Por otro lado, en la centralita FreePBX se han creado dos extensiones, 1001 y 1002, destinadas al uso con teléfonos IP, como se muestra en la Figura 4.19. Estas extensiones permiten realizar y recibir llamadas dentro de la red local del sistema de telefonía.

	Extension	Name	CW	DND	FM/FM	CF	CFB	CFU	Type	Actions
<input type="checkbox"/>	1001	1001	<input checked="" type="checkbox"/>	<input type="checkbox"/>	pjsip					
<input type="checkbox"/>	1002	1002	<input checked="" type="checkbox"/>	<input type="checkbox"/>	pjsip					

Showing 1 to 2 of 2 rows

Figura 4.19: Extensiones configuradas en la centralita FreePBX

Para cada una de estas extensiones se ha configurado un buzón de voz, permitiendo que los usuarios dejen mensajes cuando no se puede atender una llamada. Esta funcionalidad resulta especialmente útil en entornos donde no siempre es posible responder inmediatamente. En la Figura 4.20 se muestra un ejemplo de esta configuración, correspondiente a la extensión 1001. Entre las opciones disponibles se encuentran la definición de la contraseña del buzón, el envío de mensajes por correo electrónico, y la posibilidad de reproducir el identificador de llamada (CID) y los datos del mensaje (fecha y hora).

The screenshot shows a web-based administrative interface for managing voicemail accounts. At the top, there is a navigation bar with links: Admin, Applications, Connectivity, Dashboard, Reports, Settings, and UCP. Below the navigation bar, the title "Voicemail" is displayed, followed by a sub-menu with tabs: Usage, Settings, Dialplan Behavior, and Timezone Definitions. The main content area is titled "Account View Links:" and contains three tabs: Account Settings (selected), Account Usage, and Account Advanced Settings. The "Account Settings" tab displays various configuration options for extension 1001:

Name	1001
Voicemail Password	1001
Email Address	[Empty]
Pager Email Address	[Empty]
Email Attachment	<input checked="" type="checkbox"/> yes <input type="checkbox"/> No
Play CID	<input checked="" type="checkbox"/> yes <input type="checkbox"/> No
Play Envelope	<input checked="" type="checkbox"/> yes <input type="checkbox"/> No
Delete Voicemail	<input checked="" type="checkbox"/> yes <input type="checkbox"/> No
Call-Me Number	1001

On the right side of the interface, there is a sidebar with two entries: "1001" and "1002".

Figura 4.20: Configuración del buzón de voz para la extensión 1001

Por último, los dispositivos conectados a la red obtienen sus direcciones IP mediante el protocolo DHCP, el cual se encuentra ejecutándose en el ordenador físico (PC1) del laboratorio.

Capítulo 5

Conclusiones y líneas futuras

El presente Trabajo de Fin de Grado ha permitido diseñar una infraestructura de red moderna y escalable cogiendo de referencia el pliego de proyectos del Consorcio de Aguas de la Zona Gaditana, centrada en la mejora de la conectividad, la seguridad y la integración de servicios en sus distintas sedes. A través del uso de tecnologías como SD-WAN, direccionamiento IPv6, telefonía IP y cortafuegos de nueva generación.

Durante el desarrollo del proyecto se ha realizado un análisis detallado de los requisitos técnicos y se ha diseñado una topología en estrella con una arquitectura de red jerárquica de tres capas (núcleo, distribución y acceso). Además, se han seleccionado los dispositivos de red, teniendo en cuenta su rendimiento, escalabilidad, compatibilidad y coste.

La simulación de la red mediante GNS3 ha servido para validar parcialmente el diseño propuesto, a pesar de las limitaciones técnicas de la herramienta frente a entornos reales basados en soluciones como Cisco Meraki.

A partir del trabajo realizado, se proponen las siguientes líneas de trabajo que pueden servir para mejorar el desarrollo y evolución del proyecto:

- **Implantación de sistemas en la nube:** implementar la centralita FreePBX en la plataforma Microsoft Azure, aprovechando la escalabilidad y disponibilidad que ofrece la nube. Además, se recomienda integrar Microsoft Sentinel como plataforma de respuesta ante incidentes, permitiendo la monitorización, detección y gestión centralizada de amenazas y eventos de seguridad relacionados con la telefonía IP y otros servicios críticos.
- **Automatización de la configuración de red:** usar herramientas como Ansible o scripts Python para automatizar el despliegue y configuración de routers y switches en la simulación.
- **Automatización y monitorización avanzada:** desplegar herramientas de monitorización complementarias como Zabbix para lograr una supervisión más detallada de los servicios y dispositivos no gestionados por Meraki.
- **Evaluación del rendimiento simulado y mejora continua:** realizar pruebas de estrés, análisis de tráfico y simulaciones de escenarios críticos en entornos virtuales como GNS3, con el objetivo de validar el diseño propuesto, optimizar su comportamiento teórico y detectar posibles debilidades en la arquitectura de red.

Capítulo 6

Summary and Conclusions

This Final Degree Project has enabled the design of a modern and scalable network infrastructure based on the project specifications of the Consorcio de Aguas de la Zona Gaditana, focused on improving connectivity, security and the integration of services at its various sites. Through the use of technologies such as SD-WAN, IPv6 addressing, IP telephony and new generation firewalls.

During the development of the project, a detailed analysis of the technical requirements has been carried out and a star topology has been designed with a hierarchical network architecture of three layers (core, distribution and access). In addition, network devices have been selected, taking into account their performance, scalability, compatibility and cost.

The simulation of the network using GNS3 has served to partially validate the proposed design, despite the technical limitations of the tool compared to real environments based on solutions such as Cisco Meraki.

Based on the work carried out, the following lines of work are proposed that can be used to improve the development and evolution of the project:

- **Implementation of systems in the cloud:** implement the FreePBX PBX on the Microsoft Azure platform, taking advantage of the scalability and availability offered by the cloud. In addition, it is recommended to integrate Microsoft Sentinel as an incident response platform, enabling centralised monitoring, detection and management of threats and security events related to IP telephony and other critical services.
- **Network configuration automation:** use tools such as Ansible or Python scripts to automate the deployment and configuration of routers and switches in the simulation.
- **Automation and advanced monitoring:** deploy complementary monitoring tools such as Zabbix for more detailed monitoring of services and devices not managed by Meraki.
- **Simulated performance evaluation and continuous improvement:** perform stress tests, traffic analysis and simulations of critical scenarios in virtual environments such as GNS3, in order to validate the proposed design, optimise its theoretical behaviour and detect possible weaknesses in the network architecture.

Capítulo 7

Presupuesto

En este capítulo se detalla los costes asociados al desarrollo del proyecto, incluyendo el tiempo estimado para cada tarea y el coste total del proyecto. Por lo que se refiere a gastos de hardware, software o licencias, no se han considerado ya que el proyecto se ha desarrollado utilizando herramientas de código abierto y simuladores que no requieren licencias. En cuanto al hardware utilizado, es el equipo personal que ya estaba disponible antes del inicio del proyecto.

7.1. Costes del proyecto

Para calcular los costes de personal, se ha considerado un salario anual de 28.000 euros brutos para un Ingeniero Informático Junior en España, con lo que el coste por hora sería de aproximadamente 15 euros brutos. Para el desarrollo del proyecto, se ha estimado un total de 300 horas de trabajo distribuidas en las siguientes tareas:

Tarea	Horas estimadas	Coste estimado (euros)
Investigación preliminar	20	150 €
Análisis de requisitos	20	300 €
Diseño de la red	40	600 €
Selección de hardware y software	20	300 €
Implementación en simuladores	100	1500 €
Pruebas y ajustes	50	750 €
Redacción de la memoria	50	600 €
Total	300	4200 €

Tabla 7.1: Costes de personal

El coste total del proyecto se muestra en la tabla 7.2.

Partida	Coste (euros)
Licencias de software	0 €
Amortización de equipos informáticos	72 €
Costes de personal	4200 €
Otros gastos	50 €
Subtotal	4322 €
IGIC	302,54 €
Total	4624,54 €

Tabla 7.2: Presupuesto.

Apéndice A

Instalación de programas necesarios

La instalación de los programas necesarios para el desarrollo de este Trabajo de Fin de Grado se ha realizado en un equipo con Ubuntu 22.04 LTS. Las características hardware del equipo son las siguientes:

- Procesador: AMD Ryzen 5 2600 Six-Core @ 12x 3,4GHz
- Tarjeta gráfica: NVIDIA GeForce RTX 2060
- Memoria RAM: 16 GB
- 256 GB SSD
- Sistema operativo: Ubuntu 22.04 LTS

A.1. Instalación y configuración de GNS3

Para instalar GNS3 se va a utilizar el gestor de paquetes de Ubuntu, apt.

```
1 sudo add-apt-repository ppa:gns3/ppa  
2 sudo apt update  
3 sudo apt install gns3-gui gns3-server
```

Una vez instalado GNS3 se comprobará que se ha instalado correctamente ejecutando el siguiente comando:

```
1 gns3 --version
```

y así se comprobará que se ha instalado correctamente. En este caso, la versión que se ha usado es la 2.2.54. Por otro lado, GNS3 permite la integración de imágenes QEMU/KVM para emular dispositivos de red. Para ello, es recomendable contar con soporte para **KVM** habilitado en el sistema. Esto mejora el rendimiento de las máquinas virtuales dentro de GNS3. Para hacer esta comprobación se va a utilizar el paquete `cpu-checker`. La instalación del mismo se hace con:

```
1 sudo apt install cpu-checker
```

Una vez instalado el paquete, se puede comprobar si el sistema tiene soporte para KVM ejecutando `kvm-ok`:

```
1 INFO: /dev/kvm exists  
2 KVM acceleration can be used
```

El resultado debería ser el que se muestra en pantalla. Si no es así, se debe habilitar la virtualización por hardware o que esté desactivada en la BIOS.

Para que todo funcione correctamente, se debe modificar los permisos del ejecutable `ubridge` para que pueda ser ejecutado por el usuario que ejecuta GNS3.

```
1 sudo chmod 755 /usr/bin/ubridge
```

Además, para poder hacer uso de las máquinas virtuales dentro del simulador hay que hacer funcionar KVM. La instalación de este componente se debió hacer al instalar GNS3. Sin embargo, para tener los permisos necesarios debemos añadir el usuario que ejecuta GNS3 al grupo kvm.

```
1 sudo adduser $USER kvm
```

Una vez hecho esto, se debe reiniciar el sistema para que los cambios surtan efecto. Una vez reiniciado el sistema, se puede iniciar GNS3 y comprobar que todo funciona correctamente.

A.2. Instalación de VirtualBox

Para instalar VirtualBox [41] se debe descargar el paquete de instalación desde la página oficial de VirtualBox para la versión del sistema operativo que se esté usando. En este caso, se está usando Ubuntu 22.04 LTS, por lo que se debe descargar el paquete de instalación para esta versión.

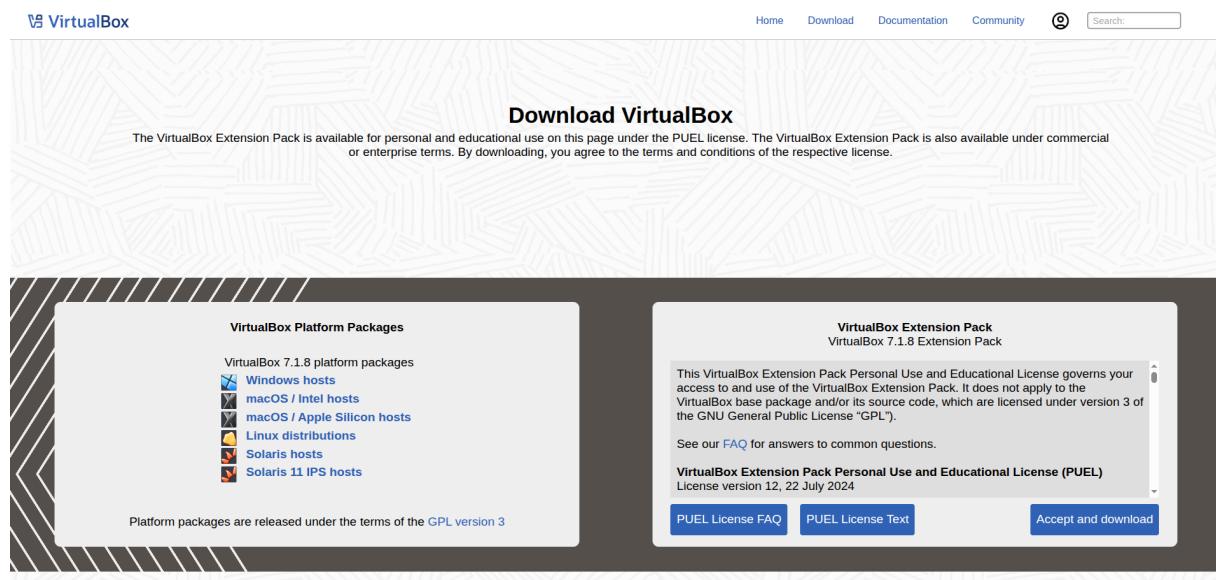


Figura A.1: Descarga de VirtualBox

Elegimos la opción de Download VirtualBox for Linux hosts, en este caso, y elegimos la distribución de Linux que se esté usando. En este caso, se está usando Ubuntu 22.04 LTS, por lo que se debe elegir la opción de Ubuntu 22.04 (64-bit).



Figura A.2: Descarga de VirtualBox

Una vez descargado el paquete, se debe instalar. Para ello, se debe abrir una terminal y navegar hasta la carpeta donde se ha descargado el paquete.

```
1 cd ~/Descargas
2 sudo dpkg -i virtualbox-7.1_7.1.8-168469~Ubuntu~jammy_amd64.deb
```

Si se produce algún error de dependencias, se puede solucionar ejecutando el siguiente comando:

```
1 sudo apt --fix-broken install
```

Una vez instalado VirtualBox, se puede comprobar que se ha instalado correctamente ejecutando el siguiente comando:

```
1 virtualbox --help
```

y así se comprobará que se ha instalado correctamente. En este caso, la versión que se ha usado es la 7.1.8.

A.2.1. Instalación FreePBX

Para instalar FreePBX [42], primero es necesario acceder a la página oficial y descargar el instalador correspondiente a la versión del sistema operativo que se esté utilizando. En la sección Download, se debe desplegar la opción View Previous Versions para seleccionar la versión deseada. En este caso, se ha descargado la imagen ISO de la versión SNG7-PBX16-64bit-2302-1, como se muestra en la figura A.3.

[▲ View Previous Versions](#)

FreePBX Distro Download Links

Below is a list of the different download versions and links to each one.

For older archived copies of the FreePBX Distro, click [here](#).

The links below are downloaded from our US Based Server.

64 BIT DOWNLOADS

SNG7-PBX16-64bit-2302-1
Release Date: February 2023
FreePBX 16 • Linux 7.8 • Asterisk 16, 18 or 19
Release Notes
This ISO can be written directly to a USB drive and installed without the need for any conversion tools.
FULL ISO SHA256 MD5SUM
HISTORICAL (End of Life) SNG7-PBX-64bit-1904
Release Date: May 2019
FreePBX 14 • Linux 7.6 • Asterisk 13 or 16 Supports UEFI and Legacy BIOS booting
This ISO can be written directly to a USB drive and installed without the need for any conversion tools.
FULL ISO SHA256 MD5SUM

STABLE SNG7-PBX-64bit-2203-2

Release Date: March 2022
FreePBX 15 • Linux 7.8 • Asterisk 13, 16 or 17 Supports UEFI and Legacy BIOS booting
Release Notes
This ISO can be written directly to a USB drive and installed without the need for any conversion tools.
FULL ISO SHA256 MD5SUM

Figura A.3: Descarga de FreePBX

Una vez descargado el paquete, se debe montar la imagen ISO en una máquina virtual de VirtualBox. Para ello, se debe crear una nueva máquina virtual en VirtualBox, seleccionamos Nueva y seleccionar la imagen ISO descargada como disco de arranque y se configura la máquina virtual con los siguientes parámetros:

- Nombre: FreePBX
- Tipo: Linux
- Versión: Red Hat (64-bit)
- Omitir instalación desatendida: No
- Memoria RAM: 1024 MB
- Procesador: 1 CPU
- Disco duro virtual: 20 GB

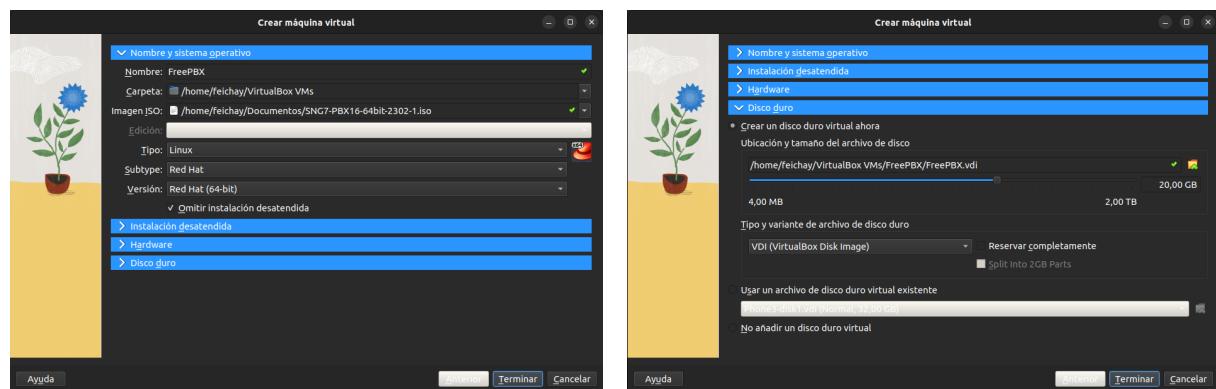


Figura A.4: Configuración de la máquina virtual para FreePBX

Una vez creada la máquina virtual, se debe configurar dos adaptadores de red. Pero antes, se debe crear un nuevo Adaptador solo anfitrión en VirtualBox, para ello ejecutamos el siguiente comando en la terminal:

```
1 sudo VBoxManage hostonly create
```

Esto creará un nuevo adaptador de red solo para el anfitrión. A continuación, se debe configurar los adaptadores de red para la máquina virtual FreePBX. Para ello, se debe seleccionar la máquina virtual creada y hacer clic en Configuración. En la sección Red, se debe seleccionar el adaptador Adaptador 1 y configurarlo de la siguiente manera:

- Habilitar adaptador de red: Sí
- Conectado a: Adaptador puente
- Nombre: <nombre de la interfaz de red del equipo>
- Promiscuo: Permitir todo
- Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)
- Dirección MAC: Dejar en blanco
- Cable conectado: Sí

A continuación, se debe configurar el Adaptador 2 de la siguiente manera:

- Habilitar adaptador de red: Sí
- Conectado a: Adaptador solo anfitrión
- Nombre: vboxnet0
- Promiscuo: Permitir todo
- Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)
- Dirección MAC: Dejar en blanco
- Cable conectado: Sí

Una vez creados los adaptadores de red, vamos a asignar una dirección IP al adaptador Adaptador sólo anfitrión creado anteriormente. Esto es para usar esta interfaz en la simulación de GNS3. Para ello, en la parte superior izquierda de la ventana de VirtualBox, donde aparece Herramientas le damos al botón de propiedades y seleccionamos la pestaña Red. Y una vez dentro de la pestaña, vemos el adaptador creado anteriormente, vboxnet0, y abajo de este configuraremos la dirección IP y la máscara de subred. En este caso, se ha configurado la dirección IP 192.168.1.135 y la máscara de subred 255.255.255.240.

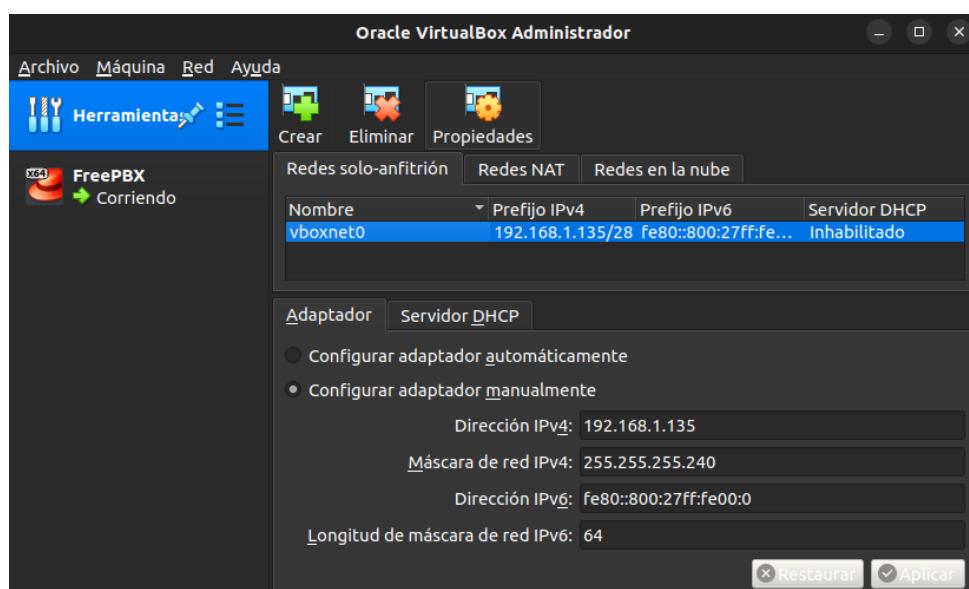


Figura A.5: Configuración de la red en VirtualBox

Una vez configurada la red, se debe iniciar la máquina virtual y seguir las instrucciones de instalación de FreePBX. Seleccionamos la primera opción y pulsamos Enter para iniciar la instalación. A continuación, saldrá FreePBX Standard y pulsamos Enter nuevamente para continuar con la instalación. Ya dentro de panel de configuración de FreePBX, hay que configurar el usuario y la contraseña para el usuario root. Para simplicidad, se ha configurado el usuario root con la contraseña root. Y esperamos a que se complete la instalación. Una vez completada la instalación, vamos a apagar la máquina virtual para eliminar el disco de instalación y arrancar desde el disco duro virtual.

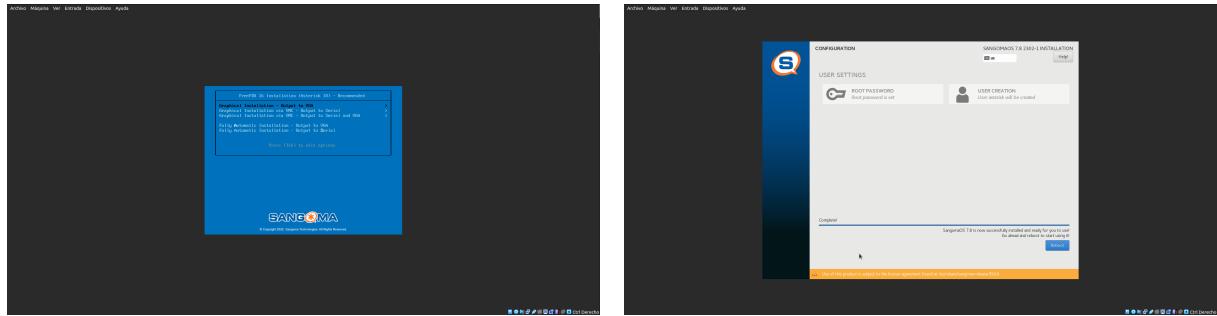


Figura A.6: Configuración de la máquina virtual para FreePBX

Para ello, vamos a la configuración de la máquina virtual y en la sección Almacenamiento eliminamos el disco de instalación como se muestra en la figura A.7.

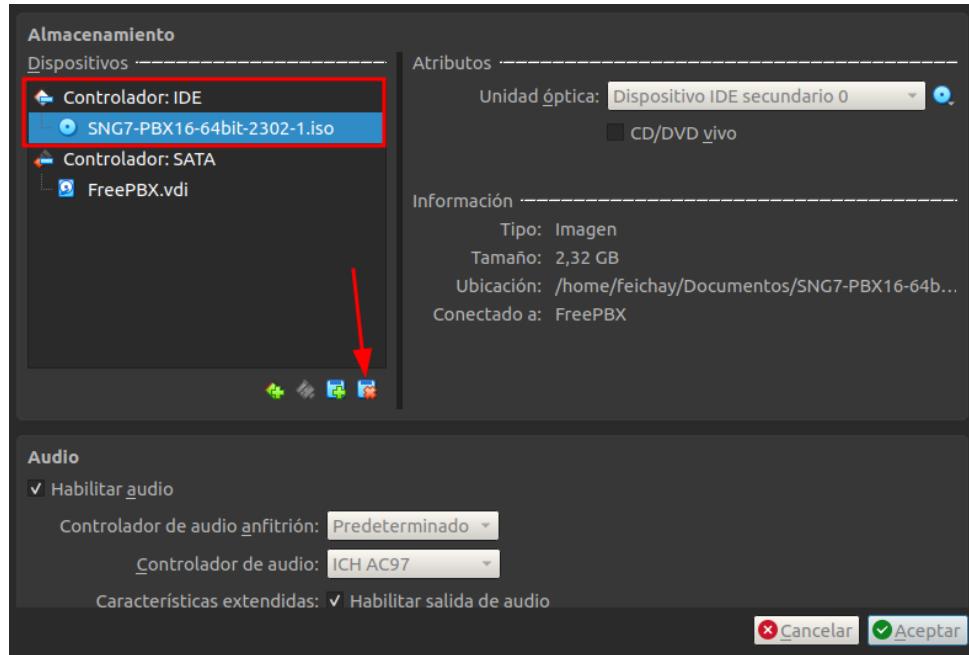


Figura A.7: Instalación de FreePBX

Una vez eliminado el disco de instalación, iniciamos la máquina virtual y accedemos al panel de configuración de FreePBX con la dirección IP que se le ha asignado a la máquina virtual. En la figura A.8 se muestra la dirección IP asignada a la máquina virtual, que en este caso es 192.168.1.31.

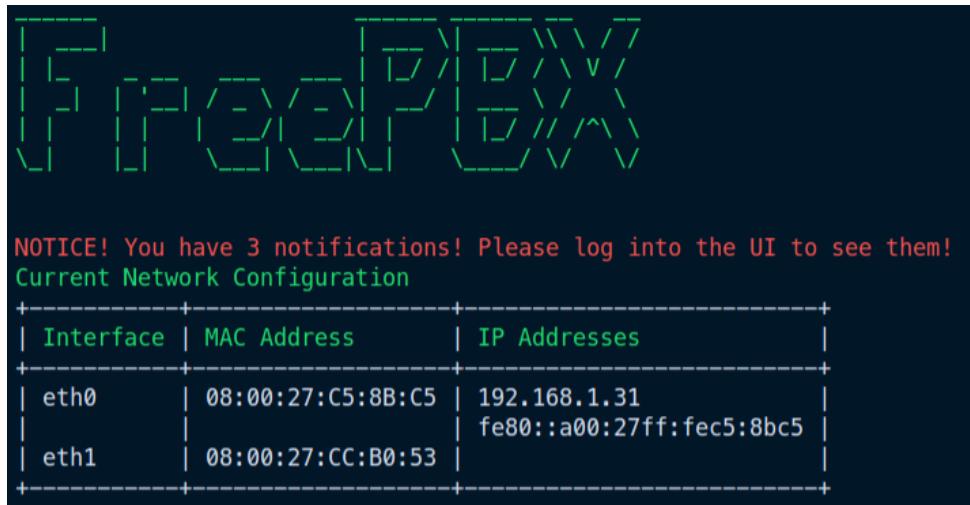


Figura A.8: Panel de configuración de FreePBX

Para acceder al panel de configuración de FreePBX, se debe abrir un navegador web y acceder a la dirección IP asignada a la máquina virtual. En este caso, se ha accedido a la dirección <http://192.168.1.31/admin>. Una vez accedido al panel de configuración, se debe de crear el usuario administrador. Para simplificar, se ha creado el usuario admin con la contraseña admin.

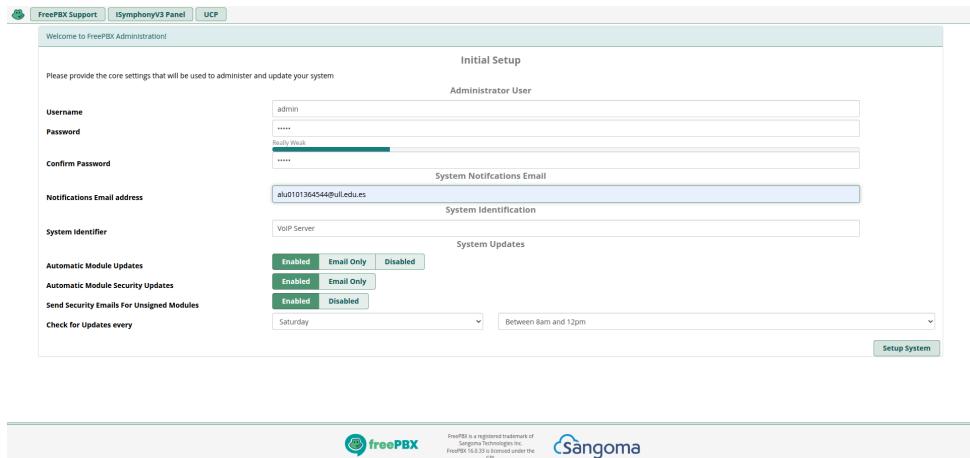


Figura A.9: Configuración de FreePBX

A.2.2. Instalacion Softphone

Para la simulación de telefonos IPs en GNS3, se ha utilizado una máquina virtual ligera con el sistema operativo Windows 7 obtenido de un video tutorial de Youtube [40] de Método para simular redes VoIP en GNS3. Para instalar la máquina virtual, se ha descargado desde el enlace que proporciona el video tutorial y se ha importado a VirtualBox como un disco duro virtual en formato .vdi con el sistema operativo Windows 7 instalado y ya configurado.

Para importar la máquina virtual, se debe abrir VirtualBox y seleccionar Nueva para crear una nueva máquina virtual. Se debe poner un nombre, por ejemplo Phone1, seleccionar el tipo de sistema operativo, Windows, y la versión como Windows 7 (64-bit).

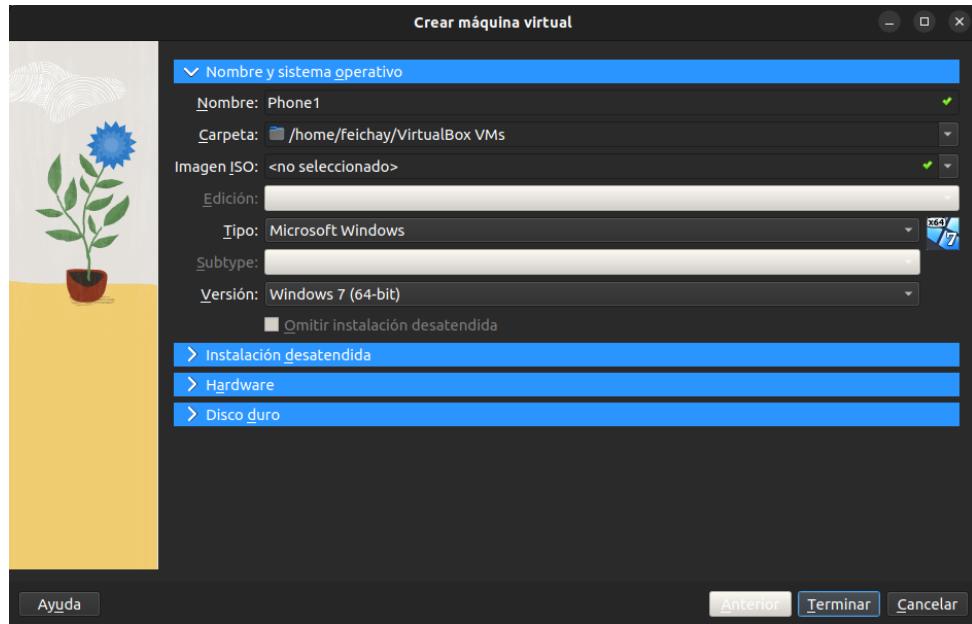


Figura A.10: Configuración de la máquina virtual para Softphone

Luego, se debe asignar una cantidad de memoria RAM (256 MB es suficiente) y 1 CPU.

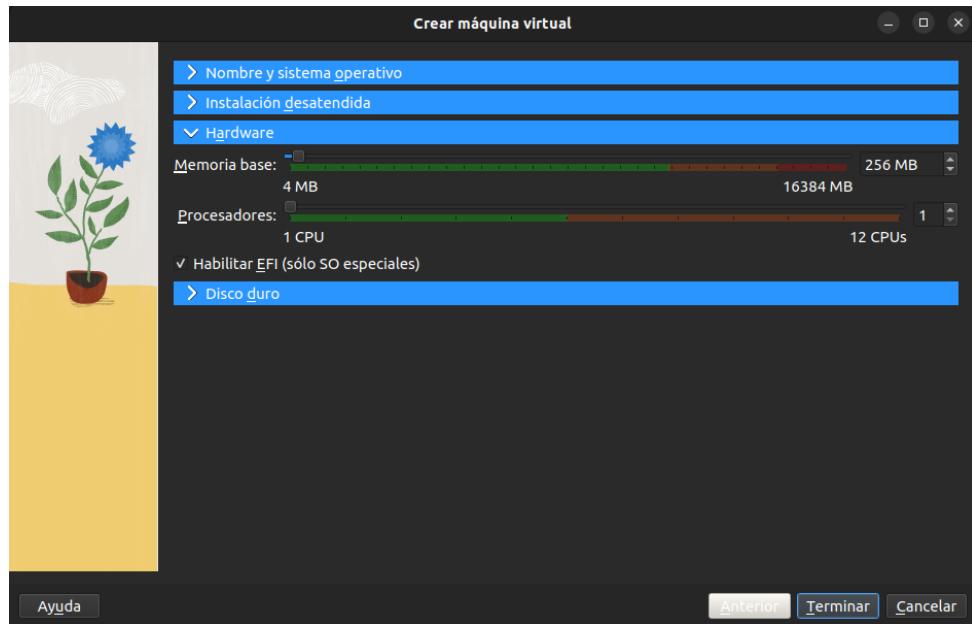


Figura A.11: Configuración de la máquina virtual para Softphone

Por último, se debe seleccionar el disco duro virtual que se ha descargado previamente. Para ello, se debe seleccionar la opción Usar un archivo de disco duro virtual existente y seleccionar el archivo descargado.

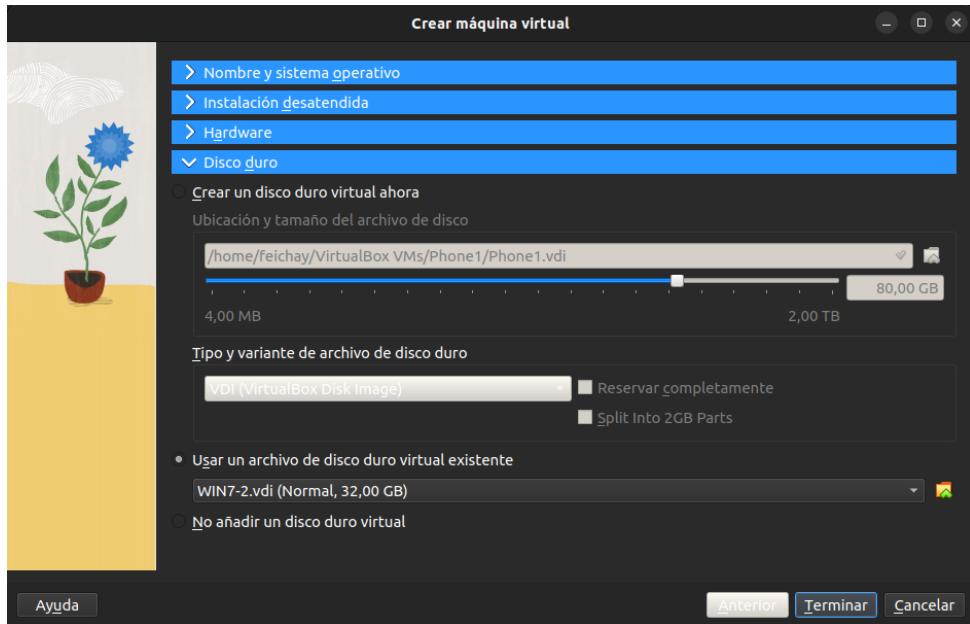


Figura A.12: Configuración de la máquina virtual para Softphone

A.3. Instalación de Docker

Para instalar Docker [43] y Docker Compose [44] en Ubuntu, se deben seguir los siguientes pasos:

A.3.1. Añadir el repositorio Docker

Primero, instalar todas las dependencias necesarias usando el siguiente comando:

```
1 sudo apt update
2 sudo apt install apt-transport-https ca-certificates curl software-properties-common -y
```

Después de instalar todas las dependencias, hay que descargar y añadir la clave GPG de Docker CE (Docker Community Edition) con el siguiente comando:

```
1 curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
```

Ahora, añadimos el repositorio de Docker CE con el siguiente comando. Es importante notar que aunque la guía original mencione "focal"(para Ubuntu 20.04), para Ubuntu 22.04 (Jammy Jellyfish) se debería usar "jammy". Sin embargo, si se sigue una guía específica que indica "focal" funciona, se puede mantener, pero es recomendable usar la versión correspondiente a la distribución:

```
1 sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
```

O, si se desea usar "focal" explícitamente:

```
1 sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"
```

Por último, verificar que se ha añadido el repositorio con el siguiente comando:

```
1 apt-cache policy docker-ce
```

A.3.2. Instalar Docker y Docker Compose

Ahora, hay que instalar los paquetes de Docker usando el siguiente comando:

```
1 sudo apt update  
2 sudo apt install docker-ce -y
```

Una vez está Docker instalado, hay que verificar que Docker está corriendo correctamente:

```
1 sudo systemctl status docker
```

Después, hay que instalar Docker Compose. La forma de instalar Docker Compose puede variar. Una forma común es descargarlo directamente desde GitHub. Sin embargo, si está disponible en los repositorios (como 'docker-compose-plugin' o 'docker-compose' v2), esa sería la forma preferida. La instrucción 'apt install docker-compose -y' instalará la versión disponible en los repositorios de Ubuntu, que podría ser la v1. Para la v2, que se integra como un plugin de Docker CLI, los pasos serían diferentes.

```
1 sudo apt install docker-compose -y
```

Para verificar la instalación de Docker Compose:

```
1 docker-compose --version
```

Apéndice B

Configuración de los servicios y dispositivos

B.1. Configuración de los routers de la red de ISP

Aquí se detalla la configuración de los routers utilizados en la simulación de la red de ISP, incluyendo los routers PE (Provider Edge), P (Provider) y CE (Customer Edge).

B.1.1. Configuración de los routers PE

Router PE1

```
1 /system identity set name=PE1
2 /interface bridge add name=lo0
3 /ip address add address=1.1.1.11/32 interface=lo0 network=1.1.1.11
4 /ip address add address=10.0.0.1/30 interface=ether1 network=10.0.0.0
5 /ip address add address=172.16.0.1/30 interface=ether2 network=172.16.0.0
6 /ip address add address=10.0.0.13/30 interface=ether3 network=10.0.0.12
7
8 /routing ospf instance add name=backbone router-id=1.1.1.11
9 /routing ospf area add name=backbone area-id=0.0.0.0 inst=backbone
10 /routing ospf interface-template add interface=lo0 network=1.1.1.11/32 area=backbone
11 /routing ospf interface-template add interface=ether1 network=10.0.0.1/30 area=backbone
12
13 /mpls ldp add afi=ip lsr-id=1.1.1.11 transport-addresses=1.1.1.11
14 /mpls ldp interface add interface=lo0
15 /mpls ldp interface add interface=ether1
16 /mpls settings set dynamic-label-range=10000-11999
17
18 /routing bgp template set default address-families=ip,vpnv4 as=65000 router-id=1.1.1.11
19 /routing bgp connection
20 add connect=yes disabled=no listen=yes local.address=1.1.1.11 .role=ibgp \
   name=toPE2 remote.address=1.1.1.12 .as=65000 templates=default
21 /routing bgp connection
22 add connect=yes disabled=no listen=yes local.address=1.1.1.11 .role=ibgp \
   name=toPE3 remote.address=1.1.1.13 .as=65000 templates=default
23 /routing bgp connection
24 add connect=yes disabled=no listen=yes local.address=1.1.1.11 .role=ibgp \
   name=toPE4 remote.address=1.1.1.14 .as=65000 templates=default
25
26 /ip vrf add name=CE1 interfaces=ether2
27
28 /routing bgp vpn
29 add export.redistribute=connected,static,bgp .route-targets=65000:100 \
30
31
32
```

```

33 import.route-targets=65000:100 label-allocation-policy=per-vrf name=\n
34   bgp-mpls-vpn-1 route-distinguisher=65000:100 vrf=CE1\n
35\n
36 /routing bgp connection\n
37   add as=65000 connect=yes disabled=yes listen=yes local.address=172.16.0.1 \\\n
38     .role=ebgp name=toCE1 output.default-originate=always remote.address=\\\n
39       172.16.0.2 .as=65500 router-id=1.1.1.11 routing-table=CE1 vrf=CE1\n
40\n
41 /routing bgp connection add as=65000 connect=yes disabled=yes listen=yes local.address=172.16.0.1 \\\n
42     .role=ebgp name=toCE1 output.default-originate=always remote.address=172.16.0.2 .as=65500\n
43     router-id=1.1.1.11 routing-table=CE1 vrf=CE1\n
44\n
45 /ip firewall mangle\n
46   add action=mark-routing chain=prerouting dst-address=!192.168.0.0/16 \\\n
47     in-interface=ether2 new-routing-mark=main passthrough=yes\n
48 /ip route add gateway=172.16.0.2@CE1 routing-table=CE1\n
49 /ip route add gateway=10.0.0.14\n
50 /ip route add dst-address=172.16.0.0/30 gateway=CE1@CE1 routing-table=main

```

Router PE2

```

1 /system identity set name=PE2\n
2 /interface bridge add name=lo0\n
3 /ip address add address=1.1.1.12/32 interface=lo0\n
4 /ip address add address=172.16.0.5/30 interface=ether1\n
5 /ip address add address=10.0.0.5/30 interface=ether2\n
6\n
7 /routing ospf instance add name=backbone router-id=1.1.1.12\n
8 /routing ospf area add name=backbone area-id=0.0.0.0 inst=backbone\n
9 /routing ospf interface-template add interface=lo0 network=1.1.1.12/32 area=backbone\n
10 /routing ospf interface-template add interface=ether2 network=10.0.0.5/30 area=backbone\n
11\n
12 /mpls ldp add afi=ip lsr-id=1.1.1.12 transport-addresses=1.1.1.12\n
13 /mpls ldp interface add interface=ether2\n
14 /mpls settings set dynamic-label-range=12000-13999\n
15\n
16 /routing bgp template set default address-families=ip,vpnv4 as=65000 router-id=1.1.1.12\n
17 /routing bgp connection add name=toPE1 template=default local.address=1.1.1.12 local.role=ibgp\n
18   remote.address=1.1.1.11 remote.as=65000 connect=yes listen=yes\n
19 /routing bgp connection add name=toPE3 template=default local.address=1.1.1.12 local.role=ibgp\n
20   remote.address=1.1.1.13 remote.as=65000 connect=yes listen=yes\n
21 /routing bgp connection add name=toPE4 template=default local.address=1.1.1.12 local.role=ibgp\n
22   remote.address=1.1.1.14 remote.as=65000 connect=yes listen=yes\n
23\n
24 /ip vrf add name=CE2 interfaces=ether1\n
25\n
26 /routing bgp vpn add route-distinguisher=65000:100 import.route-targets=65000:100 vrf=CE2\n
27   label-allocation-policy=per-vrf export.route-targets=65000:100 .redistribute=connected,static,bgp\n
28\n
29 /routing bgp connection add name=toCE2 router-id=1.1.1.12 as=65000 local.address=172.16.0.5\n
30   .role=ebgp remote.address=172.16.0.6 .as=65500 routing-table=CE2 vrf=CE2 connect=yes\n
31   listen=yes output.default-originate=always

```

Router PE3

```
1 /system identity set name=PE3
2 /interface bridge add name=lo0
3 /ip address add address=1.1.1.13/32 interface=lo0
4 /ip address add address=10.0.0.9/30 interface=ether1
5 /ip address add address=172.16.0.9/30 interface=ether2
6
7 /routing ospf instance add name=backbone router-id=1.1.1.13
8 /routing ospf area add name=backbone area-id=0.0.0.0 inst=backbone
9 /routing ospf interface-template add interface=lo0 network=1.1.1.13/32 area=backbone
10 /routing ospf interface-template add interface=ether1 network=10.0.0.9/30 area=backbone
11
12 /mpls ldp add afi=ip lsr-id=1.1.1.13 transport-addresses=1.1.1.13
13 /mpls ldp interface add interface=ether1
14 /mpls settings set dynamic-label-range=14000-15999
15
16 /routing bgp template set default address-families=ip,vpnv4 as=65000 router-id=1.1.1.13
17 /routing bgp connection add name=toPE1 template=default local.address=1.1.1.13 local.role=ibgp
    remote.address=1.1.1.11 remote.as=65000 connect=yes listen=yes
18 /routing bgp connection add name=toPE2 template=default local.address=1.1.1.13 local.role=ibgp
    remote.address=1.1.1.12 remote.as=65000 connect=yes listen=yes
19 /routing bgp connection add name=toPE4 template=default local.address=1.1.1.13 local.role=ibgp
    remote.address=1.1.1.14 remote.as=65000 connect=yes listen=yes
20
21 /ip vrf add name=CE3 interfaces=ether2
22
23 /routing bgp vpn add route-distinguisher=65000:100 import.route-targets=65000:100 vrf=CE3
    label-allocation-policy=per-vrf export.route-targets=65000:100 .redistribute=connected,static,bgp
24
25 /routing bgp connection add name=toCE3 router-id=1.1.1.13 as=65000 local.address=172.16.0.9
    .role=ebgp remote.address=172.16.0.10 .as=65500 routing-table=CE3 vrf=CE3 connect=yes
    listen=yes output.default-originate=always
```

B.1.2. Configuración de los routers P

Router P1

```
1 /system identity set name=P1
2 /interface bridge add name=lo0
3 /ip address add address=1.1.1.1/32 interface=lo0
4 /ip address add address=10.0.0.18/30 interface=ether1
5 /ip address add address=10.0.0.26/30 interface=ether2
6 /ip address add address=10.0.0.6/30 interface=ether3
7 /ip address add address=10.0.0.10/30 interface=ether4
8
9 /routing ospf instance add name=backbone router-id=1.1.1.1
10 /routing ospf area add name=backbone area-id=0.0.0.0 inst=backbone
11 /routing ospf interface-template add interface=lo0 network=1.1.1.1/32 area=backbone
12 /routing ospf interface-template add interface=ether1 network=10.0.0.18/30 area=backbone
13 /routing ospf interface-template add interface=ether2 network=10.0.0.26/30 area=backbone
14 /routing ospf interface-template add interface=ether3 network=10.0.0.6/30 area=backbone
15 /routing ospf interface-template add interface=ether4 network=10.0.0.10/30 area=backbone
16
```

```

17 /mpls ldp add afi=ip lsr-id=1.1.1.1 transport-addresses=1.1.1.1
18 /mpls ldp interface add interface=lo0
19 /mpls ldp interface add interface=ether1
20 /mpls ldp interface add interface=ether2
21 /mpls ldp interface add interface=ether3
22 /mpls ldp interface add interface=ether4
23 /mpls settings set dynamic-label-range=20000-21999

```

Router P2

```

1 /system identity set name=P3
2 /interface bridge add name=lo0
3 /ip address add address=1.1.1.3/32 interface=lo0
4 /ip address add address=10.0.0.21/30 interface=ether1
5 /ip address add address=10.0.0.17/30 interface=ether2
6 /ip address add address=10.0.0.2/30 interface=ether3
7 /ip address add address=10.0.0.14/30 interface=ether4
8
9 /routing ospf instance add name=backbone router-id=1.1.1.3
10 /routing ospf area add name=backbone area-id=0.0.0.0 inst=backbone
11 /routing ospf interface-template add interface=lo0 network=1.1.1.3/32 area=backbone
12 /routing ospf interface-template add interface=ether1 network=10.0.0.21/30 area=backbone
13 /routing ospf interface-template add interface=ether2 network=10.0.0.17/30 area=backbone
14 /routing ospf interface-template add interface=ether3 network=10.0.0.2/30 area=backbone
15 /routing ospf interface-template add interface=ether4 network=10.0.0.14/30 area=backbone
16
17 /mpls ldp add afi=ip lsr-id=1.1.1.3 transport-addresses=1.1.1.3
18 /mpls ldp interface add interface=lo0
19 /mpls ldp interface add interface=ether1
20 /mpls ldp interface add interface=ether2
21 /mpls ldp interface add interface=ether3
22 /mpls ldp interface add interface=ether4
23 /mpls settings set dynamic-label-range=24000-25999

```

Router P3

```

1 /system identity set name=P3
2 /interface bridge add name=lo0
3 /ip address add address=1.1.1.3/32 interface=lo0
4 /ip address add address=10.0.0.21/30 interface=ether1
5 /ip address add address=10.0.0.17/30 interface=ether2
6 /ip address add address=10.0.0.2/30 interface=ether3
7 /ip address add address=10.0.0.14/30 interface=ether4
8
9 /routing ospf instance add name=backbone router-id=1.1.1.3
10 /routing ospf area add name=backbone area-id=0.0.0.0 inst=backbone
11 /routing ospf interface-template add interface=lo0 network=1.1.1.3/32 area=backbone
12 /routing ospf interface-template add interface=ether1 network=10.0.0.21/30 area=backbone
13 /routing ospf interface-template add interface=ether2 network=10.0.0.17/30 area=backbone
14 /routing ospf interface-template add interface=ether3 network=10.0.0.2/30 area=backbone
15 /routing ospf interface-template add interface=ether4 network=10.0.0.14/30 area=backbone
16

```

```

17 /mpls ldp add afi=ip lsr-id=1.1.1.3 transport-addresses=1.1.1.3
18 /mpls ldp interface add interface=lo0
19 /mpls ldp interface add interface=ether1
20 /mpls ldp interface add interface=ether2
21 /mpls ldp interface add interface=ether3
22 /mpls ldp interface add interface=ether4
23 /mpls settings set dynamic-label-range=24000-25999

```

B.1.3. Configuración de los routers CE

Router CE1

```

1 /system identity set name=CE1
2 /interface bridge add name=lo0
3 /ip address add address=1.1.1.21/32 interface=lo0 network=1.1.1.21
4 /ip address add address=192.168.1.1/24 interface=ether1 network=192.168.1.0
5 /ip address add address=172.16.0.2/30 interface=ether2 network= 172.16.0.0
6
7 /ip firewall address-list add address=192.168.1.0/24 list=BGP_OUT
8 /ip firewall nat add action=masquerade chain=srcnat dst-address=!192.168.0.0/16 out-interface=ether2
9
10 /ip route add gateway=172.16.0.1
11
12 /routing bgp connection
13 add as=65500 connect=yes listen=yes local.address=172.16.0.2 .role=ebgp name=\
14 toPE1 output.network=BGP_OUT remote.address=172.16.0.1 .as=65000 router-id=\
15 1.1.1.21

```

Router CE2

```

1 /system identity set name=CE3
2 /interface bridge add name=lo0
3 /ip address add address=1.1.1.23/32 interface=lo0
4 /ip address add address=172.16.0.10/30 interface=ether1
5 /ip address add address=192.168.3.1/24 interface=ether2
6
7 /ip firewall address-list add address=192.168.3.0/24 list=BGP_OUT
8 /routing bgp connection add name=toPE3 as=65500 router-id=1.1.1.23 local.address=172.16.0.10
     .role=ebgp remote.address=172.16.0.9 remote.as=65000 output.network=BGP_OUT
     connect=yes listen=yes

```

Router CE3

```

1 /system identity set name=CE3
2 /interface bridge add name=lo0
3 /ip address add address=1.1.1.23/32 interface=lo0
4 /ip address add address=172.16.0.10/30 interface=ether1
5 /ip address add address=192.168.3.1/24 interface=ether2
6
7 /ip firewall address-list add address=192.168.3.0/24 list=BGP_OUT
8 /routing bgp connection add name=toPE3 as=65500 router-id=1.1.1.23 local.address=172.16.0.10
     .role=ebgp remote.address=172.16.0.9 remote.as=65000 output.network=BGP_OUT
     connect=yes listen=yes

```

B.2. Configuración de la Oficina Central

B.2.1. Configuración router CE1

Se presenta a continuación la configuración del router CE1, que incluye la creación de VLANs, la asignación de direcciones IP y la configuración de DHCP Relay para reenviar solicitudes al servidor DHCP ubicado en la DMZ.

```
1 # -----
2 # Identidad
3 /system identity set name=CE1
4
5 # -----
6 # Habilitar todas las interfaces físicas
7 /interface ethernet enable [find]
8
9 # -----
10 # Crear Bonding con LACP (802.3ad) (EtherChannel)
11 /interface bonding add name=bond1 mode=802.3ad slaves=ether1,ether2
   transmit-hash-policy=layer-2-and-3
12
13 # -----
14 # VLANs sobre el bonding
15 /interface vlan add name=vlan10-datos vlan-id=10 interface=bond1 mtu=1480
16 /interface vlan add name=vlan20-voz  vlan-id=20 interface=bond1 mtu=1480
17 /interface vlan add name=vlan30-dmz  vlan-id=30 interface=bond1 mtu=1480
18
19 # -----
20 # Asignar direcciones IPv6 a cada VLAN
21 /ipv6 address add address=2001:db8:1234:0100::1/64 interface=vlan10-datos
22 /ipv6 address add address=2001:db8:1234:0101::1/64 interface=vlan20-voz
23 /ipv6 address add address=2001:db8:1234:0102::1/64 interface=vlan30-dmz
24
25 # -----
26 # Configuración VRRP en las VLANs
27 /interface vrrp add name=vrrp-datos interface=vlan10-datos vrid=10 priority=150 version=3
   v3-protocol=ipv6 mtu=1480
28 /interface vrrp add name=vrrp-voz  interface=vlan20-voz  vrid=20 priority=150 version=3
   v3-protocol=ipv6 mtu=1480
29 /interface vrrp add name=vrrp-dmz  interface=vlan30-dmz  vrid=30 priority=150 version=3
   v3-protocol=ipv6 mtu=1480
30
31 # Direcciones virtuales VRRP
32 /ipv6 address add address=2001:db8:1234:0100::2/64 interface=vrrp-datos
33 /ipv6 address add address=2001:db8:1234:0101::2/64 interface=vrrp-voz
34 /ipv6 address add address=2001:db8:1234:0102::2/64 interface=vrrp-dmz
35
36 # -----
37 # Conexión directa con CE1_Backup (enlace de sincronización)
38 /interface ethernet enable ether3
39 /ipv6 address add address=2001:db8:1234:0103::1/64 interface=ether3
40
41 # -----
42 # DHCPv6 relay en VLANs
```

```

43 /ipv6 dhcp-relay add name=relay-datos interface=vlan10-datos dhcp-server=2001:db8:1234:0102::132
    link-address=2001:db8:1234:0100::1 disabled=no
44 /ipv6 dhcp-relay add name=relay-voz interface=vlan20-voz dhcp-server=2001:db8:1234:0102::132
    link-address=2001:db8:1234:0101::1 disabled=no
45
46 #
47 # Neighbor Discovery (RA, DNS)
48 /ipv6 nd add interface=vlan10-datos advertise-dns=yes managed-address-configuration=yes
    other-configuration=yes ra-lifetime=1800 ra-preference=low
    dns=2001:db8:1234:0102::133,2001:db8:1234:0102::134
49 /ipv6 nd add interface=vlan20-voz advertise-dns=yes managed-address-configuration=yes
    other-configuration=yes ra-lifetime=1800 ra-preference=low
    dns=2001:db8:1234:0102::133,2001:db8:1234:0102::134
50 /ipv6 nd add interface=vlan30-dmz advertise-dns=yes
    dns=2001:db8:1234:0102::133,2001:db8:1234:0102::134
51
52 #
53 # Firewall básico IPv6
54 /ipv6 firewall filter add chain=forward action=accept protocol=udp dst-port=53 comment="Permitir
    tráfico DNS"
55 /ipv6 firewall filter add chain=forward action=accept protocol=tcp dst-port=53 comment="Permitir
    tráfico DNS"
56 /ipv6 firewall filter add chain=forward action=accept protocol=udp dst-port=547 comment="Permitir
    tráfico DHCPv6"
57 /ipv6 firewall filter add chain=forward action=accept comment="Permitir comunicación entre VLANs"
58 /ipv6 firewall filter add chain=forward action=accept protocol=icmpv6 comment="Permitir tráfico
    ICMPv6 entre VLANs y servidor DNS"
59 /ipv6 firewall filter add chain=forward action=accept src-address=2001:db8:1234:0100::/64
    dst-address=2001:db8:1234:0102::/64 comment="Datos → DMZ"
60 /ipv6 firewall filter add chain=forward action=accept src-address=2001:db8:1234:0101::/64
    dst-address=2001:db8:1234:0102::/64 comment="Voz → DMZ"
61 /ipv6 firewall filter add chain=forward action=accept src-address=2001:db8:1234:0102::/64
    dst-address=2001:db8:1234:0100::/64 comment="DMZ → Datos"
62 /ipv6 firewall filter add chain=forward action=accept src-address=2001:db8:1234:0102::/64
    dst-address=2001:db8:1234:0101::/64 comment="DMZ → Voz"
63
64 #
65 # Activar fast-path (si aplica)
66 /ip settings set allow-fast-path=yes
67
68 #
69 # Guardar configuración
70 /system backup save name=CE1

```

B.2.2. Configuración del router CE1_backup ARREGLAR

```

1 #
2 # Identidad
3 /system identity set name=CE1-Backup
4
5 #
6 # Habilitar todas las interfaces físicas
7 /interface ethernet enable [find]

```

```

8
9 # -----
10 # Crear Bonding con LACP (802.3ad) (EtherChannel)
11 /interface bonding add name=bond1 mode=802.3ad slaves=ether1,ether2
    transmit-hash-policy=layer-2-and-3
12
13 # -----
14 # VLANs sobre el bonding
15 /interface vlan add name=vlan10-datos vlan-id=10 interface=bond1 mtu=1480
16 /interface vlan add name=vlan20-voz  vlan-id=20 interface=bond1 mtu=1480
17 /interface vlan add name=vlan30-dmz  vlan-id=30 interface=bond1 mtu=1480
18
19 # -----
20 # Asignar direcciones IPv6 a cada VLAN
21 /ipv6 address add address=2001:db8:1234:0100::1/64 interface=vlan10-datos
22 /ipv6 address add address=2001:db8:1234:0101::1/64 interface=vlan20-voz
23 /ipv6 address add address=2001:db8:1234:0102::1/64 interface=vlan30-dmz
24
25 # -----
26 # Configuración VRRP en las VLANs
27 /interface vrrp add name=vrrp-datos interface=vlan10-datos vrid=10 priority=100 version=3
    v3-protocol=ipv6 mtu=1480
28 /interface vrrp add name=vrrp-voz  interface=vlan20-voz  vrid=20 priority=100 version=3
    v3-protocol=ipv6 mtu=1480
29 /interface vrrp add name=vrrp-dmz  interface=vlan30-dmz  vrid=30 priority=100 version=3
    v3-protocol=ipv6 mtu=1480
30
31 # Direcciones virtuales VRRP
32 /ipv6 address add address=2001:db8:1234:0100::2/64 interface=vrrp-datos
33 /ipv6 address add address=2001:db8:1234:0101::2/64 interface=vrrp-voz
34 /ipv6 address add address=2001:db8:1234:0102::2/64 interface=vrrp-dmz
35
36 # -----
37 # Conexion directa con CE (enlace de sincronización)
38 /interface ethernet enable ether3
39 /ipv6 address add address=2001:db8:1234:0103::2/64 interface=ether3
40
41 # -----
42 # DHCPv6 relay en VLANs
43 /ipv6 dhcp-relay add name=relay-datos interface=vlan10-datos dhcp-server=2001:db8:1234:0102::132
    link-address=2001:db8:1234:0100::1 disabled=no
44 /ipv6 dhcp-relay add name=relay-voz  interface=vlan20-voz  dhcp-server=2001:db8:1234:0102::132
    link-address=2001:db8:1234:0101::1 disabled=no
45
46 # -----
47 # Neighbor Discovery (RA, DNS)
48 /ipv6 nd add interface=vlan10-datos advertise-dns=yes managed-address-configuration=yes
    other-configuration=yes ra-lifetime=1800 ra-preference=low
    dns=2001:db8:1234:0102::133,2001:db8:1234:0102::134
49 /ipv6 nd add interface=vlan20-voz  advertise-dns=yes managed-address-configuration=yes
    other-configuration=yes ra-lifetime=1800 ra-preference=low
    dns=2001:db8:1234:0102::133,2001:db8:1234:0102::134

```

```

50 /ipv6 nd add interface=vlan30-dmz advertise-dns=yes
      dns=2001:db8:1234:0102::133,2001:db8:1234:0102::134

51 #
52 # -----
53 # Firewall básico IPv6
54 /ipv6 firewall filter add chain=forward action=accept protocol=udp dst-port=53 comment="Permitir
      tráfico DNS"
55 /ipv6 firewall filter add chain=forward action=accept protocol=tcp dst-port=53 comment="Permitir
      tráfico DNS"
56 /ipv6 firewall filter add chain=forward action=accept protocol=udp dst-port=547 comment="Permitir
      tráfico DHCPv6"
57 /ipv6 firewall filter add chain=forward action=accept comment="Permitir comunicación entre VLANs"
58 /ipv6 firewall filter add chain=forward action=accept protocol=icmpv6 comment="Permitir tráfico
      ICMPv6 entre VLANs y servidor DNS"
59 /ipv6 firewall filter add chain=forward action=accept src-address=2001:db8:1234:0100::/64
      dst-address=2001:db8:1234:0102::/64 comment="Datos → DMZ"
60 /ipv6 firewall filter add chain=forward action=accept src-address=2001:db8:1234:0101::/64
      dst-address=2001:db8:1234:0102::/64 comment="Voz → DMZ"
61 /ipv6 firewall filter add chain=forward action=accept src-address=2001:db8:1234:0102::/64
      dst-address=2001:db8:1234:0100::/64 comment="DMZ → Datos"
62 /ipv6 firewall filter add chain=forward action=accept src-address=2001:db8:1234:0102::/64
      dst-address=2001:db8:1234:0101::/64 comment="DMZ → Voz"

63 #
64 # -----
65 # Activar fast-path (si aplica)
66 /ip settings set allow-fast-path=yes

67 #
68 # -----
69 # Guardar configuración
70 /system backup save name=CE1-Backup

```

B.2.3. Docker Compose para los servicios de red

```

1 services:
2 dns-primary-ipv6:
3   build:
4     context: ./dns-primary-ipv6
5     dockerfile: Dockerfile
6     image: dns-primary-ipv6:latest
7     container_name: dns-primary-ipv6
8     hostname: dns-primary-ipv6
9     networks:
10    services_net:
11      ipv6_address: 2001:db8:1234:0102::133
12    volumes:
13      - ./dns-primary-ipv6/named.conf.options:/etc/bind/named.conf.options
14      - ./dns-primary-ipv6/named.conf.local:/etc/bind/named.conf.local
15      - ./dns-primary-ipv6/zones/:/etc/bind/zones/
16    cap_add:
17      - NET_ADMIN
18    privileged: true
19    restart: unless-stopped
20

```

```

21 dns-secondary-ipv6:
22   build:
23     context: ./dns-secondary-ipv6
24     dockerfile: Dockerfile
25   image: dns-secondary-ipv6:latest
26   container_name: dns-secondary-ipv6
27   hostname: dns-secondary-ipv6
28   networks:
29     services_net:
30       ipv6_address: 2001:db8:1234:0102::134
31   volumes:
32     - ./dns-secondary-ipv6/named.conf.options:/etc/bind/named.conf.options
33     - ./dns-secondary-ipv6/named.conf.local:/etc/bind/named.conf.local
34     - ./dns-secondary-ipv6/zones/:/etc/bind/zones/
35   cap_add:
36     - NET_ADMIN
37   privileged: true
38   restart: unless-stopped
39
40 dhcp6-server:
41   build:
42     context: ./dhcp6-server
43     dockerfile: Dockerfile
44   image: dhcp6-server:latest
45   container_name: dhcp6-server
46   hostname: dhcp6-server
47   networks:
48     services_net:
49       ipv6_address: 2001:db8:1234:0102::132
50   volumes:
51     - ./dhcp6-server/dhcpd6.conf:/etc/dhcp/dhcpd6.conf
52     - ./dhcp6-server/isc-dhcp-server:/etc/default/isc-dhcp-server
53   cap_add:
54     - NET_ADMIN
55   privileged: true
56   restart: unless-stopped
57
58 networks:
59   services_net:
60     driver: bridge
61     enable_ipv6: true
62     ipam:
63       driver: default
64       config:
65         - subnet: "2001:db8:1234:0102::/64"

```

B.2.4. Servidor DHCP

Aquí se presenta la configuración del servidor DHCP, tanto el Dockerfile como los archivos de configuración.

B.2.4.1. Dockerfile para el servidor DHCP

```
1 FROM ubuntu:20.04
2
3 # Evitar prompts interactivos durante la instalación
4 ENV DEBIAN_FRONTEND=noninteractive
5
6 # Actualizar e instalar paquetes necesarios
7 RUN apt-get update && apt-get install -y \
8     isc-dhcp-server \
9     iputils-ping \
10    net-tools \
11    iproute2 \
12    procps \
13    && apt-get clean \
14    && rm -rf /var/lib/apt/lists/*
15
16 # Crear directorio para logs y leases
17 RUN mkdir -p /var/log /var/lib/dhcp /var/run
18
19 # Crear archivo de leases inicial (requerido por dhcpcd)
20 RUN touch /var/lib/dhcp/dhcpd6.leases
21
22 # Establecer permisos correctos
23 RUN chown -R dhcpcd:dhcpcd /var/lib/dhcp /var/log
24 RUN chmod 644 /var/lib/dhcp/dhcpd6.leases
25
26 # Copiar archivos de configuración del DHCP
27 COPY dhcpd6.conf /etc/dhcp/dhcpd6.conf
28 COPY isc-dhcp-server /etc/default/isc-dhcp-server
29
30 # Establecer permisos correctos para los archivos de configuración
31 RUN chmod 644 /etc/dhcp/dhcpd6.conf
32 RUN chmod 644 /etc/default/isc-dhcp-server
33
34 # Crear script de inicio
35 RUN echo '#!/bin/bash\n'
36 # Configurar IP estática dinámicamente\n
37 ip -6 addr add 2001:db8:1234:0102::132/64 dev eth0\n\
38 ip -6 route add default via 2001:db8:1234:0102::1\n\
39 echo "nameserver 2001:db8:1234:0102::133" > /etc/resolv.conf\n\
40 echo "nameserver 2001:db8:1234:0102::134" >> /etc/resolv.conf\n\
41 # Iniciar servidor DHCP\n\
42 exec dhcpcd -6 -cf /etc/dhcp/dhcpd6.conf -d eth0; exec bash' > /start.sh
43
44 RUN chmod +x /start.sh
45
46 # Crear usuario dhcpcd si no existe
47 RUN useradd -r -s /bin/false dhcpcd 2>/dev/null || true
48
49 # Exponer puerto DHCP
50 EXPOSE 547/udp
51
```

```
52 # Usar el script de inicio  
53 CMD ["/start.sh"]
```

B.2.4.2. Archivo dhcpcd6.conf

```
1 default-lease-time 600;  
2 max-lease-time 7200;  
3 authoritative;  
4  
5 option dhcp6.domain-search "cazg.es";  
6 option dhcp6.name-servers 2001:db8:1234:0102::133, 2001:db8:1234:0102::134;  
7  
8 # VLAN Datos: 2001:db8:1234:0100::/64  
9 subnet6 2001:db8:1234:0100::/64 {  
10   range6 2001:db8:1234:0100::2 2001:db8:1234:0100::ffff;  
11 }  
12  
13 # VLAN Voz: 2001:db8:1234:0101::/64  
14 subnet6 2001:db8:1234:0101::/64 {  
15   range6 2001:db8:1234:0101::2 2001:db8:1234:0101::ffff;  
16 }  
17  
18 # VLAN DMZ: 2001:db8:1234:0102::/64  
19 subnet6 2001:db8:1234:0102::/64 { }
```

B.2.5. Servidor DNS Primario

Aquí se presenta la configuración del servidor DNS primario, tanto el Dockerfile como los archivos de configuración.

B.2.5.1. Dockerfile para el servidor DNS primario

```
1 FROM ubuntu:20.04  
2  
3 # Evitar prompts interactivos durante la instalación  
4 ENV DEBIAN_FRONTEND=noninteractive  
5  
6 # Actualizar e instalar paquetes necesarios  
7 RUN apt-get update && apt-get install -y \  
8   bind9 \  
9   bind9utils \  
10  bind9-doc \  
11  iputils-ping \  
12  net-tools \  
13  ifupdown \  
14  && apt-get clean \  
15  && rm -rf /var/lib/apt/lists/*  
16  
17 # Crear directorios necesarios  
18 RUN mkdir -p /etc/bind/zones /var/cache/bind /var/lib/bind /var/log/named  
19  
20 # Copiar archivos de configuración DNS  
21 COPY named.conf.options /etc/bind/
```

```

22 COPY named.conf.local /etc/bind/
23 COPY zones/ /etc/bind/zones/
24
25 # Establecer permisos correctos para bind
26 RUN chown -R bind:bind /etc/bind/zones /var/cache/bind /var/lib/bind /var/log/named
27 RUN chmod 755 /etc/bind/zones
28 RUN chmod 775 /var/cache/bind
29 RUN chmod 644 /etc/bind/named.conf.options /etc/bind/named.conf.local
30 RUN chmod 644 /etc/bind/zones/*
31
32 # Crear script de inicio
33 RUN echo '#!/bin/bash\n\
34 # Configurar IP estática dinámicamente\n\
35 ip addr add 192.168.1.133/28 dev eth0\n\
36 ip route add default via 192.168.1.131\n\
37 echo "nameserver 192.168.1.133" > /etc/resolv.conf\n\
38 echo "nameserver 192.168.1.134" >> /etc/resolv.conf\n\
39 # Iniciar servidor DNS\n\
40 exec named -g -c /etc/bind/named.conf -u bind; exec bash' > /start.sh
41
42 RUN chmod +x /start.sh
43
44 # Exponer puertos DNS
45 EXPOSE 53/udp 53/tcp
46
47 # Comando por defecto
48 CMD ["/start.sh"]

```

B.2.5.2. Archivo /etc/bind/named.conf.options

```

1 options {
2     directory "/var/cache/bind";
3
4     // Solo escuchar en IPv6
5     listen-on-v6 { 2001:db8:1234:0102::133; };
6     listen-on { none; }; // Deshabilitar IPv4
7
8     // Habilitar recursión
9     recursion yes;
10
11    // Permitir consultas solo desde red local
12    allow-query {
13        2001:db8:1234::/48;
14        localhost;
15    };
16
17    // Permitir recursión solo a clientes autorizados
18    allow-recursion {
19        2001:db8:1234::/48;
20        localhost;
21    };
22
23    // Permitir caché de DNS para red local

```

```

24 allow-cache {
25     2001:db8:1234::/48;
26     localhost;
27 };
28
29 // Redirigir consultas externas a resolvers públicos (opcional pero recomendado)
30 forwarders {
31     2001:4860:4860::8888;
32     2001:4860:4860::8844;
33 };
34
35 // Validación DNSSEC
36 dnssec-validation auto;
37
38 // No anunciararse como autoritativo en respuestas NXDOMAIN
39 auth-nxdomain no;
40 };

```

B.2.5.3. Archivo /etc/bind/named.conf.local

```

1 // Zona directa principal - nombre -> IP
2 zone "cazg.es" {
3     type master;
4     file "/etc/bind/zones/db.cazg.es";
5     allow-transfer { 2001:db8:1234:0102::134; }; // ns2 IP IPv6
6     notify yes;
7     also-notify { 2001:db8:1234:0102::134; };
8 };
9
10 // Zona inversa para red de servicios (2001:db8:1234:0102::/64)
11 zone "2.0.1.0.4.3.2.1.8.b.d.0.1.0.0.2.ip6.arpa" {
12     type master;
13     file "/etc/bind/zones/db.2001.db8.1234.0102";
14     allow-transfer { 2001:db8:1234:0102::134; }; // ns2 IP IPv6
15     notify yes;
16     also-notify { 2001:db8:1234:0102::134; };
17 };

```

B.2.5.4. Archivo /etc/bind/zones/db.cazg.es

```

1 $TTL 60
2 @ IN SOA ns1.cazg.es. admin.cazg.es. (
3             2025070102 ; Serial
4             60        ; Refresh
5             60        ; Retry
6             60        ; Expire
7             60 )       ; TTL mínimo
8
9 ; Servidores de nombres
10    IN NS ns1.cazg.es.
11    IN NS ns2.cazg.es.
12

```

```
13 ; Servidores DNS e infraestructura local
14 ns1 IN AAAA 2001:db8:1234:0102::133
15 ns2 IN AAAA 2001:db8:1234:0102::134
16 dhcp IN AAAA 2001:db8:1234:0102::132
```

B.2.5.5. Archivo /etc/bind/zones/db.2001.db8.1234.0102

B.2.6. Servidor DNS Secundario

Aquí se presenta la configuración del servidor DNS secundario, tanto el Dockerfile como los archivos de configuración.

B.2.6.1. Dockerfile para el servidor DNS secundario

```
1 FROM ubuntu:20.04
2
3 # Evitar prompts interactivos durante la instalación
4 ENV DEBIAN_FRONTEND=noninteractive
5
6 # Actualizar e instalar paquetes necesarios
7 RUN apt-get update && apt-get install -y \
8     bind9 \
9     bind9utils \
10    bind9-doc \
11    iputils-ping \
12    net-tools \
13    ifupdown \
14    && apt-get clean \
15    && rm -rf /var/lib/apt/lists/*
16
17 # Crear directorios necesarios
18 RUN mkdir -p /etc/bind/zones /var/cache/bind /var/lib/bind /var/log/named
19
20 # Copiar archivos de configuración DNS
```

```

21 COPY named.conf.options /etc/bind/
22 COPY named.conf.local /etc/bind/
23
24 # Establecer permisos correctos para bind
25 RUN chown -R bind:bind /etc/bind/zones /var/cache/bind /var/lib/bind /var/log/named
26 RUN chmod 755 /etc/bind/zones
27 RUN chmod 775 /var/cache/bind
28 RUN chmod 644 /etc/bind/named.conf.options /etc/bind/named.conf.local
29
30 # Crear script de inicio
31 RUN echo '#!/bin/bash\n'
32 # Configurar IP estática dinámicamente\n
33 ip addr add 192.168.1.134/28 dev eth0\n\
34 ip route add default via 192.168.1.131\n\
35 echo "nameserver 192.168.1.133" > /etc/resolv.conf\n\
36 echo "nameserver 192.168.1.134" >> /etc/resolv.conf\n\
37 # Iniciar servidor DNS\n\
38 exec named -g -c /etc/bind/named.conf -u bind; exec bash' > /start.sh
39
40 RUN chmod +x /start.sh
41
42 # Exponer puertos DNS
43 EXPOSE 53/udp 53/tcp
44
45 # Comando por defecto
46 CMD ["/start.sh"]

```

B.2.6.2. Archivo /etc/bind/named.conf.options

```

1 options {
2     directory "/var/cache/bind";
3
4     // ns2 escucha solo en su propia IP
5     listen-on-v6 { 2001:db8:1234:0102::134; };
6     listen-on { none; };
7
8     // Permitir consultas solo desde red local
9     allow-query {
10         2001:db8:1234::/48;
11         localhost;
12     };
13
14     // Permitir recursión para red local
15     recursion yes;
16     allow-recursion {
17         2001:db8:1234::/48;
18         localhost;
19     };
20
21     // Permitir uso del caché DNS
22     allow-cache {
23         2001:db8:1234::/48;
24         localhost;

```

```

25    };
26
27    // Redirigir consultas externas si no es autoritativo
28    forwarders {
29        2001:4860:4860::8888;
30        2001:4860:4860::8844;
31    };
32
33    // Seguridad
34    dnssec-validation auto;
35    auth-nxdomain no;
36};

```

B.2.6.3. Archivo /etc/bind/named.conf.local

```

1 // Zona directa principal - nombre -> IP
2 zone "cazg.es" {
3     type slave;
4     file "/etc/bind/zones/db.cazg.es";
5     masters { 2001:db8:1234:0102::133; }; // ns1 IP IPv6
6 };
7
8 // Zona inversa para red de servicios (2001:db8:1234:0102::/64)
9 zone "2.0.1.0.4.3.2.1.8.b.d.0.1.0.0.2.ip6.arpa" {
10    type slave;
11    file "/etc/bind/zones/db.2001.db8.1234.0102";
12    masters { 2001:db8:1234:0102::133; }; // ns1 IP IPv6
13};

```

B.2.7. Configuración del contenedor Docker para pruebas de red

Aquí se presenta la configuración del contenedor Docker para pruebas de red, incluyendo el Dockerfile, el script de entrada y el archivo de configuración de Docker Compose.

B.2.7.1. Dockerfile para el contenedor de pruebas de red

```

1 FROM debian:bookworm-slim
2
3 RUN apt-get update && apt-get install -y --no-install-recommends \
4     iproute2 \
5     iputils-ping \
6     curl \
7     tcpdump \
8     net-tools \
9     dnsutils \
10    traceroute \
11    iputils-tracepath \
12    vim \
13    bash \
14    isc-dhcp-client \
15    && apt-get clean \
16    && rm -rf /var/lib/apt/lists/*
17

```

```

18 COPY entrypoint.sh /entrypoint.sh
19 RUN chmod +x /entrypoint.sh
20
21 ENTRYPOINT ["/entrypoint.sh"]

```

B.2.7.2. Script de entrada para el contenedor de pruebas de red

```

1#!/bin/bash
2
3# Forzar resolución DNS al arranque
4echo "nameserver 2001:db8:1234:0102::132" > /etc/resolv.conf
5echo "nameserver 2001:db8:1234:0102::133" >> /etc/resolv.conf
6
7# Quedarse activo
8exec bash

```

B.2.7.3. Docker Compose para el contenedor de pruebas de red

```

1 services:
2   pc-docker:
3     container_name: pc-docker
4     build:
5       context: .
6       dockerfile: Dockerfile
7     privileged: true
8     network_mode: bridge
9     sysctls:
10       net.ipv6.conf.all.disable_ipv6: 0
11       net.ipv6.conf.default.disable_ipv6: 0
12     restart: unless-stopped

```

B.3. Configuración de sedes remotas e ISP

B.3.1. Configuración del router CE1 (Oficina Central)

```

1 /interface bridge add name=lo0
2 /interface ethernet
3 set [ find default-name=ether1 ] disable-running-check=no
4 set [ find default-name=ether2 ] disable-running-check=no
5 set [ find default-name=ether3 ] disable-running-check=no
6 set [ find default-name=ether4 ] disable-running-check=no
7 set [ find default-name=ether5 ] disable-running-check=no
8 set [ find default-name=ether6 ] disable-running-check=no
9 set [ find default-name=ether7 ] disable-running-check=no
10 set [ find default-name=ether8 ] disable-running-check=no
11
12 /port set 0 name=serial0
13
14 /ip address add address=192.170.0.1 interface=lo0 network=192.170.0.1
15 /ip address add address=10.0.0.1/30 interface=ether4 network=10.0.0.0
16
17 # Conexion con el router CE1_backup

```

```

18 /interface ethernet enable ether3
19 /ip address add address=192.168.1.249/30 interface=ether3
20
21 # Crear Bonding con LACP (802.3ad) (EtherChannel)
22 /interface bonding add name=bond1 mode=802.3ad slaves=ether1,ether2
   transmit-hash-policy=layer-2-and-3
23
24 # VLANs sobre el bonding
25 /interface vlan add name=vlan10-datos vlan-id=10 interface=bond1 mtu=1480
26 /interface vlan add name=vlan20-voz  vlan-id=20 interface=bond1 mtu=1480
27 /interface vlan add name=vlan30-dmz  vlan-id=30 interface=bond1 mtu=1480
28
29 # Asignar direcciones IP
30 /ip address add address=192.168.1.1/26 interface=vlan10-datos
31 /ip address add address=192.168.1.65/26 interface=vlan20-voz
32 /ip address add address=192.168.1.129/28 interface=vlan30-dmz
33
34 # Configuración VRRP en las VLANs
35 /interface vrrp add name=vrrp-datos interface=vlan10-datos vrid=10 priority=150
36 /interface vrrp add name=vrrp-voz interface=vlan20-voz vrid=20 priority=150
37 /interface vrrp add name=vrrp-dmz interface=vlan30-dmz vrid=30 priority=150
38
39 # Direcciones virtuales VRRP
40 /ip address add address=192.168.1.3/26 interface=vrrp-datos
41 /ip address add address=192.168.1.67/26 interface=vrrp-voz
42 /ip address add address=192.168.1.131/28 interface=vrrp-dmz
43
44 # DHCP relay
45 /ip dhcp-relay add name=relay-datos interface=vlan10-datos local-address=192.168.1.1
   dhcp-server=192.168.1.132 disabled=no
46 /ip dhcp-relay add name=relay-voz interface=vlan20-voz local-address=192.168.1.65
   dhcp-server=192.168.1.132 disabled=no
47 /ip dhcp-relay add name=relay-dmz interface=vlan30-dmz local-address=192.168.1.129
   dhcp-server=192.168.1.132 disabled=no
48
49 # Firewall básico
50 /ip firewall filter add chain=forward action=accept protocol=udp src-port=67,68 dst-port=67,68
   comment="Permitir tráfico DHCP"
51 /ip firewall filter add chain=forward action=accept comment="Permitir comunicación entre VLANs"
52
53 /ip dhcp-client add interface=ether1
54 # Exportar las redes de cliente a la VPN MPLS
55 /ip firewall address-list add address=192.168.1.0/26 list=BGP_OUT
56 /ip firewall address-list add address=192.168.1.64/26 list=BGP_OUT
57 /ip firewall address-list add address=192.168.1.128/28 list=BGP_OUT
58 /ip firewall nat add action=masquerade chain=srcnat dst-address=!192.168.0.0/16 out-interface=ether4
59
60 /ip route add gateway=10.0.0.2
61
62 /routing bgp connection
63 add as=65500 connect=yes listen=yes local.address=10.0.0.1 .role=ebgp name=\
   toPE2 output.network=BGP_OUT remote.address=10.0.0.2 .as=65000 router-id=\
   192.170.0.1
64
65

```

```

66 /system identity set name=CE1
67
68 # Asegurarte que ether1 está habilitado (por si acaso)
69 /interface ethernet set [find name=ether1] disabled=no
70
71
72 /system note set show-at-login=no

```

B.3.2. Servidor DHCP

B.3.2.1. Dockerfile para el servidor DHCP

```

1 FROM ubuntu:20.04
2
3 # Evitar prompts interactivos durante la instalación
4 ENV DEBIAN_FRONTEND=noninteractive
5
6 # Actualizar e instalar paquetes necesarios
7 RUN apt-get update && apt-get install -y \
8     isc-dhcp-server \
9     iputils-ping \
10    net-tools \
11    iproute2 \
12    procps \
13    && apt-get clean \
14    && rm -rf /var/lib/apt/lists/*
15
16 # Crear directorio para logs y leases
17 RUN mkdir -p /var/log /var/lib/dhcp /var/run
18
19 # Crear archivo de leases inicial (requerido por dhcpcd)
20 RUN touch /var/lib/dhcp/dhcpcd.leases
21
22 # Establecer permisos correctos
23 RUN chown -R dhcpcd:dhcpcd /var/lib/dhcp /var/log
24 RUN chmod 644 /var/lib/dhcp/dhcpcd.leases
25
26 # Copiar archivos de configuración del DHCP
27 COPY dhcpcd.conf /etc/dhcp/dhcpcd.conf
28 COPY isc-dhcp-server /etc/default/isc-dhcp-server
29
30 # Establecer permisos correctos para los archivos de configuración
31 RUN chmod 644 /etc/dhcp/dhcpcd.conf
32 RUN chmod 644 /etc/default/isc-dhcp-server
33
34 # Crear script de inicio
35 RUN echo '#!/bin/bash\n\
36 # Configurar IP estática dinámicamente\n\
37 ip addr add 192.168.1.132/28 dev eth0\n\
38 ip route add default via 192.168.1.131\n\
39 echo "nameserver 192.168.1.133" > /etc/resolv.conf\n\
40 echo "nameserver 192.168.1.134" >> /etc/resolv.conf\n\
41 # Iniciar servidor DHCP\n'

```

```

42 exec dhcpcd -4 -cf /etc/dhcp/dhcpcd.conf -d eth0; exec bash' > /start.sh
43
44 RUN chmod +x /start.sh
45
46 # Crear usuario dhcpcd si no existe
47 RUN useradd -r -s /bin/false dhcpcd 2>/dev/null || true
48
49 # Exponer puerto DHCP
50 EXPOSE 67/udp
51
52 # Usar el script de inicio
53 CMD ["/start.sh"]

```

B.3.2.2. Archivo dhcpcd.conf

```

1 default-lease-time 600;
2 max-lease-time 7200;
3 authoritative;
4
5 option domain-name "cazg.es"; # Dominio de la red
6 option domain-name-servers 192.168.1.133, 192.168.1.134; # IPs de los DNS primario y secundario
7
8 # Subred para VLAN 10 (Datos)
9 subnet 192.168.1.0 netmask 255.255.255.192 {
10   range 192.168.1.4 192.168.1.62;
11   option routers 192.168.1.3;
12   option broadcast-address 192.168.1.63;
13 }
14
15 # Subred para VLAN 20 (Voz)
16 subnet 192.168.1.64 netmask 255.255.255.192 {
17   range 192.168.1.68 192.168.1.126;
18   option routers 192.168.1.67;
19   option broadcast-address 192.168.1.127;
20 }
21
22 # Subred para VLAN 30 (DMZ)
23 subnet 192.168.1.128 netmask 255.255.255.240 {
24   # No se asignan IPs dinámicamente ya que son servidores con IPs fijas
25   option routers 192.168.1.131;
26   option broadcast-address 192.168.1.143;
27 }

```

B.3.3. Servidores DNS

B.3.3.1. Configuración del servidor DNS primario

Dockerfile para el servidor DNS primario

```

1 FROM ubuntu:20.04
2
3 # Evitar prompts interactivos durante la instalación
4 ENV DEBIAN_FRONTEND=noninteractive
5

```

```

6 # Actualizar e instalar paquetes necesarios
7 RUN apt-get update && apt-get install -y \
8   bind9 \
9   bind9utils \
10  bind9-doc \
11  iputils-ping \
12  net-tools \
13  ifupdown \
14  && apt-get clean \
15  && rm -rf /var/lib/apt/lists/*
16
17 # Crear directorios necesarios
18 RUN mkdir -p /etc/bind/zones /var/cache/bind /var/lib/bind /var/log/named
19
20 # Copiar archivos de configuración DNS
21 COPY named.conf.options /etc/bind/
22 COPY named.conf.local /etc/bind/
23 COPY zones/ /etc/bind/zones/
24
25 # Establecer permisos correctos para bind
26 RUN chown -R bind:bind /etc/bind/zones /var/cache/bind /var/lib/bind /var/log/named
27 RUN chmod 755 /etc/bind/zones
28 RUN chmod 775 /var/cache/bind
29 RUN chmod 644 /etc/bind/named.conf.options /etc/bind/named.conf.local
30 RUN chmod 644 /etc/bind/zones/*
31
32 # Crear script de inicio
33 RUN echo '#!/bin/bash\n\
34 # Configurar IP estática dinámicamente\n\
35 ip addr add 192.168.1.133/28 dev eth0\n\
36 ip route add default via 192.168.1.131\n\
37 echo "nameserver 192.168.1.133" > /etc/resolv.conf\n\
38 echo "nameserver 192.168.1.134" >> /etc/resolv.conf\n\
39 # Iniciar servidor DNS\n\
40 exec named -g -c /etc/bind/named.conf -u bind; exec bash' > /start.sh
41
42 RUN chmod +x /start.sh
43
44 # Exponer puertos DNS
45 EXPOSE 53/udp 53/tcp
46
47 # Comando por defecto
48 CMD ["/start.sh"]

```

Archivo /etc/bind/named.conf.options

```

1 options {
2   directory "/var/cache/bind";
3
4   // Escucha solo en su IP privada
5   listen-on { 192.168.1.133; };
6   listen-on-v6 { none; } // si no estás usando IPv6 aquí
7

```

```

8 // Consultas permitidas desde red local
9 allow-query {
10     192.168.1.0/28;
11     localhost;
12 };
13
14 // Reenvío a DNS externos para dominios no autoritativos
15 forwarders {
16     8.8.8.8;
17     1.1.1.1;
18 };
19
20 // Habilitar recursión para la red local
21 recursion yes;
22 allow-recursion {
23     192.168.1.0/28;
24     localhost;
25 };
26
27 // Permitir uso del caché
28 allow-cache {
29     192.168.1.0/28;
30     localhost;
31 };
32
33 dnssec-validation auto;
34 auth-nxdomain no;
35 };

```

Archivo /etc/bind/named.conf.local

```

1 // Zona directa nombre -> IP
2 zone "cazg.es" {
3     type master;
4     file "/etc/bind/zones/db.cazg.es";
5     allow-transfer { 192.168.1.134; }; // ns2 IP privada
6 };
7
8 // Zona inversa IP -> nombre
9 zone "1.168.192.in-addr.arpa" {
10    type master;
11    file "/etc/bind/zones/db.192.168.1"; // subred 192.168.1.0/28
12    allow-transfer { 192.168.1.134; }; // ns2 IP privada
13 };

```

Archivo /etc/bind/zones/db.cazg.es

```

1 $TTL 60
2 @ IN SOA ns1.cazg.es. admin.cazg.es. (
3             2025051001 ; Serial
4             60        ; Refresh
5             60        ; Retry

```

```

6          60           ; Expire
7          60 )           ; TTL
8
9      IN    NS    ns1.cazg.es.
10     IN    NS    ns2.cazg.es.
11 ns1   IN    A     192.168.1.133
12 ns2   IN    A     192.168.1.134
13 dhcp  IN    A     192.168.1.132

```

Archivo /etc/bind/zones/db.192.168.1

```

1 $TTL 60
2 @ IN SOA ns1.cazg.es. admin.cazg.es. (
3             2025051001 ; Serial
4             60        ; Refresh
5             60        ; Retry
6             60        ; Expire
7             60 )       ; TTL
8
9     IN    NS    ns1.cazg.es.
10    IN    NS    ns2.cazg.es.
11 133   IN    PTR   ns1.cazg.es.
12 134   IN    PTR   ns2.cazg.es.
13 132   IN    PTR   dhcp.cazg.es.

```

B.3.3.2. Configuración del servidor DNS secundario

Dockerfile para el servidor DNS secundario

```

1 FROM ubuntu:20.04
2
3 # Evitar prompts interactivos durante la instalación
4 ENV DEBIAN_FRONTEND=noninteractive
5
6 # Actualizar e instalar paquetes necesarios
7 RUN apt-get update && apt-get install -y \
8     bind9 \
9     bind9utils \
10    bind9-doc \
11    iputils-ping \
12    net-tools \
13    ifupdown \
14    && apt-get clean \
15    && rm -rf /var/lib/apt/lists/*
16
17 # Crear directorios necesarios
18 RUN mkdir -p /etc/bind/zones /var/cache/bind /var/lib/bind /var/log/named
19
20 # Copiar archivos de configuración DNS
21 COPY named.conf.options /etc/bind/
22 COPY named.conf.local /etc/bind/
23
24 # Establecer permisos correctos para bind

```

```

25 RUN chown -R bind:bind /etc/bind/zones /var/cache/bind /var/lib/bind /var/log/named
26 RUN chmod 755 /etc/bind/zones
27 RUN chmod 775 /var/cache/bind
28 RUN chmod 644 /etc/bind/named.conf.options /etc/bind/named.conf.local
29
30 # Crear script de inicio
31 RUN echo '#!/bin/bash\n\
32 # Configurar IP estática dinámicamente\n\
33 ip addr add 192.168.1.134/28 dev eth0\n\
34 ip route add default via 192.168.1.131\n\
35 echo "nameserver 192.168.1.133" > /etc/resolv.conf\n\
36 echo "nameserver 192.168.1.134" >> /etc/resolv.conf\n\
37 # Iniciar servidor DNS\n\
38 exec named -g -c /etc/bind/named.conf -u bind; exec bash' > /start.sh
39
40 RUN chmod +x /start.sh
41
42 # Exponer puertos DNS
43 EXPOSE 53/udp 53/tcp
44
45 # Comando por defecto
46 CMD ["/start.sh"]

```

Archivo /etc/bind/named.conf.options

```

1 options {
2     directory "/var/cache/bind";
3
4     // Escuchar en su propia IP
5     listen-on { 192.168.1.134; };
6     listen-on-v6 { none; };
7
8     // Permitir consultas solo desde la red local
9     allow-query {
10         192.168.1.0/28;
11         localhost;
12     };
13
14     // Permitir recursión desde la red local
15     recursion yes;
16     allow-recursion {
17         192.168.1.0/28;
18         localhost;
19     };
20
21     // Permitir uso de caché
22     allow-cache {
23         192.168.1.0/28;
24         localhost;
25     };
26
27     // Reenvío a resolvers públicos
28     forwarders {

```

```

29     8.8.8.8;
30     1.1.1.1;
31 };
32
33 dnssec-validation auto;
34 auth-nxdomain no;
35 };

```

Archivo /etc/bind/named.conf.local

```

1 // Zona directa nombre -> IP
2 zone "cazg.es" {
3   type slave;
4   file "/etc/bind/zones/db.cazg.es";
5   masters { 192.168.1.133; }; // ns1 IP privada
6 };
7
8 // Zona inversa IP -> nombre
9 zone "1.168.192.in-addr.arpa" {
10   type slave;
11   file "/etc/bind/zones/db.192.168.1"; // subred 192.168.1.0/28
12   masters { 192.168.1.133; }; // ns1 IP privada
13 };

```

B.3.4. Configuración del router CE2 (San Cristóbal)

```

1 # Identidad
2 /system identity set name=CE2
3
4 # Habilitar interfaces físicas
5 /interface ethernet enable [find]
6
7 # VLANs sobre ether1
8 /interface vlan add interface=ether1 vlan-id=10 name=vlan10-datos
9 /interface vlan add interface=ether1 vlan-id=20 name=vlan20-voz
10
11 # Asignar direcciones IP
12 /ip address add address=192.168.2.1/26 interface=vlan10-datos
13 /ip address add address=192.168.2.33/26 interface=vlan20-voz
14
15 # Pool de direcciones DHCP
16 /ip pool add name=pool_datos ranges=192.168.2.2-192.168.2.30
17 /ip pool add name=pool_voz ranges=192.168.2.34-192.168.2.62
18
19 # Servidor DHCP para VLAN 10 (Datos)
20 /ip dhcp-server add name=dhcp_datos interface=vlan10-datos address-pool=pool_datos disabled=no
21 /ip dhcp-server network add address=192.168.2.0/26 gateway=192.168.2.1
22
23 # Servidor DHCP para VLAN 20 (Voz)
24 /ip dhcp-server add name=dhcp_voz interface=vlan20-voz address-pool=pool_voz disabled=no
25 /ip dhcp-server network add address=192.168.2.32/26 gateway=192.168.2.33
26

```

```

27 # Firewall: bloquear tráfico entre VLANs
28 /ip firewall filter add chain=forward action=drop src-address=192.168.2.0/26
   dst-address=192.168.2.32/26 comment="Bloquear Datos -> Voz"
29 /ip firewall filter add chain=forward action=drop src-address=192.168.2.32/26
   dst-address=192.168.2.0/26 comment="Bloquear Voz -> Datos"
30
31 # Habilitar IP forwarding
32 /ip settings set allow-fast-path=yes
33
34 # Direcciones IP para BGP e interconexión MPLS
35 /ip address add address=20.0.0.1/30 interface=ether2 network=20.0.0.0
36
37 # Loopback
38 /interface bridge add name=lo0
39 /ip address add address=192.170.0.5 interface=lo0 network=192.170.0.5
40
41 # Exportar las redes a la VPN MPLS
42 /ip firewall address-list add address=192.168.2.0/26 list=BGP_OUT
43 /ip firewall address-list add address=192.168.2.32/26 list=BGP_OUT
44
45 # Configuración eBGP con PE2
46 /routing bgp connection add name=toPE2 as=65500 router-id=192.170.0.5 \
  local.address=20.0.0.1 .role=ebgp remote.address=20.0.0.2 remote.as=65000 \
  output.network=BGP_OUT connect=yes listen=yes
47
48
49 # Asegurarte que ether1 está habilitada
50 /interface ethernet set [find name=ether1] disabled=no
51
52
53 # Guardar configuración final
54 /system backup save name=CE2

```

B.4. Configuración de los switches

Aquí se puede ver la configuración de los switches usados en las simulaciones de este proyecto.

B.4.1. Configuración del switch de distribución

```

1 enable
2 configure terminal
3 hostname SW_Distribucion
4 no ip routing
5 spanning-tree mode rapid-pvst
6
7 ! VLANs
8 vlan 10
9   name Datos
10 exit
11 vlan 20
12   name Voz
13 exit
14 vlan 30
15   name DMZ

```

```

16 exit
17
18 !
19 ! EtherChannel 1: CE1 (Router Principal)
20 ! Puertos: Gi0/0 y Gi0/1
21 interface range GigabitEthernet0/0 - 1
22   description EtherChannel to Router CE1
23   switchport trunk encapsulation dot1q
24   switchport mode trunk
25   channel-group 1 mode active
26   spanning-tree portfast trunk
27   no shutdown
28 exit
29
30 interface Port-channel1
31   description Port-Channel to Router CE1
32   switchport trunk encapsulation dot1q
33   switchport mode trunk
34   spanning-tree portfast trunk
35   no shutdown
36 exit
37
38 !
39 ! EtherChannel 2: CE1_Backup (Router Secundario)
40 ! Puertos: Gi0/2 y Gi0/3
41 interface range GigabitEthernet0/2 - 3
42   description EtherChannel to Router CE1_Backup
43   switchport trunk encapsulation dot1q
44   switchport mode trunk
45   channel-group 2 mode active
46   spanning-tree portfast trunk
47   no shutdown
48 exit
49
50 interface Port-channel2
51   description Port-Channel to Router CE1_Backup
52   switchport trunk encapsulation dot1q
53   switchport mode trunk
54   spanning-tree portfast trunk
55   no shutdown
56 exit
57
58 !
59 ! EtherChannel 3: SW_Acceso_DMZ
60 ! Puertos: Gi1/0 y Gi1/1
61 interface range GigabitEthernet1/0 - 1
62   description EtherChannel to SW_Acceso_DMZ
63   switchport trunk encapsulation dot1q
64   switchport mode trunk
65   channel-group 3 mode active
66   no shutdown
67 exit
68

```

```

69 interface Port-channel3
70   description Port-Channel to SW_Acceso_DMZ
71   switchport trunk encapsulation dot1q
72   switchport mode trunk
73   no shutdown
74 exit
75
76 ! -----
77 ! EtherChannel 4: SW_Acceso_LAN
78 ! Puertos: Gi1/2 y Gi1/3
79 interface range GigabitEthernet1/2 - 3
80   description EtherChannel to SW_Acceso_LAN
81   switchport trunk encapsulation dot1q
82   switchport mode trunk
83   channel-group 4 mode active
84   no shutdown
85 exit
86
87 interface Port-channel4
88   description Port-Channel to SW_Acceso_LAN
89   switchport trunk encapsulation dot1q
90   switchport mode trunk
91   no shutdown
92 exit
93
94 end
95 write memory

```

B.4.2. Configuración del switch de acceso LAN

```

1 enable
2 configure terminal
3 hostname SW_Acceso_LAN
4 no ip routing
5 spanning-tree mode rapid-pvst
6
7 vlan 10
8   name Datos
9 exit
10 vlan 20
11   name Voz
12 exit
13
14 ! Puertos de acceso VLAN 10
15 interface range GigabitEthernet0/2-3, GigabitEthernet1/1-3, GigabitEthernet2/0
16   description VLAN Datos
17   switchport mode access
18   switchport access vlan 10
19   no shutdown
20 exit
21
22 ! Puertos de acceso VLAN 20
23 interface range GigabitEthernet2/1-3, GigabitEthernet3/0-3

```

```

24  description VLAN Voz
25  switchport mode access
26  switchport access vlan 20
27  no shutdown
28 exit
29
30 ! ---- EtherChannel hacia SW_Distribucion ----
31 interface range GigabitEthernet0/0, GigabitEthernet0/1
32  description Trunks hacia SW_Distribucion
33  switchport trunk encapsulation dot1q
34  switchport mode trunk
35  channel-group 4 mode active
36  no shutdown
37 exit
38
39 interface Port-channel4
40  description EtherChannel a SW_Distribucion
41  switchport trunk encapsulation dot1q
42  switchport mode trunk
43  no shutdown
44 exit
45
46 end
47 write memory

```

B.4.3. Configuración del switch de acceso DMZ

```

1 enable
2 configure terminal
3 hostname SW_Acceso_DMZ
4 no ip routing
5 spanning-tree mode rapid-pvst
6
7 vlan 30
8  name DMZ
9 exit
10
11 ! Puertos de acceso VLAN 30
12 interface range GigabitEthernet0/2-3, GigabitEthernet1/0-3
13  description VLAN DMZ
14  switchport mode access
15  switchport access vlan 30
16  no shutdown
17 exit
18
19 ! ---- EtherChannel hacia SW_Distribucion ----
20 interface range GigabitEthernet0/0, GigabitEthernet0/1
21  description Trunks hacia SW_Distribucion
22  switchport trunk encapsulation dot1q
23  switchport mode trunk
24  channel-group 3 mode active
25  no shutdown
26 exit

```

```

27 interface Port-channel3
28   description EtherChannel a SW_Distribucion
29   switchport trunk encapsulation dot1q
30   switchport mode trunk
31   no shutdown
32
33 exit
34
35 end
36 write memory

```

B.5. Docker Compose para la FreePBX

```

1 version: '3.8'
2
3 services:
4   freepbx:
5     image: tiredofit/freepbx:latest
6     container_name: freepbx
7     restart: always
8     network_mode: "host"
9     ports:
10      - "80:80" # Web interface HTTP
11      - "443:443" # Web interface HTTPS
12      - "5060:5060/udp" # SIP UDP
13      - "5160:5160/udp" # SIP UDP Alternative
14      - "18000-18100:18000-18100/udp" # RTP Ports
15     environment:
16      - VIRTUAL_HOST=freepbx.local
17      - RTP_START=18000
18      - RTP_FINISH=18100
19      - ASTERISKVERSION=18
20      - DB_EMBEDDED=TRUE # Usa base de datos SQLite embebida
21     volumes:
22      - ./data:/data
23      - ./logs:/var/log

```

Apéndice C

Otros apéndices

C.1. Script para la generación del mapa con las diferentes sedes

Se creó un script en Python para generar un mapa con las diferentes sedes de la empresa que se encuentran en la tabla 1.1.

```
1 import folium
2 from geopy.geocoders import Nominatim
3 import time
4
5 sites = [
6     {"name": "Oficina central", "address": "Calle Ancha, Jerez de la Frontera, Spain", "coordenates": [36.68830069473355, -6.141331723620025]},
7     {"name": "ETAP de Cuartillos", "address": "Cuartillos, Jerez de la Frontera, Spain", "coordenates": [36.677837, -6.008313]},
8     {"name": "ETAP de Montañés", "address": "Carretera Puerto Real - Paterna, Spain", "coordenates": [36.520725003331606, -6.043437235454119]},
9     {"name": "ETAP de Algar", "address": "Carretera de acceso a Algar, Cádiz, Spain", "coordenates": [36.65415095709361, -5.643843877011512]},
10    {"name": "ETAP de Paterna", "address": "Paterna de Rivera, Cádiz, Spain", "coordenates": [36.527809, -5.863061]},
11    {"name": "San Cristóbal", "address": "Antigua carretera Jerez - El Puerto, Spain", "coordenates": [36.645474914003536, -6.126661833443614]},
12    {"name": "Depósito de Cádiz", "address": "Zona Franca, Cádiz, Spain", "coordenates": [36.5059990355522, -6.265044690365919]}
13 ]
14
15 map_sites = folium.Map(location=[36.6868, -6.1367], zoom_start=10)
16
17 for site in sites:
18     try:
19         folium.Marker(
20             location=site["coordenates"],
21             popup=site["name"],
22             tooltip=site["name"]
23         ).add_to(map_sites)
24
25         folium.Marker(
26             site["coordenates"],
27             icon=folium.DivIcon(
28                 icon_size=(150, 36),
```

```
29         icon_anchor=(75, 30),
30         html=f'<div style="font-size: 12pt; font-weight: bold; text-align:
center;">{site["name"]}</div>',
31     )
32 ).add_to(map_sites)
33
34 print(f"Added marker for {site['name']} at {site['coordenates'][0]}, {site['coordenates'][1]}")
35 except Exception as e:
36     print(f"Error processing {site['name']}: {e}")
37
38 map_sites.save("sites_map.html")
39 print("Map saved to sites_map.html")
```

Bibliografía

- [1] Ejarque Cristina, "Conexión de redes extendidas." <https://educacion.sanjuan.edu.ar/mesj/LinkClick.aspx?fileticket=wwvjjQg4rI%3D&tabid=678&mid=1743>, 2025. Ministerio de Educación de San Juan. Accedido: 30 de junio de 2025.
- [2] Angel H., "Entendiendo las bases de MPLS casi desde cero." <https://borrowbits.com/2018/09/entendiendo-las-bases-de-mpls-casi-desde-cero/>, 2018. Redes MPLS: entendiendo sus bases (casi desde cero).
- [3] Wikipedia, "SD-WAN." <https://es.wikipedia.org/wiki/SD-WAN>, 2025. Wikipedia sobre SD-WAN. Accedido: 2 de julio de 2025.
- [4] Wikipedia, "Virtual Private Network." https://es.wikipedia.org/wiki/Red_privada_virtual, 2025. Red Privada Virtual.
- [5] Gerencia del Consorcio de Aguas de la Zona Gaditana, "Expediente 006-2020: Servicio de telecomunicaciones de voz, fijas y móviles, red de acceso de datos, Intranet e Internet del Consorcio de Aguas de la Zona Gaditana." https://contrataciondelestado.es/wps/poc?uri=deeplink:detalle_licitacion&idEvl=svIvypWr12kSugstABGr5A%3D%3D, 2020. Pliego de condiciones.
- [6] Versa Networks Inc, "SD-WAN de Versa Networks." <https://versa-networks.com/es/sd-wan/>, 2025. Página oficial de Versa Networks sobre SD-WAN. Accedido: 26 de marzo de 2025.
- [7] Hewlett Packard Enterprise, "¿Qué es SD-WAN?" <https://www.hpe.com/es/es/what-is-sd-wan.html>, 2025. Hewlett Packard Enterprise sobre SD-WAN. Accedido: 26 de marzo de 2025.
- [8] Wikipedia, "Multiprotocol Label Switching." https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching, 2025. Wikipedia sobre Multiprotocol Label Switching.
- [9] VoIP Studio, "¿Qué es VoIP? La guía completa." <https://voipstudio.com/es/blog/que-es-voip-la-guia-completa/>, 2025. Guía completa sobre VoIP. Accedido: 26 de marzo de 2025.
- [10] Wikipedia, "Multiprotocol Border Gateway Protocol." https://en.wikipedia.org/wiki/Multiprotocol_BGP, 2025. Wikipedia sobre Multiprotocol BGP. Accedido: 26 de marzo de 2025.
- [11] LinkedIn, "What are the security implications of using Multiprotocol BGP?" [https://www.linkedin.com/advice/1/what-security-implications-using-multiprotocol?](https://www.linkedin.com/advice/1/what-security-implications-using-multiprotocol/)

lang=es&lang=es&originalSubdomain=es, 2025. LinkedIn sobre las implicaciones de seguridad del uso de Multiprotocol BGP. Accedido: 26 de marzo de 2025.

- [12] Wikipedia, “Border Gateway Protocol.” https://es.wikipedia.org/wiki/Border_Gateway_Protocol, 2025. Wikipedia sobre Border Gateway Protocol. Accedido: 26 de marzo de 2025.
- [13] Wikipedia, “GNS3: Software de simulación de redes.” <https://es.wikipedia.org/wiki/GNS3>, 2025. Wikipedia sobre GNS3.
- [14] CCNA desde Cero, “¿qué es GNS3? ¿cómo usarlo?” <https://ccnadesdecero.es/que-es-gns3-como-usarlo/>. Accedido: 24 de junio de 2025.
- [15] Wikipedia, “Wireshark.” <https://es.wikipedia.org/wiki/Wireshark>, 2025. Wireshark.
- [16] Hogan B., “Cómo instalar y usar Docker en Ubuntu 20.04.” <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-20-04-es>, 2020. Tutorial sobre la instalación y uso de Docker en Ubuntu.
- [17] Oracle Corporation, “Introducción a VirtualBox.” <https://www.virtualbox.org/manual/topics/Introduction.html#Introduction>, 2025. Introducción a VirtualBox.
- [18] MicroSIP, “MicroSIP.” <https://www.micsip.org/>, 2025. MicroSIP softphone for Windows based on PJSIP.
- [19] Grandstream, “Grandstream GRP2601.” https://www.grandstream.com/hubfs/Product_Documentation/Datasheet_GRP2601_Spanish.pdf, 2025. Grandstream GRP2601. Accedido: 30 de junio de 2025.
- [20] MikroTik, “RouterBOARD 2011UiAS-RM.” <https://mikrotik.com/product/RB2011UiAS-RM>, 2025. RouterBOARD 2011UiAS-RM. Accedido: 30 de junio de 2025.
- [21] TP-Link, “Switch TP-Link T2500G-10TS.” <https://www.tp-link.com/ec/service-provider/managed-switch/t2500g-10ts/>, 2025. TP-Link T2500G-10TS. Accedido: 30 de junio de 2025.
- [22] Cisco Meraki, “MX Warm Spare - High Availability Pair.” https://documentation.meraki.com/MX/Deployment_Guides/MX_Warm_Spare_-_High_Availability_Pair#:~:text=than%2030%20seconds.-,Routed%20Warm%20Spare,used%20as%20a%20routed%20gateway., 2025. Cisco Meraki sobre el modo de alta disponibilidad (Warm Spare). Accedido: 30 de junio de 2025.
- [23] Router-switch.com, “Cisco 9300-24P-E.” <https://www.router-switch.com/c9300-24p-e.html#tab-download>, 2025. Cisco 9300-24P-E. Accedido: 26 de junio de 2025.
- [24] Cisco, “Cisco 9300-24P-E.” <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html#Platformdetails>, 2025. Cisco 9300-24P-E. Accedido: 26 de junio de 2025.
- [25] Router-switch.com, “Cisco 3560-CX-12PD-S.” <https://www.router-switch.com/ws-c3560cx-12pd-s-p-16549.html>, 2025. Cisco 3560-CX-12PD-S. Accedido: 26 de junio de 2025.

- [26] Cisco, “Cisco 3560-CX-12PD-S.” <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-cx-series-switches/datasheet-c78-733229.html>, 2025. Cisco 3560-CX-12PD-S. Accedido: 26 de junio de 2025.
- [27] Cisco, “Cisco WS-C2960L-16TS-LL.” <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-l-series-switches/nb-06-cat2960-l-ser-data-sheet-cte-en.html>, 2025. Cisco WS-C2960L-16TS-LL. Accedido: 26 de junio de 2025.
- [28] Grandstream, “Grandstream GRP2612.” https://www.grandstream.com/hubfs/Product_Documentation/datasheet_grp2612_english.pdf, 2025. Grandstream GRP2612. Accedido: 30 de junio de 2025.
- [29] Fortinet, “Fortinet Next-Generation Firewall.” <https://www.fortinet.com/lat/products/next-generation-firewall>, 2025. Fortinet NGFW. Accedido: 2 de julio de 2025.
- [30] Microsoft, “¿Qué es Microsoft Sentinel?” <https://learn.microsoft.com/es-es/azure/sentinel/overview?tabs=defender-portal>, 2024. Microsoft Sentinel. Accedido: 26 de junio de 2025.
- [31] Valentinas C., “What is FreePBX and why use it for your phone service.” <https://www.hostinger.com/in/tutorials/what-is-freepbx>, 2025. Tutorial sobre FreePBX. Accedido: 26 de marzo de 2025.
- [32] Microsoft, “Microsoft Azure.” <https://azure.microsoft.com/es-es>, 2025. Microsoft Azure. Accedido: 2 de julio de 2025.
- [33] Freshworks, “¿Qué es IVR?” <https://www.freshworks.com/es/freshcaller-cloud-pbx/ivr/#:~:text=%C2%BFQu%C3%A9%20es%20IVR?,fin%20de%20resolver%20sus%20consultas.>, 2025. Freshworks sobre IVR. Accedido: 2 de julio de 2025.
- [34] Julien Duponchelle, “Imagen del MikroTik Cloud Hosted Router en GNS3.” <https://gns3.com/marketplace/appliances/mikrotik-cloud-hosted-router>, 2024. MikroTik Cloud Hosted Router.
- [35] Wikipedia, “Virtual Router Redundancy Protocol.” https://es.wikipedia.org/wiki/Virtual_Router_Redundancy_Protocol, 2025. Wikipedia sobre Virtual Router Redundancy Protocol.
- [36] Wikipedia, “Rapid Spanning Tree Protocol.” https://es.wikipedia.org/wiki/Rapid_Spanning_Tree_Protocol, 2025. Wikipedia sobre Rapid Spanning Tree Protocol.
- [37] Wikipedia, “Neighbor Discovery.” https://es.wikipedia.org/wiki/Neighbor_Discovery, 2025. Wikipedia sobre Neighbor Discovery. Accedido: 2 de julio de 2025.
- [38] Debian, “Información sobre Debian “bookworm”.” <https://www.debian.org/releases/stable/>, 2025. Debian. Accedido: 2 de julio de 2025.
- [39] D. Carpio Ortiz, “Desarrollo y configuración de un entorno MPLS en equipos Mikrotik y simulado en GNS3.” Trabajo de Fin de Grado, Universitat Politècnica de València. Disponible en: <https://riunet.upv.es/handle/10251/203233>, 2023.
- [40] Carlos Ernesto Carrillo Arellano, “Método para simular redes VoIP en GNS3.” <https://www.youtube.com/watch?v=2k1J6u56fEQ&t=1937s>, 2023. Tutorial en YouTube sobre la simulación de redes VoIP utilizando GNS3.

- [41] Oracle Corporation, “VirtualBox: Software de virtualización multiplataforma.” <https://www.virtualbox.org/>, 2025. Página oficial de Oracle VM VirtualBox.
- [42] FreePBX, “FreePBX: Software de centralita telefónica IP.” <https://www.freepbx.org/>, 2025. Página oficial de FreePBX.
- [43] DigitalOcean, “Cómo instalar y usar Docker en Ubuntu 20.04.” <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-20-04>, 2020. Tutorial sobre la instalación y uso de Docker en Ubuntu.
- [44] DigitalOcean, “Cómo instalar y usar Docker Compose en Ubuntu 20.04.” <https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-compose-on-ubuntu-20-04>, 2020. Tutorial sobre la instalación y uso de Docker Compose en Ubuntu.
- [45] Orange, “Orange para PYMES.” <https://www.orange.es/empresas/pymes>, 2025.
- [46] Telefónica, “Conectividad inteligente para empresas.” <https://www.telefonicaempresas.es/soluciones-digitales/conectividad-inteligente>, 2025.
- [47] Vodafone, “Optimiza tu red WAN.” <https://www.vodafone.es/c/empresas/es/sd-wan/>, 2025.
- [48] Meraki Shop, “Cisco Meraki MX95.” <https://www.merakishop.es/cisco-meraki-mx95-firewall.html>, 2025.
- [49] Meraki Shop, “Cisco Meraki MX85.” <https://www.merakishop.es/cisco-meraki-mx85-firewall.html>, 2025.
- [50] Meraki Shop, “Cisco Meraki MX67.” <https://www.merakishop.es/cisco-meraki-mx67-firewall.html>, 2025.